МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

ЧАКРЯН ВАДИМ ХАЗАРОВИЧ

УДК 621.391

МОДЕЛІ ТА МЕТОДИ МАРШРУТИЗАЦІЇ ТРАФІКУ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ З УРАХУВАННЯМ ВИМОГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Спеціальність 05.12.02 – Телекомунікаційні системи та мережі

АВТОРЕФЕРАТ

дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2017

Дисертацією є рукопис.

Робота виконана в Харківському національному університеті радіоелектроніки, Міністерства освіти і науки України.

Науковий керівник: кандидат технічних наук, доцент
СНІГУРОВ Аркадій Владиславович,
Харківський національний університет
радіоелектроніки,
доцент кафедри інфокомунікаційної інженерії.

Офіційні опоненти: доктор технічних наук, професор
ТОЛЮПА Сергій Васильович,
Київський національний університет
імені Тараса Шевченка МОН України,
професор кафедри кібербезпеки
та захисту інформації;

кандидат технічних наук,
ОДАРЧЕНКО Роман Сергійович,
Національний авіаційний університет,
Навчально-науковий інститут аеронавігації МОН України,
доцент кафедри телекомунікаційних систем.

Захист відбудеться «31» січня 2018 року о 13 годині на засіданні спеціалізованої вченої ради Д 64.052.09 в Харківському національному університеті радіоелектроніки за адресою: Україна, 61166, м. Харків, пр. Науки, 14.

З дисертацією можна ознайомитися у бібліотеці Харківського національного університету радіоелектроніки за адресою: 61166, м. Харків, пр. Науки, 14.

Автореферат розісланий «____» _____2017 року.

Учений секретар
спеціалізованої вченої ради О.Б. Ткачова

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Однією з найважливіших задач сучасних телекомунікаційних мереж (ТКМ) є маршрутизація потоку пакетів (ПП). При цьому найбільш поширені в сучасних ТКМ інтернет протокол 4 версії (Internet Protocol version 4, IPv4) та інтернет протокол 6 версії (Internet Protocol version 6, IPv6), однією з функцій яких є адресація вузлів; протоколи динамічної маршрутизації (ДМ), як міждоменного, так і внутрішнього шлюзу, в безпроводових та проводових мережах; програмне забезпечення маршрутизаторів, є вразливими та їх компрометація може призвести до порушення інформаційної безпеки (ІБ) транзитного ПП.

Як свідчить аналіз малодослідженою областю є забезпечення ІБ транзитного ПП в ТКМ при використанні протоколів динамічної маршрутизації (ПДМ), що працюють в проводових мережах в рамках однієї автономної системи і відносяться до протоколів маршрутизації внутрішнього шлюзу (Internal Gateway Protocol, IGP). Такими протоколами є: протокол маршрутної інформації (Routing Information Protocol, RIP), протокол динамічної маршрутизації з відстежуванням стану каналів зв’язку (КЗ) «найкоротший відкритий шлях першим» (Open Shortest Path First, OSPF) та удосконалений прокол маршрутизації внутрішнього шлюзу (Enhanced Interior Gateway Routing Protocol, EIGRP). Наведена область вибрана для постановки науково-прикладної задачі роботи.

Таким чином, тема дисертації та науково-прикладна задача, яка полягає в підвищенні інформаційної безпеки ПП в процесі його динамічної маршрутизації (ДМ) в ТКМ шляхом урахування ризиків порушення конфіденційності, цілісності та доступності транзитних даних як додаткових параметрів вибору оптимального шляху передачі, є актуальними.

Зв’язок роботи з науковими програмами, планами та темами. Дисертаційна робота безпосередньо пов'язана з реалізацією основних положень «Стратегії кібербезпеки України», «Концепції національної інформаційної політики», «Концепції Національної програми інформатизації» та «Концепції інформаційної безпеки України».

Мета та задачі дослідження. Метою дисертаційної роботи є підвищення інформаційної безпеки потоку пакетів в процесі його динамічної маршрутизації в ТКМ із застосуванням протоколів IGP.

У дисертаційній роботі розв’язані такі окремі **задачі дослідження**: аналіз сучасних підходів, технологій і ПДМ в ТКМ; аналіз сучасних методів і технік порушення безпеки даних, що передаються в ТКМ в процесі динамічної маршрутизації ПП, а також методів і підходів до оцінки ризиків захищеності ПП і живучості мережі; аналіз існуючих моделей динамічної маршрутизації; розробка методу оцінки ризику порушення інформаційної безпеки ПП для маршрутів, які обираються ПДМ; розробка методу динамічного вибору оптимального маршруту передачі ПП з урахуванням вимог ІБ; удосконалення моделей динамічної маршрутизації шляхом врахування

ризику інформаційної безпеки (РІБ) в процесі вибору оптимального маршруту; перевірка ефективності запропонованих моделей і методів динамічної маршрутизації з урахуванням РІБ і розробка практичних рекомендацій на їх основі.

Об'єкт дослідження. Процес маршрутизації потоку пакетів в телекомунікаційній мережі з урахуванням вимог інформаційної безпеки.

Предмет дослідження. Моделі і методи підвищення інформаційної безпеки потоку пакетів в процесі його динамічної маршрутизації в телекомунікаційних мережах.

Методи дослідження. В роботі використовувалися методи оцінки живучості інформаційних систем, елементи математичного аналізу, математичної статистики і випадкових процесів, методи аналізу ризиків, методи оптимізації та прийняття рішень, імітаційне моделювання процесу одношляхової і багатошляхової маршрутизації, ймовірнісно-статистичні методи, засновані на напівмарковських процесах і перетвореннях Лапласа, методи експериментального дослідження для виявлення взаємозв'язків різних параметрів маршрутизатора при передачі ПП, а також аналітичне та імітаційне моделювання процесів, що впливають на ІБ ПП в процесі його маршрутизації в ТКМ.

Наукова новизна отриманих результатів. У ході вирішення поставленої задачі, автором були отримані наступні наукові результати:

1. Вперше запропоновано метод оцінки покажчику ризику інформаційної безпеки шляхів передачі ПП, новизною якого є врахування таких параметрів як: ефективність та вразливість маршрутизаторів мережі, а також ймовірність здійснення атаки типу відмова в обслуговуванні на маршрутизатори в заданий момент часу. Це дозволило 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 (ПЗ) вузлу, чи взагалі виводять його з ладу; атак на перемаршрутизацію даних по не ефективним шляхам. Використання моделі дозволило динамічно оцінювати ймовірність своєчасної 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.

Обґрунтованість та достовірність отриманих в дисертаційній роботі наукових результатів 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.

Наукове значення роботи полягає в розробці моделей і методів підвищення ІБ ПП в процесі його динамічної маршрутизації в ТКМ шляхом врахування РІБ вузлів мережі як додаткового параметру вибору оптимального шляху передачі даних. **Практичне значення** отриманих результатів полягає у підвищенні РІБ ПП в процесі його динамічної маршрутизації в ТКМ у середньому на 10% за рахунок використання запропонованих в даній роботі математичних моделей та методів.

Практична значимість отриманих результатів дисертації також підтверджується їх застосуванням у дослідницьких роботах з питань несанкціонованого доступу в мобільні системи зв‘язку та при розробці перспективних протоколів динамічної маршрутизації в сучасних мультисервісних телекомунікаційних системах у Харківському державному регіональному науково-технічному центрі з питань технічного захисту інформації, в навчальному процесі кафедри інфокомунікаційної інженерії Харківського національного університету радіоелектроніки (ХНУРЕ) в дисципліні «Безпека інформації в інформаційно-комунікаційних системах», при розробці системи мережевого обміну Пристрою радіомоніторингу КХ діапазону Р-677 УИДЯ.466948.006 на Державному підприємстві «Центральне конструкторське бюро «Протон».

Особистий внесок здобувача. Наукові результати, наведені в дисертаційній роботі, здобувач отримав самостійно. У роботах, опублікованих у співавторстві, автору дисертаційної роботи належать: в роботі [1] удосконалена модель пошуку оптимального шляху передачі ПП в заданій ТКМ з урахуванням РІБ на основі метрики протоколу RIP; в роботі [10] запропонована напівмарківська модель процесу передачі ПП в ТКМ, яка дозволяє представити динаміку процесу в умовах інформаційних атак з урахуванням його ймовірнісно-часових характеристик; в роботі [12] запропоновано метод, який дозволяє розрахувати ризик ІБ мережевого маршрутизатора на підставі метрик стандарту загальної системи оцінки вразливостей (Common Vulnerability Scoring System version 2, CVSS v2) розробленого Національним інститутом стандартів та технологій (National Institute of Standards and Technologies, NIST); в роботі [14] проаналізовано існуючі вразливості стека протоколів IPv6; в роботі [15] проведено аналіз методів захисту від

загроз шляхом впровадження механізмів безпеки, покликаних збільшити ІБ для стека протоколів IPv6; в роботі [18] запропоновано метод, який дозволяє запобігти перевантаженню одного з КЗ при використанні стандартного методу балансування навантаження по шляхах нерівнозначної вартості протоколу EIGRP; в роботі [19] запропоновано метод врахування РІБ в формулі розрахунку метрики ПДМ EIGRP, який дозволяє динамічно вибирати найбільш безпечний маршрут передачі ПП, при цьому враховуючи стандартні показники метрики протоколу EIGRP. Також отримано патент на корисну модель маршрутизації трафіку за допомогою протоколу EIGRP з урахуванням вимог ІБ, наукова новизна результатів якого полягає у врахуванні РІБ маршруту в формулі розрахунку метрики протоколу EIGRP, що дозволяє вибирати маршрут передачі ПП в ТКМ за критерієм «якість-безпека» [22].

Апробація результатів дисертації. Основні результати дисертаційної роботи доповідалися на наукових семінарах кафедри інфокомунікаційної інженерії ХНУРЕ, а також на Міжнародних конференціях та форумах, таких як 23rd International Crimean Conference on Microwave and Telecommunication Technology (Севастополь, 2013); Перша міжнародна науково-практична конференція Проблеми інфокомунікацій. Наука і технології. (Харків, 2013); 1st International IEEE Conference on Problems of Infocommunications. Science and Technology (Харків, 2014); 2nd International IEEE Conference on Problems of Infocommunications. Science and Technology (Харків, 2015); 12th International Conference on Experience of Designing and Application of CAD Systems in Microelectronics (Україна, Поляна-Свалява, 2013); International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (Львів, 2014); International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (Львів, 2016), на міжнародних форумах і конференціях ХНУРЕ та ін. [2-9, 11, 13, 16-17, 21].

Публікації. Основні положення відображені в 8-ми статтях, 7 з яких опубліковано у фахових наукових виданнях України [1, 10, 12, 14, 15, 18, 20], одна опублікована в іноземному виданні [19], також отримано один патент на корисну модель [22]. Апробація результатів дисертації проходила в ході чотирнадцятьох міжнародних науково-технічних конференцій [2-9, 11, 13, 16-17, 21], з яких шість [6-8, 13, 17, 21] проходили під егідою IEEE та індексуються в міжнародних наукометричних базах Scopus та IEEE Xplore Digital Library.

Структура дисертації. Дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та 10 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.

ЗМІСТ РОБОТИ

У **вступі** розкрито основний зміст і загальний стан проблеми і окремих завдань підвищення інформаційної захищеності транзитного ПП, 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.

У **першому розділі** роботи проводиться аналіз актуальності теми дослідження, методів порушення процесу маршрутизації та ІБ ПП, а також методів забезпечення ІБ ПП в ТКМ. В ході аналізу літератури виявлено, що малодослідженою областю є забезпечення ІБ транзитного ПП в ТКМ при використанні ПДМ, що працюють в проводових мережах в рамках однієї автономної системи і належать до протоколів IGP, прикладами яких є RIP, OSPF та EIGRP. Також в ході аналізу виявлено, що проблеми забезпечення конфіденційності та цілісності ПП, що передається в ТКМ, вирішуються за рахунок використання криптографічних протоколів, які не захищають від атак типу відмова в обслуговуванні (Denial of Service, DoS); єдиним стандартизованим механізмом безпеки в ПДМ, що досліджуються в даній роботі, є автентифікація джерел оновлень; механізми мережевого захисту в сучасних ТКМ не мають превентивних заходів безпеки, щоб попередити виникнення загрози та реагують за фактом реалізації атаки.

Визначені вимоги до РІБ, параметрів РІБ та методів врахування РІБ в метриках ПДМ. Вимогами до РІБ та його параметрів визначені наступні: РІБ повинен розраховуватися на основі кількісних методів оцінки ризику; РІБ повинен бути нормованим та лежати в межах [0;1], параметри РІБ мають бути розраховані на основі математично обґрунтованих показників, або за допомогою методології, що мінімізують людський суб’єктивізм. Вимогами, щодо методів врахування РІБ в формулах метрик ПДМ є: РІБ повинен збільшувати значення метрики шляху; РІБ повинен мати достатню вагу, щоб змінити вибір оптимального шляху в умовах наявності загроз інформаційної безпеки; значення метрик повинні лежати в межах, що описані в стандартах для відповідних протоколів маршрутизації; в удосконалених формулах розрахунку метрик повинні враховуватися базові параметри, які враховуються і в стандартних формулах метрик відповідних протоколів; РІБ не повинен призводити до того, щоб значення метрики шляху передачі дорівнювало нулю.

Також в першому розділі поставлена науково-практична задача, яка полягає в підвищенні ІБ ПП в процесі його ДМ в ТКМ шляхом урахування ризиків порушення конфіденційності, цілісності та доступності транзитних даних як додаткових параметрів вибору оптимального шляху передачі.

У **другому розділі** запропоновані методи розрахунку РІБ транзитного ПП для заданого шляху передачі в процесі маршрутизації: статичний та динамічний.

В статичному методі розрахунку РІБ враховується три параметри:

1. Параметр РІБ, що розраховується за стандартом NIST CVSS v2;
2. Параметр РІБ, що розраховується на основі ефективності маршрутизаторів мережі (ЕММ);
3. Параметр РІБ, що розраховується на основі ентропії ПП.

Для розрахунку першого параметра РІБ, основаного на оцінці метрик вразливостей кожного з маршрутизаторів в досліджуваному маршруті на основі стандарту NIST CVSS v2, в даній роботі пропонується використовувати наступну формулу:

$$R_{CVSS} = \frac{\sum_{i=1}^{n} B_{score_i}}{N_{враз.}} \cdot \frac{1}{10}, \tag{1}$$

де B_{score_i} – покажчик базової метрики i вразливості, знайденої на заданому маршрутизаторі, при $i = \overline{1, N_{враз.}}$; $N_{враз.}$ – загальна кількість вразливостей, що знайдені на заданому маршрутизаторі. Так як $B_{score_i} \in [0;10]$, то поділ на 10 забезпечує необхідні межі для параметру РІБ, а саме $R_{CVSS} \in [0;1]$.

Розрахунок значення B_{score_i} виконується згідно із NIST CVSS v2:

$$B_{score_i} = \lceil ((0{,}6 \cdot I) + (0{,}4 \cdot E) - 1{,}5) \cdot f(I) \rceil^{1-dec}, \tag{2}$$

$$I = 10{,}41 \cdot (1 - (1 - I_c) \cdot (1 - I_i) \cdot (1 - I_a)), \tag{3}$$

$$E = 20 \cdot A \cdot A_v \cdot A_c, \tag{4}$$

$$f(I) = \begin{cases} 0, \text{ якщо } I = 0 \\ 1{,}176, \text{ якщо } I \neq 0 \end{cases}, \tag{5}$$

де I – збиток; E – можливість експлуатації; $f(I)$ – функція від збитку; $\lceil \ \rceil^{1-dec}$ – округлення в більшу сторону з точністю до однієї десятої; I_c – збиток від порушення конфіденційності; I_i – збиток від порушення цілісності; I_a – збиток від порушення доступності; A – вимоги до автентифікації; A_v – вектор доступу; A_c – складність доступу.

Другий параметр РІБ розраховується як ризик порушення глобальної ефективності мережі при видаленні одного з маршрутизаторів i та всіх його каналів зв'язку з ТКМ у разі успішної реалізації загрози

$$R_{\theta_i} = \frac{\xi - \xi_i}{\xi} \cdot P^i_{загр.}, \text{ при } R_{\theta_i} \in (0;1], \tag{6}$$

де ξ – глобальна ефективність ТКМ; ξ_i – глобальна ефективність ТКМ, у випадку видалення маршрутизатора i та всіх його КЗ; $P^i_{загр.}$ – ймовірність реалізації загрози виведення з ладу маршрутизатора i та всіх його каналів зв'язку.

У даній роботі запропоновано вдосконалений метод обчислення глобальної ефективності ТКМ, який дозволяє враховувати такі параметри мережі як пропускна здатність і затримка передачі ПП в КЗ:

$$\xi = \frac{1}{n \cdot (n-1)} \cdot \sum_{\substack{i,j=1 \\ i \neq j}}^{n} \frac{1}{\min\limits_{p \in P_{i,j}} \mu_p}, \tag{7}$$

де $\min\limits_{p \in P_{i,j}} \mu_p$ – мінімальне значення метрики одного з шляхів p з множини шляхів $P_{i,j}$ між вузлами i, j; n – кількість вузлів в заданій мережі. При цьому:

$$\mu_p = \sum_{l \in p} \mu_l, \tag{8}$$

$$\mu_l = \left(\frac{10^8}{B^{ij}_{min}} + D^{ij}_{sum} \right) \cdot c_{scale}, \; i \neq j, \tag{9}$$

де $\sum\limits_{l \in p} \mu_l$ – сума метрик кожного з КЗ l, що входять в шлях p; B^{ij}_{min} – значення зваженого покажчика пропускної здатності для КЗ між вузлами i, j, кбіт/с; D^{ij}_{sum} – сума затримок в КЗ між вузлами i, j, мкс; c_{scale} – константа масштабування, яка дорівнює 256.

В топологіях ТКМ з однорідною структурою різниця між ЕММ різних шляхів передачі може коливатися в одиницях процентів, що може зменшити вплив РІБ на метрику шляху. Для збільшення розкиду значень ЕММ в даній роботі пропонується використовувати параметр масштабування x_{scale}:

$$R_{\theta_i} = \frac{\xi - x_{scale} \cdot \xi_i}{\xi}, \tag{10}$$

$$x_{scale} = \frac{\xi}{\max\limits_{i}(\xi_i)}, \tag{11}$$

де $\max\limits_{i}(\xi_i)$ – максимальне значення ефективності мережі у випадку видалення одного з маршрутизаторів i.

Розрахунок третього параметра РІБ оснований на аналізі ентропії ПП, що надходить на входи маршрутизаторів в досліджуваному маршруті. Даний параметр не враховується при розрахунку РІБ шляху, проте він застосовується для детектування DoS атаки, яка може здійснюватися на один з маршрутизаторів ТКМ. Ентропія розраховується на основі IP адреси та TCP/UDP портів отримувача ПП, які в подальшому будуть називатися сокетом.

У даній роботі пропонується удосконалений метод для визначення наявності або відсутності DoS атаки на один з маршрутизаторів ТКМ в заданий момент часу, який виражається наступними формулами:

$$\left.\begin{aligned} R_{etr} = \frac{\left|SMA_i - etr_t\right| - \beta \cdot \sigma_{SMA_i}}{\left|SMA_i - etr_t\right|} \cdot \rho \cdot K_{self}, \; при \; \left|SMA_i - etr_t\right| \geq \beta \cdot \sigma_{SMA_i} \\ R_{etr} = 0, \; при \; \left|SMA_i - etr_t\right| \leq \beta \cdot \sigma_{SMA_i} \end{aligned}\right\}, \tag{12}$$

$$etr_t = -\sum_{i=1}^{n} p_i \cdot \log(p_i), \tag{13}$$

$$p_i = \frac{f_i}{N_{сокетів,w}}, \tag{14}$$

де R_{etr} – ризик наявності DoS атаки на заданий маршрутизатор; SMA_i – останнє обчислене значення простого рухомого середнього (РС) значень ентропії; etr_t – значення ентропії в момент часу t; β – цілочисельна константа масштабування, $\beta = 3$; ρ – параметр, який визначає відношення кількості бітів, що поступили на вхід маршрутизатора, до кількості бітів, які маршрутизатор може обробити, тобто $\rho = \lambda / \mu$; K_{self} – параметр, який визначається як відношення усіх пакетів $N_{всі}$, що поступили на маршрутизатор, до кількості пакетів, в яких в якості отримувача вказаний сам маршрутизатор (IP-адреса маршрутизатора) $N_{маршр.}$, тобто $K_{self} = N_{всі} / N_{маршр.}$; p_i – ймовірність появи i-го сокету; f_i – частота появи i-го сокету, $N_{сокетів,w}$ – загальна кількість сокетів, які були отримані за один інтервал вимірювання w.

З метою вибору алгоритму РС був зібрана вибірка пакетів з реальної ТКМ. За результатами аналізу було виявлено, що просте РС швидше реагує на зміни значень ентропії, а також демонструє менше середньоквадратичне відхилення від реальних значень ентропії у порівнянні з адаптивною РС Кауфмана приблизно на 21,7%, та у порівнянні з РС з динамічним періодом усереднення приблизно на 16,9%. Тому в даній роботі пропонується використовувати саме алгоритм простого РС для розрахунку середніх значень ентропії ПП.

Застосування параметру R_{etr} дозволяє ввести поступову шкалу і визначати атаку тільки в разі, якщо $R_{etr} > R_{прийнят.}$, де $R_{прийнят.}$ – це максимально прийнятний ризик, при якому наявність ризику здійснення DoS атаки можна ігнорувати, при цьому $R_{прийнят.} \in [0;1]$.

Для розрахунку ризику досліджуваного маршруту статичним методом в даній роботі пропонується наступна формула:

$$R_{p_{i,j}} = 1 - \left(1 - K_{CVSS} \cdot \frac{\sum_{m \in p} R_{CVSS_m}}{n_p}\right) \cdot \left(1 - K_{\theta} \cdot \left(1 - \frac{\sum_{m \in p} R_{\theta_m}}{n_p}\right)\right), \quad (15)$$

де $R_{p_{i,j}}$ – РІБ всього шляху p при передачі ПП між вузлами i, j, при $i \neq j$; K_{CVSS} та K_{θ} – коефіцієнти важливості параметрів ризику R_{CVSS} та R_{θ} відповідно, при цьому $K_{CVSS} \in [0;1]$, $K_{\theta} \in [0;1]$; $\sum_{m \in p} R_{CVSS_m}$ – сума параметрів ризику R_{CVSS} кожного з маршрутизаторів m в шляху p; $\sum_{m \in p} R_{\theta_m}$ – сума параметрів ризику R_{θ} кожного з маршрутизаторів m в шляху p; n_p – загальна кількість маршрутизаторів в шляху p.

Коефіцієнти важливості пропонується задати як бінарні змінні, які можуть приймати лише значення 0 або 1, тобто $K_{CVSS} \in \{0;1\}$ та $K_{\theta} \in \{0;1\}$. Тоді існує чотири комбінації, які пропонується використовувати у наступних випадках:

1. $K_{CVSS} = 0$, $K_{\theta} = 0$ – у випадку, якщо РІБ шляху не використовується. У стандартному випадку активується даний варіант коефіцієнтів;

2. $K_{CVSS} = 1$, $K_{\theta} = 0$ – у випадку, коли максимальний пріоритет віддається забезпеченню конфіденційності та цілісності транзитного ПП;

3. $K_{CVSS} = 0$, $K_{\theta} = 1$ – у випадку, коли максимальний пріоритет віддається забезпеченню захисту маршрутизаторів ТКМ від DoS атак;

4. $K_{CVSS} = 1$, $K_{\theta} = 1$ – не рекомендована комбінація.

Випадок $K_{CVSS} = K_\theta = 1$ не рекомендується використовувати, тому що врахування обох параметрів РІБ одночасно може призвести до усереднення результатів, або повної відсутності впливу одного з них. Для того, щоб враховувати лише один з параметрів РІБ, використовується параметр ризику можливої DoS атаки, який розраховується на основі ентропії ПП. DoS атака детектується, якщо $R_{ent} > R_{прийнят.}$, при цьому $R_{прийнят.}$ задається адміністратором ТКМ, але в стандартному випадку $R_{прийнят.} = 0$. При виконанні умови $R_{ent} > R_{прийнят.}$ коефіцієнти будуть наступні – $K_{CVSS} = 0$, $K_\theta = 1$, в протилежному випадку – $K_{CVSS} = 1$, $K_\theta = 0$.

Переваги статичного методу розрахунку РІБ ПП полягають в малому споживанні операційних ресурсів аналізаторів і маршрутизаторів, оскільки статичні параметри не схильні до частих змін. З іншого боку недоліком статичного підходу є неможливість врахування параметрів, що змінюються в реальному масштабі часу.

В роботі з метою врахування динамічних параметрів ТКМ, таких як:

1. Інтенсивність вхідного ПП (λ);
2. Інтенсивність обробки ПП маршрутизаторами в заданому шляху передачі (μ);
3. Кількість маршрутизаторів в заданому шляху передачі (N_m);
4. Завантаженість ЦПМ на маршрутизаторах в заданому шляху передачі (L_{CPU});

запропоновано динамічний метод розрахунку РІБ ПП для заданого шляху передачі. В даному методі РІБ транзитного ПП визначається через ризик $R_{m,дост.}$ несвоєчасної доставки ПП по заданому шляху передачі, що може мати місце в тому числі і внаслідок кібератак:

$$R_{m,дост.} = \left(1 - P_{m,дост.}\right) \cdot P_{загрози}, \tag{16}$$

де $\left(1 - P_{m,дост.}\right)$ – ймовірність несвоєчасної доставки (ЙНД) ПП вузлу-отримувачу; $P_{m,дост.}$ – ймовірність своєчасної доставки (ЙСД) ПП вузлу-отримувачу; $P_{загрози}$ – ймовірність реалізації загрози, що приводить до зниження ЙСД ПП отримувачу.

Для розрахунку ЙСД ПП в роботі удосконалено модель передачі пакетів від вузла-відправника до вузла-отримувача в умовах кібератак, в якій час передачі пакетів від вузла i до вузла j для шляху m можна знайти як

$$t_m = \sum_{n=1}^{N_m} t_{n,m}^{пер.} + \sum_{n=1}^{N_m} t_{n,m}^{обс.}, \tag{17}$$

де N_m – кількість маршрутизаторів у m-му шляху; $t_{n,m}^{пер.}$ – час передачі ПП по КЗ, що прилягає до n-го маршрутизатора m-го шляху; $t_{n,m}^{обс.}$ – тривалість обслуговування ПП n-м маршрутизатором m-го шляху.

Якщо прийняти як допущення, що маршрутизатор представляє собою одноканальну систему масового обслуговування з очікуванням, а вхідним потоком є пуассонівський потік, то щільність ймовірності розподілу часу обслуговування ПП n-м маршрутизатором буде описуватися показовим законом:

$$f_{обс._n}(t) = \beta_{обс.} \cdot e^{\beta_{обс.} \cdot t}, \tag{18}$$

де $\beta_{обс.} = \mu \cdot (1 - \rho)$ – інтенсивність обслуговування ПП маршрутизатором з урахуванням часу його обробки і часу очікування пакета в черзі, при $\rho = \frac{\lambda}{\mu}$; λ – інтенсивність ПП на вході маршрутизатора; μ – інтенсивність обробки ПП маршрутизатором.

Для аналізу впливу завантаженості ЦПМ на процес маршрутизації ПП було проведено експерименти на реальному мережевому обладнанні компанії Cisco – маршрутизаторах моделі 2801, з операційними системами IOS 12.4(11)XJ3 та IOS 12.4(12). Для генерації шкідливого ПП в ході експерименту використовувалися програми t50 та tcpreplay, а для зчитування значень завантаженості ЦПМ використовувався протокол SNMP. Це дозволило врахувати вплив завантаженості ЦПМ на процес маршрутизації ПП. Для цього у наведеній моделі пропонується враховувати динамічну зміну інтенсивності обслуговування пакета маршрутизатором з урахуванням часу його обробки і часу очікування пакета в черзі

$$\left.\begin{array}{c} \beta_{обс.} = \left\lfloor V_{1\%,маршр.,i} \cdot \left(L_{CPU,\,max,\,i} - L_{CPU,i,t}\right) \right\rfloor, \text{ при } \beta_{обс.} \le \mu - \lambda \\ \beta_{обс.} = \mu - \lambda, \text{ при } \beta_{обс.} > \mu - \lambda \end{array}\right\}, \tag{19}$$

де $V_{1\%,маршр.,i}$ – інтенсивність передачі ПП, яка необхідна для створення завантаженості процесора в 1% на маршрутизаторі i; $L_{CPU,max,i}$ – максимальне значення завантаженості ЦПМ на маршрутизаторі i; $L_{CPU,i,t}$ – оцінка завантаженості ЦПМ на маршрутизаторі i в момент часу t.

При цьому

$$L_{CPU,i,t} = L_{CPU,процесів} + L_{CPU,ПП}, \tag{20}$$

де $L_{CPU,процесів}$ – завантаженість ЦПМ процесами, які запущені на маршрутизаторі (в тому числі шкідливими); $L_{CPU,ПП}$ – завантаженість ЦПМ внаслідок маршрутизації ПП.

В запропонованій моделі щільність розподілу ймовірності часу передачі пакетів по заданому шляху $f_m(t)$ розраховувалося при різних параметрах функціонування маршрутизаторів λ, μ, L_{CPU} та кількості маршрутизаторів в шляху N_m шляхом згортки щільностей $f_{m,обс._n}(t)$ розподілу ймовірності часу обслуговування пакетів кожним n-м маршрутизатором в шляху m, при $n = \lfloor 1; N_m \rfloor$, за формулою:

$$f_m(t) = f_{m,обс._1}(t) * f_{m,обс._2}(t) * \ldots * f_{m,обс._n}(t). \quad (21)$$

Шукана щільність розподілу часу передачі пакетів по шляху $f_m(t)$ отримується прямим перетворенням Лапласа щільностей $f_{m,обс._n}(t)$, перемноженням їх зображень, зворотним перетворенням Лапласа. Інтегрування щільності розподілу ймовірності часу передачі пакетів від вузла i до вузла j для m-го шляху $f_m(t)$ за часом дозволяє визначити ймовірність доставки ПП до кінцевого вузла за заданий час:

$$P_{m,дост.}(t) = \int_0^t f_m(t)dt. \quad (22)$$

Запропонована модель дозволила оцінити такі особливості функціонування системи маршрутизації в умовах кібератак, як: наявність DoS ПП на вході маршрутизаторів, перевантаження ЦПМ шкідливими процесами та перемаршрутизація ПП по неоптимальному шляху передачі, що дозволяє розраховувати РІБ транзитного ПП для заданого шляху передачі на основі динамічних параметрів ТКМ. Перевагами моделі є можливість врахування впливу динамічно змінюваних факторів, що впливають на працездатність і якість обслуговування (Quality of Service, QoS) ТКМ, і забезпечення взаємозв'язку QoS з ІБ ПП, в той же час недоліком є ресурсомісткість обчислень, що виконуються в рамках представленої моделі.

У **третьому розділі** представлені вдосконалені потокові моделі вирішення задачі вибору оптимального шляху з використанням метрик таких ПДМ як: RIP, OSPF, EIGRP, особливістю яких є врахування РІБ в формулах розрахунку метрик для зазначених протоколів. При цьому РІБ враховується як додатковий параметр загальної формули обчислення метрики маршрутів, що дозволяє враховувати також і стандартні параметри метрики, які можуть бути різні для різних протоколів маршрутизації, наприклад, ПЗ, затримка, надійність і завантаженість КЗ.

В даній роботі пропонується враховувати в формулах розрахунку метрик ПДМ лише один з параметрів РІБ одночасно: або $R_{p_{i,j}}$, який визначає ризик порушення конфіденційності, доступності та цілісності транзитного ПП, або $R_{m,дост.}$, який визначає ризик несвоєчасної

доставки ПП по заданому шляху передачі. Для цього визначається множина $\{K_{CVSS}, K_\theta; K_p\}$ та наступні обмежуючі умови:

$$\left.\begin{array}{c} K_{CVSS} \cup K_\theta \neq 0 \rightarrow K_P = 0, \\ K_P \neq 0 \rightarrow K_{CVSS} = 0,\ K_\theta = 0, \end{array}\right\} \tag{23}$$

де K_{CVSS} та K_θ – коефіцієнти для врахування параметрів метрик NIST CVSS і EMM відповідно, які застосовуються для розрахунку параметра $R_{p_{i,j}}$; K_P – коефіцієнт, який визначає, чи буде враховуватися параметр $R_{m,дост.}$ в формулі розрахунку метрики, при цьому $K_P \in \{0;1\}$.

В даній роботі метод врахування РІБ в метриці протоколу RIP пропонується формалізувати наступним виразом:

$$M_{p_{i,j};RIP} = \left\lfloor \frac{Hops_{i,j} + K_R \cdot 15^{R_{p_{i,j}} + K_P \cdot R_{m,дост.}}}{2^{K_R}} \right\rfloor, \tag{24}$$

де $R_{p_{i,j}}$ – РІБ для шляху p при передачі ПП між вузлами i, j, при $R_{p_{i,j}} \in [0;1]$; K_R – коефіцієнт, який дозволяє активувати або деактивувати врахування РІБ у формулі розрахунку метрики, $K_{RIP} \in \{0;1\}$; $R_{m,дост.}$ – РІБ несвоєчасної доставки ПП при його передачі від вузла i до вузла j по m-му шляху, при цьому $R_{m,дост.} \in [0;1]$; K_P – коефіцієнт, який визначає, чи буде враховуватися параметр $R_{m,дост.}$ в формулі розрахунку метрики, при цьому $K_P \in \{0;1\}$.

В метриці протоколу OSPF РІБ пропонується враховувати наступним чином:

$$M_{p_{i,j};OSPF} = \left\lfloor \left(\sum_{k \in p_{i,j}} LC_k \right) \cdot \left(C_{OSPF,scale} \right)^{K_R \cdot \left(R_{p_{i,j}} + K_P \cdot R_{m,дост.} \right)} \right\rfloor, \tag{25}$$

$$LC_k = \left\lfloor \frac{B_{ref}}{B_{real}} \right\rfloor, \tag{26}$$

де $C_{OSPF,scale}$ – коефіцієнт масштабування, що дорівнює 256; $\sum_{k \in p_{i,j}} LC_k$ – сума вартостей усіх КЗ k, що входять в шлях $p_{i,j}$; B_{ref} – параметр, що встановлюється адміністратором ТКМ, стандартно $B_{ref} = 10^8$, біт/с.

Врахування РІБ в метриці протоколу EIGRP пропонується формалізувати як:

$$M_{p_{i,j};EIGRP} = \left[\left(K_1 \cdot B^p_{min} + \frac{K_2 \cdot B^p_{min}}{256\text{-}L^p_{max}} + K_3 \cdot \frac{D^p_{sum}}{10} \right) \cdot \frac{K_5}{K_4 + R^p_{min}} \right] \cdot \left(C_{scale}\right)^{\left(2-\left(K_R - K_R \cdot \left(R_{p_{i,j}} + K_P \cdot R_{m,\text{дост.}}\right)\right)\right)}, \quad (27)$$

$$B^p_{min} = \left\lfloor \frac{10^7}{\mathbf{min}\left(B^{l,p}_{i,j}\right)} \right\rfloor, \quad (28)$$

$$D^p_{sum} = \sum_{i \neq j} D^p_{i,j}, \ p \in P_{i,j}, \quad (29)$$

де B^p_{min} – найменше значення зваженого показника ПЗ в шляху p, кбіт/с; L^p_{max} – найбільша завантаженість одного з КЗ в шляху p; D^p_{sum} – сумарна затримка в шляху, мкс; R^p_{min} – найменша надійність одного з КЗ в шляху p; $P_{i,j}$ – всі можливі шляхи в заданій ТКМ при передачі інформації між вузлами i, j при $i \neq j$; C_{scale} – коефіцієнт масштабування, $C_{scale} = 16$; K_1, K_2, K_3, K_4, K_5 – коефіцієнти, які дозволяють враховувати в метриці вищевказані параметри, при цьому за замовчуванням для даних коефіцієнтів використовуються наступні значення: $K_1 = K_3 = 1$ та $K_2 = K_4 = K_5 = 0$; $\mathbf{min}\left(B^{l,p}_{i,j}\right)$ – найменша ПЗ одного з КЗ l в шляху p при передачі пакетів між вузлами i, j, при $i \neq j$, кбіт/с; $D^p_{i,j}$ – затримка ПП в кожному з КЗ, що входять в шлях p при передачі інформації між вузлами i, j, при $i \neq j$, мкс.

У **четвертому розділі** проведено кількісний аналіз удосконалених моделей динамічної маршрутизації. Для тестування запропонованих моделей були проведені експерименти з використанням середовища MATLAB. Розв'язання задачі одношляхової маршрутизації зводиться до пошуку найкоротшого шляху і формалізується як задача булевого програмування, яку можна вирішити за допомогою функції bintprog інструментарію «Optimization Toolbox» пакета MATLAB. Розв'язання задачі багатошляхової маршрутизації зводиться до вирішення оптимізаційної задачі лінійного програмування з використанням функції linprog інструментарію «Optimization Toolbox» пакета MATLAB.

Приклад кількісного аналізу наводиться на основі однієї з досліджуваних топологій, що представлена на рис. 1. У наведеній топології усі канали зв'язку мають пропускну здатність 100 мбіт/с та затримку 10 мс. ПП передається з маршрутизатора R1 до WAN. При використанні стандартних метрик ПДМ оптимальним шляхом передачі ПП для ПДМ, що досліджуються в даній роботі, буде шлях R1 –> R2 –> R6.

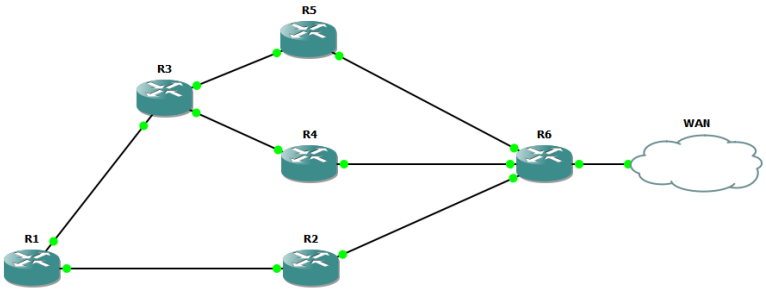
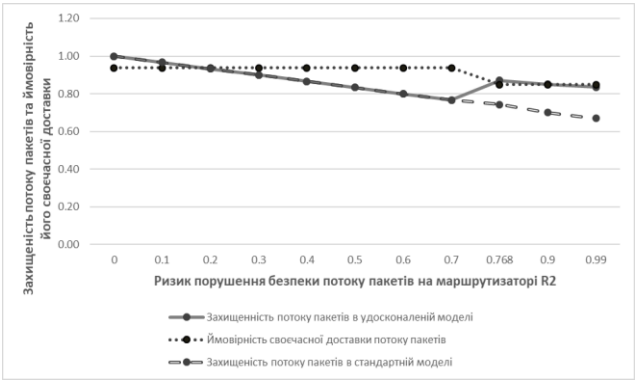
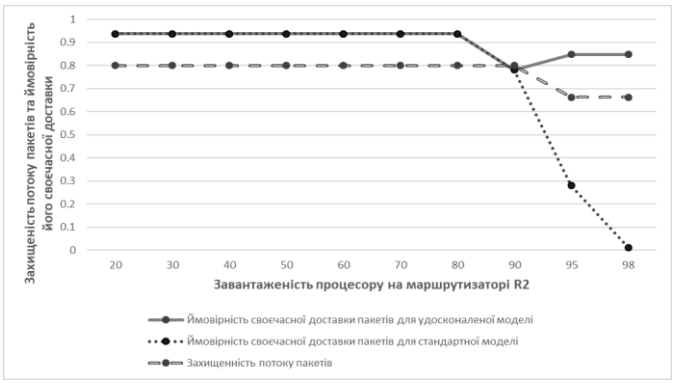


Рис. 1. Топологія мережі для проведення кількісного аналізу

На графіках рис. 2 представлені результати кількісного аналізу для ПДМ з використанням метрик RIP, OSPF, EIGRP, при цьому на графіках а, в, ґ представлено зростання захищеності ПП при зменшенні його ЙСД для відповідних протоколів, а на графіках б, г, д навпаки – зростання ЙСД ПП при зменшенні його захищеності для відповідних протоколів.



а)



б)

Рис. 2. Результати експериментів для ДМ ПП з використанням метрики протоколу RIP для випадків коли: а – використовується РІБ, що розраховується на основі статичних параметрів; б – використовується РНД ПП

На графіку а, рис. 2, відображена ситуація перемаршрутизації ПП по запасним шляхам, коли РІБ ПП на маршрутизаторі R2 досягає величини 0,768. При використанні вдосконаленого моделі ДМ та метрики протоколу RIP ПП балансується між доступними шляхами, що дозволило підвищити захищеність ПП приблизно на 4%. При цьому ЙСД зменшилася приблизно на 9%.

Подібні результати отримані також для інших ПДМ. Так використання вдосконаленого моделі ДМ та метрики протоколу OSPF дозволило підвищити захищеність ПП приблизно на 14%, при цьому ЙСД зменшилася приблизно на 8%, а для метрики протоколу EIGRP – підвищити захищеність ПП приблизно на 13%, при цьому ЙСД зменшилася приблизно на 9%.

На графіку б, рис. 2, відображена ситуація перемаршрутизації ПП по запасним шляхам, коли завантаженість ЦПМ на маршрутизаторі R2 досягає величини 95%. При цьому на

маршрутизаторах задані наступні значення: $R_{CVSS_{R1}} = 0{,}2$, $R_{CVSS_{R2}} = 0{,}2$, $R_{CVSS_{R3}} = 0{,}4$, $R_{CVSS_{R4}} = 0{,}55$, $R_{CVSS_{R5}} = 0{,}5$, $R_{CVSS_{R6}} = 0{,}2$. При використанні вдосконаленої моделі ДМ та метрики RIP ПП повністю перемаршрутизується через маршрутизатор R3, що дозволило підвищити ЙСД приблизно на 14%, при цьому захищеність ПП зменшилася також приблизно на 14%. При використанні метрики протоколу OSPF – ПП повністю перемаршрутизується через маршрутизатор R3 при завантаженості ЦПМ 90% на R2, що дозволило підвищити ЙСД приблизно на 14%, при цьому захищеність ПП зменшилася також приблизно на 14%. При використанні метрики протоколу EIGRP – ПП повністю перемаршрутизується через маршрутизатор R3 при завантаженості ЦПМ 90% на R2, що дозволило підвищити ЙСД приблизно на 15%, при цьому захищеність ПП зменшилася також приблизно на 14%.

ВИСНОВКИ ПО РОБОТІ

В роботі вирішено актуальну науково-прикладну задачу, що полягала у розробці моделей та методів підвищення ІБ ПП, що маршрутизується в ТКМ, шляхом врахування РІБ вузлів мережі як додаткового параметру вибору оптимального маршруту передачі. При цьому отримані наступні результати:

1. Проведено аналіз методів розрахунку РІБ ПП в ТКМ. За результатами аналізу запропоновано розділити методи на дві групи: статичні та динамічні. В статичному методі ризик змінюється за тригером та при фізичній зміні топології мережі, в динамічному – при зміні параметрів ТКМ та маршрутизаторів в масштабі реального часу. В статичному методі ризик розраховується на основі параметрів метрик вразливостей NIST CVSS v2 та ЕММ, в динамічному – на основі ймовірності своєчасної доставки ПП.
2. Недоліком методу розрахунку РІБ на основі статичних параметрів є те, що у РІБ різних шляхів передачі можуть враховуватися параметри маршрутизаторів, які входять в усі шляхи, що аналізуються, одночасно. Так при однаковому номінальному значенню РІБ декількох шляхів, їх середні значення будуть відрізнятися в залежності від кількості маршрутизаторів в шляху, що не є коректним.
3. Для розрахунку ЕММ запропоновано використовувати параметри ПЗ та затримки в КЗ ТКМ, а також ввести додатковий параметр масштабування. Це дозволило враховувати в ЕММ параметри ТКМ, які можуть впливати на якість обслуговування ПП, а також збільшити розкид значень ЕММ, що дозволило збільшити вплив РІБ на метрики ПДМ.
4. Проведено аналіз впливу різних методів розрахунку рухомого середнього (РС) на детектування DoS атаки шляхом аналізу ентропії ПП. За результатами аналізу вибрано метод простого РС, так як даний метод швидше реагує на зміну ентропії ПП та демонструє

менше середньоквадратичне відхилення: у порівнянні з методом адаптивної РС Кауфмана приблизно на 21,7%, та у порівнянні з методом РС з динамічним періодом усереднення приблизно на 16,9%.

5. Проведено аналіз впливу завантаженості ЦПМ маршрутизаторів в заданому шляху передачі на процес маршрутизації ПП. Експериментальні дослідження проводилися для маршрутизаторів компанії Cisco моделі 2801 та були використані при проведенні кількісного аналізу запропонованих в роботі моделей та методів.
6. Розроблено математичну модель процесу передачі ПП в умовах кібератак, новизною якої є можливість проведення розрахунків при наявності DoS атак на маршрутизатори ТКМ; шкідливих процесів на маршрутизаторах, які знижують ПЗ вузлу, чи взагалі виводять його з ладу; атак на перемаршрутизацію даних по не ефективним шляхам. Це стало можливим завдяки розв'язанню задачі знаходження щільності розподілу ймовірності часу передачі ПП при різних умовах роботи маршрутизаторів мережі, а також врахуванні впливу завантаженості ЦПМ в заданому шляху передачі на процес маршрутизації ПП. Пропонується використовувати дану модель для знаходження РІБ несвоєчасної доставки ПП вузлу-отримувачу.
7. Розроблено моделі одношляхової та багатошляхової маршрутизації ПП в ТКМ, новизною яких є врахування РІБ разом з базовими параметрами в формулах розрахунку метрик шляхів для таких ПДМ, як: RIP, OSPF, EIGRP. Використання запропонованих моделей дозволило вибирати шлях передачі ПП в ТКМ на основі критерію «безпека-якість» та знизити ризики порушення конфіденційності, цілісності, доступності та своєчасної доставки транзитного ПП.
8. Проведено кількісний аналіз запропонованих моделей з використанням метрик ПДМ: RIP, OSPF, EIGRP. За результатами аналізу в заданій ТКМ для протоколу RIP удосконалена модель продемонструвала підвищення захищеності ПП на 4% при зменшенні ЙСД ПП на 9%, та підвищення ЙСД ПП на 14% при зниженні захищеності ПП на 14%; для протоколу OSPF – підвищення захищеності ПП на 14% при зменшенні ЙСД ПП на 8%, та зростання ЙСД ПП на 14% при зменшенні захищеності ПП на 14%; для протоколу EIGRP – зростання захищеності ПП на 13% при зменшенні ЙСД ПП на 9%, та зростання ЙСД ПП на 15% при зменшенні захищеності на 14%.

ПУБЛІКАЦІЇ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Снегуров А.В. Метод формирования метрик маршрутизации, основанный на рисках информационной безопасности / А.В. Снегуров, В.Х. Чакрян // Системи управління, навігації та зв'язку – Вип. 4(24). – 2012. – С. 105-110.

2. Снігуров А.В. Підхід до управління маршрутизацією в безпроводових телекомунікаційних мережах спеціального призначення, функціонуючих в умовах інформаційної протидії / А.В. Снігуров, В.Х. Чакрян // Захист інформації і безпека інформаційних систем : ІІ міжнародна наук.-техн.конф. : Збірник тез доповідей – Львів, 2013. – С. 16-17.
3. Скибин В.П. Определение нарушений штатного режима функционирования сети с использованием формализованной процедуры оценки наблюдаемого процесса / В.П. Скибин, В.Х. Чакрян // Радиоэлектроника и молодежь в XXI веке : XVII международный молодежный форум : Збірник тез доповідей – Харків, 2013. – Т. 4. – С. 220-221.
4. Смирнов А.О. Организация защищенной корпоративной сети с использованием программного средства HIAB от компании Outpost / А.О. Смирнов, В.Х. Чакрян // Радиоэлектроника и молодежь в XXI веке : XVII международный молодежный форум : Збірник тез доповідей – Харків, 2013. – Т. 4. – С. 224-225.
5. Снегуров А.В. Особенности формирования метрики маршрутизации, основанных на рисках информационной безопасности / А.В. Снегуров, В.Х. Чакрян // Радиоэлектроника и молодежь в XXI веке : XVII международный молодежный форум : Збірник тез доповідей – Харків, 2013. – Т. 4. – С. 226-227.
6. Snegurov A.V. The approach for selection of a routing metric in special-purpose wireless networks under the influence of radio-electronic investigation / A.V. Snegurov, V.K. Chakryan, A.A. Mamedov // Microwave and Telecommunication Technology (CriMiCo) : 23rd International Crimean Conference : Proc. of the conference – Sevastopol, 2013. – P. 470-471.
7. Snegurov A.V. Intrusion detection method according to the characteristics of refreshing process / A.V. Snegurov, V.P. Skibin, V.H. Chakryan // Microwave and Telecommunication Technology (CriMiCo) : 23rd International Crimean Conference : Proc. of the conference – Sevastopol, 2013. – P. 484-485.
8. Snigurov A. (19-23 Feb. 2013) Approach of routing metrics formation based on information security risk / A. Snigurov, V. Chakryan // Experience of Designing and Application of CAD Systems in Microelectronics (CADSM) : 12th International Conference : Proc. of the conference – Lviv, 2013. – C. 339-340.
9. Снегуров А.В. Механизм повышения живучести телекоммуникационной сети путем выбора метрики маршрутизации с использованием теории риска информационной безопасности / А.В. Снегуров, В.Х. Чакрян // Проблемы инфокоммуникаций. Наука и

технологии (PICS&T-2013) : Сборник научных трудов первой международной научно-практической конференции : Збірник тез доповідей – Харків, 2013. – С. 81-84.

10. Снегуров А.В. Полумарковская модель оценки качества управления трафиком в телекоммуникационных сетях с предвычислением путей в условиях наличия угроз информационной безопасности / А.В. Снегуров, В.Х. Чакрян // Системи обробки інформації. – 2013. – Вип. 9(116). – С. 167-173.
11. Snigurov A. Semi-Markov Model of Traffic Control Quality Assurance in Telecommunication Networks with Routes Precalculation Considering Risks of Information Security / A. Snigurov, V. Chakrian // Modern Problems of Radio Engineering, Telecommunications and Computer Science : international Conference TCSET : Proc. of the conference – Lviv, 2014. – P. 578-580.
12. Снегуров А.В. Подход к вычислению рейтинга информационной безопасности сетевых устройств / А.В. Снегуров, В.Х. Чакрян // Системи обробки інформації. – 2014. – Вип. 1(117). – С. 150-155.
13. Snigurov A. The DoS attack risk calculation based on the entropy method and critical system resources usage / A. Snigurov, V. Chakrian // Problems of Infocommunications. Science and Technology (PICS&T-2014) : First International IEEE Conference : Proc. of the conference – Kharkiv, 2014. – P. 186-187.
14. Снегуров А.В. Угрозы информационной безопасности стека протоколов IPv6 / А.В. Снегуров, В.Х. Чакрян // Збірник наукових праць Харківського університету повітряних сил. – Вип. 4(41). – 2014. – С. 53-60.
15. Снегуров А.В. Механизмы обеспечения безопасности стека протоколов IPv6 / А.В. Снегуров, В.Х. Чакрян // Системи обробки інформації. – 2015. – Вип. 1(126). – С. 154-161.
16. Снегуров А.В. Расчет уязвимости сети на основе структурно-функционального анализа ее топологии / А.В. Снегуров, В.Х. Чакрян // Радиоэлектроника и молодежь в XXI веке : XIX международный молодежный форум : Збірник тез доповідей – Харків, 2015. – Т. 4. – С. 132-133.
17. Snihurov A. Improvement of EIGRP Protocol Routing Algorithm Based on Information Security Metrics / A. Snihurov, V. Chakrian // Problems of Infocommunications. Science and Technology (PICS&T-2015): Second International IEEE Conference : Proc. of the conference – Kharkiv, 2015. – P. 263-265.
18. Снегуров А.В. Усовершенствование алгоритма маршрутизации с балансировкой нагрузки по путям неравнозначной стоимости для протокола EIGRP / А.В. Снегуров, В.Х. Чакрян // Системы обробки інформації. – 2015. – Вип. 10(135). – С. 133-139.

19. Snihurov A. Improvement of EIGRP Protocol Routing Algorithm with the Consideration of Information Security Risk Parameters / A. Snihurov, V. Chakrian // Scholars Journal of Engineering and Technology. – 2015. – Вип. 3(8). – С. 707-714.
20. Снегуров А.В. Анализ устойчивости ко взлому современных механизмов парольной защиты операционных систем / А.В. Снегуров, В.Х. Чакрян // Восточно-Европейский журнал передовых технологий – 2011. – Т. 2. – № 10. – С. 27-29.
21. Snigurov A. Approach to Determination of Priority for Nodes of Telecommunication Network Functioning under DDOS-attacks in Order to Provide Quality of Service / A. Snigurov, V. Chakrian // Modern Problems of Radio Engineering, Telecommunications and Computer Science : international Conference TCSET : Proc. of the conference – Lviv, 2016. – P. 537-539.
22. Пат. 107617 України, МПК (2016.01) H04L 12/00. Спосіб маршрутизації трафіку за допомогою протоколу EIGRP з урахуванням вимог інформаційної безпеки / Снігуров А.В., Чакрян В.Х.; власник Харківський національний університет радіоелектроніки. – № u201600667; заявл. 27.01.2016; опубл. 10.06.2016, бюл. № 11.

АНОТАЦІЯ

Чакрян Вадим. Моделі та методи маршрутизації трафіку в телекомунікаційних мережах з урахуванням вимог інформаційної безпеки. – Рукопис. Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі. – Харківський національний університет радіоелектроніки, Харків, 2017.

Дисертаційна робота присвячена розв‘язанню актуальної наукової задачі, яка полягає в підвищенні інформаційної безпеки (ІБ) потоку пакетів (ПП) в процесі його динамічної маршрутизації (ДМ) в телекомунікаційній мережі (ТКМ) шляхом урахування ризиків порушення конфіденційності, цілісності та доступності транзитних даних як додаткових параметрів вибору оптимального шляху передачі.

В ході вирішення поставленої наукової задачі удосконалена математична модель процесу передачі ПП 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. Це стало можливим завдяки вирішенню задачі знаходження щільності розподілу ймовірності часу передачі ПП при різних законах розподілу надходження та обробки ПП на кожному з маршрутизаторів, а також врахуванні впливу завантаженості центрального процесору маршрутизаторів в заданому шляху передачі на процес маршрутизації ПП. Пропонується використовувати дану модель для знаходження РІБ несвоєчасної доставки ПП вузлу-отримувачу.

Розроблено новий метод оцінки ризику інформаційної безпеки (РІБ) шляхів передачі ПП, новизною якого є врахування таких параметрів як: ефективність та вразливість маршрутизаторів мережі, а також ймовірність здійснення атаки типу відмова в обслуговуванні на маршрутизатори в заданий момент часу. Це дозволило оцінювати ризики порушення конфіденційності, цілісності та доступності ПП при його передачі по заданому шляху.

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

Ключові слова: динамічна маршрутизація, ризик інформаційної безпеки, RIP, OSPF, EIGRP.

АННОТАЦИЯ

Чакрян Вадим. Модели и методы маршрутизации трафика в телекоммуникационных сетях с учетом требований информационной безопасности. – Рукопись. Диссертация на соискание ученой степени кандидата технических наук по специальности 05.12.02 – телекоммуникационные системы и сети. – Харьковский национальный университет радиоэлектроники, Харьков, 2017.

Диссертация посвящена решению актуальной научной задачи, которая заключается в повышении информационной безопасности (ИБ) потока пакетов (ПП) в процессе его динамической маршрутизации (ДМ) в телекоммуникационной сети (ТКС) путем учета рисков нарушения конфиденциальности, целостности и доступности транзитных данных как дополнительных параметров выбора оптимального пути передачи.

В работе проведен анализ влияния различных типов атак на систему маршрутизации и на ее параметры функционирования, на основе которого разработан новый метод оценки риска информационной безопасности (РИБ) путей передачи ПП, новизной которого является учет таких параметров как: эффективность и уязвимость маршрутизаторов сети, а также вероятность осуществления атаки типа отказ в обслуживании (Denial of Service, DoS) на маршрутизаторы в заданный момент времени. Это позволило оценивать риски нарушения конфиденциальности, целостности и доступности ПП при его передаче по заданному пути.

Усовершенствован метод расчета эффективности маршрутизаторов сети (ЭМС), который основан на математических методах теории живучести информационных систем. Усовершенствование состоит в использовании параметров пропускной способности (ПС) и задержки в каналах связи ТКС, а также ввести дополнительный параметр масштабирования. Это позволило учитывать в ЭМС параметры ТКС, которые могут влиять на качество обслуживания ПП.

В основе динамического метода расчета риска лежит усовершенствованная математическая модель процесса передачи ПП в условиях кибератак, новизной которой является возможность проведения расчетов при наличии: DoS атак на маршрутизаторы сети; вредоносных процессов на маршрутизаторах, которые снижают ПС узла, или вообще выводят его из строя; атак на перемаршрутизацию ПП по неэффективным путям. Усовершенствование модели заключается в использовании прямого и обратного преобразования Лапласа над свертками плотностей распределения времени обслуживания ПП маршрутизаторами, что позволяет проводить расчеты с учетом различных условий функционирования маршрутизаторов, а также модель учитывает загруженность центрального

процессора маршрутизаторов в заданном пути передачи, что позволяет оценить влияние системных процессов маршрутизатора на маршрутизацию ПП. Использование модели позволило динамично оценивать риск несвоевременной доставки ПП на конечный узел по заданному пути в условиях загруженности маршрутизаторов сети вследствие кибератак.

Также в работе получили дальнейшее развитие модели однопутевой и многопутевой маршрутизации ПП в ТКС в условиях кибератак. Новизной моделей является учет РИБ вместе с базовыми параметрами в формулах расчета метрик путей. Использование предложенных моделей позволило выбирать путь передачи ПП в ТКС на основе критерия «безопасность-качество» и снизить риски нарушения конфиденциальности, целостности, доступности и своевременной доставки транзитного ПП.

По результатам количественного анализа предложенных моделей однопутевой и многопутевой маршрутизации для исследуемых протоколов динамической маршрутизации в заданной ТКС для протокола RIP усовершенствованная модель продемонстрировала повышение защищенности ПП на 4% при уменьшении вероятности своевременной доставки (ВСД) ПП на 9%, и повышение ВСД ПП на 14% при снижении защищенности ПП на 14%; для протокола OSPF - повышение защищенности ПП на 14% при уменьшении ВСД ПП на 8%, и увеличение ВСД ПП на 14% при уменьшении защищенности ПП на 14%; для протокола EIGRP - увеличение защищенности ПП на 13% при уменьшении ВСД ЧП на 9%, и увеличение ВСД ПП на 15% при уменьшении защищенности на 14%.

Ключевые слова: динамическая маршрутизация, риск информационной безопасности, RIP, OSPF, EIGRP.

ABSTRACT

Chakrian Vadym. Models and methods of traffic routing in telecommunication networks considering information security requirements. – Manuscript. Dissertation for the degree of a candidate of technical sciences majoring in 05.12.02 – telecommunication systems and networks. − Kharkiv National University of Radio Electronics, Kharkiv, 2017.

The dissertation is dedicated to the solution of the relevant scientific problem, which is to increase the information security (IS) of the packet flow (PF) in the process of its dynamic routing (DR) in the telecommunication network (TCN), taking into account the risks of violation of confidentiality, integrity and availability of transit data as additional parameters for choosing the optimal route.

In the course of solving the given scientific problem, the model of PF routing under cyberattacks has been improved due to the use of direct and reverse Laplace transformation over the convolutions of distribution of service time densities of PP by routers and taking into account the load of the routers' control processing unit in a given transmission path. The advantage of the proposed model is the

possibility of conducting calculations in the presence of: denial of service (DoS) attacks on the routers of the network; malicious processes on routers that reduce node bandwidth, or even eliminate it; attacks on the re-routing of the PP by not effective paths. The use of the model allowed to dynamically assess the risk of late delivery of PP to the recipient as a result of cyberattacks.

A new method for assessing the information security risk (ISR) has been developed, the novelty of which is consideration of account such parameters as: efficiency and vulnerability of network routers, as well as the likelihood of DoS attacks implementation on routers at a given time. This allowed to assess the risks of violation of confidentiality, integrity and availability of PF during transmission on a given path.

The further development of the model of single-path and multi-path routing of the PF in the TCN has been received. The novelty of the models is to consider ISR together with the basic parameters in the formulas for calculating the paths metrics. The use of the proposed models allowed choosing the path of transmission of PF in the TCN based on the “security-quality” criterion and reducing the risks of violation of confidentiality, integrity, availability and timely delivery of transit PF.

Key Words: dynamic routing, information security risk, RIP, OSPF, EIGRP.