МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

Кваліфікаційна наукова
праця на правах рукопису

ЧАКРЯН ВАДИМ ХАЗАРОВИЧ

УДК 621.391

ДИСЕРТАЦІЯ

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

Спеціальність: 05.12.02 – Телекомунікаційні системи та мережі
172 – Телекомунікації та радіотехніка
Подається на здобуття наукового ступеня кандидата технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____В.Х. Чакрян
Науковий керівник Снігуров Аркадій Владиславович, кандидат технічних наук, доцент.

Ідентичність всіх примірників дисертації засвідчую:
Учений секретар спеціалізованої вченої ради /О.Б. Ткачова/

Харків – 2017

АНОТАЦІЯ

Чакрян В.Х. Моделі та методи маршрутизації трафіку в телекомунікаційних мережах з урахуванням вимог інформаційної безпеки. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук (доктора філософії) за спеціальністю 05.12.02 «Телекомунікаційні системи та мережі» (172 – Телекомунікації та радіотехніка). – Харківський національний університет радіоелектроніки, Харків, 2017.

У першому розділі роботи представлено аналіз існуючих наукових досліджень за темою дисертації. На основі аналізу було виявлено, що малодослідженою областю є забезпечення інформаційної безпеки (ІБ) транзитного потоку пакетів (ПП) в телекомунікаційній мережі (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), таких як: 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). Відсутність стандартизованих методів забезпечення ІБ, окрім автентифікації джерела оновлень, та відсутність наукових досліджень, щодо впливу ризику інформаційної безпеки (РІБ) на маршрутизаторах в заданому шляху на вибір оптимального шляху передачі ПП, стали факторами для постановки науково-практичної задачі дисертаційної роботи, яка полягає у підвищенні ІБ ПП в процесі його динамічної маршрутизації (ДМ) в ТКМ шляхом урахування ризиків порушення конфіденційності, цілісності та доступності транзитних даних як додаткових критеріїв вибору оптимального шляху передачі.

У другому розділі представлені методи розрахунку РІБ, який може розраховуватися на основі статичних або динамічних параметрів. До статичних параметрів відносяться: метрики критичності вразливості, що розраховуються за стандартом 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), а також ефективність маршрутизатора мережі (ЕММ). До динамічних параметрів відноситься: ймовірність своєчасної доставки (ЙСД) ПП до вузла-отримувача.

РІБ шляху на основі статичних параметрів розраховується як середнє значення одного з параметрів (метрик вразливостей чи ЕММ) всіх маршрутизаторів в заданому шляху. Так як одночасно враховується лише один з параметрів, то для прийняття рішення про те, який з параметрів буде активний, запропоновано використовувати додатковий параметр, який визначає наявність чи відсутність атаки типу відмова в обслуговуванні (Denial of Service, DoS) на маршрутизатори ТКМ. Параметр розраховується на основі аналізу ентропії ПП і, якщо він перевищує задану порогову величину, то РІБ шляху розраховується на основі ЕММ, в протилежному випадку – на основі метрик вразливостей.

РІБ шляху на основі динамічних параметрів розраховується як ризик несвоєчасної доставки (РНД) ПП вузлу-отримувачу. Розрахунки виконуються за допомогою розробленої моделі процесу передачі ПП в ТКМ в умовах кібератак. Новизною моделі є можливість проведення розрахунків при наявності: атак типу відмова в обслуговуванні на маршрутизатори мережі; шкідливих процесів на маршрутизаторах, які знижують пропускну здатність (ПРЗД) вузлу, чи взагалі виводять його з ладу; атак на перемаршрутизацію даних по не ефективним шляхам. В якості параметрів дана модель використовує: кількість маршрутизаторів в заданому шляху передачі, інтенсивність вхідного ПП, інтенсивність обробки ПП маршрутизаторами, та завантаженість центрального процесору маршрутизаторів (ЦПМ). Для аналізу впливу ЦПМ на інтенсивність обробки ПП маршрутизатором були проведені експерименти на реальному обладнанні Cisco, а отримані результати були використані у запропонованій моделі.

У третьому розділі представлені розроблені 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. Також наводиться аналіз методів врахування РІБ шляху в формулах розрахунку метрик протоколів RIP, OSPF, EIGRP. В результаті аналізу вибрані методи, які:

- демонструють зростаючу експоненційну залежність вихідного покажчику метрики від РІБ шляху;
- в яких при більших значеннях РІБ зростає значення метрики;
- в яких РІБ не призводить до випадків, коли метрика дорівнює нулю;
- в яких в метриці враховуються стандартні параметри для відповідних ПДМ.

За результатами кількісного аналізу, наведеного в четвертому розділі, в заданій ТКМ в умовах роботи 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%; 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%; протоколу EIGRP – зростання захищеності ПП на 13% при зменшенні ЙСД ПП на 9%, та зростання ЙСД ПП на 15% при зменшенні захищеності на 14%. Також на основі кількісного аналізу удосконалених моделей виявлено, що моделі коректно працюють в ТКМ, в яких усі КЗ мають однакову ПРЗД. При цьому в ТКМ, в яких існують КЗ з різною ПРЗД використання удосконалених моделей може призвести до маршрутизації ПП по шляхам з достатньою ПРЗД, але з більшим значенням РІБ.

Ключові слова: динамічна маршрутизація, RIP, OSPF, EIGRP, метрика, шлях передачі пакетів, поток пакетів, маршрутизатор, QoS, ризик інформаційної безпеки, CVSS, живучість інформаційної системи, DoS.

ABSRTACT

Chakrian V. Models and methods of traffic routing in telecommunication networks considering information security demands. – Qualification research work as a manuscript.

The thesis for a candidate degree (Ph.D.) majoring in 05.12.02 «Telecommunication systems and networks» (172 – Telecommunications and radio engineering). – Kharkiv National University of Radio Electronics, Kharkiv, 2017.

The first section of the paper presents an analysis of existing research on the topic of the dissertation. On the basis of the analysis, it was discovered that the low-level area is to provide information security (IS) of a transit packet flow (PF) in a telecommunication network (TCN) using dynamic routing protocols (DRP), working in the wired networks within one autonomous system and belonging to the internal gateway protocols (IGP), such as: Routing Information Protocol (RIP), Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP). Lack of standardized information security methods, except authentication of the updates source, and the lack of research on the impact of information security risk (ISR) on routers in a given path on the choice of an optimal PF routing path, became the factors for setting the scientific and practical task of the dissertation – to increase of IS of a PP in the process of its dynamic routing (DR) in a TCN taking into account the risks of violation of the confidentiality, integrity and availability of transit data as additional parameters for choosing the optimal route.

The second section presents the calculation methods of ISR, which can be calculated on the basis of static or dynamic parameters. The static parameters include:

critical vulnerability metrics calculated using a Common Vulnerability Scoring System version 2 (CVSS v2) standard created by National Institute of Standards and Technologies (NIST), as well as the efficiency of the network router (ENR). Dynamic parameters include: the probability of timely delivery (PTD) of a PF to the receiving node.

ISR of the path based on static parameters is calculated as the average of one of the parameters (vulnerability metrics or ENR) of all routers in a given route. Since at the same time only one of the parameters is taken into account, it is suggested to use an additional parameter that determines the presence or absence of the Denial of Service (DoS) attack on TCN routers to decide which of the parameters will be active. The parameter is calculated based on the entropy analysis of a PF and, if it exceeds the specified threshold, then ISR of the route is calculated on the basis of ENR, otherwise – on the basis of the vulnerability metrics.

ISR of the path based on dynamic parameters is calculated as the probability of untimely delivery (PUD) of a PF to a destination. The calculations are performed with the help of the developed model of a PF routing in a TCN under cyberattacks. The novelty of the model is the possibility of conducting calculations when it exists: a DoS attack on routers of a TCN; malicious processes on routers that reduce bandwidth (BW) of the routers, or even totally make it unavailable; attacks on re-routing of data by ineffective routes. As parameters this model uses: the number of routers in a given route, the intensity of incoming PF, the intensity of a PF processing by routers, and a load of central processing unit (CPU) of routers. To analyze the impact of a CPU on intensity of a PF processing by a given router experiments on real Cisco equipment were conducted, and the obtained results were used in the proposed model.

The third section presents the developed models of singlepath and multipath routing of a PF in a TCN, the novelty of which is an accounting of an ISR along with the basic parameters in the formulas for calculating the routing metrics for such DRP as: RIP, OSPF, EIGRP. The use of the proposed models made it possible to choose an optimal route of transmission of a PF in a TCN based on the criteria «security-quality» and reduce the risks of violation of confidentiality, integrity, availability and timely delivery of a transit PF. Also, the analysis of a route ISR accounting methods is presented in formulas

for calculating metrics for such DRP as: RIP, OSPF, EIGRP. As a result the methods with the next characteristics were chosen:

- they show a growing exponential dependence of a final metric result on the ISR of a route;
- for larger values of an ISR, the value of the metric increases;
- an ISR does not lead to situations when the metric becomes equal to zero;
- the metric take into account the standard parameters of the corresponding DRP.

As a result of the quantitative analysis given in the fourth section, for a given TCN for RIP an improved model has demonstrated an increase of a PF IS by 4% while decreasing PTD of a PF by 9%, and an increase of PF PTD by 14% while decreasing a PF IS by 14%; for OSPF – an increase of a PF IS by 14% while decreasing PTD of a PF by 8%, and an increase of PF PTD by 14% while decreasing a PF IS by 14%; for EIGRP – an increase of a PF IS by 13% while decreasing PTD of a PF by 9%, and an increase of PF PTD by 15% while decreasing a PF IS by 14%. Also, based on the quantitative analysis of the improved models, it was found that the models are correctly working in TCN where all links between routers have similar BW. While in TCN where links can have different BW the usage of the improved model may lead to routing of PF via links with enough BW but with bigger ISR.

Key words: dynamic routing, RIP, OSPF, EIGRP, metric, route, packet flow, router, QoS, information security risk, CVSS, survivability of the information system, DoS.

Список публікацій здобувача:

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 : II міжнародна наук.-техн.конф. : Тези доп. – 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 : Тези доп. – Хакрів, 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 : Тези доп. – Хакрів, 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 : Тези доп. – Хакрів, 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 : Тези доп. – Севастопіль, 2013. – С. 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 : Тези доп. – Севастопіль, 2013. – С. 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 : Тези доп. – Львів, 2013. – С. 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 : Тези доп. – Хакрів, 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 : Тези доп. – Львів, 2014. – С. 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 : Тези доп. – Хакрів, 2014. – С. 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 : Тези доп. – Хакрів, 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 : Тези доп. – Хакрів, 2015. – С. 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 : Тези доп. – Львів, 2016. – С. 537-539.
22. Пат. 107617 Україн, 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.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ ТА ТЕРМІНІВ

CEF – Cisco Express Forwarding, технологія «експрес передачі» компанії Cisco.

CVSS – Common Vulnerability Scoring System, Стандарт оцінки вразливостей.

DoS – Denial of Service, атака типу відмова в обслуговуванні.

EIGRP – Enhanced Interior Gateway Routing Protocol, удосконалений прокол маршрутизації внутрішнього шлюзу.

IGP – Interior Gateway Protocol, протокол внутрішнього шлюзу.

IPv4 – Internet Protocol version 4, Інтернет протокол версії 4.

IPv6 – Internet Protocol version 6, Інтернет протокол версії 6.

MAC – Media Access Control, адреса управління доступом до мережі.

NIST – National Institute of Standards and Technologies, національний інститут стандартів та технологій.

OSPF – Open Shortest Path First, протокол динамічної маршрутизації з відстежуванням стану КЗ «найкоротший відкритий шлях першим».

QoS – Quality of Service, якості обслуговування.

RIP – Routing Information Protocol, протокол маршрутної інформації.

SFTP – Secure Shell File Transport Protocol, протоколу передачі файлів через безпечний протокол доступу до командної строки

SNMP – Simple Network Management Protocol, простий протокол керування мережею.

ГЕМ – глобальна ефективність мережі.

ДМ – динамічна маршрутизація.

ПДМ – протокол динамічної маршрутизації.

ЕММ – ефективність маршрутизатора мережі.

ІБ – інформаційна безпека.

ЙСД – ймовірність своєчасної доставки.

КЗ – канал зв’язку.

ПЗ – програмне забезпечення.

ПРЗД – пропускна здатність каналу зв’язку.

ПП – поток пакетів.

РНД – ризик несвоєчасної доставки.

РС – рухоме середнє.

СКВ – середнє квадратичне відхилення.

ТКМ – телекомунікаційна мережа.

ЦПМ – центральний процесор маршрутизатора.

ВВЕДЕННЯ

Актуальність теми. Однією з найважливіших задач сучасних ТКМ є маршрутизація 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 [1-3, 59]; протоколи динамічної маршрутизації (ДМ), як міждоменного, так і внутрішнього шлюзу, в безпроводових та проводових мережах [4-11]; програмне забезпечення маршрутизаторів (наприклад компанії Cisco [12, 13]), є вразливими та їх компрометація може призвести до порушення ІБ транзитного ПП.

Узагальнення основних закономірностей, виявлених при аналізі дослідницьких робот за темою роботи, дозволяє зробити висновок, що більше уваги приділяється безпроводовим ТКМ [14, 15, 18-21, 25-34, 37, 41] та меншу кількість робот можна віднести до проводових ТКМ [16-18, 22-24, 38-43]. При цьому в деяких роботах наведено лише механізми захисту для самого процесу роботи ПДМ, і в них не враховуються атаки на саму мережу та інші протоколи [19, 28, 39-43]. Виходячи з цього, механізми безпеки транзитного ПП при використанні ПДМ внутрішнього шлюзу у проводових мережах наведено лише в роботах [16-18, 22-24], але в них відсутня інформація про те, як саме автори пропонують розраховувати рівні загроз, вразливостей та ризиків порушення ІБ ПП.

В результаті аналізу джерел літератури можна зробити висновок, що малодослідженою областю є забезпечення ІБ транзитного ПП в ТКМ при використанні ПДМ, що працюють в проводових мережах в рамках однієї автономної системи і відносяться до протоколів маршрутизації IGP, таких як: RIP, OSPF та 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 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 ІБ ПП в процесі його динамічної маршрутизації в ТКМ із застосуванням протоколів IGP.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- 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 шляху 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 і достовірність наукових положень, висновків і рекомендацій. 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. Запропоновані в роботі математичні методи розрахунку РІБ і його врахування як одного з критеріїв вибору оптимального шляху передачі ПП в ТКМ при використанні ПДМ, дозволили виявити і запропонувати нові практичні рішення для збільшення ІБ ПП в ТКМ.

За результатами аналізу в заданій ТКМ в умовах роботи 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%; 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%; протоколу EIGRP – зростання захищеності ПП на 13% при зменшенні ЙСД ПП на 9%, та зростання ЙСД ПП на 15% при зменшенні захищеності на 14%. Також на основі кількісного аналізу удосконалених моделей виявлено, що моделі коректно працюють в ТКМ, в яких усі КЗ мають однакову

ПРЗД. При цьому в ТКМ, в яких існують КЗ з різною ПРЗД використання удосконалених моделей може призвести до маршрутизації ПП по шляхам з достатньою ПРЗД, але з більшим значенням РІБ.

Всі отримані результати можуть бути використані при проектуванні ТКМ.

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 (рис. А.1).
- в навчальному процесі кафедри інфокомунікаційної інженерії Харківського національного університету радіоелектроніки (ХНУРЕ) в дисципліні «Безпека інформації в інформаційно-комунікаційних системах» (рис. А.2).
- при розробці системи мережевого обміну Пристрою радіомоніторингу КХ діапазон Р-677 УИДЯ.466948.006 на Державному підприємстві «Центральне конструкторське бюро «Протон» (рис. А.3, рис. А.4).

Особистий внесок здобувача.

Основні наукові результати, наведені в дисертації та авторефераті, викладені в публікаціях [46-67]. У роботах, опублікованих у співавторстві, автору дисертаційної роботи належить:

- В статті [46] запропоновано метод, який дозволяє врахувати показник РІБ в процесі динамічної маршрутизації. Удосконалення моделі пошуку оптимального шляху передачі ПП в заданій ТКМ на основі алгоритму протоколу RIP з урахуванням РІБ.
- В роботі [55] запропоновано напівмарковська модель процесу передачі ПП в ТКМ, яка дозволяє представити динаміку процесу в умовах

інформаційних атак з урахуванням його ймовірнісно-часових характеристик.

- В роботі [57] запропоновано метод, який дозволяє розрахувати ризик ІБ мережевого маршрутизатора на підставі метрик стандарту NIST CVSS v2.
- В статті [59] проаналізовано існуючі вразливості стека протоколів IPv6.
- В статті [60] проведено аналіз методів захисту від загроз шляхом впровадження механізмів безпеки, покликаних збільшити ІБ для стека протоколів IPv6.
- В роботі [63] апропоновано метод, який дозволяє запобігти перевантаженню одного з КЗ при використанні стандартного методу балансуванню навантаження по шляхах нерівнозначної вартості протоколу EIGRP.
- В статті [64] запропоновано метод врахування РІБ в формулі розрахунку метрики ПДМ EIGRP, який дозволяє динамічно вибирати найбільш безпечний шлях передачі ПП, при цьому враховуючи стандартні показники метрики протоколу EIGRP.
- В роботі [67] отримано патент на корисну модель маршрутизації трафіку за допомогою протоколу EIGRP з урахуванням вимог ІБ, наукова новизна результатів якого полягає у врахуванні РІБ шляху в формулі розрахунку метрики протоколу EIGRP, що дозволяє вибирати шлях передачі ПП в ТКМ за критерієм «якість-безпека».

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 (Хакрів, 2015); 12th International Conference on Experience of Designing and Application of CAD Systems in Microelectronics (Ukraine, Polyana-Svalyava, 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. [47-54, 56, 58, 61-62].

Публікації. Основні положення відображені в 8-ми статтях, 7 з яких опубліковано у фахових наукових виданнях України [46, 55, 57, 59, 60, 63, 66, 67], одна опублікована в іноземному виданні [64], також отримано один патент на корисну модель [67]. Апробація результатів дисертації проходила в ході тринадцятьох доповідей на міжнародних науково-технічних конференціях [47-54, 56, 58, 61-62], з яких шість [51-53, 58, 62, 65] 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.

РОЗДІЛ 1
АНАЛІЗ ВЗАЄМОЗВ‘ЯЗКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

За останнє десятиріччя розвиток мережевих та інформаційних технологій дозволи покращити якість сервісу, понизити вартість послуг, що сприятливо позначається на задоволенні потреб користувачів. Однак разом із настільки бурхливим розвитком технологій виникає все більше потреб в автоматизації процесів, так як зростає кількість задіяних пристроїв, якими потрібно управляти. Такий висновок можна зробити виходячи зі збільшення обороту грошових коштів в телекомунікаційній сфері [44], що свідчить про збільшення закупок мережевого обладнання. Також збільшення кількості активних пристроїв можна підтвердити, проаналізувавши статистику, що вказує на наближення концепції Інтернету речей [45].

Дана робота присвячена питанням безпеки ПП в процесі його ПП в ТКМ. ПДМ дозволяють, шляхом обміну службовими повідомленнями оновлень між маршрутизаторами мережі, обирати оптимальний шлях передачі ПП. Удосконалення ПДМ є актуальною темою наукових досліджень, в тому числі і в області забезпеченні ІБ даних в процесі маршрутизації, що підтверджується десятками наукових публікацій за даною темою досліджень [4-7, 14-43, 46, 47, 50-56, 62-64, 67].

В даному розділі наводиться аналіз загроз, вразливостей та механізмів захисту процесів маршрутизації в телекомунікаційних мережах, що дозволяє підтвердити актуальність теми дослідження та постановити наукову задачу.

1.1. Обґрунтування актуальності

Протоколи мережевої маршрутизації вразливі до атак, які можуть призвести до порушення цілісності, доступності, а також конфіденційності потоку пакетів, що передається в мережі. Наприклад, вразливими можна вважати: протоколи IPv4 та IPv6 [1-3], протоколи маршрутизації в безпроводових мережах [4-6], протоколи маршрутизації в проводових мережах [7, 8], протоколи міждоменної маршрутизації [9-11]. Також вразливості присутні і в ПЗ самих маршрутизаторів, що може призвести до їх компрометації чи виходу з ладу та викликати порушення інформаційної безпеки ПП, що передається в мережі. Наприклад, в продуктах компанії Cisco з 1999 по 2017 роки знайдено більше 2900 вразливостей [12], деякі з них стосуються безпосередньо обладнання маршрутизації [13].

Велика кількість вразливостей протоколів маршрутизації в сучасних ТКМ призвела до активізації дослідницьких робот в цьому напрямі, в яких пропонуються різноманітні підходи до вирішення задачі підвищення інформаційної безпеки ПП в процесі маршрутизації.

Так в роботах [14, 37] представлені сучасні ПДМ в безпроводових мережах, а також проблеми пов‘язані з інформаційною безпекою в даних мережах. Розглядаються майбутні тренди та сучасні відкриті наукові досліди щодо безпечної маршрутизації в безпроводових мережах. В [41] проаналізовано основні атаки на протоколи маршрутизації в проводових та безпроводових мережах, а також представлені механізми захисту, які можна впровадити для збільшення захищеності динамічних протоколів маршрутизації від наведених атак.

В деяких роботах в якості механізму захисту пропонується передавати повідомлення між користувачами мережі по різним шляхам, розділивши його на декілька частин. Так, наприклад в роботах [15, 16] пропонується новий спосіб багатошляхової маршрутизації з метою передачі повідомлення різними шляхами мережі, в якій організація процесу знаходження багатьох шляхів виконується за допомогою модифікованого алгоритму Дейкстри, а розбиття повідомлень виконується на основі порогової схеми Шаміра. У [17] запропоновано потокову

модель багатошляхової маршрутизації та вдосконалену модель розподілу фрагментів за шляхами, що не перетинаються, а в роботах [23, 24] потокову модель за шляхами, що перетинаються за вузлами, в ТКМ; у першому випадку модель може надавати вирішення не оптимальне за якістю обслуговування, а в другому – за безпекою ПП; в цілому модель забезпечує відмовостійкість та безпеку, з одного боку, та якість обслуговування з іншого. В роботі [18] запропоновано алгоритм розділення та зборки секретного повідомлення для багатошляхової маршрутизації в мобільних мережах, в якому розбиття повідомлення виконується на основі використання періодичної функції типу $y = \mathbf{cos}(x)$ та рівняння «хвилі». Для збалансування кількості фрагментів повідомлення, що передаються за шляхами, що не перетинаються у роботі [22] запропоновано модифікований безпечний протокол для надійної доставки даних (Secure Protocol for REliable dAta Delivery, SPREAD), що дозволило передавати найменшу кількість фрагментів по шляхам з найбільшою ймовірністю їх компрометації, а по шляхам з найменшою ймовірністю компрометації передавати найбільшу кількість фрагментів.

Також багато досліджень проводиться для протоколів маршрутизації в безпроводових мережах. Так в роботі [19] представлено модифікований більш ефективний безпечний ПДМ для безпроводових ad-hoc мереж (Ad hoc On-Demand Distance Vector, AODV), що надає вищий рівень безпеки та ефективності роботи мережі, за рахунок зменшення перевантажень та затримок, ніж його існуючий аналог. У [20] запропоновано модифікований протокол маршрутизації в ad-hoc мережах, який враховує співвідношення сигнал-шум (ССШ) для виконання кластеризації вузлів, що дозволяє групувати вузли в кластери та обрати головний вузол та другорядні вузли на основі ССШ, та в якому безпека ПП досягається шляхом ізоляції шкідливих вузлів на основі аналізу шаблону маршрутизації. В [21] пропонується новий алгоритм безпечної ПП в безпроводових мережах (Cross layer secure and resource-aware on demand routing, CSROR), який вибирає оптимальний шлях на основі його безпечності для передачі даних, а також враховує різні міжшарові параметри. В роботі [25] запропоновано спосіб організації,

багатошляхової безпечної маршрутизації в безпроводовій мережі MPLS, що дозволяє збільшити швидкість обробки інформації та захищеність ПП. В [26] запропонований спосіб підвищення безпеки маршрутизації в безпроводових мережах за допомогою теорії ігор, який дозволяє на 15-20% підвищити безпеку передачі інформації та забезпечити більш рівномірну загрузку системи передачі даних. У [27] запропоновано використання протоколу маршрутизації за вимогою на основі довіри (Trust Based Secure on Demand Routing Protocol, TSDRP), який гарантує, що пакети не будуть передаватися через зловмисні вузли, також, порівняно зі стандартним протоколом AODV, зросла кількість пакетів доставлених до кінцевих вузлів, зменшилась затримка передачі пакетів та ПРЗД залишилась на тому ж рівні. У роботі [28] розглядаються вразливості найбільш поширених протоколів безпечної маршрутизації в безпроводових сітчастих мережах (mesh network, MN) та пропонується новий протокол безпечної безпроводової сітчастої мережі (Secure Wireless Mesh Protocol, SWMP), який вирішує недоліки існуючих протоколів. В роботі [29] розглянуто атаки на протоколи маршрутизації на основі довіри і запропоновано метод розрахунку довіри для протидії даним атакам; представлено удосконалений алгоритм маршрутизації, який враховує метрики довіри та якості обслуговування, який, за результатами симуляції, діє краще, ніж існуючі аналоги у мережах з щільною кількістю вузлів. У [30] пропонується новий протокол встановлення стабільних та надійних шляхів (Establishing Stable and Reliable Routes, E-STAR) у гетерогенних багатоскачкових безпроводових мережах, при цьому аналітичні результати дослідження показали, що запропонований протокол може підвищити швидкість доставки пакетів за рахунок встановлення стабільних шляхів. Новий багатошляховий протокол маршрутизації з балансуванням навантаження для безпроводових сітчастих мереж представлено у роботі [31], в якому реалізовані механізми захисту від перенавантаження та безпечної доставки ПП декількома шляхами. В [32] пропонується підхід до безпечної маршрутизації в безпроводових сітчастих мережах, який дозволяє захиститись від багатьох атак на систему маршрутизації при цьому зберігаючи енергетичну ефективність вузлів мережі. У роботі [33] представлено алгоритм

безпечної передачі пакетів в безпроводовій мережі, який дозволяє виключити з процесу маршрутизації зловмисні вузли. В [34] представлено алгоритм маршрутизації ПП в безпроводовій мережі, який дозволяє підвищити безпечність передачі пакетів та зменшити споживання енергії вузлами мережі.

Також є окремі дослідження для протоколів маршрутизації в проводових мережах. Наприклад, в роботах [35, 36] запропоновано протокол безпечної маршрутизації на основі динамічної Байесової сигнальної гри та теорії ігор для аналізу профілів нормального та зловмисного вузлів, а для вирішення проблеми недостатньої інформації авторами запропоновано використання вчиненої Байесової рівноваги для удосконалення процесу сигнальної гри. З результатів аналізу досліджень механізмів захисту для таких протоколів маршрутизації як RIPv2, OSPF, EIGRP [38], можна зробити висновок, що більшість механізмів безпеки, яка пропонується для захисту інформації в мережі не пов‘язані напряму з протоколами маршрутизації, а також в деяких роботах пропонуються застарілі підходи до забезпечення інформаційної безпеки. У роботі [39] аналізуються атаки помилкової суміжності та замаскованого повідомлення оновлення для протоколу OSPF, а також запропоновані механізми захисту від даних атак. В [40] пропонується використання алгоритму Діффі-Геллмана та шифрування інформації, конвертованої у зображення, за допомогою симетричного ключа для забезпечення автентифікації та цілісності для протоколу OSPF, що дозволяє зменшити накладні витрати та збільшити надійність у порівнянні з існуючими методами. Результати досліджень в [42] дозволили збільшити захищеність пакетів оновлень від підміни та збільшити надійність передачі даних в мережі шляхом впровадження додаткової ролі маршрутизатора-аналізатора, який повинен перевіряти усі пакети оновлень протоколу OSPF та проводити додаткові перевірки: чи дійсно існує заявлений шлях, та чи дійсно метрика шляху є кращою за метрики вже існуючих шляхів. Підхід наведений у [43] дозволяє виявляти активні атаки на ПДМ з відстежуванням стану КЗ «найкоротший відкритий шлях першим» (Open Shortest Path First, OSPF) та протокол маршрутної інформації (Routing Information Protocol, RIP) авторами пропонується виявляти атаки на ПДМ за допомогою ханіпота (HoneyPoT, HPT),

задача якого полягає у відправленні маршрутизаторам мережі пакети-запроси окремих протоколів маршрутизації та аналізувати відповіді від них, визначаючи таким чином, чи не був скомпрометований той чи інший маршрутизатор.

Узагальнення основних закономірностей, виявлених при аналізі наведених дослідницьких робот, дозволяє зробити наступні висновки [14-43]:

a. В роботах пропонуються декілька способів підвищення рівня ІБ ПП, що передається в мережі:
   i. Розділення одного повідомлення на декілька фрагментів та їх передача по різних маршрутах в мережі з наступною зборкою на кінцевому вузді або приграничному маршрутизаторі [16-18, 22-25];
   ii. Врахування різних параметрів, наприклад: надійності, безпеки, довіри вузлам мережі, QoS при виборі шляхів передачі ПП за рахунок модифікації існуючих ПДМ, або шляхом пропонування нових протоколів [15, 19, 20, 21, 26-36, 39-42].
b. Деякі роботи направлені виключно на підвищення надійності та доступності передачі ПП в мережі [21, 27, 30-32, 34-36].
c. Ряд робот направлений виключно на захист процесу роботи самих ПДМ, при цьому в них не враховуються атаки на саму мережу та інші протоколи, які приймають участь в процесі маршрутизації [19, 28, 39-43].
d. В роботах [15-18, 22-24] відсутня інформація про те, як саму автори пропонують розраховувати рівні загроз, вразливостей та ризики порушення ІБ ПП.
e. Більшість робот направлено на дослідження безпечної передачі даних в безпроводових мережах [14, 15, 18-21, 25-34, 37, 41] та меншу кількість робот можна віднести до проводових мереж [16-18, 22-24, 38-43].

Виходячи з пункту e) менша кількість робот присвячена дослідженням безпеки передачі ПП в проводових ТКМ [16-18, 22-24, 38-43]. При цьому, виходячи з пункту c), в деяких роботах наведено лише механізми захисту для самого процесу роботи ПДМ, і в них не враховуються атаки на саму мережу та інші протоколи [19, 28, 39-43]. Виходячи з цього, механізми безпеки транзитного ПП при використанні

ПДМ внутрішнього шлюзу у проводових мережах наведено лише в роботах [16-18, 22-24], але в них, виходячи з пункту d), відсутня інформація про те, як саме автори пропонують розраховувати рівні загроз, вразливостей та ризиків порушення інформаційної безпеки ПП.

До IGP в проводових мережах відносяться такі ПДМ як: RIPv2 [68], протокол маршрутної інформації наступного покоління (Routing Infromation Protocol Next Generation, RIP-ng) [69], OSPFv2 [70], OSPFv3 [71] та EIGRP [72]. Дослідження щодо забезпечення інформаційної безпеки саме для цих протоколів пропонується в якості постановки науково-практичної задачі в даній роботі.

Перш ніж перейти до аналізу методів інформаційної безпеки в протоколах динамічної маршрутизації необхідно розглянути вразливості та механізми захисту процесів маршрутизації в сучасних ТКМ.

1.2. Аналіз сучасних методів порушення процесу маршрутизації та інформаційної безпеки транзитного ПП

Відповідно до Указу Президента України про положення про технічних захист інформації в Україні та Закону Верховної Ради України про захист інформації в інформаційно-телекомунікаційних системах, далі в роботі будуть використовуватися наступні терміни [75-76]:

- конфіденційність – властивість інформації бути захищеною від несанкціонованого ознайомлення;
- цілісність – властивість інформації бути захищеною від несанкціонованого спотворення, руйнування, знищення;
- доступність – властивість інформації бути захищеною від несанкціонованого блокування;
- блокування інформації – дії, в результаті яких доступ до інформації стає неможливим;

- витік інформації – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, які не мають права доступу до неї;
- порушення цілісності інформації – несанкціоновані дії по відношенню до інформації, внаслідок яких змінюється її зміст.

Під атаками на блокування інформації розуміються DoS атаки чи розподіленої атаки відмови в обслуговуванні (Distributed Denial of Service, DDoS), або ж атаки, що викликають неприйнятне зниження працездатності мережевих вузлів (тобто таке, яке знижую параметри QoS нижче ніж встановлено вимогами в заданій ТКМ), шляхом вичерпання таких ресурсів мережевих вузлів як: процесорний час та завантаженість процесору, об'єм оперативної пам'яті, завантаженість або об'єм постійної пам'яті та ПРЗД КЗ. Під атаками перенаправлення розуміються атаки, які дозволяють направити легітимний ПП на вузол, який контролюється зловмисником, з метою подальшого порушення цілісності, витоку та/або блокування інформації.

Поняття інформаційної безпеки визначається відповідно до проекту концепції інформаційної безпеки України [77].

Для здійснення успішного порушення процесу маршрутизації зловмиснику необхідно створити таку ситуацію, коли:

- в мережі відсутній доступ до шляху передачі ПП між вузлом-відправником i та вузлом-отримувачем j;
- в мережі відсутній такий шлях передачі ПП між вузлом-відправником i та вузлом-отримувачем j, який дозволяв би забезпечити належну якість обслуговування ПП;
- в мережі присутній шлях, який контролюється зловмисником, по якому передається інформація що потребує захисту [76].

Для успішного порушення інформаційної безпеки транзитного ПП в мережі зловмиснику потрібно:

- або успішно здійснити атаку, яка дозволить перехоплювати дані, які передаються між вузлом-відправником i та вузлом-отримувачем j, що може призвести до порушення цілісності, витоку або блокуванню інформації;
- або успішно здійснити атаку, яка дозволить порушити цілісність ПП (наприклад, за допомогою фізичного впливу на середовище передачі ПП), який передається між вузлом-відправником i та вузлом-отримувачем j;
- або ж успішно здійснити атаку типу DoS з метою порушення зв'язності мережі та зниженню швидкодії маршрутизаторів, що призведе до зниження рівня QoS в мережі або повної відсутності можливості доставки ПП між вузлом-відправником i та вузлом-отримувачем j.

Введемо наступні мережеві параметри, на які можуть впливати різного роду інформаційні атаки:

- λ – ПП, що поступає до мережі або на вхід мережевого вузла;
- μ – інтенсивність обробки пакетів мережевим вузлом;
- t – час передачі пакетів;
- D – затримка, яка викликана обробкою пакетів на проміжних вузлах (маршрутизаторах) мережі та передачею пакетів по фізичному середовищу в лініях зв'язку;
- J – джиттер, проявляється в тому, що послідовність пакетів прибуває до отримувача у нерегулярні моменти часу;
- PL – втрати пакетів;
- EB – ефективна ПРЗД, тобто, ПРЗД в каналі зв'язку без врахування передачі керуючих даних;
- Err – бітові помилки в процесі передачі пакетів;

- SR – критичні ресурси мережевих вузлів, такі як: процесорний час та завантаженість процесору, об'єм оперативної пам'яті, завантаженість або об'єм постійної пам'яті та ПРЗД КЗ.

На кожен з вищенаведених параметрів мережі може здійснюватися небажаний вплив в процесі здійснення атаки на ТКМ. В залежності від типу атаки будуть погіршуватися різні параметри мережі.

Введемо наступні позначення для спрощення запису змін параметрів ТКМ:

- $X\uparrow$ – параметр X зростає;
- $X\downarrow$ – параметр X знижується;
- $\rightarrow$ – знак, що означає перехід від одного параметру до іншого, який викликаний наслідковим зв'язком, наприклад: $X\uparrow\rightarrow Y\downarrow$ – зниження параметру Y, внаслідок підвищення параметру X.

В статті [59] наведено атаки, які здійснюються на протоколи мережевого рівня базової еталонної моделі взаємодії відкритих систем (Open Systems Interconnection, OSI) та можуть бути використані для порушення процесу маршрутизації:

- атака на процес виявлення маршрутизатору в IPv6;
- атака на механізм автоматичного налаштування IPv6 адрес (StateLess Address AutoConfiguration, SLAAC);
- атака на процес виявлення адреси управління доступом до мережі (Media Access Control, MAC) в IPv6;
- атака на процес виявлення дублювання IPv6 адрес;
- впровадження в ТКМ підробленого серверу протоколу динамічної конфігурації хостів (Dynamic Host Configuration Protocol, DHCP);
- маніпуляція оновленнями ПДМ;
- атака на переповнення кеш-пам'яті маршрутизатора;
- здійснення DoS за допомогою протоколу міжмережевих керуючих повідомлень (Internet Control Message Protocol, ICMP);

- наводнення пакетів протоколу IPv6 типу сповіщення маршрутизатора (Router Advertisement, RA);
- здійснення DoS атаки за допомогою криптографічно генерованих адрес (Cryptographically Generated Address, CGA);
- DoS атаки шляхом маніпуляції параметрами максимальної одиниці передачі (Maximum Transmission Unit, MTU);
- DoS атака шляхом зміни полів часу життя (Time To Live, TTL) та поточного ліміту ретрансляції пакету (Current Hop Limit, CHL) для проколів IPv4 та IPv6 відповідно;
- виснаження адрес на DHCP сервері.

В силу тематичної специфіки статті [59] до неї включено не всі атаки, тому нижче перераховані ще декілька атак, які можуть вплинути на процес маршрутизації ПП:

- Атаки шляхом наводнення пакетів – реалізуються за рахунок відправки в мережу великої кількості пакетів, частіше за все малого розміру. Це призводить до значних витрат ресурсів вузлів мережі, в тому числі і маршрутизаторів.
- Атаки на переповнення буферу – реалізуються шляхом експлуатації вразливостей в ПЗ маршрутизаторів за рахунок переповнення стеку або кучі, що викликає DoS атаку окремої мережевої служби чи вузла в цілому.
- Атаки можливі шляхом проникнення на мережевий вузол з правами адміністратора – реалізуються шляхом перехоплення сесії протоколу реалізації текстового терміналу (TErminaL NETwork, TELNET), підбору строки доступу з правами на читання та запис для простого протоколу керування мережею (Simple Network Management Protocol, SNMP), чи шляхом злому пароля адміністратору вузла (про техніки та різноманітні методи підбору паролів написано в статті [66]). Також можливо отримати доступ до консолі управління вузлом шляхом експлуатації його вразливостей, як наведено в атаках на переповнення буферу, але при цьому викликаючи не DoS атаку, а повернення консолі управління після чого

може потребуватися етап підвищення привілеїв користувача для отримання адміністративних прав.

- Порушення фізичного середовища передачі ПП – реалізується шляхом фізичного впливу на лінії зв'язку за допомогою перерізання кабелів або електромагнітних перешкод.

В табл. Б.1 представлені атаки та їх належність до певного типу атак (на доступність вузлів, чи перенаправлення ПП).

Далі необхідно визначити, які наслідки можуть виникнути в разі реалізації зловмисником тієї чи іншої атаки.

У випадку виникнення атаки, яка викликає перенаправлення ПП, зловмисник може (згідно табл. Б.1: № 1, 2, 3, 5, 6):

- порушити цілісність ПП, що передається в мережі, тоді $Err \uparrow \rightarrow PL \uparrow \rightarrow t = \infty$;
- або реалізувати DoS атаку шляхом відкидання пакетів, тоді $t = \infty$;
- або перехоплювати та копіювати дані, а потім відправляти їх в незмінному стані вузлу-отримувачу, тоді $D \uparrow$ та $J \uparrow$.

У випадку виникнення атаки на порушення доступності зловмисник може:

- збільшити споживання ресурсів вузла шляхом реалізації повільної DoS атаки, тоді $SR \uparrow \rightarrow D \uparrow$ та $SR \uparrow \rightarrow \mu \downarrow$ (згідно табл. Б.1: № 10, 11);
- збільшити споживання ресурсів вузлом шляхом реалізації атаки наводнення пакетами, тоді $\lambda \uparrow \rightarrow SR \uparrow \rightarrow D \uparrow$ та $\lambda \uparrow \rightarrow SR \uparrow \rightarrow \mu \downarrow$ (згідно табл. Б.1: № 8, 14);
- реалізувати DoS атаку на вузол-отримувач, тоді $t = \infty$ (згідно табл. Б.1: № 4, 12, 13, 15);
- реалізувати DoS атаку на маршрутизатор(-и) мережі, тоді, у разі відсутності запасного шляху $t = \infty$, а в разі, якщо запасний шлях є, то можливо $D \uparrow$ (згідно табл. Б.1: № 7, 8, 9, 10, 14, 15);
- знизити ефективність передачі даних, тоді $EB \downarrow$ (згідно табл. Б.1: № 11);

- порушити середовище передачі ПП, тоді $t = \infty$ (згідно табл. Б.1: № 17).

Згідно табл. Б.1 атака №16 є універсальною. Так, у випадку, коли зловмисник отримав можливість керувати налаштуваннями маршрутизатору, він може, як відключити мережеві служби, викликавши тим самим DoS атаку, або ж перенаправити ПП на необхідний йому вузол-отримувача чи по потрібному йому шляху передачі в ТКМ.

Далі наводиться аналіз методів забезпечення ІБ сучасних ТКМ з метою виявлення їх недоліків та визначення шляхів їх повного або часткового усунення за допомогою удосконалення моделей та методів ПДМ, що досліджуються в даній роботі.

1.3. Аналіз методів забезпечення інформаційної безпеки в сучасних телекомунікаційних мережах

Для забезпечення ІБ та захисту від наведених атак на процес маршрутизації в ТКМ необхідно застосовувати комплексні заходи безпеки, такі як:

- Налаштування механізмів захисту на кінцевих вузлах:
  - налаштувати автоматичне оновлення ПЗ;
  - встановити на кінцевих вузлах системи виявлення/запобігання вторгнень (Host Intrusion Detection/Prevention System, HIDPS) [78, 79];
  - встановити антивірус;
  - встановити брандмауер.
- Налаштування механізмів безпеки на комутаторах [80, 81]:
  - налаштувати віртуальні локальні мережі (Virtual Local Area Network, VLAN);
  - налаштувати функції фільтрації MAC-адрес та захисту портів;
  - налаштувати інспекцію протоколу знаходження MAC-адреси (Address Resolution Protocol, ARP);

- налаштувати механізм удосконалення валідації адреси відправника (Source Address Validation Improvement);
- налаштувати механізм відстежування IPv6 адрес, та механізм захисту адреси відправника і префіксу для протокола IPv6;
- налаштувати механізм контролю шторму;
- увімкнути та перевірити коректність налаштувань протоколу остового дерева (Spanning Tree Protocol, STP).

- Налаштування механізмів безпеки на маршрутизаторах [60, 82, 83]:
  - налаштувати механізм захисту відправника IP адреси;
  - налаштувати листи доступу для протоколів IPv4/IPv6;
  - налаштувати безпечний протокол виявлення сусідів (Secure Neighbor Discovery, SEND);
  - налаштувати механізм захисту адрес доставки для IPv6;
  - налаштувати автентифікацію для динамічних протоколів маршрутизації.
- Впровадження протоколів безпечної передачі інформації:
  - на внутрішніх сервісах (внутрішньо корпоративних) використовувати протоколи безпечної передачі інформації, таких як: SNMP версії 3, захищений протокол передачі гіпертексту (HyperText Transfer Protocol Secure, HTTPS), безпечний протокол передачі файлів (File Trasfer Protocol Secure, FTPS), протокол безпечного копіювання (Secure CoPy, SCP), захищений протокол доступу до командної строки (Secure Shell, SSH).
  - налаштувати безпечний обмін внутрішньо корпоративною інформацією, що проходить через глобальну мережу, з використанням протоколів безпечного тунелювання: протокол захисту Інтернет протоколу (Internet Protocol security, IPsec), протокол тунелювання точка-точка (Point-to-Point Tunneling Protocol, PPTP) або інші протоколи створення захищеннях віртуальних приватних мереж (Virtual Private Network, VPN).

- Використання систем виявлення/запобігання вторгнень (Intrusion Detection/Prevention System, IDPS) [78, 79]:
    - встановити та налаштувати IDPS систему в відповідно до вимог інформаційної безпеки компанії.
- Забезпечення фізичної безпеки мережевих вузлів:
    - встановити обладнання в спеціальних серверних шафах;
    - налаштувати систему контролю доступу до серверних шаф;
    - налаштувати систему кондиціювання;
    - налаштувати протипожежну систему;
    - забезпечити резервування ресурсів на випадок стихійного лиха чи форс-мажорних обставин.
- Створення політик ІБ [84-86]:
    - політика оновлень ПЗ;
    - політика проведення аналізу ризиків ІБ;
    - політика проведення аудитів та тестувань ІБ;
    - політика реагування на інциденти ІБ;
    - політика проведення розслідувань наслідків порушення ІБ;
    - політика фізичного доступу до приміщень з підвищеним рівнем доступу;
    - політика управління змінами;
    - політика налаштування механізмів ІБ (особливо в мережевої безпеки);
    - додаткові політики.

Механізми безпеки, що наведено віще, дозволяють налаштувати мінімально прийнятний рівень ІБ в ТКМ. Кожен з механізмів безпеки має свої особливості та повинен застосовуватися тільки у випадку необхідності.

В деяких випадках механізми безпеки самі по собі можуть призвести до можливої реалізації атаки. Багато з механізмів фільтрації, які покликані відмежувати небажаний ПП та контролювати доступ в мережу, потребують додаткових ресурсів вузлу, на якому вони налаштовані. Ресурсномісткі механізми

можуть призвести до вичерпання ресурсів фільтруючого вузлу, тоді $SR\uparrow \to D\uparrow$ та можливо $SR\uparrow \to J\uparrow$, або до DoS атаки, тоді $SR\uparrow \to t=\infty$. Одним з прикладів атаки на механізми захисту може послугувати атака наводнення пакетами CGA.

В даній роботі передбачається, що більшості атак порушення конфіденційності та цілісності інформації може уникнути шляхом використання сучасних криптографічних протоколів передачі інформації, наприклад: IPsec, PPTP, HTTPS, SSH і т.п. Однак, криптографічні протоколи захищають лише смислову складову даних ПП, але не факт їхньої передачі, хоча, наприклад, в військовій сфері, розголошення самого факту передачі інформації може стати критично небезпечним. Також криптографічні протоколи не дозволяють запобігти атакам на порушення доступності інформації.

Істотним недоліком перерахованих механізмів забезпечення ІБ може стати також і те, що вони не враховують ризики порушення ІБ. Представлені механізми захисту діють реактивно, відповідаючи на загрози, що виникають, однак не володіють превентивними заходами, які дозволили б попередити виникнення згубних наслідків атаки.

1.4. Аналіз існуючих та можливих методів забезпечення інформаційної безпеки потоку пакетів при використанні протоколів динамічної маршрутизації, що досліджуються в роботі

В основу протоколів RIP, OSPF та EIGRP не покладено жодних механізмів забезпечення інформаційної безпеки транзитного ПП. Такий висновок можна зробити на основі того, що в формулах розрахунку метрик даних протоколів не враховуються які-небудь параметри, що дозволили б вибирати оптимальний шлях передачі ПП в ТКМ за критерієм інформаційної безпеки [68-72]. А також в ході аналізу наведених протоколів виявилося, що єдиним стандартним механізмом забезпечення інформаційної безпеки є автентифікація джерел оновлень [72, 73, 74].

Цей механізм розрахований на захист процесу роботи самого протоколу маршрутизації і захищає лише від атаки №6 наведеної в табл. Б.1.

Є декілька методів підвищення інформаційної безпеки транзитного ПП при використанні ПДМ:

- криптографічними методами встановити довіру між вузлами, щоб унеможливити впровадження маршрутизуючого вузла (МВ) в мережу, до якого не має довіри, при цьому підвищується захищеність самого процесу роботи протоколу маршрутизації, але не враховуються ризики неавторизованого заволодіння різними МВ мережі, пасивного прослуховування, можливого виводу МВ з ладу;

- методи передачі розділеного на частини повідомлення декількома шляхами, при цьому підвищуються конфіденційність та цілісність ПП, але такий підхід може призвести до передачі частини ПП по не ефективним шляхам;

- методи розрахунку довіри між вузлами на основі таких параметрів як: кількість ретрансльованих пакетів, часу присутності вузлу в мережі, наданні не точних даних про свій стан і т.п., з метою виключення МВ з низькою довірою з процесу маршрутизації трафіку, при цьому збільшується критерій доступності ПП, але не враховуються ризики неавторизованого заволодіння різними МВ мережі, пасивного прослуховування та перенаправлення ПП по не ефективним шляхам;

- методи розрахунку РІБ можливих шляхів передачі ПП в ТКМ з метою використання РІБ в процесі вибору оптимального шляху(-ів), при цьому, в залежності від обраних параметрів для розрахунку РІБ шляху, можливо підвищити критерії конфіденційності, цілісності та доступності ПП, але при цьому існує ризик переді ПП по не ефективному шляху навіть при відсутності реальної атаки, що може зменшити якість обслуговування (Quality of Service, QoS).

Реалізація першого методу потребує третьої довіреної сторони, або ручного розподілу асиметричних ключів між МВ. Для другого методу потрібно модифікувати процес вибору оптимальних шляхів передачі фрагментів повідомлення таким чином, щоб, з однієї сторони, фрагменти одного і того ж повідомлення не передавались по одному і тому самому шляху, та враховувати погіршення QoS з іншої. Для третього методу необхідно враховувати метрику

довіри, або як параметр стандартної метрики для протоколу маршрутизації, що використовується, або як окремого від метрики критерію вибору оптимального шляху. Для четвертого методу РІБ може враховуватися при визначенні оптимального шляху передачі так само, як і для третього методу.

Виходячи з висновку підрозділу 1.1 в сучасних дослідженнях не наводиться моделей та методів, щодо розрахунку РІБ для транзитного ПП в ТКМ та його використання в ПДМ у процесі вибору оптимального шляху передачі. Саме тому цей метод може бути вибраний для постановки науково-прикладної задачі.

Обраний метод має низку проблем, серед яких можна виділити наступні:

- невідомо на основі яких параметрів розраховувати ризики порушення конфіденційності, цілісності та доступності ПП, що передається в ТКМ за вибраними шляхами;
- в яких одиницях вимірювати РІБ та в яких межах він повинен лежати;
- невідомо як враховувати РІБ при виборі оптимального шляху таким чином, щоб збільшити критерій безпеки ПП, та при цьому мінімізувати погіршення QoS.

Для того, щоб постановити наукову задачу дослідження необхідно провести аналіз можливих шляхів вирішення наведених проблем та розробити критерії, які будуть використані при розробці моделей та методів вирішення поставленої науково-практичної задачі.

1.5. Аналіз вимог, щодо розрахунку ризику інформаційної безпеки транзитного потоку пакетів та його використання при виборі оптимального шляху передачі

Для вирішення проблем, наведених у підрозділі 1.4, для кожної з них необхідно розробити ряд вимог на основі яких можна оцінювати придатність та адекватність запропонованих моделей та методів їх вирішення.

Для вирішення поставлених проблем спершу встановимо вимоги до РІБ. В даній роботі під РІБ будемо мати на увазі величину ступеню збитків отриманих в

разі реалізації можливих загроз через вразливості об’єкта. Існує два загальних способу розрахунку РІБ: кількісний і якісний [87-89].

Якісний метод оснований на суб’єктивних оцінках експертів, щодо рівня загрози, вразливості та можливих наслідків, на основі яких розраховується величина ризику, що приводить і до суб’єктивної оцінки самого ризику. Саме тому якісні методи оцінки ризиків є неприйнятними для подальшого використання в даній роботі.

Кількісні методи оцінки ризиків оснований на статистичних показниках рівнів загроз, вразливостей та наслідків реалізації загроз, що дає змогу отримати чітке чисельне значення ризику. При цьому РІБ може виражатися в грошовому еквіваленті можливої втрати коштів, чи в довільному числовому еквіваленті, який, частіше за все нормується в межах [0;1]. Так як розрахунок вартості активів тісно пов’язаний з обробкою цієї інформації людиною, а розрахунки вартості нематеріальних активів (репутація, доброчесність, тощо) суб’єктивні за своєю природою, то оцінка РІБ в грошову еквіваленті в даній роботі використовуватися не буде.

Вимоги до РІБ:

- РІБ повинен розраховуватися на основі кількісних методів оцінки ризику;
- РІБ повинен бути нормованим та лежати в межах [0;1].

Виходячи з вимог до РІБ можна навести вимоги до параметрів, на основі яких буде розраховуватися РІБ:

- параметри РІБ мають бути розраховані на основі математично обґрунтованих показників, або за допомогою методології, що мінімізують людський суб’єктивізм;
- параметри РІБ повинні лежати в межах [0;1].

В процесі вибору оптимального шляху передачі РІБ може використовуватися як один з параметрів існуючої формули розрахунку метрики заданого протоколу маршрутизації, чи як окремий параметр. Якщо РІБ враховується в формулі розрахунку метрики, то задачу пошуку оптимального шляху зводиться до однокритеріальної, якщо ж РІБ враховується як окремий параметр – то задача є

багатокритеріальною. Стандартно в ПДМ, що досліджуються в даній роботі, вирішується однокритеріальна задача оптимізації враховуючи метрику як критерій оптимальності. Зважаючи на це і на те, що в задачах багатокритеріальної оптимізації важко знайти абсолютно вірне рішення і кінцевий результат завжди буде компромісним, то в даній роботі пропонується варіант врахування РІБ в формулах розрахунку метрик і звести задачу до однокритеріальної.

Вимогами щодо вибору методу врахування РІБ в формулах розрахунку метрик протоколів RIP, OSPF, EIGRP будемо вважити наступні:

- так як в наведених протоколах найкращий шлях вибирається за мінімальним значенням метрики, то РІБ повинен збільшувати значення метрики шляху;
- РІБ повинен мати достатню вагу, щоб змінити вибір оптимального шляху/шляхів при виборі між двома або більшою кількістю шляхів з однаковою метрикою;
- щоб не змінювати формат та структуру пакетів оновлень заданий протоколів маршрутизації, то значення метрик повинні лежати в межах, що описані в стандартах для відповідних протоколів маршрутизації: для RIP – [1;15], OSPF – [1;16777215), EIGRP – $[1;2^{64})$;
- щоб зберегти критерії QoS, які закладені в протоколах маршрутизації, то в удосконалених формулах розрахунку метрик повинні враховуватися базові параметри, які враховуються і в стандартних формулах метрик відповідних протоколів: для RIP – кількість ретрансляцій пакету, OSPF – пропускні здатності КЗ, EIGRP – ПРЗД, надійність та завантаженість КЗ і затримка пакетів;
- так як РІБ це параметр, що є протилежним QoS, то менший рівень РІБ повинен менше впливати на метрику шляху, ніж великий рівень РІБ;
- РІБ не повинен призводити до того, щоб значення метрики шляху передачі дорівнювало нулю.

На основі наведених критеріїв можна встановити чітку науково-практичну задачу.

1.6. Постановка задачі дослідження

На основі аналізу науково-дослідницьких робот за темою дисертації можна зробити висновок про те, що малодослідженою областю є забезпечення ІБ в процесі маршрутизації для протоколів IGP, таких як: RIP, OSPF та EIGRP. Відсутність врахування ризиків ІБ в даних протоколах не дозволяє вибирати шляхи передачі, які б забезпечували захищеність транзитного ПП від різного роду інформаційних атак.

З аналізу сучасних механізмів мережевої безпеки стало відомо, що в них не враховується РІБ, що не дозволяє їм діяти на упередження, щоб попередити виникнення пагубних наслідків атаки. Також стало відомо, що проблеми забезпечення конфіденційності та цілісності інформації вирішуються за мережевих допомогою криптографічних протоколів, але вони не можуть забезпечити доступність інформації. Саме тому розробка механізмів підвищення критерію доступності інформації при її передачі в ТКМ є актуальною задачею.

Керуючись висновками, які наведено вище, та вимоги, які наведено в підрозділі 1.5, можна визначити наступні задачі наукового дослідження:

- проведення досліджень з метою визначення ступеню впливу атак на доступність ПП при його передачі в ТКМ;
- вибір параметрів оцінки РІБ;
- розробка методів оцінки РІБ ПП в процесі маршрутизації в ТКМ;
- наведення рекомендацій щодо застосування РІБ при виборі оптимального шляху передачі ПП в ТКМ;
- розробка методів та моделей щодо врахування РІБ в формулах розрахунку метрик ПДМ, таких як: RIP, OSPF, EIGRP.
- проведення імітаційного моделювання стандартних та удосконалених методів і моделей вибору оптимального шляху передачі ПП в ТКМ з метою проведення порівняльного аналізу.

В якості науково-практичної задачі постановити наступну: підвищення ІБ ПП в процесі його ДМ в ТКМ шляхом урахування ризиків порушення

конфіденційності, цілісності та доступності транзитних даних як додаткових критеріїв вибору оптимального шляху передачі.

1.7. Висновки по першому розділу

1. В результаті аналізу науково-дослідницьких робот за темою дисертації можна зробити висновок, що малодослідженою областю є забезпечення ІБ транзитного ПП в ТКМ при використанні ПДМ, що працюють в проводових мережах в рамках однієї автономної системи і відносяться до протоколів IGP, таких як: RIP, OSPF та EIGRP.
2. Стандартні механізми мережевого захисту в сучасних ТКМ не мають превентивних заходів безпеки, щоб попередити виникнення загрози та реагують за фактом реалізації атаки.
3. Проблеми забезпечення конфіденційності та цілісності інформації, що передається в ТКМ вирішуються за рахунок використання криптографічних протоколів. Але дані протоколи не можуть забезпечити доступність інформації.
4. В стандартних формулах розрахунку метрик для ПДМ, що досліджуються в роботі, не враховуються параметри, що відповідають за ІБ.
5. Єдиним стандартизованим механізмом безпеки в ПДМ, що досліджуються в роботі, є автентифікація джерел оновлень.
6. Розроблені вимоги, щодо РІБ, його параметрів та методу врахування в метриках ПДМ.
7. 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.

РОЗДІЛ 2
ОЦІНКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ МАРШРУТИЗАЦІЇ ПОТОКУ ПАКЕТІВ

Виходячи з визначення РІБ – величина ступеню збитків отриманих в разі реалізації можливих загроз через вразливості об’єкта, наданого в першому розділі роботи, наведемо загальну формулу його розрахунку:

$$R = T_v \cdot I ,$$

де T_v – ймовірність реалізації загрози T через задану вразливість v;

I – збиток.

Збиток може розраховуватися у грошовому еквіваленті, в довільній шкалі рівнів, чи в процентному співвідношенні. При цьому можливий рівень збитку може залежати від наступних параметрів: критичності активу, на який направлена загроза, кількості активів, які постраждають у разі успішної реалізації загрози, ступеню порушення конфіденційності, цілісності чи доступності досліджуваного об’єкту. Для позбавлення суб’єктивності при розрахунках збитків в даній роботі пропонується використовувати лише дані та інформацію, які можна отримати з самого досліджуваного об’єкту чи системи. Наприклад, якщо об’єктом дослідження є ТКМ, то можна використовувати наступні дані: параметри мережі, характеристики ПП, що в ній передаються, вразливості вузлів мережі, налаштування систем та протоколів на вузлах мережі, та інші.

В свою чергу ймовірність реалізація загрози може розраховуватися в залежності від декількох параметрів, наприклад: наявності чи відсутності механізмів захисту та їхньої ефективності, мотивованності нападника, вірогідності знаходження підходящої вразливості, частоті поява заданої загрози в середовищах, що подібні досліджуваному. Для того, щоб запобігти суб’єктивності розрахунків

приймемо обмеження, яке полягає в тому, що в разі існування вразливості в системі вона однозначно буде використана для реалізації загрози, тобто $T_v = 1$.

В даному розділі пропонується розраховувати РІБ на основі двох груп параметрів: статичних та динамічних. Статичні параметри змінюються лише при визначених обставинах, наприклад, за таймером чи у випадку зміни в фізичному середовищі ТКМ, в свою чергу, динамічні параметри можуть змінюватися не залежно від визначених тригерів, наприклад, величина вхідного ПП, затримки пакетів, завантаженість вузлів мережі.

Згідно з критеріями вибору параметрів на основі яких може розраховуватися РІБ в якості статичних параметрів в даній роботі пропонується використовувати:

- метрики критичності вразливостей, які розраховуються на основі NIST CVSS v2 [90]. Метрики визначаються для вразливостей, знайдених на маршрутизаторах заданої ТКМ за допомогою автоматизованих сканерів вразливостей. Даний параметр можна вважати статичним, так як він змінюється тільки після пересканування мережі сканером вразливостей, що може відбуватися за таймером або вручну адміністратором.
- ефективність маршрутизаторів мережі. Цей параметр змінюється лише при зміні фізичної топології ТКМ та розраховується на основі ПРЗД і затримки в КЗ.

В якості динамічного параметру пропонується використовувати ЙСД ПП на кінцевий вузол, який залежить від інтенсивності вхідного ПП, інтенсивності обробки ПП маршрутизаторами, кількості маршрутизаторів та завантаженості ЦПМ в заданому шляху передачі.

2.1. Статичні методи оцінки ризику інформаційної безпеки транзитного потоку пакетів для заданого шляху передачі

В даному розділі пропонується використовувати два параметра розрахунку РІБ: параметр критичності вразливостей маршрутизаторів R_{CVSS}, який

розраховується на основі метрик стандарту NIST CVSS v2, а також параметр ефективності маршрутизаторів ТКМ R_θ. На основі цих двох параметрів пропонується розраховувати РІБ для подальшого його використання в процесах ДМ для вибору шляху передачі ПП на основі критерію «QoS-безпека».

Також слід зазначити, що параметр R_{CVSS} дає змогу оцінити ризик порушення конфіденційності, цілісності та доступності транзитного ПП шляхом оцінки критичності вразливостей на маршрутизаторах в заданому шляху передачі, які може використати зловмисник. В свою чергу, параметр R_θ дає змогу знайти ефективність маршрутизаторів в заданому шляху передачі, яка виражається як зменшення ефективності передачі ПП в мережі у разі видалення заданого маршрутизатору та всіх його КЗ з мережі. Збереження найбільш ефективних маршрутизаторів дає змогу мінімізувати втрати ефективності передачі, тим самим забезпечуючи доступність. Таким чином для максимізації критерії конфіденційності та цілісності транзитного ПП будемо використовувати параметр R_{CVSS}, а для максимізації критерію доступності – параметр R_θ. При цьому врахування обох параметрів одночасно може призвести до усереднення результатів, або превалювання одного параметру над іншим. Для вирішення цієї проблеми в даній роботі пропонується використовувати одночасно лише один з параметрів, а якості критерію вибору того, який саме з них враховувати в формулі розрахунку РІБ, використовувати параметр ризику, що відображає можливу наявність DoS атаки на маршрутизатори ТКМ, та розраховується на основі аналізу ентропії транзитного ПП. Якщо параметр ризику можливої наявності DoS атаки перевищує задану величину, то використовується параметр R_θ, в іншому випадку використовується R_{CVSS}.

Перевагою оцінки РІБ на основі статичних параметрів є те, що подібні методі не вимогливі до обчислювальних ресурсів. Недоліком подібного методу є те, що вони не дозволяють враховувати в РІБ параметри ТКМ, які змінюються незалежно від визначених тригерів.

2.1.1. Метод розрахунку параметра критичності вразливостей маршрутизаторів

В якості автоматизованих сканерів вразливостей можуть виступати [91]. Всі вони можуть сканувати вузли ТКМ та знаходити відомі вразливості, перевіряючи їх за власними базами сигнатур. У випадку виявлення поведінки системи, що співпадає з сигнатурою вразливості – сканер сигналізує про це та зберігає знахідку в журналах подій.

Для більшості сигнатур вразливостей, в подібних сканерах, метрики критичності вразливостей, розраховані за стандартом NIST CVSS v2 вже існують та наводяться разом із результатами сканування автоматично. Якщо вразливість нова, то для неї експертами розраховується параметр критичності методом, який вказано в стандарті CVSS. Також для вразливості створюється унікальний опис, присвоюється ім’я та ідентифікатор і всі ці дані публікуються у базі поширених вразливостей (Common Vulnerabilities and Exposures, CVE) [92]. Сканери використовують дану базу для створення сигнатур пошуку нових вразливостей або ж дізнатися параметри існуючих. З цього можна зробити висновок, що параметр критичності буде однаковий для різних сканерів вразливостей, що робить подібну систему оцінки універсальною.

На момент написання даної роботи використовується стандарт NIST CVSS v2.0 [90], однак створено і новий стандарт CVSS версії 3.0 [93-96] на основі якого також розраховують метрики критичності вразливостей та наводять їх разом з метриками розрахованими за CVSS версії 2. Так як метрики CVSS версії 3 розраховані не для всіх вразливостей, то, на момент написання роботи, пропонується використовувати метрики розраховані за CVSS версії 2.

В стандарті NIST CVSS v2 критичність вразливостей оцінюється на основі декількох глобальних груп метрик:

- базові метрики – постійні та не змінюються з часом;
- тимчасові метрики – не постійні та можуть змінюватися з часом;

- метрики навколишнього середовища – дозволяють деталізувати базові та тимчасові метрики та врахувати особливості середовища в якому знаходиться вразливість, що підлягає оцінці.

Тимчасові метрики та метрики навколишнього середовища розраховуються окремо для кожного окремо взятого випадку та можуть змінювати кінцевий покажчик критичності вразливості, виходячи з певної ситуації в структурі ТКМ. В даній роботі пропонується використовувати лише базові метрики, так як вони є універсальними і не змінюються незалежно від того в якому середовищі знаходиться вразливість та не потребують ручного втручання оператора ТКМ.

Параметр критичності вразливостей на заданому маршрутизаторі в даній роботі пропонується розраховувати за формулою:

$$R_{CVSS} = \frac{\sum_{i=1}^{n} B_{score_i}}{N_{враз.}} \cdot \frac{1}{10}, \qquad (2.1)$$

де B_{score_i} – покажчик базової метрики i вразливості, знайденої на заданому маршрутизаторі, при $i = \overline{1, N_{враз.}}$;

$N_{враз.}$ – загальна кількість знайдених вразливостей на маршрутизаторі.

Так як $B_{score_i} \in [0;10]$, то поділ на 10 забезпечує нормування параметру критичності вразливостей маршрутизатора $R_{CVSS} \in [0;1]$.

Подальші розрахунки параметрів виконуються згідно з CVSS v2, а стандартні значення для параметрів, які використовуються в розрахунках, наведено у додатку В:

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

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

$$E = 20 \cdot A \cdot A_v \cdot A_c,$$

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

де I – збиток;

E – можливість експлуатації;

$f(I)$ – функція від збитку, розрахунок якої наведено нижче;

$\lceil \ \rceil_{1-dec}$ – 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.

Перевагою даного методу можна вважати простоту. Критичність вразливостей на основі базових метрик стандарту NIST CVSS розраховується експертами та є універсальною і незмінною. Розрахована критичність може бути використана при створенні сигнатур сканерів вразливостей, які дозволяють в автоматизованому режимі виявляти вразливості та їх рівні критичності на вузлах ТКМ.

Недоліком даного методу можна вважати те, що деякі з параметрів тимчасових метрик та метрик навколишнього середовища вразливості неможливо розрахувати без участі оператора ТКМ. Даний фактор позбавляє гнучкості наведений метод оцінки параметру РІБ та не дозволяє в автоматизованому режимі врахувати багато з параметрів сучасних ТКМ.

2.1.2. Метод розрахунку параметра ризику інформаційної безпеки шляхом оцінки ефективності маршрутизаторів

Якщо представити структуру ТКМ як зважений орієнтованого графа $G = (V, E)$, де множина вершин V моделює множину вузлів мережі, а множина дуг E описує множину КЗ між ними, то, виходячи з термінології теорії живучості інформаційних систем, вразливість мережі – це оцінка зниження глобальної ефективності мережі (ГЕМ) у випадку видалення одного чи більше вузлів мережі та всіх його КЗ [97, 98]. Під ефективністю мережі мається на увазі ефективність передачі ПП в ній. Для запобігання плутанини з термінологією в даній роботі використовується термін «ефективність маршрутизатора мережі» (ЕММ), який рівнозначний терміну ефективності мережі, та на основі якого пропонується розраховувати параметр РІБ. За фізичним змістом параметр ЕММ відображає наскільки зменшиться ефективність передачі ПП в мережі в разі видалення маршрутизатора з усіма його КЗ. За допомогою вказаного параметру можна знайти найбільш і найменш ефективні маршрутизатори мережі.

Вважається, що ефективність передачі даних між вузлами зворотно пропорційна віддалі між ними. Однак формула розрахунку середнього шляху в мережі може виявитися нескінченною у зв'язку з тим, що деякі мережі можуть виявитися незв'язними. Для врахування подібних випадків пропонується використовувати ГЕМ, яка відображає середній інверсний шляхта розраховується за формулою [97]:

$$\xi = \frac{1}{n \cdot (n-1)} \cdot \sum_{i \neq j} \frac{1}{d_{i,j}}, \tag{2.2}$$

де $d_{i,j}$ – мінімальна відстань між вузлами i, j, при умові $i \neq j$ розрахунок проводиться між кожною парою вузлів заданій мережі;

n – кількість вузлів в заданій мережі.

ЕММ i розраховується за наступною формулою [97, 98]:

$$\theta_i = \frac{\xi - \xi_i}{\xi}, \text{ при } \theta_i \in (0;1], \tag{2.3}$$

де ξ – ГЕМ;

ξ_i – ГЕМ у випадку видалення i-го вузла та усіх його КЗ.

ЕММ i, що розраховується за формулою (2.3), вказує наскільки погіршиться ефективність передачі ПП в мережі у випадку видалення заданого маршрутизатора i та усіх його КЗ. При цьому, в стандартній формулі розрахунку глобальної ефективності (2.2) з теорії живучості інформаційних систем, параметр $d_{i,j}$ представляє собою відстань між вузлами i, j та вимірюється кількістю вузлів в заданому шляху передачі які знаходяться між вузлами i, j. З точки зору ТКМ параметр $d_{i,j}$ вказує на кількість ретрансляцій пакету через маршрутизатори мережі при його передачі між вузлами i, j за заданим шляхом. Такий підхід не дозволяє визначити найбільш ефективний маршрутизатор мережі в силу того, що він не враховує багатьох з факторів сучасних ТКМ, таких як, наприклад: затримка пакетів, ПРЗД та завантаженість КЗ, надійність та інші.

В даній роботі пропонується змінити підхід до розрахунку ГЕМ, замінивши мінімальну відстань між парою вузлів $d_{i,j}$ на мінімальну метрику одного з шляхів p з множини шляхів $P_{i,j}$ між вузлами i, j. При цьому, нехай кожній дузі $(i, j) \in E$ графу G відповідає ПРЗД КЗ $\mu_{i,j}$ та затримка обробки і передачі пакетів $D_{i,j}$. Тоді метрика визначається за наступними формулами:

$$M_p = \sum_{m \in p} M_m, \tag{2.4}$$

де $\sum_{m \in p} M_m$ – сума метрик кожного з КЗ m, які входять в шлях p;

$$M_m = \left(\frac{10^8}{\mu_{min}^{i,j}} + D_{sum}^{i,j} \right) \cdot c_{scale}, \tag{2.5}$$

де B_{min}^{ij} – значення зваженого покажчику ПРЗД для КЗ між вузлами i, j, при $i \neq j$, кбіт/с;

$D_{sum}^{i,j}$ – сума затримок в каналі зв'язку між вузлами i, j, при $i \neq j$, мкс;

c_{scale} – масштабуюча константа, яка дорівнює 256.

Тоді формула розрахунку ГЕМ приймає вигляд:

$$\xi = \frac{1}{n \cdot (n-1)} \cdot \sum_{i \neq j} \frac{1}{\min\limits_{p \in P_{i,j}} \mu_p}, \tag{2.6}$$

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, при умові $i \neq j$ розрахунок проводиться між кожною парою вузлів в заданій мережі;

n – кількість вузлів в заданій мережі.

З урахуванням методу, запропонованого в формулах (2.4)-(2.6), параметр ЕММ дозволяє знайти найбільш ефективні маршрутизатори в заданій ТКМ. Відповідно, чим більша величина параметру θ_i, тим ефективнішим є маршрутизатор i та тим менш бажаний його вихід з ладу.

Для прикладу, розглянемо топологію на рис. 2.1. Кожен КЗ між вузлами має однакову ПРЗД 100 мбіт/с та однакову затримку 10 мкс.

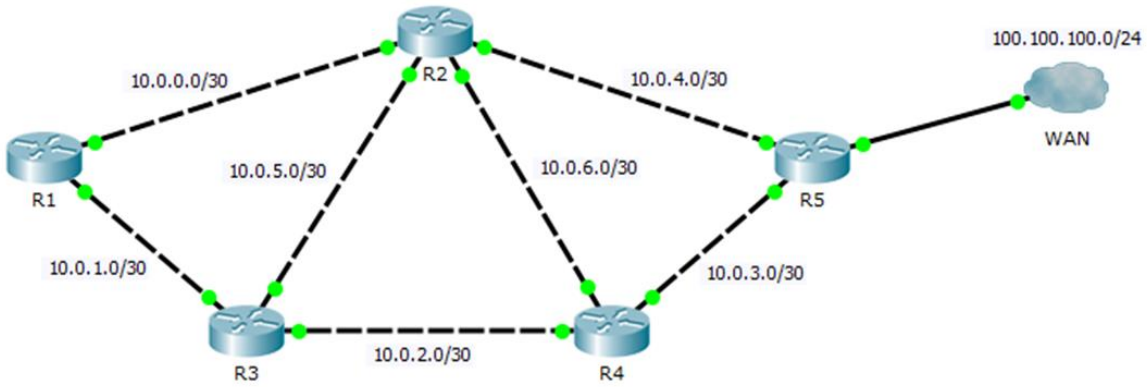


Рис. 2.1. Топологія мережі для прикладу розрахунку ЕММ

Для того, щоб знайти параметр ЕММ уявімо мережу в вигляді графу, роль вершин якого грають вузли R1, R2, R3, R4, R5, WAN та ребер, роль яких відіграють КЗ між маршрутизаторами. Вирішення задачі вибору найкоротшого шляху, в даному випадку, формалізується як задача булевого програмування, яку можна вирішити за допомогою функції bintprog інструментарію «Optimization Toolbox» пакету «матрична лабораторія» (MATrix LABoratory, MATLAB) (додаток Г).

Якщо враховувати, що структурна схема та параметри ТКМ задані у відповідності з топологією на рис. 2.1, то моделювання покаже наступні результати розрахунків параметра ЕММ:

$$\theta_{R1} = 0{,}904;\ \theta_{R2} = 0{,}928;\ \theta_{R3} = 0{,}91;\ \theta_{R4} = 0{,}9153;\ \theta_{R5} = 0{,}7943.$$

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}:

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

$$x_{scale} = \frac{\xi}{\mathbf{max}(\xi_i)}.$$

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

Параметр x_{scale} дозволяє нормувати значення ЕММ відносно найбільшої ГЕМ у випадку видалення одного з маршрутизаторів ТКМ. З урахуванням нормування в результаті моделювання отримані наступні результати:

$$\theta_{R1} = 0{,}5333;\ \theta_{R2} = 0{,}65;\ \theta_{R3} = 0{,}5625;\ \theta_{R4} = 0{,}5882;\ \theta_{R5} = 0.$$

Порівняльний аналіз різниць максимальної та поточної ЕММ наведено в табл. 2.1.

Таблиця 2.1

Різниця між максимальною величиною ЕММ та поточною величиною ЕММ до та після нормування

	$\theta_{R2} - \theta_{R1}$	$\theta_{R2} - \theta_{R2}$	$\theta_{R2} - \theta_{R3}$	$\theta_{R2} - \theta_{R4}$	$\theta_{R2} - \theta_{R5}$
До нормування	0,024	0	0,018	0,0127	0,1337
Після нормування	0,1167	0	0,0875	0,0618	0,65
Приріст різниці в процентах	486,25%	0%	486,11%	486,61%	486,16%

Як видно з табл. 2.1 наведений метод нормування для даного прикладу збільшив різницю між ЕММ в середньому приблизно на 486,2%.

Параметр РІБ визначемо, як ризик порушення глобальної ефективності ТКМ при видаленні i-го маршрутиазтора та всіх його каналів зв'язку у разі успішної реалізації загрози

$$R_{\theta_i} = \theta_i \cdot P^i_{загр.},$$

де $P^i_{загр.}$ – ймовірність реалізації загрози виведення з ладу маршрутизатора i та всіх його каналів зв'язку, при цьому в даній роботі будемо вважати $P_{загр.} = 1$.

Перевагою використання даного параметру РІБ є те, що його потрібно перераховувати лише при фізичних змінах в топології ТКМ, а саме при зміні: кількості маршрутизаторів в ТКМ та КЗ між ними, а також ПРЗД та затримок пакетів в КЗ. Це дає змогу зменшити навантаження на вузли-аналізатори. Недоліком можна назвати те, що даний параметр дозволяє оцінити лише ризики порушення критерію доступності.

2.1.3. Метод розрахунку параметр ризику наявності атаки типу відмова в обслуговуванні шляхом аналізу ентропії потоку пакетів

Детектуванню DoS атак на основі аналізу ентропії ПП присвячено ряд публікацій [99-102]. В даному випадку пропонується не просто розпізнавати наявність чи відсутність DoS атаки, але вимірювати можливість її наявності та детектувати атаку лише при перевищенні заданого рівня прийнятності.

Параметрами, на основі яких може вимірюватися ентропія можуть виступати:

- поля заголовків кадру, пакету чи сегменту, в основному, такі як адреси Інтернет протоколу (Internet Protocol, IP) відправника та отримувача пакетів, а також порти «протоколу контролю передачі» (Transmission Control Protocol, TCP) та «протоколу датаграм користувача» (User Datagram Protocol, UDP);

- кількість отриманих пакетів за заданий інтервал часу;
- об’єм окремого типу ПП за заданий інтервал часу.

Для проведення експериментів були вибрані наступні критерії: IP адреса та TCP/UDP порти отримувача пакетів, які в подальшому будуть називатися сокетом.

Для розрахунку ентропії використовуються наступні формули:

$$H = -\sum_{i=1}^{n} p_i \cdot \mathbf{log}(p_i),$$

$$p_i = \frac{f_i}{N_{сокетів,w}},$$

де 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.

В публікаціях параметр w пропонується вимірювати в часовому інтервалі, зазвичай в секундах, а також в даних статтях вказано, що параметр w необхідно підбирати в кожному взятому випадку окремо [99-102]. В даній роботі пропонується вимірювати параметр w в кількості пакетів, які необхідно отримати для проведення одного виміру.

Для того, щоб визначити початок атаки необхідно постійно спостерігати за ентропією ПП. Даний процес здійснюється шляхом застосування рухомого середнього (РС). Існує багато варіацій РС. Для того, щоб вибрати конкретну реалізацію РС були проведені експерименти над тестовими зразками ПП, отриманих в результаті спостереження за ТКМ кафедри Інкомунікаційних систем Харківського національного університету радіоелектроніки. В якості функцій РС для аналізу були вибрані:

1. Просте РС [103];

2. Адаптивна РС Кауфмана [103, 104];

3. РС з динамічним періодом усереднення [104].

В пункті 2 та 3 вищенаведеного списку використовується різновид експоненційного згладженого РС, ваговий коефіцієнт в яких може динамічно змінюватися в залежності від значень, що аналізуються. Ці РС використовуються в технічному аналізі цін на фондовій біржі, основною метою яких є адаптивна зміна константи, що згладжує результат, в залежності від коливань цін на ринку. Наприклад, коли ціни змінюються в незначному діапазоні або не змінюються зовсім – то перевага надається попередньому значенню РС, коли ціни коливаються – перевага віддається поточному значенню, причому, чим більше коливання цін, тим більшу вагу буде мати поточне значення.

Просте РС розраховується за формулою:

$$SMA_t = \frac{1}{n}\sum_{i=0}^{n-1} etr_{t-i},$$

де n – величина інтервалу згладжування, стандартно $n = 10$;

etr_t – значення ентропії ПП в момент часу t.

Адаптивне РС Кауфмана розраховується за формулами:

$$KAMA_t = C_{t,n,f,s} \cdot etr_t + \left(1 - C_{t,n,f,s}\right) \cdot KAMA_{t-1},$$

$$C_{t,n,f,s} = \left(ER_{t,n} \cdot \left(fastest - slowest\right) + slowest\right)^2,$$

$$fastest = \frac{2}{f+1},$$

$$slowest = \frac{2}{s+1},$$

$$ER_{t,n} = \frac{direction_{t,n}}{volatility_{t,n}},$$

$$direction_{t,n} = \left| etr_t - etr_{t-n-1} \right|,$$

$$volatility_{t,n} = \sum_{i=0}^{n-1} \left| etr_{t-i} - etr_{t-i-1} \right|,$$

де $KAMA_{t-1}$ – попереднє значення РС;

$C_{t,n,f,s}$ – константа згладжування;

etr_t – значення ентропії при закритті поточного періоду t.

$ER_{t,n}$ – коефіцієнт ефективності в момент часу t за період n;

$fastest$ та $slowest$ – коефіцієнти згладжування для експоненційної згладженої РС, при $f = 2$ та $s = 30$;

$direction_{t,n}$ – загальний рух значень ентропії в момент часу t за період n;

$volatility_{t,n}$ – сума шумових значень ентропії в момент часу t за період n;

n – величина інтервалу згладжування, стандартно $n = 10$;

РС з динамічним періодом усереднення розраховується за формулою:

$$VIDYA_t = etr_t \cdot F_{vidya} \cdot CMO_t + VIDYA_{t-1} \cdot \left(1 - F_{vidya} \cdot CMO_t\right),$$

$$F_{vidya} = \frac{2}{n+1},$$

$$CMO_t = \frac{UpSum_{t,n} - DnSum_{t,n}}{UpSum_{t,n} + DnSum_{t,n}},$$

$$\begin{cases} UpSum_{t,n} = \sum_{i=0}^{n} etr_i - etr_{i-1}, \text{ якщо } (etr_i - etr_{i-1}) \geq 0, \\ DnSum_{t,n} = \sum_{i=0}^{n} |etr_i - etr_{i-1}|, \text{ якщо } (etr_i - etr_{i-1}) < 0. \end{cases}$$

де etr_t – значення ентропії вибірки в момент часу t;

F_{vidya} – константа згладжування;

CMO_t – значення осцилятора цінових моментів Чанде (Chande Momentum Oscillator, CMO);

$VIDYA_{t-1}$ – попереднє значення РС;

n – величина інтервалу згладжування, стандартно $n = 10$;

$UpSum_{t,n}$ – сума додатних приростів значення ентропії за період n;

$DnSum_{t,n}$ – сума від'ємних приростів значень ентропії за період n.

Аналіз результатів, отриманих в ході експерименту, показав, що у порівнянні з простим РС, адаптивне РС Кауфмана та РС з динамічним періодом усереднення мають більше середньоквадратичне відхилення (СКВ) від реальних значень ентропії, а також вони повільніше реагують на зміни в значеннях ентропії ПП. Порівняльний аналіз СКВ для різних РС наведено у табл. 2.2.

Таблиця 2.2

Порівняльний аналіз СКВ для різних алгоритмів РС в залежності від об'єму вибірки

	$\lfloor \delta_{sma} \rfloor$	$\lfloor \delta_{kama} \rfloor$	$\lfloor \delta_{vidya} \rfloor$
$w = 50,\ n = 10$	0,721	0,812	0,801
$w = 100,\ n = 10$	0,486	0,635	0,62
$w = 300,\ n = 10$	0,441	0,571	0,518
$w = 500,\ n = 10$	0,442	0,524	0,504

Як видно з табл. 2.2, при $w = 500$ досягається найменше СКВ практично по всіх РС. На рис. рис. 2.2 показано співвідношення різних алгоритмів РС до ентропії ПП.

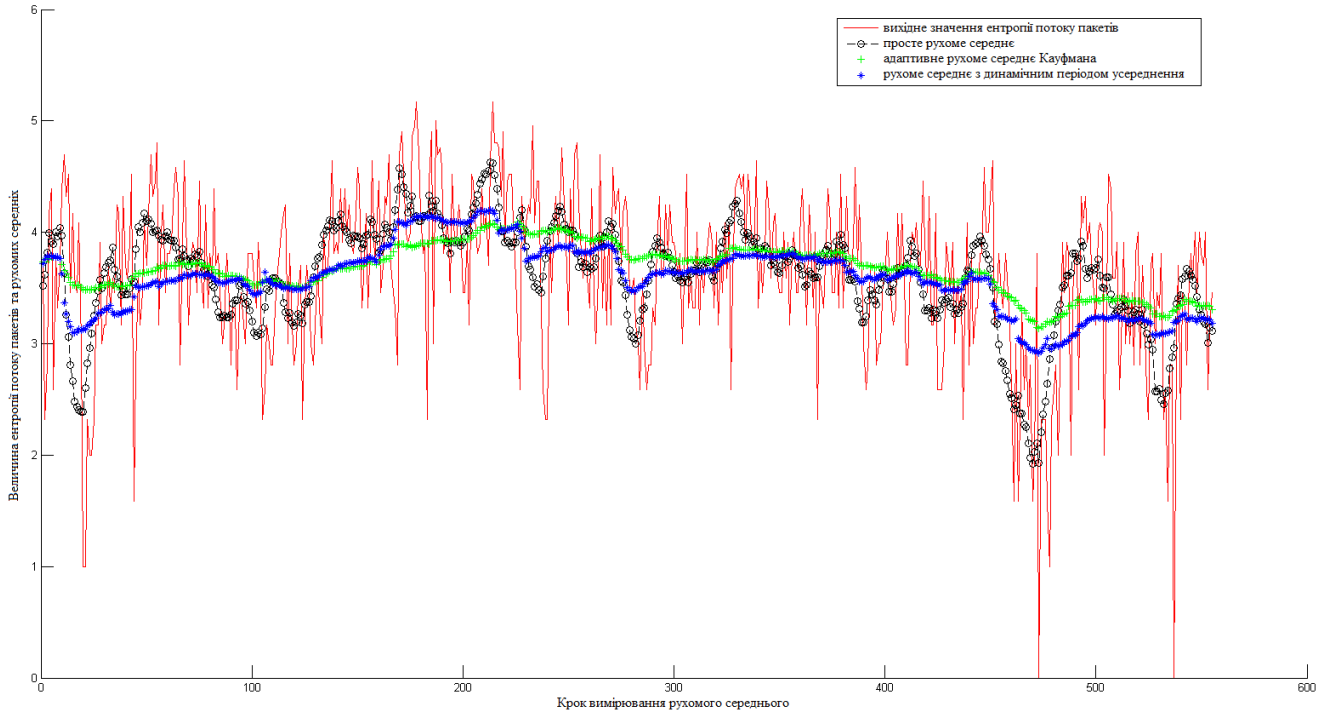


Рис. 2.2. Співвідношення різних алгоритмів РС до ентропії ПП для TCP з урахуванням, що $w = 100$ и $n = 10$

Як видно з рис. 2.2 просте РС швидше реагує на зміни в ентропії ПП, ніж інші алгоритми, що досліджувались в даному пункті. Враховуючи швидкість реакції на зміни в ентропії, менше СКВ від реальних значень, а також те, що процес надходження пакету на інтерфейс маршрутизатора є стаціонарним процесом та не залежить від минулих станів, а пакеті надходять на інтерфейс незалежно та з рівною ймовірністю – то пропонується вибрати алгоритм простого РС як основний.

Для детектування атаки використовується наступний вираз [99]:

$$\left| SMA_i - etr_t \right| \geq \beta \cdot \sigma_{SMA_i}, \qquad (2.7)$$

де SMA_i – останнє обчислене значення простого РС;

β – цілочисельна константа масштабування, $\beta > 0$.

Параметр β вибирається оператором ТКМ, при цьому стандарте значення цього параметр $\beta = 3$, тому що при менших значеннях виникає більша кількість помилкових спрацьовувань [99].

Різні типи DoS атак можуть викликати як зниження, так і підвищення ентропії ПП, в залежності від: типу атаки, алгоритму розрахунку ентропії та критерії, на основі яких розраховується ентропія. Цими факторами обумовлений вираз $\left|SMA_i - etr_t\right|$, який гарантує абсолютну невід'ємну різницю РС та поточного значення ентропії. У випадку, якщо виконується вимога (2.7) аналізатор сигналізує про наявність атаки.

В даній роботі параметр РІБ наявності DoS атаки пропонується розраховувати за наступною формулою:

$$\left.\begin{array}{c} R_{etr} = \dfrac{\left|SMA_i - etr_t\right| - \beta \cdot \sigma_{SMA_i}}{\left|SMA_i - etr_t\right|} \cdot \rho \cdot K_{self}, \; при \; \left|SMA_i - etr_t\right| \geq \beta \cdot \sigma_{SMA_i}, \\ R_{etr} = 0, \; при \; \left|SMA_i - etr_t\right| \leq \beta \cdot \sigma_{SMA_i}, \end{array}\right\} \qquad (2.8)$$

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 $K_{self} = N_{всі} / N_{маршр.}$.

Використання наведеного методу дозволяє знизити кількість хибних спрацьовувань та покращити точність визначення величини параметру ризику за допомогою додаткових параметрів ρ та K_{self}, як показано у формулі (2.8). Параметр ρ вказує на завантаженість заданого маршрутизатора. У випадку, коли

маршрутизатор не завантажений і може виконувати свою основну функцію, то розглядати наявність DoS атаки на нього не має сенсу не залежно від ентропії ПП. Параметр K_{self} відображає долю пакетів, які спрямовані на сам маршрутизатор. У випадку, якщо даний параметр наближається до нуля, то неможливо стверджувати, що DoS атака спрямована саме на цей маршрутизатор, а можливо лише припустити, що проблеми з продуктивністю маршрутизатора викликана побічними факторами, наприклад: великим об'ємом легітимного ПП, запуском ресурсномістких процесів на самому маршрутизаторі і т.п.

Існують різні методи розрахунку ентропії, наприклад: інформаційна ентропія, ентропія з зі стисненням даних, швидка ентропія (fast entropy, FA). Також наведено аналіз різних алгоритмів розрахунку ентропії та їх вплив на можливість детектування розподілених атак типу відмова в обслуговуванні (Distributed Denial of Service, DDoS) з урахуванням помилок першого та другого роду, а також швидкісних характеристик алгоритмів [99-100]. Не залежно від того, який алгоритм розрахунку ентропії буде вибраний в якості основного – подальші розрахунки згідно з методом, представленим в даному пункті роботи.

Недоліки наведеного методу:

1. У випадку тривалої DoS атаки РС зміститься до аномального рівня ентропії та умова (2.7) перестане виконуватися, тоді $R_{etr} = 0$. Таким чином сформується «звикання до атаки».

2. Хибне спрацьовування може активізувати механізми захисту без нагальної на то потреби.

3. Даний метод не може виявити повільні DoS атаки, так як подобного роду атаки слабко змінюють ентропію ПП та параметри ρ і K_{self}.

4. Даний метод не гарантує безпомилкове виявлення DoS атаки, а лише передбачає можливість її наявності виходячи з умови (2.7).

Параметр ризику R_{etr} пропонується застосовувати в якості ознаки для виявлення наявності DoS атаки. При $R_{etr} > 0$ можна зробити припущення, що DoS атака здійснюється в даний момент часу. Але перевагою використання саме

параметру ризику R_{etr}, що розраховується за формулою (2.8), у порівнянні з простою умовою (2.7), полягає в тому, що R_{etr} дозволяє ввести градаційну шкалу та визначати атаку тільки у випадку, коли:

$$R_{etr} > R_{прийнят.},$$

де $R_{прийнят.}$ – це максимально прийнятний рівень ризику, при якому сигнал про наявність атаки можна ігнорувати, при цьому $R_{прийнят.} \in [0;1]$.

Ручне налаштування $R_{прийнят.}$ надає змогу зменшити кількість хибних спрацьовувань для окремих ТКМ, так як для кожної з них ентропія ПП залежить від характеристик самого ПП властивих заданій ТКМ.

2.1.4. Метод розрахунку ризику інформаційної безпеки транзитного потоку пакетів для заданого шляху передачі на основі статичних параметрів

Для розрахунку РІБ на основі статичних параметрів пропонується використовувати стандартний метод, відомий з теорії ризиків інформаційної безпеки:

$$R_{p_{i,j}} = 1 - \prod_{x \in X} (1 - R_x),$$

де R_x – ризик одного з параметрів x з множини параметрів X, при цьому в даній роботі $X \in \{R_{CVSS}; R_\theta\}$.

В даній роботі пропонується враховувати параметри РІБ наступним чином:

$$R_{p_{i,j}} = 1 - \left(1 - K_{CVSS} \cdot \frac{\sum_{m \in p} R_{CVSS_m}}{n_p}\right) \cdot \left(1 - K_{\theta} \cdot \left(1 - \frac{\sum_{m \in p} R_{\theta_m}}{n_p}\right)\right), \qquad (2.9)$$

де $R_{p_{i,j}}$ – РІБ 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 $K_{CVSS} \in [0;1]$, $K_{\theta} \in [0;1]$;

R_{CVSS_m} – параметри ризику R_{CVSS} кожного з маршрутизаторів m в шляху p;

R_{θ_m} – параметри ризику R_{θ} кожного з маршрутизаторів m в шляху p;

n_p – загальна кількість маршрутизаторів в шляху p.

Коефіцієнти важливості K_{CVSS} та K_{θ} дозволяють варіювати відповідні параметри РІБ, на основі яких виконується розрахунок РІБ шляху. Необхідно відзначити, що ляд коректної роботи запропонованого метода розрахунку РІБ шляху, дані коефіцієнти повинні бути однакові на всіх маршрутизаторах мережі.

На рис. 2.3 наведено графік, який відображає залежність РІБ шляху $R_{p_{i,j}}$ (на графіку позначений як R) від відповідних параметрів РІБ: R_{θ} (на графіку позначений як Rsurv) та R_{CVSS} (на графіку позначений як Rcvss). На графіку зображено 5 дослідів, на протязі кожного досліду параметр R_{θ} залишається незмінним але зростає у кожному новому досліді на 0,2 у межах [0,1; 0,9], при цьому параметр R_{CVSS} у кожному досліді змінюється в межах [0;1] з кроком 0,1.

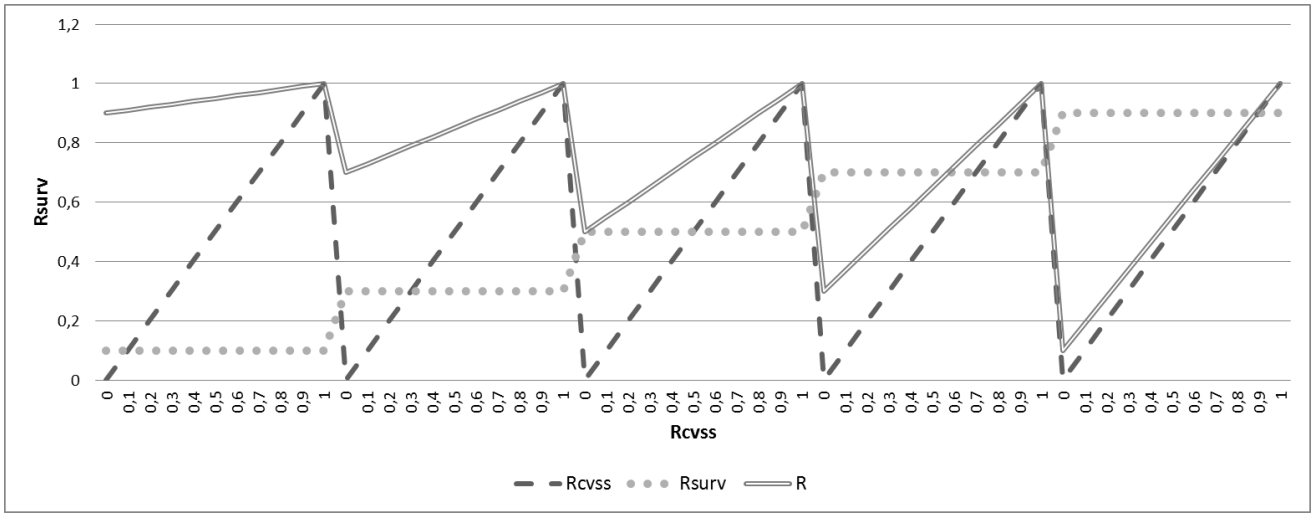


Рис. 2.3. Графік залежності РІБ шляху передачі ПП від параметрів РІБ

З графіку (рис. 2.3) видно, що при малих значеннях R_θ, РІБ шляху $R_{p_{i,j}}$ близький до одиниці та плавно наближається до неї із зростанням R_{CVSS}, а при збільшенні значень у подальших дослідах R_θ, РІБ шляху $R_{p_{i,j}}$ приймає значення все більше наближені до 0 та різко наближається до 1 при збільшенні R_{CVSS}.

Так як параметр R_θ враховує зниження ефективності передачі ПП в мережі у випадку виходу з ладу маршрутизаторів мережі, то даний параметр враховує ризики критерію доступності та його пропонується використовувати у випадках, коли необхідно задіяти засоби захисту від DoS атак.

В свою чергу параметр R_{CVSS} враховує вразливості, які можуть бути використані для порушення різних критеріїв безпеки: конфіденційності, доступності та цілісності. В загальному виді даний параметр вказує наскільки заданий маршрутизатор схильний до того, щоб бути вдало атакованим.

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. Стандартно активується даний варіант коефіцієнтів. Адміністратор ТКМ може змінити його на один з нижченаведених;

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. Як вказано у пункті 2.1.3, 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 – $K_{CVSS}=1,\ K_{\theta}=0$.

Також необхідно зауважити, що РІБ розрахований на основі ЕММ не дозволяє попередити чи зупинити DoS атаку, а лише призваний зменшити її ефект шляхом перемаршрутизації ПП з метою захисту від перенавантаження найбільш ефективний маршрутизатор ТКМ. Перемаршрутизація ПП може надати більше часу для аналізу ситуації механізмам попередження DoS атак, які повинні виділити з загального ПП окремі шкідливі потоки для їх подальшого блокування. Розробка моделей і методів аналізу та блокування DoS атак не э задачею даної дисертаційної роботи та потребують окремих додаткових досліджень.

Слід також відзначити, що параметр R_{θ} дозволяє знайти найбільш ефективний маршрутизатор в ТКМ, тоді існує проблема, яка полягає в тому, що у випадку врахування лише параметру R_{θ} в формулі розрахунку РІБ шляху, ПП буде передаватися по шляхах з найбільш ефективними маршрутизаторами. Це легко продемонструвати: якщо $K_{CVSS}=0$ та $K_{\theta}=1$, тоді $R_{p_{i,j}}=1-R_{\theta_i}$, і тоді при зростанні R_{θ} РІБ шляху буде зменшуватися і, виходячи з критеріїв врахування РІБ

в процесі вибору оптимального шляху передачі (наведено у 1 розділі), це призведе до зменшення метрик маршрутів де R_θ буде найбільшим і наблизить їх вибір в якості оптимальних.

В такому випадку, якщо існує декілька шляхів до кінцевого вузла, то пропонується:

- пріоритетний та довірчий ПП передавати по шляху з найбільш ефективними маршрутизаторами;

- не пріоритетний або недовірчий ПП передавати по шляху з найменш ефективними маршрутизаторами.

Пріоритетність ПП пропонується визначати виходячи з полів тип сервісу (Type of Service, ToS) у заголовку пакету IPv4, або поля класу трафіку (Traffic Class, TC) в заголовку пакету IPv6. Довірливість ПП пропонується визначати на основі листів доступу. Правила пріоритетності та довірливості ПП мають бути задані адміністратором ТКМ. Саму ж перемаршрутизацію ПП пропонується виконувати за допомоги маршрутизації на основі політик (Policy Based Routing, PBR) при якій можна вказати пакети з якими IP адресами повинні проходити за якими шляхами. Автоматизація процесу визначення довірливості ПП є складною задачею та не розглядається в даній роботі, з іншого боку адміністратор може визначити службові ПП в якості довірливих та налаштувати ACL таким чином, щоб у разі потреби саме службовий ПП передавався за оптимальним шляхом, а весь інший ПП перемаршрутизувався за іншими шляхами.

2.2. Динамічні методи оцінки ризику інформаційної безпеки транзитного потоку пакетів для заданого шляху передачі

В даній роботі пропонується використовувати параметр ЙСД ПП до кінцевого вузла за заданий проміжок часу по заданому шляху. ЙСД ПП є динамічною величиною, яка залежить від інтенсивності вхідного ПП, інтенсивності обробки ПП маршрутизаторами, а також від кількості

маршрутизаторів в заданому шляху. В свою чергу, інтенсивність обробки ПП залежить від завантаженості ЦПМ. В даній роботі пропонується метод оцінки залежності завантаженості ЦПМ від типу та інтенсивності ПП, що поступає на маршрутизатор. Отримані результати використовуються при розрахунку ЙСД в якості додаткових параметрів, які впливають на інтенсивність обробки ПП на заданому маршрутизаторі.

Перевагою оцінки РІБ на основі динамічних параметрів є те, що методи їх розрахунку дозволяють враховувати параметри, які змінюються в реальному масштабі часу. Недоліком подібних методів є те, що РІБ шляху передачі може змінюватися з такою частотою, що може створити критичне навантаження на оперативну пам’ять та завантаженість процесору на вузлах-аналізаторах, тому що потрібно як перераховувати сам РІБ, так і параметрів, які від нього залежать, наприклад – метрик ПДМ.

2.2.1. Дослідження впливу завантаженості центрального процесору маршрутизаторів на процес маршрутизації потоку пакетів

У маршрутизатора є декілька видів ресурсів, які вливають на його працездатність: оперативна пам'ять, центральний процесор, постійна пам'ять, буфери інтерфейсів, загальний буфер, ПРЗД КЗ та загальна інтенсивність оборки ПП. Повна завантаженість одного з критичних системних ресурсів призведе до того, що маршрутизатор не зможе виконувати основну функцію – визначати оптимальний шлях передачі ПП, а також може почати відкидати транзитні пакети.

В даному пункті представлені експериментальні дані, які дозволяють виявити взаємозв'язку інтенсивності передачі ПП (завантаженості ПРЗД), завантаженості ЦПМ і затримки передачі пакетів між вузлом-відправником і вузлом-одержувачем. Також пропонується метод, який дозволяє використовувати отримані закономірності в процесі визначення оптимального шляху передачі ПП.

2.2.1.1. Опис умов проведення експерименту на реальному обладнанні компанії Cisco

З метою проведення експериментальних дослідів була створена топологія (рис. 2.4) з використанням реального обладнання компанії Cisco.

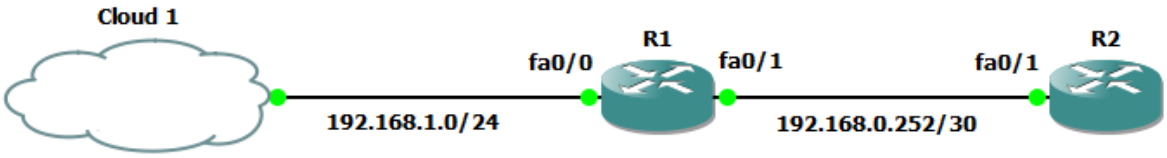


Рис. 2.4. Топологія для проведення дослідів із завантаженості ЦПМ

В елементі топології “Cloud 1” на рис. 2.4 емулюється комп’ютер з операційною системою Kali Linux. Вузли R1 та R2 є маршрутизаторами компанії Cisco моделі 2801, на маршрутизаторі R1 встановлена операційна система IOS 12.4(11)XJ3, а на R2 – IOS 12.4(12). Усі КЗ мають однакову ПРЗД 100 мбіт/с.

Для збільшення споживання системних ресурсів вузлом R1, з якого збираються статистичні дані, комп'ютер в Cloud 1 емулює наводнення пакетів, які передаються на маршрутизатор R2. Наводнення мережі пакетами проводиться з використанням утиліт t50, tcpdump і tcpreplay, вбудованих в стандартний набір утиліт збірки Kali Linux. Поток пакетів від утиліти t50 був записаний за допомогою tcpdump і відтворювався за допомогою tcpreplay з різними швидкостями, при цьому аналізувалися різні показники завантаженості системних ресурсів. В якості системних ресурсів для аналізу обрані: завантаженість ПРЗД КЗ між Cloud 1 і R1, завантаженість центрального процесора R1, а також затримка передачі ПП, яка вимірюється як затримка передачі ICMP exo-запитів (Echo-Request, ERQ) від Cloud 1 до маршрутизатора R2 плюс затримка передачі ICMP exo-відповідей (Echo-Reply, ERP) від R2 до Cloud 1.

Для збору даних використовується протокол SNMP. Пристрої Cisco автоматично підраховують завантаженість системного процесора за 5 секунд, за 1 хвилину і за 5 хвилин. Для збору даних використовуються наступні ідентифікатори об'єктів:

- .1.3.6.1.2.1.2.2.1.10.1 – кількість вхідних пакетів на інтерфейс маршрутизатора R1 КЗ між Cloud 1 і R1 (значення показника змінюються кожні 10 секунд, $\omega = 10$ сек);
- .1.3.6.1.2.1.2.2.1.5.1 – ПРЗД інтерфейсу маршрутизатора R1 КЗ між Cloud 1 і R1 (значення показника статичні);
- .1.3.6.1.4.1.9.9.109.1.1.1.1.6 – середня завантаженість ЦПМ R1 за 5 секунд (значення показника змінюються кожні 5 секунд, $\omega = 5 сек$).

Значення завантаженості ЦПМ можна отримувати з SNMP бази безпосередньо. Однак значення завантаженості КЗ в SNMP базі не зберігаються, для розрахунку даного показника використовується наступна формула:

$$L_{кан.св.,t} = \frac{(IfInOctets_t - IfInOctets_{t-1}) \cdot 8 \cdot 100}{\omega \cdot IfSpeed},$$

де $IfInOctets_t$ – кількість вхідних октетів ПП на інтерфейс в момент часу t;

ω – інтервал одного вимірювання, в даному випадку $\omega = 10 сек$;

$IfSpeed$ – ПРЗД інтерфейсу.

Час проведення одного експерименту складає 180 секунд. За час одного експерименту аналізатор отримує 36 значень завантаженості процесора і 18 значень завантаженості КЗ (швидкості передачі даних в мережу). Для того щоб зрівняти кількість значень завантаженості процесора і КЗ, попарно підраховуються середні значення завантаженості ЦПМ:

$$\frac{L_{CPU,1} + L_{CPU,2}}{2}, \ldots, \frac{L_{CPU,35} + L_{CPU,36}}{2}.$$

Таким чином отримуються 18 значень завантаженості ЦПМ та КЗ. У свою чергу, кількість ERQ відправлених на маршрутизатор R2 для вимірювання

затримки, може бути різним від експерименту до експерименту, так як безпосередньо залежить від часу ERL.

2.2.1.2. Аналіз результатів першого дослідження з двома маршрутизаторами та без активації додаткових служб на маршрутизаторі

Даний дослід проводився без активації будь-яких додаткових мережевих служб. Було проведено 5 експериментів, які відрізнялися швидкістю передачі шкідливого трафіку в мережу.

На рис. 2.5 наведено графік, який відображає затримку ПП в залежності від завантаженості ЦПМ.

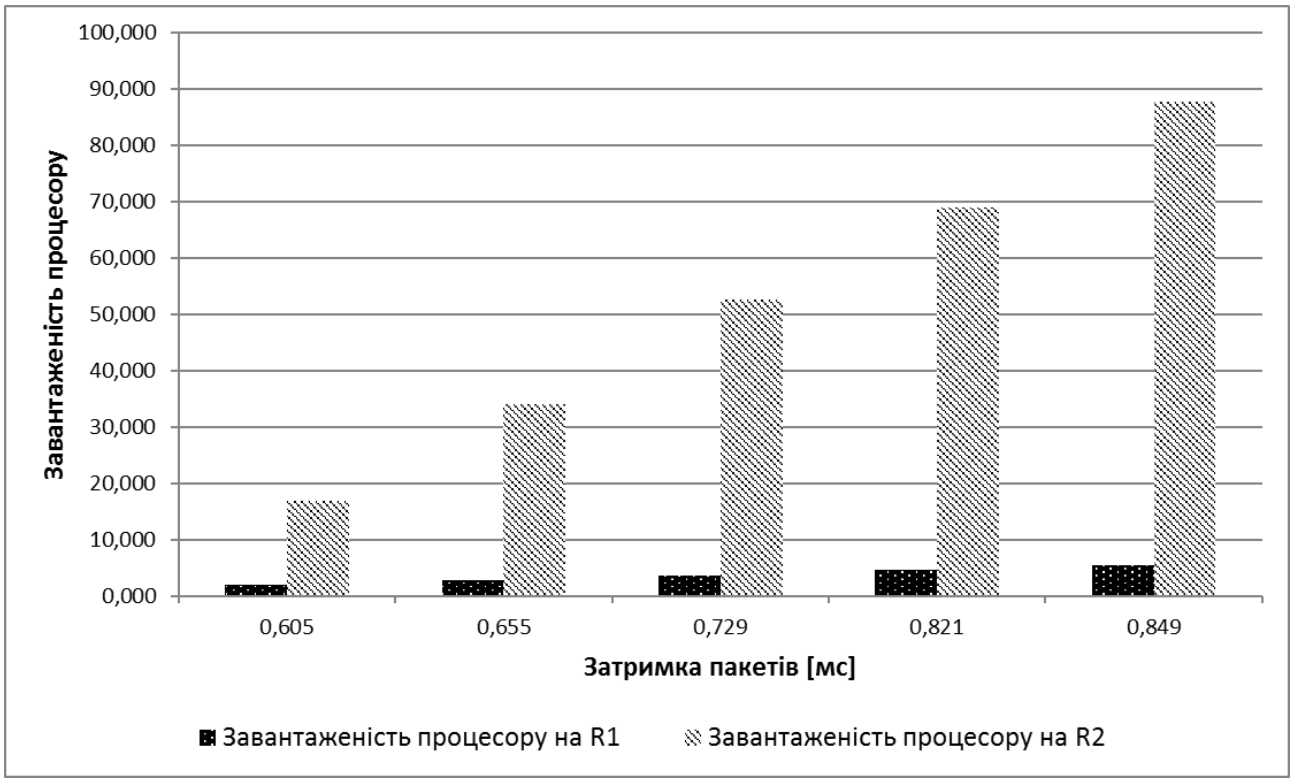


Рис. 2.5. залежність затримки ПП від завантаженості ЦПМ на маршрутизаторах R1 та R2

На рис. 2.6 та рис. 2.7 представлені графіки, у яких по осі абсцис розташовані середні значення швидкості передачі даних в мережу (еквівалентно завантаженості ПРЗД КЗ) в кожному експерименті, а по осі ординат – середня швидкість передачі

даних, яка необхідна, щоб завантажити процесор маршрутизатора на 1%, в кожному експерименті відповідно.

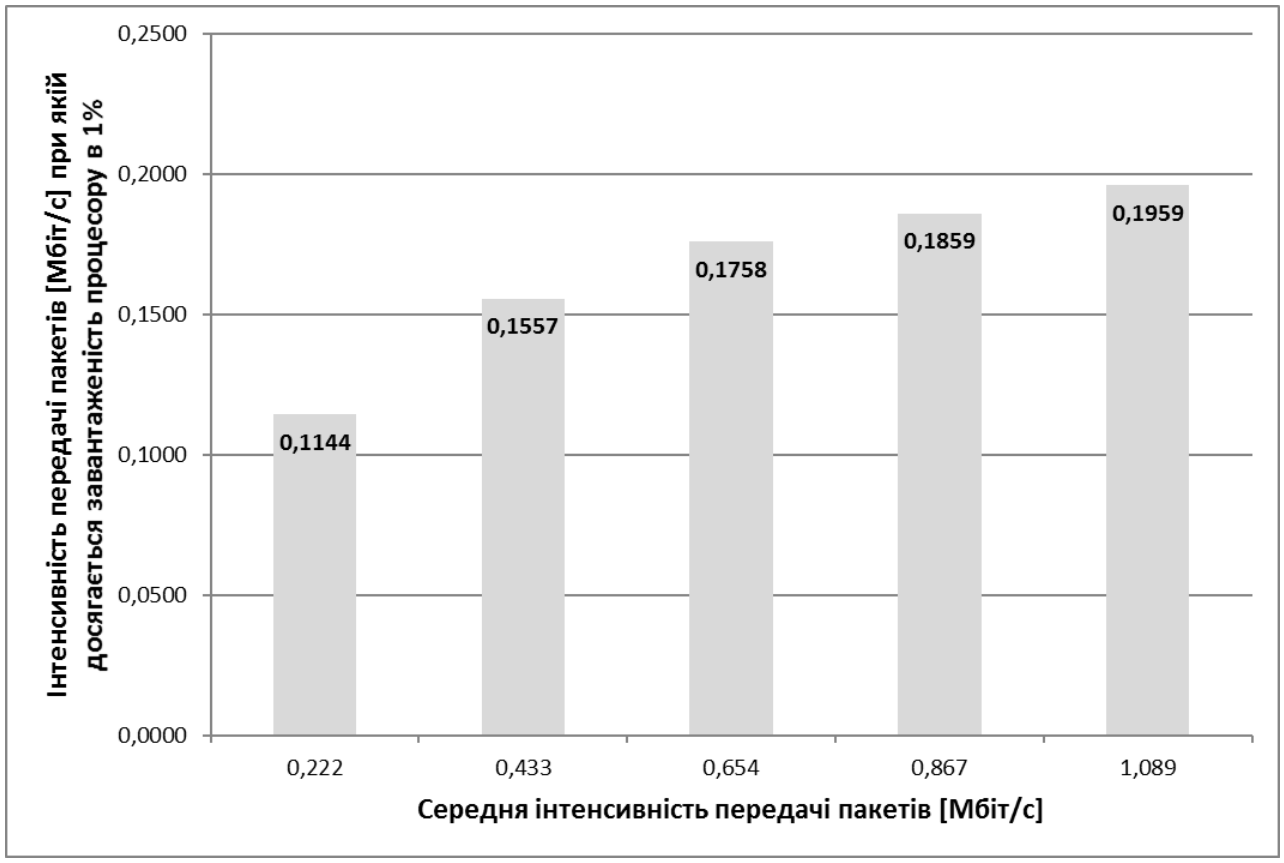


Рис. 2.6. Залежність необхідної швидкості передачі даних для створення завантаженості процесора в 1% від середньої інтенсивності передачі ПП для маршрутизатора R1

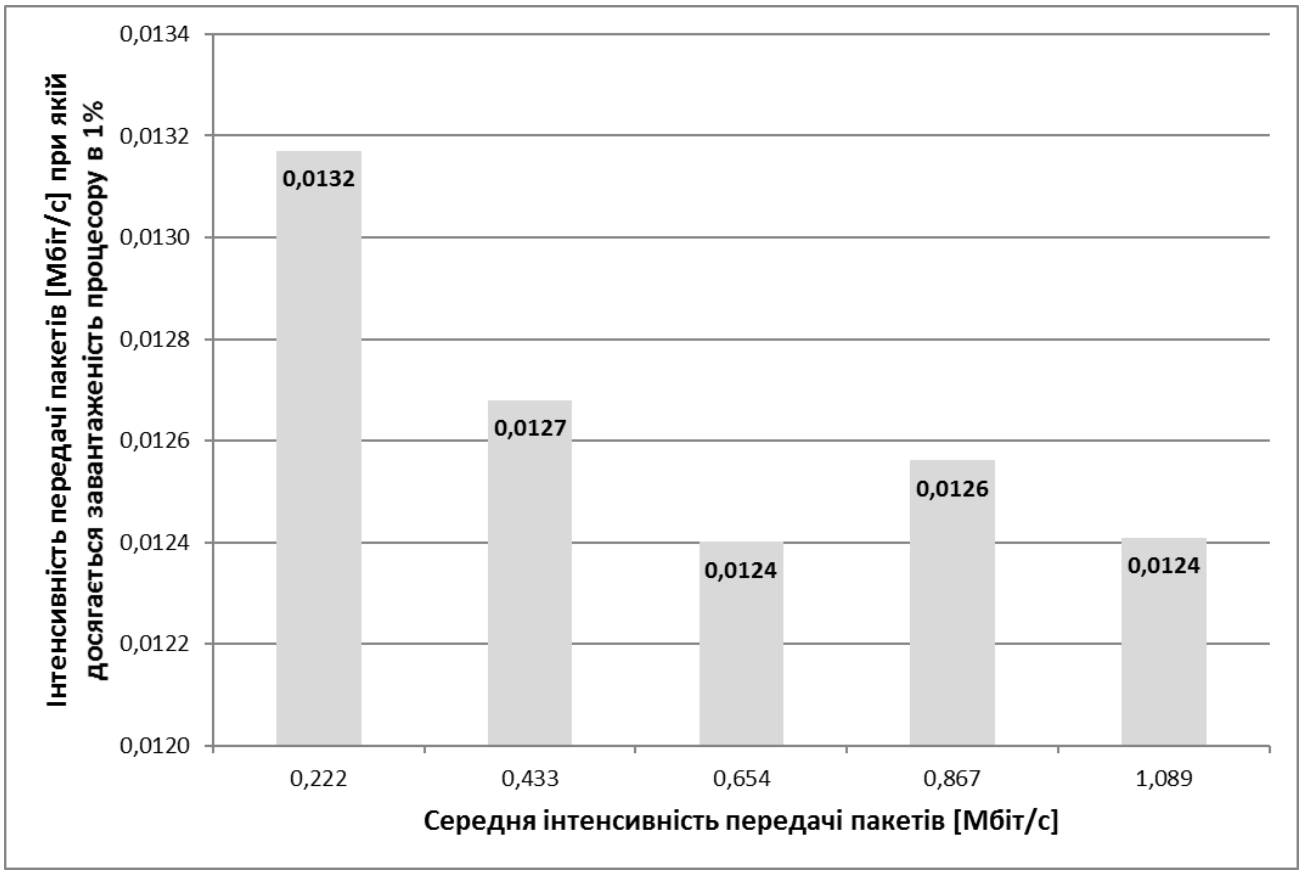


Рис. 2.7. Залежність необхідної інтенсивності передачі даних для створення завантаженості процесора в 1% від середньої інтенсивності передачі ПП для маршрутизатора R2

Інтенсивність передачі ПП, необхідна для створення завантаженості процесора в 1% визначається за такою формулою:

$$V_{1\%} = \frac{L_{кан.зв.,\, ср.,t}}{L_{CPU\ i,ср.,t}}, \tag{2.10}$$

де $L_{кан.зв.,\, ср.}$ – середня завантаженість ПРЗД КЗ в експерименті t;

$L_{CPU\ i,ср.,t}$ – середня завантаженість процесора досліджуваного маршрутизатора i в експерименті t, при цьому для розрахунку середнього значення використовується алгоритм підрахунку простого арифметичного середнього значення.

При аналізі графіків на рис. 2.6 і рис. 2.7 можна сказати, що маршрутизатор R1 вимагає більш ніж в 10 разів більшу інтенсивність надходження на нього ПП для створення завантаженості процесора в 1%, ніж маршрутизатор R2. Це пов’язано тією особливістю, що маршрутизатор R1 лише передає пакети, а маршрутизатор R2 змушений їх обробляти, так як є одержувачем.

Графік, представлений на рис. 2.6, має явний висхідний тренд. Це означає, що зі збільшенням інтенсивності передачі на нього ПП потрібно буде дедалі більша інтенсивність ПП для створення завантаженості ЦПМ на 1%.

Незважаючи на гадану неоднорідність результатів, представлених на рис. 2.7, різниця між результатами коливається в межах 10 кбіт/с, що можна вважати несуттєвим.

2.2.1.3. Аналіз результатів другого досліду з двома маршрутизаторами і оцінкою збільшення затримки передачі пакетів при маршрутизації

В даному досліді не було активовано ніяких додаткових мережевих служб ні на R1 ні на R2. Завданням досліду було вимірювання підвищення затримки в процесі прийняття рішення про маршрутизації вузлом R1. Для цього на вузол R1 подавався ПП з метою підвищити навантаження на його ЦПМ, в цей же час вимірювалась затримка ERQ-ERL між пристроєм в Cloud 1 і маршрутизатором R2.

В даному експерименті проводилося 5 експериментів, які відрізнялися швидкістю передачі ПП.

На рис. 2.8 представлений графік, який відображає затримку ERQ-ERL між Cloud 1 та R2 (як показано в топології на рис. 2.4) в залежності від завантаженості ЦПМ R1. А на рис. 2.9 представлений графік, який відображає з якою інтенсивністю необхідно передавати ПП, щоб завантажити ЦПМ на 1% в залежності від середньої швидкості передачі ПП через заданий маршрутизатор.

Рис. 2.8. Залежність затримки ERQ-ERL від завантаженості ЦПМ R1 в процесі маршрутизації пакетів

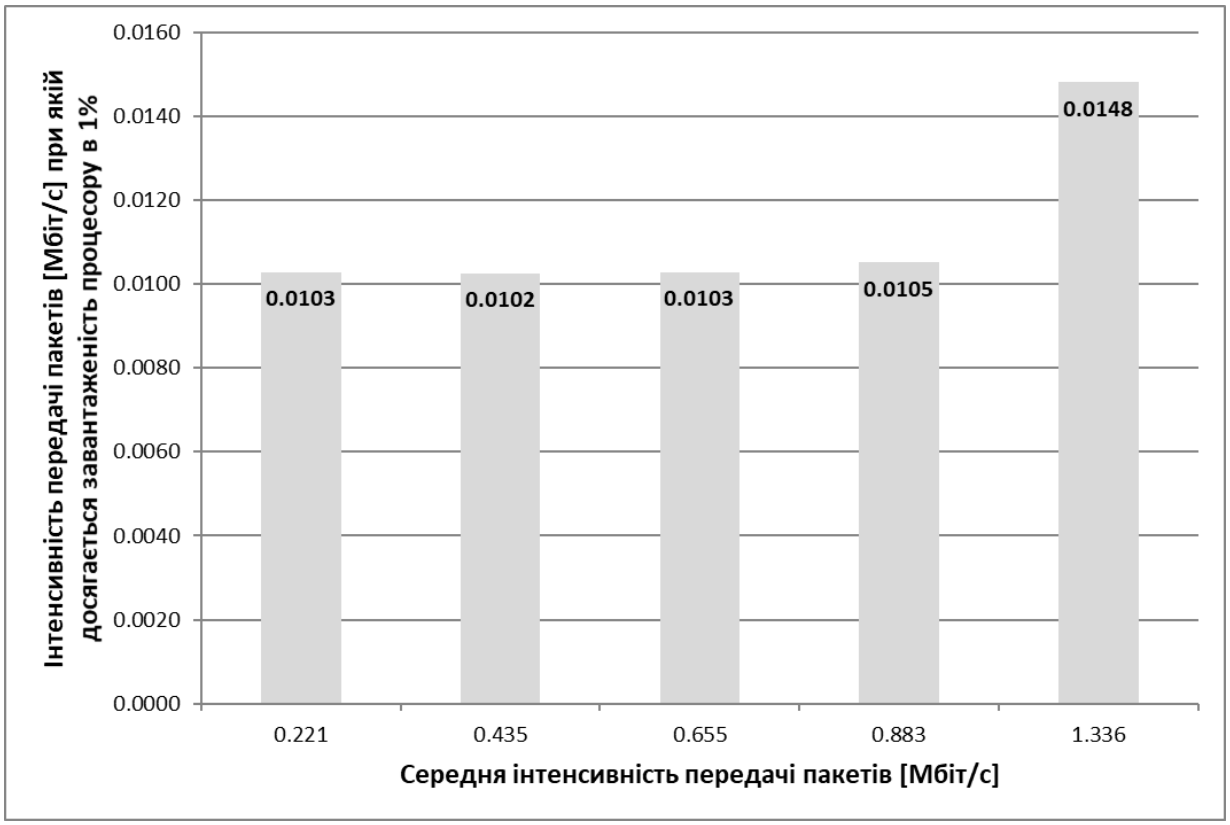


Рис. 2.9. Залежність необхідної інтенсивності передачі ПП для створення завантаженості ЦПМ в 1% в процесі маршрутизації від середньої інтенсивності передачі ПП на маршрутизатор R1

Зміна в затримці в даному експерименті відображає саме збільшення в затримці прийняття рішення при маршрутизації пакетів, а не безпосередньої обробки пакетів (тобто, в такій ситуації, коли пакети призначені лише для маршрутизації, а сам маршрутизатор не є їх кінцевим одержувачем). Маючи цю статистику можна розрахувати наступний параметр:

$$D_{1\%} = \frac{L_{зат.,ср.,t} - L_{зат.,ср.,t-1}}{L_{CPU,ср.,t} - L_{CPU.,ср.,t-1}}, \quad (2.11)$$

де $L_{зат.,ср.,t}$ – усереднене значення затримки в експерименті t;

$L_{CPU,ср.,t}$ – усереднене значення завантаженості ЦПМ в експерименті t.

Параметр $D_{1\%}$ вказує, наскільки зміниться затримка доставки ПП при завантаженості центрального процесора маршрутизатора в 1%. Даний показник дозволяє зв'язати параметр затримки доставки ПП з параметром завантаженості ЦПМ.

Параметр $D_{1\%}$ безпосередньо пов’язаний з параметром $V_{1\%}$. Так $V_{1\%}$ вказує на те, з якою інтенсивністю потрібно передавати ПП, щоб завантажити ЦПМ на 1%, а $D_{1\%}$ вказує на те, наскільки при цьому збільшитися затримка передачі ПП.

За допомогою параметрів $D_{1\%}$ та $V_{1\%}$ можна:

- варіювати швидкість передачі даних через певний маршрутизатор в ТКМ для забезпечення заданого рівня затримки передачі ПП;
- передбачати чи витримає маршрутизатор додаткове навантаження зі збереженням необхідного рівня затримки передачі ПП;
- розраховувати ризик перевантаженості ЦПМ;
- забезпечити перемаршрутизацію трафіку за маршрутами з найменшим ризиком перевантаженості ЦПМ.

Розраховуючи значення $D_{1\%}$ необхідно враховувати, що у формулі враховується середнє значення затримки на поточному та попередньому кроці і ця вимога обов'язково повинна бути дотримана. Так як в нашому досліді проведено 5 експериментів, то отримано 4 значення даного параметру:

$$D_{1\%,t=2} = 0{,}00019,\ D_{1\%,t=3} = 0{,}00114,\ D_{1\%,t=4} = 0{,}00107,\ D_{1\%,t=5} = 0{,}00011.$$

Усереднені простою арифметичною середньою функцією значення параметрів $D_{1\%}$ та $V_{1\%}$ для даного досліду:

$$D_{1\%} = 0{,}00063 \text{ мс},\ V_{1\%} = 0{,}0112 \text{ мбіт/с}.$$

Аналізуючи усереднені показники, представлені вище можна зробити висновок, що при збільшенні швидкості передачі даних на 11 кбіт/с маршрутизатор R1 вносить додаткові 0,00063 мс затримки в процесі прийняття рішення про маршрутизацію кожного з пакетів.

2.2.1.4. Аналіз результатів третього експерименту з одним маршрутизатором і передачею не шкідливого потоку пакетів

Даний експеримент відрізнявся тим, що в топології використовується один маршрутизатор до різних портів якого підключені клієнт і сервер. Також в даному експерименті відсутній ПП, що генерується програмою t50, замість нього клієнт скачує файл об'ємом в 5 ГБ з сервера за допомогою протоколу передачі файлів через безпечний протокол доступу до командної строки (Secure Shell File Transport Protocol, SFTP). Результати даного експерименту можна застосовувати в розрахунках завантаженості процесора при передачі не шкідливого трафіку.

За результатами даного експерименту параметр $V_{1\%} = 3{,}0684$ мбіт/с. В такому випадку, процесор маршрутизатора може забезпечити передачу ПП зі швидкістю понад 300 мбіт/с, що значно більше ПРЗД одного окремо взятого порту

маршрутизатора. Це обумовлюється тим, що маршрутизатор одночасно може приймати і передавати поток пакетів по декількох портам, тому, в даному випадку, оцінюється загальна ПРЗД заданого маршрутизатора.

2.2.1.5. Можливі шляхи застосування параметрів завантаженості центрального процесору маршрутизатору та затримки доставки пакетів в процесі визначення оптимального шляху передачі

Маршрутизатор, який передає дані і не є їх одержувачем, відображає в параметрах показниках $V_{1\%}$ та $D_{1\%}$ залежності інтенсивності передачі ПП і затримки від завантаженості ЦПМ. Позначимо їх як $V_{1\%,\,маршр.,\,i}$ та $D_{1\%,\,маршр.,\,i}$ відповідно, кожен з яких відображає відповідне значення для процесу маршрутизації на i-му маршрутизаторі.

Розрахувавши параметри $V_{1\%,\,маршр.,\,i}$ та $D_{1\%,\,маршр.,\,i}$ для кожного маршрутизатора в шляху можна розрахувати граничну інтенсивність передачі ПП в даному маршруті з урахуванням обмежень для запобігання перевантажень і дотримання граничного значення затримки. Даний підхід може бути реалізований в такий спосіб:

$$V_{max,\,p} = \left\lfloor \frac{D_{max,\,p} - L_{зад.,t,\,p}}{\sum\limits_{i \in p} \frac{D_{1\%,\,маршр.,i}}{V_{1\%,\,маршр.,i}}} \right\rfloor,$$

де $V_{max,\,p}$ – максимально допустима інтенсивність передачі ПП в шляху p з урахуванням обмежень;

D_{max} – максимально допустима затримка в шляху p;

$L_{зад.,t}$ – оцінка затримки в момент часу t для шляху p;

$\sum_{i \in p} \frac{D_{1\%,\,маршр.,i}}{V_{1\%,\,маршр.,i}}$ – сума співвідношення параметрів $V_{1\%,\,маршр.,i}$ та $D_{1\%,\,маршр.,i}$ для усіх транзитних маршрутизаторів i, які входять в шлях p.

Для запобігання перевантажень ЦПМ на маршрутизаторах в заданому шляху, необхідно ввести додаткове обмеження:

$$V_{max,\,p} \le \left\lfloor \min_{i \in p} \left(V_{1\%,\,маршр.,i} \cdot \left(L_{CPU,\,max,\,i} - L_{CPU,\,i,\,t} \right) \right) \right\rfloor, \; при \;\; i \in p, \qquad (2.12)$$

де $V_{1\%,\,маршр.,i}$ – значення параметру $V_{1\%,\,маршр.,i}$ маршрутизатора i, який входить в шлях p;

$L_{CPU,\,max,\,i}$ – максимальне значення завантаженості ЦПМ на маршрутизаторі i, який входить в шлях p;

$L_{CPU,\,i,\,t}$ – оцінка завантаженості ЦПМ на маршрутизаторі i, який входить в шлях p, в момент часу t, при цьому проводиться пошук мінімального значення на всіх маршрутизаторах в заданому шляху p.

Якщо умова (2.12) не виконується, то

$$V_{max,\,p} = \left\lfloor \min_{i \in p} \left(V_{1\%,\,маршр.,i} \cdot \left(L_{CPU,\,max,\,i} - L_{CPU,\,i,\,t} \right) \right) \right\rfloor, \; при \;\; i \in p. \qquad (2.13)$$

Слід зазначити, що значення параметрів D_{max} та $L_{CPU,\,max,\,i}$ задаються адміністратором мережі. Параметр D_{max} може бути визначений для всієї ТКМ в цілому, а може бути заданий для кожного шляху окремо. Параметр $L_{CPU,\,max,\,i}$ може бути заданий однаковим для всієї ТКМ в цілому, а може бути заданий для кожного маршрутизатора окремо, при цьому стандартно $L_{CPU,\,max,\,i} = 99$.

Параметр $V_{max,\,p}$ може бути використаний в процесі вибору шляху для передачі даних в мережі. Чим більше значення параметру $V_{max,\,p}$, тим більше доступного для використання ЦПМ у маршрутизаторів заданого шляху для здійснення маршрутизації ПП.

2.2.1.6. Фактори, що впливають на завантаженість центрального процесору маршрутизатора в процесі передачі потоку пакетів

Параметри $V_{1\%}$ та $D_{1\%}$ залежать від факторів, які можуть впливати на процес маршрутизації ПП заданим вузлом і привести до зміни завантаженості ЦПМ:

1. Алгоритмів обробки трафіку даним маршрутизатором. Наприклад, на маршрутизаторах компанії Cisco використовується технологія «експрес передачі» компанії Cisco (Cisco Express Forwarding, CEF), яка дозволяє проводити процес маршрутизації ПП на спеціальних фізичних модулях, не використовуючи ресурси ЦПМ [105, 106]. У статті [107] компанія Cisco аргументує вибір того чи іншого алгоритму обробки і маршрутизації ПП, а в статті [108] вказується, що пакети, які не можуть бути передані за допомогою CEF, призводять до збільшення споживання ресурсів ЦПМ.
2. Характеристик ПП, що подається на маршрутизатор. Наприклад, в роботах [109, 110] показано як в залежності від довжин пакетів і кількості пакетів, що подаються на маршрутизатор, може змінюватися ступінь впливу переданого ПП на завантаженість ЦПМ.
3. Активністю додаткових мережевих служб, які можуть впливати на порядок обробки ПП. Наприклад, в статтях [109, 111] наведені дослідження зі зміни ступеня впливу переданого на маршрутизатор ПП на ЦПМ в разі використання протоколу трансляції мережевих адрес (Network Address Translation, NAT) і листів доступу відповідно. В статті [112] серед інших причин, що впливають на завантаженість ЦПМ також вказані: шифрування та фрагментація ПП.

Параметр завантаженості ЦПМ $L_{CPU,i,t}$ залежить не тільки від переданого на маршрутизатор ПП, а й від багатьох інших факторів. Наприклад, наведені дослідження, які вказують, що процес протоколу граничного шлюзу (Border Gateway Protocol, BGP) може здійснювати значний вплив на ЦПМ [113, 116]. Також представлено багато інших факторів, що впливають на доступність ЦПМ на маршрутизаторах Cisco, серед яких: різні мережеві процеси, комунікація по телетайп (TeleTYpe, TTY) лініях, SNMP, BGP, передача ПП в обхід CEF, кадри ARP і ПП протоколу міжмережевого обміну пакетами (Internetwork Packet Exchange, IPX), та інші [112-120]. Також можливе підвищення споживання ресурсів ЦПМ в разі його зараження маршрутизатора шкідливим програмним забезпеченням, або різних атаках, які можуть привести до надмірного використання ресурсів ЦПМ легітимними мережевими сервісами.

2.2.2. Метод розрахунку ризику інформаційної безпеки шляху на основі ймовірності своєчасної доставки ПП в залежності від покажчику завантаженості центрального процесору маршрутизаторів

В даному пункті представлено динамічний метод визначення РІБ, який основний на обчисленні ЙСД ПП на кінцевий вузол. Для визначення ЙСД пропонується використовувати розроблену модель процесу маршрутизації ПП 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 ПРЗД вузлу, чи взагалі виводять його з ладу; атак на перемаршрутизацію даних по не ефективним шляхам. Використання моделі дозволяє оцінювати ЙСД пакетів на кінцевий вузол по заданому шляху в залежності від величини вхідного потоку, інтенсивності обробки ПП маршрутизаторами, кількості маршрутизаторів в заданому шляху, та завантаженості центрального процесору маршрутизаторів.

2.2.2.1. Розробка моделі процесу передачі ПП в умовах кібератак

Дослідження з моделювання процесів функціонування складних технічних систем в умовах конфлікту (протидії з боку зловмисників або протиборчих організаційно-технічних систем) здійснено в ряді робіт, наприклад, в [121-123]. Однак питання моделювання процесу функціонування системи передачі потоку пакетів в умовах наявності інформаційних атак в відомій літературі вивчені не були. Саме тому в роботі запропонована нова модель процесу передачі ПП в умовах кібератак, в якій час передачі пакетів від вузла i до вузла j для шляху m можна знайти, використовуючи наступний вираз:

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

де N_m – кількість маршрутизаторів в m-му шляху;

$t_{n,m}^{пер.}$ – час передачі пакетів по КЗ, що прилягав до n-го маршрутизатора m-го шляху;

$t_{n,m}^{обс.}$ – тривалість обслуговування ПП n-м маршрутизатором m-го шляху.

Час обслуговування пакетів маршрутизатором складається з часу очікування пакета в черзі і часу обробки пакета маршрутизатором. Якщо час обробки пакета фіксоване і зазвичай невеликий (від декількох мікросекунд до декількох десятків мікросекунд), то час очікування пакета в черзі коливається в дуже широких межах і є, як правило, випадковою величиною.

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

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

де $\beta_{обс.}$ – інтенсивність обслуговування пакета маршрутизатором з урахуванням часу його обробки і часу очікування пакета в черзі [124];

Параметр $\beta_{обс.}$ розраховується наступним чином:

$$\beta_{обс.} = \mu \cdot (1 - \rho), \text{ при } \rho = \frac{\lambda}{\mu},$$

$$\text{тобто } \beta_{обс.} = \mu - \lambda, \tag{2.14}$$

де λ – інтенсивність ПП на вході маршрутизатора;

μ – інтенсивність обробки ПП маршрутизатором.

Для визначення щільності розподілу ймовірності часу передачі пакетів від вузла i до вузла j для m-го шляху $f_m(t)$ необхідно провести згортку щільностей розподілення $f_{m,обс._n}(t)$, при $n = [1; N_m]$ для всіх маршрутизаторів m-го шляху:

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

де згортка двох щільностей розподілення, наприклад $f_{m,обс._1}(t)$ та $f_{m,обс._2}(t)$ визначається виразом:

$$f_{m,обс._{1,2}} = \int_{-\infty}^{+\infty} f_{m,обс._1}(\tau) \cdot f_{m,обс._2}(t - \tau) dt.$$

У разі, коли кількість вузлів в шляху три і більше, завдання згортки щільності розподілу $f_{m,обс._n}(t)$ є трудомісткою задачею.

Якщо прийняти припущення, що випадковий час обслуговування ПП маршрутизаторами ТКМ є незалежні величини, і час затримки пакетів в шляху визначається сумою часу обслуговування ПП кожним маршрутизатором, то щільність розподілу ймовірності часу передачі ПП від вузла i до вузла j можна описати Гамма розподілом. При цьому щільність розподілу $f_m(t)$ визначається наступним виразом:

$$f_m(t) = \frac{\beta_{обс.}^{\alpha}}{\Gamma(\alpha)} \cdot t^{\alpha-1} \cdot e^{-\beta_{обс.} \cdot t},$$

де $\Gamma(\alpha)$ – функція Ейлера другого порядку.

Однак великим недоліком даної моделі є припущення однакових умов функціонування всіх маршрутизаторів досліджуваного шляху передачі. В умовах, коли DoS атаці піддається один або декілька маршрутизаторів в шляху, таке припущення некоректне.

Відомо, що у разі застосування перетворення Лапласа, згортку функцій можна звести в просторі зображень до операції множення. Зворотне перетворення Лапласа дозволяє отримати шукану функцію дійсної змінної. Тому в даній роботі пропонується вдосконалена модель, в якій функціонування кожного маршрутизатора описується в вигляді моделі M/M/1 з різними параметрами λ та μ, згортка щільностей розподілу $f_{m,обс._n}(t)$ часу обслуговування ПП маршрутизаторами замінюється перетворенням Лапласа, проводиться перемноження зображень даних функцій та отримується шукана щільність розподілу часу передачі ПП по шляху зворотним перетворенням Лапласа.

Інтегрування щільності розподілу ймовірності часу передачі ПП від вузла i до вузла j для m-го шляху $f_{m,обс._n}(t)$ за часом дозволяє визначити ймовірність доставки пакетів до кінцевого вузла за заданий час:

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

Приклад розрахунку щільності розподілу ймовірності часу передачі пакетів від вузла i до вузла j представлено на графіках а) зліва на рис. 2.10-2.12. ЙСД ПП до кінцевого вузла в залежності від часу представлені на графіках б) праворуч на рис. 2.10-2.12.

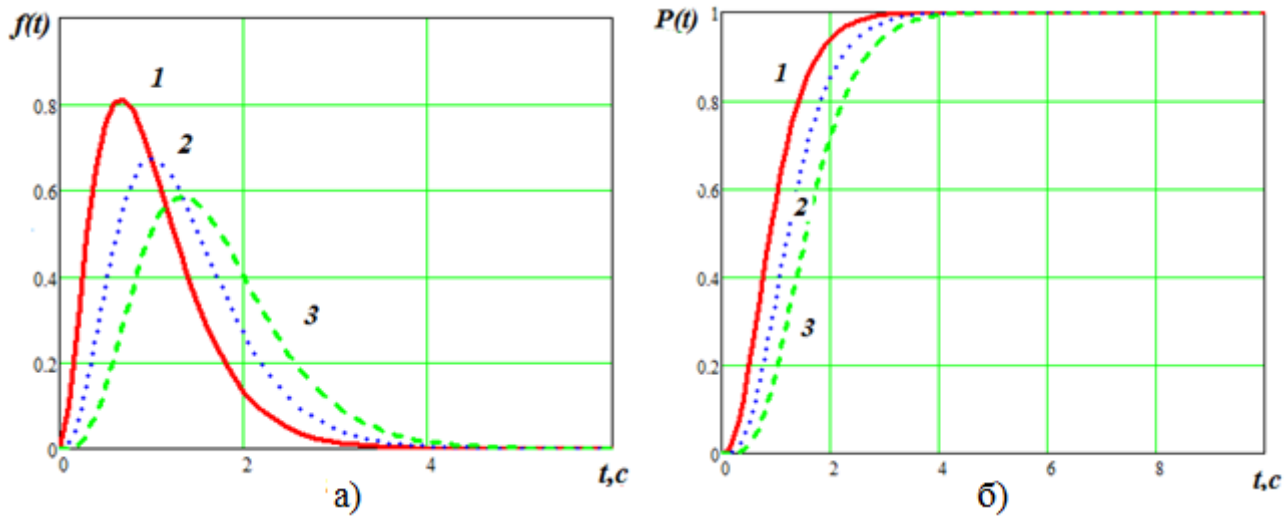


Рис. 2.10. Щільності розподілу часу передачі ПП та ЙСД ПП в залежності від часу при однаковій кількості маршрутизаторів і їх завантаженості в шляхах передачі

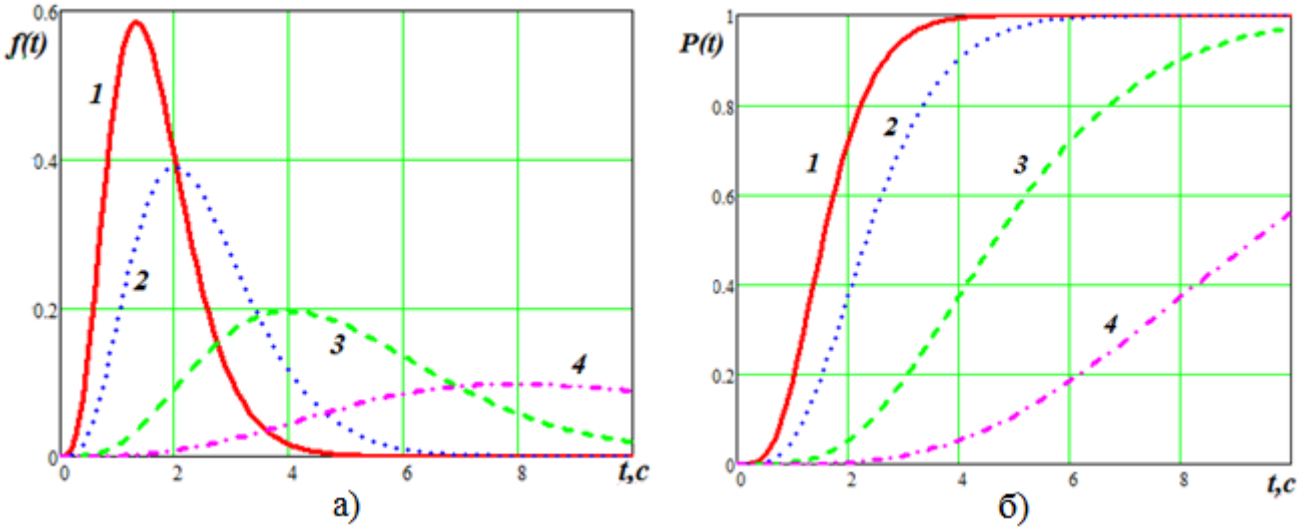


Рис. 2.11. Щільності розподілу часу передачі пакетів та ЙСД ПП в залежності від часу для одного шляху з 4 маршрутизаторами з їх рівномірно змінною завантаженістю

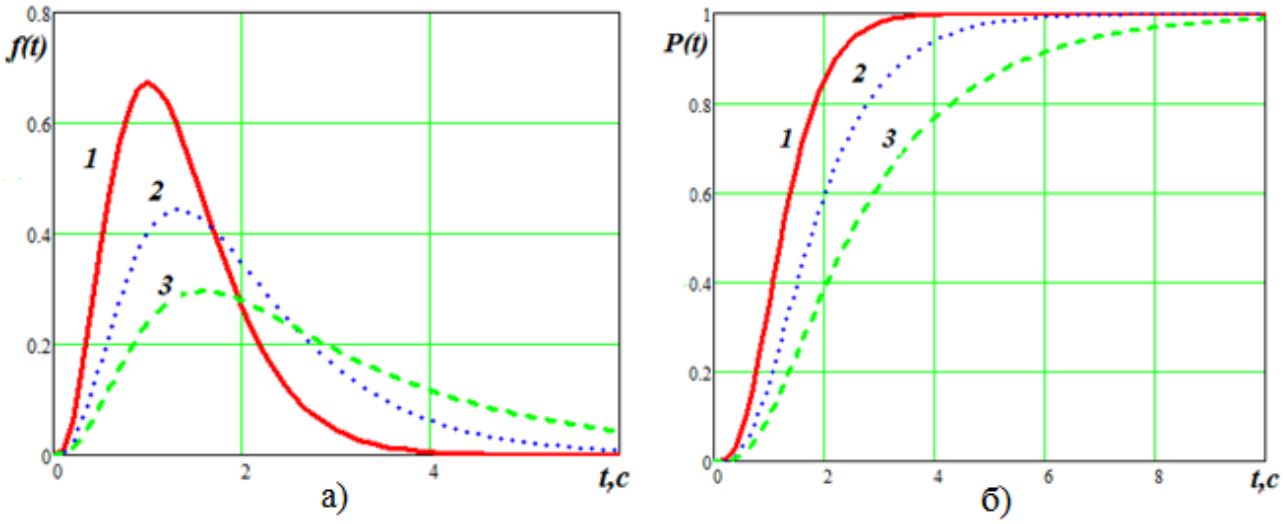


Рис. 2.12. Щільності розподілу часу передачі ПП та ЙСД ПП в залежності від часу для одного шляху, що містить 4 маршрутизатора зі змінною завантаженістю одного з них

На рис. 2.10 представлені графіки з трьома кривими на кожному з них, де номери кривих позначають наступні ситуації:

- 1 – шлях з 3 маршрутизаторами, на кожному з яких $\rho = 0{,}7$;
- 2 – шлях з 4 маршрутизаторами, на кожному з яких $\rho = 0{,}7$;
- 3 – шлях з 5 маршрутизаторами, на кожному з яких $\rho = 0{,}7$;

На рис. 2.11 представлені графіки з чотирма кривими на кожному з них, де номери кривих позначають наступні ситуації:

- 1 – шлях з 4 маршрутизаторами, на кожному з яких $\rho = 0{,}7$;
- 2 – шлях з 4 маршрутизаторами, на кожному з яких $\rho = 0{,}8$;
- 3 – шлях з 4 маршрутизаторами, на кожному з яких $\rho = 0{,}9$;
- 4 – шлях з 4 маршрутизаторами, на кожному з яких $\rho = 0{,}95$;

На рис. 2.12 представлені графіки з трьома кривими на кожному з них, де номери кривих позначають наступні ситуації:

- 1 – шлях з 4 маршрутизаторами, на кожному з яких $\rho = 0{,}7$;
- 2 – шлях з 4 маршрутизаторами, в якому на трьох маршрутизаторах $\rho = 0{,}7$, а на одному маршрутизаторі $\rho = 0{,}9$;
- 3 – шлях з 4 маршрутизаторами, в якому на трьох маршрутизаторах $\rho = 0{,}7$, а на одному маршрутизаторі $\rho = 0{,}95$;

Наведена модель дозволяє оцінити ЙСД ПП за заданий час в різних ситуаціях, наприклад: в разі, коли ТКМ функціонує в нормальному режимі, або, коли на ТКМ здійснюється атака, що впливає на час доставки пакетів. Так на рис. 2.10 відображена ситуація для нормального функціонування ТКМ. На рис. 2.11 відображена ситуація при якій в мережі поступово вичерпуються ресурси маршрутизаторів. На рис. 2.12 відображена ситуація, коли один з маршрутизаторів в маршруті піддається DoS атаці.

Наведемо приклад використання запропонованої моделі. Для цього розглянемо топологію ТКМ, яка представлена на рис. 2.13.

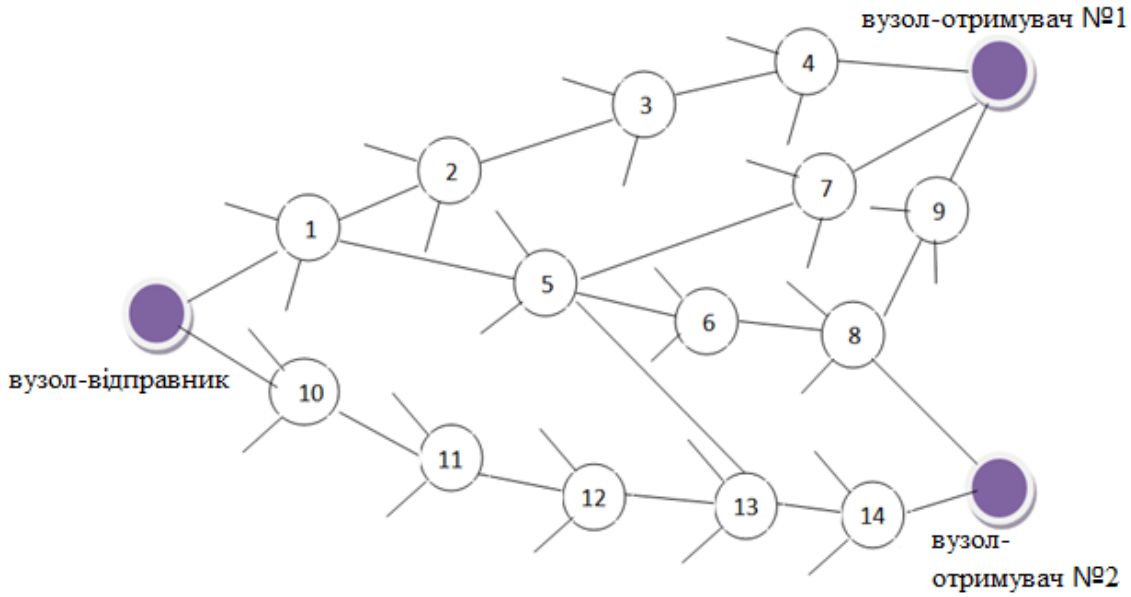


Рис. 2.13. Топологія ТКМ з одним вузлом-відправником та двома вузлами-отримувачами ПП

В топології на рис. 2.13 зображено вузол-відправник, два вузла-отримувача та 14 проміжних вузлів. Далі, в даному підпункті, під вузлами будемо розуміти маршрутизатори ТКМ.

Шляхи передачі ПП від вузла-відправника до вузла-отримувача №1:

- шлях №1 – вузол-відправник→1→2→3→4→вузол-отримувач №1;
- шлях №2 – вузол-відправник→1→5→7→ вузол-отримувач №1;
- шлях №3 – вузол-відправник→1→5→6→8→9→ вузол-отримувач №1.

Шляхи передачі ПП від вузла-відправника до вузла-отримувача №1:

- шлях №4 – вузол-відправник→10→11→12→13→14→вузол-отримувач №2;
- шлях №5 – вузол-відправник→1→5→6→8→вузол-отримувач №2;
- шлях №6 – вузол-відправник→1→5→13→14→вузол-отримувач №2.

Всі проміжні маршрутизатори є елементами інших шляхів передачі і навантаження на них також може створювати ПП інших абонентів ТКМ.

Припустимо, що в нормальних умовах функціонування ПП в ТКМ збалансований і для всіх маршрутизаторів $\rho = 0{,}7$. Оцінимо ймовірність доставки

пакетів за даними шляхами за час 2 с. Даний час вибрано в демонстративних цілях і без урахування існуючих вимог QoS або вимог до військових ТКМ.

При таких умовах ЙСД ПП буде наступною:

- для шляху №1 – $P_{1,дост.}(t) = 0{,}849$;
- для шляху №2 – $P_{2,дост.}(t) = 0{,}938$;
- для шляху №3 – $P_{3,дост.}(t) = 0{,}715$;
- для шляху №4 – $P_{4,дост.}(t) = 0{,}715$;
- для шляху №5 – $P_{5,дост.}(t) = 0{,}849$;
- для шляху №6 – $P_{6,дост.}(t) = 0{,}849$.

ЙСД ПП за 2 с від вузла відправника до вузла-отримувача №1 складає 0,997; до вузла-отримувача №2 – 0,994.

Оцінимо збільшення часу затримки ПП при повному виході з ладу вузлів в разі їх вогневого чи електромагнітного ураження, або DoS атаки. При цьому будуть виходити з ладу ті шляхи передачі ПП, в які входить атакований вузол.

Дані розрахунки проведемо для різних ситуацій штатної роботи ТКМ. Під такими різними ситуаціями будемо розуміти різну ступінь завантаженості маршрутизаторів ТКМ ПП: від нормальної завантаженості до перевантаження. Тобто для розрахунків виберемо показник $\rho_1 = 0{,}7$, $\rho_2 = 0{,}8$, $\rho_3 = 0{,}9$, $\rho_4 = 0{,}95$. При цьому завантаженість маршрутизаторів в ТКМ є рівномірною.

Результати представлені в табл. Д1-Д4 з яких можна зробити розрахунок середньої ЙСД ПП по всіх маршрутах до вузла-отримувача №1 та №2 відповідно для різної величини параметру ρ на маршрутизаторах ТКМ:

- при $\rho_1 = 0{,}7$ середня ЙСД ПП до вузла-отримувача №1 складає приблизно 0,908, а для вузла-отримувача №2 – приблизно 0,943;
- при $\rho_2 = 0{,}8$ середня ЙСД ПП до вузла-отримувача №1 складає приблизно 0,8, а для вузла-отримувача №2 – приблизно 0,759;
- при $\rho_3 = 0{,}9$ середня ЙСД ПП до вузла-отримувача №1 складає приблизно 0,352, а для вузла-отримувача №2 – приблизно 0,236;

- при $\rho_4 = 0{,}95$ середня ЙСД ПП до вузла-отримувача №1 складає приблизно 0,077, а для вузла-отримувача №2 – приблизно 0,032.

Таким чином, дана модель дозволяє враховувати погіршення показника ЙСД ПП за заданий час в разі здійснення різного роду атак на інфраструктуру ТКМ. Дана модель відкриває нові можливості дослідження впливу атак на QoS в ТКМ, а також дозволяє використовувати отримані результати для удосконалення процесу вибору оптимального шляху протоколами динамічної маршрутизації.

2.2.2.2. Удосконалення моделі передачі потоку пакетів в умовах кібератак шляхом врахування параметру завантаженості центрального процесору маршрутизаторів для оцінки ризику інформаційної безпеки шляху на основі ймовірності своєчасної доставки потоку пакетів на кінцевий вузол

Для удосконалення запропонованої полумарковської моделі маршрутизації ПП в умовах кібератак пропонується динамічно змінювати інтенсивность обслуговування пакета маршрутизатором з урахуванням часу його обробки і часу очікування пакета в черзі $\beta_{обс.}$, який в стандартному вигляді розраховується за формулою (2.14), шляхом врахування параметру завантаженості ЦПМ. Для цього скористаємося результатами досліджень, отриманих в пункті 2.2.1, а також введемо наступне обмеження $\beta_{обс.} \le \mu - \lambda$ внаслідок того, що запропонована формула розрахунку залишкової ПРЗД не враховує ні інтенсивності обробки ПП маршрутизатором, ні інтенсивності вхідного ПП, тоді:

$$\left.\begin{array}{c} \beta_{обс.} = \left\lfloor V_{1\%,\,маршр.,i} \cdot \left(L_{CPU,\,max,\,i} - L_{CPU,i,t}\right) \right\rfloor, \text{ при } \beta_{обс.} \le \mu - \lambda \\ \beta_{обс.} = \mu - \lambda, \text{ при } \beta_{обс.} > \mu - \lambda \end{array}\right\}, \qquad (2.15)$$

де $V_{1\%,маршр.,i}$ – значення параметру $V_{1\%,\,маршр.,i}$ маршрутизатор i;

μ – інтенсивність обробки ПП маршрутизатором;

λ – інтенсивність ПП, що поступає на маршрутизатор;

$L_{CPU,\,max,\,i}$ – максимальне значення завантаженості ЦПМ на маршрутизаторі i;

$L_{CPU,i,t}$ – оцінка завантаженості ЦПИ на маршрутизаторі i в момент часу t.

При цьому

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

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

$L_{CPU,ПП}$ – завантаженість ЦПМ внаслідок маршрутизації ПП.

Фізичний сенс формули (2.15) полягає в тому, що інтенсивність обробки пакетів маршрутизатором безпосередньо залежить від завантаженості ЦПМ. Наприклад, якщо маршрутизатор виконує складні операції побудови об'ємної таблиці маршрутизації і перераховує оптимальність шляхів, то його ресурсів може не вистачити на обробку пакетів, що надходять із заявленою швидкістю портів. Така ж ситуація спостерігається в разі здійснення цілеспрямованої DoS атаки на маршрутизатор.

Параметр $\beta_{обс.}$ розраховується для кожного маршрутизатору окремо та залежить від типу ПП, що подається на маршрутизатор, і алгоритмів обробки ПП даним маршрутизатором.

Як приклад, розглянемо наступну ситуацію. Припустимо, що всі маршрутизатори в топології на рис. 2.13 є маршрутизаторами моделі Cisco 2801 стандартної конфігурації, на яких встановлена операційна система IOS 12.4 (12). Також припустимо, що в мережу передається поток пакетів SFTP, а на маршрутизаторах активна технологія CEF.

Завдання полягає в оцінці ЙСД ПП від вузла-відправника для вузла-отримувача №1 при передачі ПП по одному оптимальному шляху. Припустимо, що оптимальним шляхом доставки пакетів, в даному випадку, є шлях: вузол-відправник №1 → вузол №1 → вузол №5 → вузол №7 → вузол-отримувач. Розглянемо два випадки:

- коли ЦПМ всіх маршрутизаторів в шляху завантажені однаково $L_{CPU,R1} = L_{CPU,R5} = L_{CPU,R7}$ та на них впливає процес маршрутизації SFTP ПП, що передається з інтенсивністю $\lambda = 70$ мбіт/с;
- коли ЦПМ на маршрутизаторі №1 завантажений більше на 70% внаслідок роботи системних процесів $L_{CPU,процесів} = 70$, при цьому інтенсивність ПП така ж я к і в першому випадку.

Швидкість всіх КЗ в маршруті дорівнює 100 мбіт/с. Наведемо завантаженість ЦПМ для першого і другого випадків:

- $L_{CPU,R1} = L_{CPU,R5} = L_{CPU,R7} = 23$;
- $L_{CPU,R1} = 93$; $L_{CPU,R5} = L_{CPU,R7} = 23$.

Розрахуємо параметр $\beta_{обс.}$ для оптимального шляху передачі для першого і другого випадків для першого випадку по формулі (2.15). Для того, щоб розрахувати параметр $\beta_{обс.}$ для всього шляху одночасно, а не для кожного маршрутизатору окремо, використаємо обмеження (2.12)-(2.13). Тоді:

- для першого випадку $\beta_{R1,\ R2,\ R3} = \lfloor 3{,}0684 \cdot (99 - 23) \rfloor = 30$ мбіт/с;
- для другого випадку $\beta_{R1,\ R2,\ R3} = \lfloor 3{,}0684 \cdot (99 - 93) \rfloor = 18{,}41$ мбіт/с.

Виходячи з вищенаведеного прикладу, якщо ЦПМ на маршрутизаторі №1 завантажений на 90%, то по заданому шляху передавати ПП на швидкості вище 88,41 мбіт/с не має сенсу, так як ЦПМ перенавантажиться і маршрутизатор почне відкидати пакети.

Знайдемо ЙСД ПП по заданому шляху за 150 мс:

- для першого випадку – $P_{1,дост.}(t) = 0{,}826$;
- для другого випадку – $P_{1,дост.}(t) = 0{,}521$.

З вищенаведеного прикладу видно, що завантаженість ЦПМ на одному з маршрутизаторів значно знизила можливу інтенсивність обробки ПП в шляху передачі, тим самим зменшивши ЙСД ПП по заданому шляху.

2.2.2.3. Розрахунок ризику інформаційної безпеки транзитного потоку пакетів для заданого шляху за допомогою вдосконаленої моделі передачі потоку пакетів в умовах кібератак

На основі представленої в даному пункті вдосконаленої моделі пропонується розраховувати ризик несвоєчасної доставки ПП отримувачу:

$$R_{m,дост.} = (1 - P_{m,дост.}) \cdot P_{загрози}\ , \tag{2.16}$$

де $(1 - P_{m,дост.})$ – ймовірність несвоєчасної доставки ПП отримувачу по шляху m; $P_{загрози}$ – ймовірність реалізації загрози, що призводить до зниження ЙСД ПП отримувачу.

Так як параметр $P_{загрози}$ обчислюється на основі багатьох факторів, а його розрахунок складно автоматизувати, то в даній роботі пропонується допустити, що $P_{загрози} = 1$. Тоді формула (2.16) приймає наступний вигляд:

$$R_{m,дост.} = 1 - P_{m,дост.}. \tag{2.17}$$

Виходячи з формули (2.17) можна зробити висновок, що $R_{m,дост.} \in [0;1]$, а також $P_{m,дост.}$ розраховується на основі математично обґрунтованих показників, що відповідає критеріям щодо параметрів РІБ, які встановлено в першому розділі.

Наведений в даному підпункті метод розрахунку параметру РІБ дозволяє оцінити РНД ПП отримувачу та використовувати даний параметр в процесі вибору оптимального шляху передачі ПП в ТКМ, що може дозволити підвищити критерій доступності та QoS ПП. Також наведений метод дозволяє розраховувати параметр РІБ на основі динамічних показників ТКМ, які можуть збиратися в автоматизованому режимі та не потребують аналізу з боку оператора ТКМ, тим самим повністю виключаючи суб’єктивізм при розрахунках.

В якості недоліків можна виділити те, що збір та аналіз усіх динамічних показників, необхідних для проведення розрахунків, потребують постійної підтримки зв’язку та передачі даних на вузли-аналізатори, що збільшує об’єм обміну службовими даними в ТКМ. Також самі розрахунки основані на трудомістких математичних функціях, що може створювати надмірне навантаження на центральний процесор вузлів-аналізаторів.

2.3. Висновки по другому розділу

1. В даному розділі представлено два методи розрахунку РІБ транзитного ПП для заданого шляху передачі. В основі першого методу використовуються статичні параметри ТКМ та її вузлів, тобто такі, які змінюються за тригером: за таймером, після виконання певної події, чи вручну оператором ТКМ. В основі іншого методу використовуються динамічні параметри, які змінюються в реальному масштабі часу та не потребують тригерів.
2. До статичних параметрів РІБ відносяться: критичність вразливостей знайдених на маршрутизаторах ТКМ та ЕММ ТКМ, який відображає зниження ефективності передачі ПП в ТКМ в разі видалення заданого маршрутизатору та всіх його КЗ з ТКМ. До динамічних параметрів РІБ, в даній роботі, відноситься РНД ПП вузлу-отримувачу. Усі параметри РІБ відповідають критеріям, заданим в першому розділі.
3. В РІБ, який розраховується на основі статичних параметрів, пропонується не використовувати обидва параметри одночасно. Для того, щоб проводити автоматичний вибір того чи іншого параметру в формулі розрахунку РІБ використовується додатковий параметр, який розраховується на основі аналізу ентропії потоку пакетів, що передається в ТКМ, та який відображає можливість здійснення в даний момент часу DoS атаки на заданий маршрутизатор ТКМ. Якщо ризик здійснення DoS атаки перевищує задану величину, яку задає оператор ТКМ, то для

розрахунку РІБ використовується параметр ЕММ ТКМ, в іншому випадку використовується параметр критичності вразливостей, знайдених на маршрутизаторах в заданому шляху передачі.

4. При розрахунку РІБ на основі ЕММ оптимальним вибирається шлях з найбільш ефективними маршрутизаторами ТКМ, саме тому, якщо до кінцевого вузла веде декілька шляхів, пропонується передавати по даному шляху довірливий та пріоритетний ПП. Автоматичне визначення довірливості ПП є складною задачею, але адміністратор ТКМ може вручну визначити, наприклад, службові ПП в якості довірливих та задати їх в ACL, який буде використаний в механізмі PBR для перемаршрутизації ПП за різними шляхами передачі.
5. Для розрахунку РІБ на основі ймовірності своєчасної доставки ПП використовується запропонована в даній роботі удосконалена модель передачі ПП в умовах кібератак. Для удосконалення моделі запропоновано та реалізовано врахування залежності впливу інтенсивності передачі на маршрутизатор ПП на завантаженість ЦПМ. Для встановлення даної залежності були проведені досліди на реальному телекомунікаційному обладнанні. В ході досліджень було виведено параметр $V_{1\%}$, який відображає з якою інтенсивністю необхідно подавати ПП на маршрутизатор, щоб завантажити ЦПМ на 1%. Було також встановлено, що даний параметр залежить від типу ПП та додаткових мережевих служб, які можуть бути задіяні на маршрутизаторі. Для шкідливого ПП, що генерується програмою t50 $V_{1\%} = 0{,}1656$ мбіт/с, а для стандартного SFTP ПП $V_{1\%} = 3{,}0684$ мбіт/с. Параметр $V_{1\%}$ дозволив розрахувати залишкову інтенсивність обробки ПП в залежності від завантаженості ЦПМ, в тому числі і шкідливими процесами, які можуть бути на ньому запущені.
6. РНД ПП отримувачу залежить від: інтенсивності передачі ПП в ТКМ, інтенсивності обробки ПП маршрутизаторами ТКМ, кількістю маршрутизаторів в заданому шляху передачі, та завантаженістю ЦПМ в

ТКМ. Даний параметр враховує як критерій доступності так і QoS ПП, що передається в ТКМ.

7. Представлені в даному розділі методи розрахунку РІБ можуть бути використані для їх подальшого врахування в процесах вибору оптимального шляху передачі ПП в ТКМ.

РОЗДІЛ 3
МОДЕЛІ ТА МЕТОДИ ВРАХУВАННЯ РИЗИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПРОЦЕСІ МАРШРУТИЗАЦІЇ ПОТОКУ ПАКЕТІВ

ПДМ визначають оптимальність шляху виходячи з метрики. Метрика має властивість кумулятивності та буде тим більше, чим більше проміжних маршрутизаторів знаходиться між вузлом-відправником і вузлом-отримувачем потоку пакетів. В ПДМ, які досліджуються в даній роботі, в якості критерію оптимальності використовується мінімальна метрика маршруту

$$\min_{p_{i,j} \in P_{i,j}} (M_{p_{i,j}})$$

де $M_{p_{i,j}}$ – мінімальна метрика шляху p між вузлами i, j, при $p_{i,j} \in P_{i,j}$, де $P_{i,j}$ – множина шляхів між вузлами i, j.

Для різних ПДМ метрика розраховується по-різному. Наприклад, для протоколу RIP метрика вимірюється в кількості ретрансляцій пакету, які необхідно здійснити при передачі ПП між вузлами i, j. У протоколі OSPF метрика розраховується на основі ПРЗД КЗ між маршрутизаторами, які знаходяться в шляху передачі ПП між вузлами i, j. Протокол EIGRP, на відміну від OSPF, крім ПРЗД враховує також такі параметри як: затримка, надійність і завантаженість КЗ. В безпроводових ПДМ при розрахунку метрики нерідко можна зустріти параметр залишкового заряду батареї.

В даному розділі пропонуються вдосконалені моделі вибору оптимального шляху передачі ПП в ТКМ для вибраних ПДМ, шляхом врахування РІБ в якості одного з параметрів при розрахунку метрики. Як вказано в першому розділі, варіант врахування РІБ в якості окремого критерію оптимальності розглядатися не

буде, щоб залишити задачу вибору оптимального шляху передачі однокритеріальною.

3.1. Математичні моделі вирішення задачі одношляхової та багатошляхової маршрутизації

Моделі одно,багато-шляхової маршрутизації наведено в роботах [125-128]. Під задачею одношляхової маршрутизації будемо розуміти таку, в якій вибирається єдиний оптимальний маршрут, а багатошляхової – в якій проводиться балансування ПП за різними шляхами.

Опишемо структуру ТКС за допомогою зваженого орієнтованого графа $G=(V,E)$, де множина вершин V моделює множину вузлів ТКМ, а множина дуг E описує множину КЗ між ними. Кожній дузі $(i,j)\in E$ відповідає ПРЗД КЗ $\mu_{i,j}$. Кожному k-му ПП з множини K відповідає ряд параметрів: λ_k, s_k, r_k – інтенсивність k-го ПП, вузол-відправник та вузол-отримувач відповідно. Управляючою змінною служить $X_{i,j}^k$, яка характеризує долю інтенсивності k-го ПП, що передається каналі зв'язку $(i,j)\in E$.

З метою недопущення перевантажень мережевих вузлів і мережі в цілому необхідно забезпечити виконання умов збереження потоку:

$$\left.\begin{aligned}
&\sum_{j:(i,j)\in E} X_{i,j}^k - \sum_{j:(j,i)\in E} X_{j,i}^k = 0,\ k\in K,\ i\neq s_k, r_k,\\
&\sum_{j:(i,j)\in E} X_{i,j}^k - \sum_{j:(j,i)\in E} X_{j,i}^k = 1,\ k\in K,\ i=s_k,\\
&\sum_{j:(i,j)\in E} X_{i,j}^k - \sum_{j:(j,i)\in E} X_{j,i}^k = -1,\ k\in K,\ i=r_k.
\end{aligned}\right\} \qquad (3.1)$$

Умова запобігання перевантаження каналів формалізується наступним чином:

$$\sum_{k \in K} \lambda_k \cdot X_{i,j}^k \le \mu_{i,j} \cdot \alpha, \ (i, j) \in E, \tag{3.2}$$

де α – верхній поріг використання КЗ ТКМ.

Відповідно до фізики розв'язуваної задачі при моделюванні одношляхової маршрутизації на змінні $X_{i,j}^k$ накладається наступне обмеження:

$$X_{i,j}^k \in \{0,1\}. \tag{3.3}$$

При моделюванні багатошляхової маршрутизації ПП обмеження на маршрутні змінні набувають вигляду:

$$0 \le X_{i,j}^k \le 1. \tag{3.4}$$

В ході оптимізації процесу маршрутизації будемо використовувати два типи критеріїв. Для першого типу критерію необхідно мінімізувати цільову функцію, представлену в лінійній формі виду:

$$\mathbf{min} \sum_{(i,j)} M_{i,j} \cdot X_{i,j}, \tag{3.5}$$

де КЗ присвоюється метрика $M_{i,j}$ відповідного ПДМ, формули розрахунку яких будуть представлені далі в цьому розділі.

Таким чином, при моделюванні процесів одношляхової маршрутизації використовуються вирази (3.1)-(3.3) та (3.5), а параметр α приймається константою, що дорівнює одиниці. Завдання одношляхової маршрутизації

сформулюються як оптимізаційна задача з критерієм (3.5) і обмеженнями (3.1)-(3.3).

При моделюванні багатошляхової маршрутизації, коли вибираються кілька шляхів доставки ПП, але рішення задачі маршрутизації в рамках одного ПП носить одношляховий характер – використовуються вирази (3.1)-(3.3), (3.5). В якості критерію оптимальності виступає вираз (3.5), а обмеженнями – вирази (3.1)-(3.3).

При моделюванні багатошляхової маршрутизації з балансуванням навантаження, коли вибираються кілька шляхів доставки ПП, і вирішення завдання маршрутизації в рамках одного ПП також носить багатошляховий характер, то в якості критерію оптимальності виступає вираз (3.5), а в якості обмежень вирази (3.1), (3.2), (3.4).

Вирішення даних задач формалізується як задача булевого програмування, або лінійного-програмування відповідно. Даний підхід можна реалізувати за допомогою процедур bintprog і linprog пакету MATLAB.

Дослідження даної роботи спрямовані на вдосконалення моделі вибору оптимального шляху передачі ПП для одношляхової та багатошляхової маршрутизації з використанням метрик протоколів RIP, OSPF, EIGRP, проте запропоновані підходи можуть бути застосовані і до метрик інших протоколів, як в проводових, так і в безпроводових мережах, що може послужити темою для подальших досліджень.

3.2. Розробка моделі динамічної маршрутизації з урахуванням факторів інформаційної безпеки

У даному розділі представлені вдосконалені 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: ПРЗД, затримка, надійність і завантаженість КЗ.

При даному підході змінюється формула розрахунку критерію оптимальності у виразі (3.5) $M_{i,j}$, який характеризує метрику КЗ. Далі розглядаються запропоновані в даній роботі удосконалення для кожного з вибраних ПДМ.

3.2.1. Аналіз критеріїв врахування ризику інформаційної безпеки шляху в формулах розрахунку метрик

Критерії врахування ризику інформаційної безпеки шляху в формулах розрахунку метрик для протоколів динамічної маршрутизації наведено у підрозділі 1.5. В даному пункті пропонується розглянути можливі формули з врахуванням РІБ та наводиться їх аналіз відповідності зазначеним критеріям.

Введемо наступні позначення:

- M_{old} – метрика шляху, що розраховується за стандартними формулами для відповідного ПДМ;
- M_{new} – формула розрахунку метрики з урахуванням РІБ;
- M_{max} – максимально можливе значення метрики відповідного ПДМ згідно із стандартом;
- R – РІБ транзитного ПП заданого шляху;
- k_r – коефіцієнт, що дозволяє враховувати чи не враховувати РІБ в формулі розрахунку метрики, при цьому $k_r \in \{0;1\}$, при врахуванні РІБ $k_r = 1$, а в іншому випадку $k_r = 0$;
- x – коефіцієнт масштабування, що дозволяє збільшити розкид значень метрики, при цьому $x > 1$. Для подальших досліджень виберемо $x = 16$.

Наведемо можливі формули розрахунку метрики з урахуванням РІБ:

$$M_{new} = \left\lfloor \frac{M_{old} \cdot (1+R)^{k_r}}{2^{k_r}} \right\rfloor, \tag{3.6}$$

$$M_{new} = \left\lfloor \frac{M_{old} + (M_{old})^{R} \cdot k_r}{2^{k_r}} \right\rfloor, \tag{3.7}$$

$$M_{new} = \left\lfloor \frac{M_{old} + (M_{max})^{R} \cdot k_r}{2^{k_r}} \right\rfloor, \tag{3.8}$$

$$M_{new} = \left\lfloor \frac{M_{old} + (M_{max})^{R} \cdot k_r}{(M_{old})^{k_r}} \right\rfloor, \tag{3.9}$$

$$M_{new} = \left\lfloor \frac{M_{old} \cdot x^{R \cdot k_r}}{x^{k_r}} \right\rfloor, \tag{3.10}$$

$$M_{new} = \lfloor M_{old} \cdot x^{R \cdot k_r} \rfloor, \tag{3.11}$$

$$M_{new} = \lfloor M_{old} \cdot x^{(2-(k_r - R \cdot k_r))} \rfloor, \tag{3.12}$$

$$M_{new} = \lfloor (M_{old})^{R \cdot k_r} \rfloor, \tag{3.13}$$

$$M_{new} = \left\lfloor M_{old} - \left\lfloor \frac{(M_{old} - 1)^{k_r}}{(1+R)} \right\rfloor \right\rfloor, \tag{3.14}$$

$$M_{new} = \left\lfloor M_{old} - \left\lfloor \frac{(M_{old} - 1)^{k_r}}{(M_{old})^{R}} \right\rfloor \right\rfloor. \quad (3.15)$$

Для більше детального аналізу необхідно побудувати графіки залежностей метрики від РІБ. Для цього розглянемо топологію, представлену на рис. 3.1.

Рис. 3.1. Топологія для проведення експериментів з впливом РІБ на метрику шляху передачі

В якості дослідної виберемо метрику шляху передачі ПП від маршрутизатора R1 до ТКМ 2. Для того, щоб збільшити значення метрики для ПДМ OSPF та EIGRP приймемо, що ПРЗД КЗ дорівнює 10 мбіт/с. В такому випадку метрика протоколу RIP дорівнює 3, OSPF – 40, а EIGRP – 1400.

Залежності метрики від РІБ для протоколу RIP наведено у додатку Е. Так як метрика протоколу RIP може приймати значення лише в діапазоні від 1 до 15, то необхідно вибрати метод, який дає, в тому числі, найбільшу кількість унікальних значень метрики в залежності від РІБ. Найбільша кількість змін значень спостерігається на графіках на рис. Е.6 та рис. Е.7, тобто підходящими можуть бути формули (3.11) та (3.12). Але якщо проаналізувати формули (3.11)-(3.12), то можна зробити висновок, що значення метрики може зрости у x^R чи x^2 разів відповідно, і якщо для протоколів OSPF чи EIGRP, в яких метрика може вимірюватися мільйонами, такі варіанти можуть бути прийняті до розгляду, то для протоколу RIP, в якого метрика не може перевищувати 15 – такі варіанти врахування РІБ не можуть бути оптимальними.

Відкинувши формули (3.11)-(3.12) та проаналізувавши решту графіків, можна зробити висновок, що оптимальним є графік на рис. Е.3 який відповідає формулі (3.8). Виходячи з формули (3.8) метрика не буде перевищувати стандартні

межі значень метрики, які описані у відповідних стандартах ПДМ, тобто для RIP значення метрики, з використанням формули (3.8), будуть лежати в межах [1;15].

Для протоколу OSPF максимальне значення метрики дорівнює ($2^{24}-1$), в такому випадку експоненційне зростання метрики з урахуванням РІБ $M_{new,OSPF}$ у порівнянні з її початковою величиною $M_{old,OSPF}$ без врахування РІБ може спричинити зростання метрики вище максимальної величини та призвести до недосяжності шляху передачі. Таким чином, пропонується вибирати таку формулу врахування РІБ в формулі розрахунку метрики OSPF, яка при $R=1$ призводить до $M_{new,OSPF}=M_{old,OSPF}$ та має експоненційне зростання. Проаналізувавши графіки у додатку Ж можна зробити висновок, що такими виступають: формула (3.7), якій відповідає графік на рис. Ж2, формула (3.10), якій відповідає графік на рис. Ж.5, та формула (3.13), якій відповідає графік на рис. Ж.8. Але наведені формули мають свої недоліки:

- формула (3.7) надає дуже малого розкиду значень вихідної метрики, так як мінімальне значення метрики може бути не нижче $\frac{M_{old}}{2}$;
- для максимізації розкиду значень метрики при використанні формули (3.10) необхідно, щоб $x=\left\lfloor \frac{M_{old,OSPF}}{2} \right\rfloor+1$. Проблеми з використанням формули (3.10) починаються у випадку її використання в ТКМ з великою різницею в значеннях метрик шляхів. Наприклад, уявимо, що існує $M1_{old,OSPF}$ та $M2_{old,OSPF}$ при цьому $M1_{old,OSPF} >> M2_{old,OSPF}$. Так як x повинен бути однаковим в рамках всієї ТКМ, то, якщо вибрати $x=\left\lfloor \frac{M1_{old,OSPF}}{2} \right\rfloor+1$, то так як x знаходиться в знаменнику виразу (3.10), то це з великою ймовірністю призведе до того, що $M2_{new,OSPF}$ для деяких значень R буде дорівнювати 0. Якщо ж $x=\left\lfloor \frac{M2_{old,OSPF}}{2} \right\rfloor+1$, то це з

великою ймовірністю призведе до того, що вираз (3.10) втратить властивість експоненційного зростання в залежності від R та наблизиться до лінійної залежності, що не відповідає критеріям РІБ;

- формула (3.13), в свою чергу також не відповідає критеріям РІБ, який стосується врахування стандартних параметрів метрики вибраного ПДМ, так як при $R \cdot k_r = 0$ метрика завжди дорівнює одиниці, що призводить до тотального пригнічення параметром РІБ стандартних параметрів метрики OSPF;
- у табл. Ж.1 наведені залежності M_{new} від M_{old} та R для наведених формул; з табл. Ж.1 можна зробити висновок, що усі три формули мають повторювання значень вихідної метрики для $M_{old} \leq 64$, що не є прийнятним.

Виходячи з наведених недоліків пропонується вибрати підхід за аналогією з EIGRP, в якому основні параметри метрики помножуються на коефіцієнт масштабування, в даному випадку ним виступає x. В якості таких виступають формули (3.11) та (3.12). За аналогією з EIGRP пропонується вибрати $x = 256$, а також накласти умову, що якщо $R = 0$, то $M_{new} = M_{old}$. В такому випадку вибираємо формулу (3.11).

В формулі розрахунку метрики протоколу EIGRP присутній коефіцієнт масштабування – назвемо його c_{scale}, який стандартно дорівнює 256 та покликаний збільшити розкид значень метрики [72]. В даній роботі пропонується зберегти максимально наближену до оригіналу формулу, тобто вибрати формули де x може виступати в ролі c_{scale}. В такому випадку найбільш підходящими є формули (3.11), (3.12). У додатку И наведено графіки до цих формул. Якщо порівняти графіки на рис. И.1 та рис. И.2, то можна зробити висновок, що графік на рис. И.1 відображає менш однорідну залежність значення метрики від ризику, тому за основу для розрахунку метрики протоколу EIGRP з урахуванням РІБ пропонується вибрати формулу (3.12).

3.2.2. Удосконалені формули розрахунку метрик

Стандартна формула обчислення метрики для протоколу RIP наводиться в наступному виразі:

$$M_{p_{i,j};RIP} = Hops_{i,j}, \tag{3.16}$$

де $M_{p_{i,j};RIP}$ – метрика протоколу RIP для шляху p при передачі ПП між вузлами i, j;

$Hops_{i,j}$ – кількість ретрансляцій пакету між маршрутизаторами, через які повинен пройти ПП від вузла-відправника i до вузла-отримувача j, при $Hops \in [1;15]$.

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

$$M_{p_{i,j};RIP} = \left\lfloor \frac{Hops_{i,j} + K_R \cdot 15^{R_{p_{i,j}} + K_P \cdot R_{m,дост.}}}{2^{K_R}} \right\rfloor, \tag{3.17}$$

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 – це коефіцієнт, який дозволяє активувати або деактивувати врахування РІБ у формулі розрахунку метрики протоколу RIP, $K_{RIP} \in \{0;1\}$, а при $K_{RIP} = 0$ вираз (3.17) набуває вигляд виразу (3.16);

$R_{m,дост.}$ – РНД 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 $K_P \in \{0;1\}$.

Як видно з формули (3.17) в ній враховуються параметр $R_{p_{i,j}}$, який визначає ризик порушення конфіденційності, доступності та цілісності транзитного ПП, а також $R_{m,дост.}$, який визначає РНД ПП по заданому шляху передачі. Однак у даній роботі пропонується враховувати одночасно тільки один з даних параметрів, для цього визначимо множину $\{K_{CVSS}, K_\theta; R_{m,дост.}\}$ та наступні обмежуючі умови:

$$\left.\begin{array}{r} K_{CVSS} \cup K_\theta \neq 0 \rightarrow K_P = 0, \\ K_P \neq 0 \rightarrow K_{CVSS} = 0, K_\theta = 0, \end{array}\right\} \qquad (3.18)$$

де K_{CVSS} та K_θ – це коефіцієнти для врахування R_{CVSS} та R_θ відповідно, які застосовуються у формулі (2.9) для розрахунку параметра $R_{p_{i,j}}$.

Як видно з виразу (3.17), при $R_{p_{i,j}} \in [0;1]$ та $R_{m,дост.} \in [0;1]$, а також з огляду на умови (3.18), то вираз $15^{R_{p_{i,j}} + K_P \cdot R_{m,дост.}} \in [1;15]$. Виходячи з цього, поділ на 2 забезпечує належні рамки метрики, при яких $M_{p_{i,j};RIP} \in [1;15]$. У табл. К.1 представлені значення метрики в залежності від різних значень РІБ.

Як видно з табл. К.1 вихідний показник метрики зазнає змін, наприклад, якщо $R_{p_{i,j}} = 0$ для всіх шляхів, то максимальний показник метрики для RIP в мережі не перевищує 8, тобто $\max(M_{i,j_z;RIP}) = 8$. В такому випадку порушується градація і деякі шляхи можуть стати рівнозначними, наприклад: при $R_{p_{i,j}} = 0$ шляхи, які мають $Hops_{p_{1i,j}} = 7$ та $Hops_{p_{2i,j}} = 8$ отримують однакову підсумкову метрику $M_{p_{1i,j};RIP} = M_{p_{2i,j};RIP} = 4.$ В такому випадку, при використанні багатошляхової маршрутизації, передача ПП може відбуватися за двома рівнозначним шляхами $p_{1i,j}$ і $p_{2i,j}$, хоча насправді вони не рівнозначні.

Стандартна формула розрахунку метрики протоколу OSPF [70, 71]

$$M_{p_{i,j};OSPF} = \sum_{k \in p_{i,j}} LC_k , \tag{3.19}$$

де $M_{p_{i,j};OSPF}$ – метрика протоколу OSPF для шляху p при передачі ПП між вузлами i, j;

LC_k – вартості КЗ k, що входять в шлях $p_{i,j}$.

В свою чергу вартість КЗ розраховується за наступною формулою:

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

де B_{ref} – параметр, що встановлюється адміністратором ТКМ, стандартно $B_{ref} = 10^8$;

B_{real} – параметр реальної пропускної здатності КЗ, біт/с.

В метриці протоколу OSPF РІБ пропонується враховувати наступним чином:

$$M_{p_{i,j};OSPF} = \left\lfloor \left(\sum_{k \in p_{i,j}} LC_k \right) \cdot \left(C_{OSPF,scale} \right)^{K_R \cdot \left(R_{p_{i,j}} + K_P \cdot R_{m,\text{дост.}} \right)} \right\rfloor , \tag{3.21}$$

де $C_{OSPF,scale}$ – це коефіцієнт масштабування, що дорівнює 256;

K_R – це коефіцієнт, який дозволяє активувати або деактивувати врахування РІБ у формулі розрахунку метрики протоколу OSPF, $K_R \in \{0;1\}$, а при $K_R = 0$ вираз (3.21) набуває вигляд виразу (3.19);

$R_{p_{i,j}}$ – РІБ для шляху p при передачі ПП між вузлами i, j, при $R_{p_{i,j}} \in [0;1]$;

$R_{m,дост.}$ – ризик несвоєчасної доставки ПП при їх 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 $K_P \in \{0;1\}$.

Для того щоб враховувати тільки один з параметрів $R_{p_{i,j}}$ чи $P_{m,дост.}$ у формулі розрахунку метрики протоколу OSPF (3.21) застосуємо умову (3.18).

Помноження на коефіцієнт масштабування $C_{OSPF,scale}$ може призвести до зростання метрики та її виходу за максимальне значення, що зазначено в стандарті OSPF де $M_{OSPF,max} = 16777215$ [70]. Щоб запобігти подібним випадкам пропонується наступне визначимо найбільшу допустиму метрики одного КЗ, так як метрика протоколу OSPF складається з метрик КЗ між маршрутизаторами. Для цього визначимо діаметр ТКМ використовуючи значеннями TTL, які визначені для багатоадресного мовлення (multicast traffic, MT) ПП, а так як наведена в даному розділі модель може працювати лише в рамках одного адміністративного домену, то виберемо TTL, що дорівнює 15 [130]. В такому випадку, максимальне можливе значення вартості одного КЗ для заданої ТКМ можливо знайти за наступним виразом:

$$LC_{max} = \frac{M_{OSPF,max}}{TTL_{max} \cdot C_{OSPF,scale}},$$

де $M_{OSPF,max}$ – це максимально можлива метрики OSPF згідно із відповідним стандартом, в даному випадку $M_{OSPF,max} = 16777215$;

TTL_{max} – це діаметр ТКМ, який вимірюється в максимально можливій кількості ретрансляцій ПП через пристрої мережевого рівня при його передачі від вузла i до найвіддаленішого вузла j, в даному випадку $TTL_{max} = 15$;

також $C_{OSPF,scale} = 256$.

Згідно з наведеними вище параметрами $LC_{max} = 4369$. При цьому, виходячи з формули (3.20), можна зробити висновок, що усі КЗ, що мають швидкість передачі від 100 мбіт/с та вище – мають вартість КЗ рівною 1. Сучасні технології дають змогу передавати ПП з набагато більшою швидкістю, наприклад зі швидкістю 40 гбіт/с та 100 гбіт/с [129]. Тому, в першу чергу необхідно збільшити параметр B_{ref}, який повинен бути визначений для кожної ТКМ окремо її адміністратором. Формалізуємо вираз (3.20) наступним чином:

$$LC_k = \left\lfloor \frac{B_{max}}{B_{real}} \right\rfloor, \tag{3.22}$$

де B_{max} – це максимальна ПРЗД одного з КЗ в ТКМ, яку оператор ТКМ повинен вказати вручну.

Для того, щоб знайти мінімальну ПРЗД, яку можна задати в рамках вибраної ТКМ, необхідно вирішити наступну нерівність:

$$LC_{max} \geq \left\lfloor \frac{B_{max}}{B_{real}} \right\rfloor.$$

В такому разі, якщо максимальна ПРЗД КЗ дорівнює 100 гбіт/с та $B_{max} = B_{ref} = 10^{12}$, з урахуванням виразу (3.22) та обмеження $LC_{max} \leq 1118481$ знайдемо мінімальну ПРЗД КЗ в ТКМ:

$$B_{real} \geq \left\lfloor \frac{10^{12}}{4369} \right\rfloor = 228885328 \text{ [біт/с]},$$

тобто мінімальна ПРЗД одного КЗ не повинна бути нижче ніж приблизно 229 мбіт/с, що не завжди можливо виконати. В разі виникнення різниці між

максимальною і мінімальною ПРЗД КЗ в ТКМ більше ніж в 4369 разів, необхідно вручну задавати метрику для КЗ з ПРЗД меншою за B_{ref} в 4369 разів.

У стандарті EIGRP наведено два методи розрахунку метрики: класичний та розширений [72]. У випадку використання розширеного методу з'являється можливість використання, в формулі розрахунку метрики, таких параметрів як: джиттер та залишок енергії вузла-маршрутизатора. Дані параметри можуть використовуватися при динамічній маршрутизації в безпроводових мережах. В даній роботі пропонується вибрати класичний метод розрахунку метрики.

Формула для розрахунку метрики протоколу EIGRP для шляху p при передачі ПП між вузлами i, j [72]:

$$M_{p_{i,j};EIGRP} = \left[\left(K_1 \cdot B_{min}^{p} + \frac{K_2 \cdot B_{min}^{p}}{256\text{-}L_{max}^{p}} + K_3 \cdot \frac{D_{sum}^{p}}{10} \right) \cdot \frac{K_5}{K_4 + R_{min}^{p}} \right] \cdot C_{scale}, \quad (3.23)$$

де B_{min}^{p} – найменше значення зваженого показника ПРЗД в шляху p;

L_{max}^{p} – найбільша завантаження одного з КЗ в шляху p;

D_{sum}^{p} – сумарна затримка в шляху, мкс;

R_{min}^{p} – найменша надійність одного з КЗ в шляху p;

$p \in P_{i,j}$, $P_{i,j}$ – всі можливі шляхи в заданій ТКМ при передачі інформації між вузлами i, j при $i \neq j$;

C_{scale} – коефіцієнт масштабування, $C_{scale} = 256$;

K_1, K_2, K_3, K_4, K_5 – коефіцієнти, які дозволяють враховувати (або не враховувати) в метриці вищевказані параметри, при цьому за замовчуванням для даних коефіцієнтів використовуються наступні значення: $K_1 = K_3 = 1$ та $K_2 = K_4 = K_5 = 0$.

При $K_2 = K_4 = K_5 = 1$ виникають випадки, коли динамічна зміна параметрів, таких як надійність і завантаженість КЗ, буде приводити до постійного перерахунку метрики (так як ці величини динамічно змінюються в процесі передачі ПП), що буде згубно впливати на ЦПМ. Тому Cisco не рекомендує їх використовувати при розрахунку метрики.

Розрахунок зваженого показника ПРЗД проводиться таким чином:

$$B_{min}^{p} = \left\lfloor \frac{10^7}{\mathbf{min}\left(B_{i,j}^{l,p}\right)} \right\rfloor,$$

де $\mathbf{min}\left(B_{i,j}^{l,p}\right)$ – найменша ПРЗД одного з КЗ l в шляху p при передачі пакетів між вузлами i, j, при $i \neq j$, кбіт/с.

Для розрахунку сумарної затримки шляху використовується наступна формула:

$$D_{sum}^{p} = \sum_{i \neq j} D_{i,j}^{p},$$

де $D_{i,j}^{p}$ – затримка ПП в кожному з КЗ, що входять в шлях p при передачі інформації між вузлами i, j, при $i \neq j$.

Врахування РІБ в метриці протоколу EIGRP пропонується формалізувати як:

$$M_{p_{i,j};EIGRP} = \left[\left(K_1 \cdot B_{min}^{p} + \frac{K_2 \cdot B_{min}^{p}}{256\text{-}L_{max}^{p}} + K_3 \cdot \frac{D_{sum}^{p}}{10} \right) \cdot \frac{K_5}{K_4 + R_{min}^{p}} \right] \cdot \left(C_{scale} \right)^{\left(2 - \left(K_R - K_R \cdot \left(R_{p_{i,j}} + K_P \cdot R_{m,дост.}\right)\right)\right)}, \quad (3.24)$$

де K_R – коефіцієнт, що дозволяє враховувати чи не враховувати параметри РІБ в формулі метрики, при $K_R \in \{0;1\}$;

$R_{p_{i,j}}$ – РІБ для шляху p при передачі даних між вузлами i, j, при $R_{p_{i,j}} \in [0;1]$;

$R_{m,дост.}$ – ризик несвоєчасної доставки пакетів при їх 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 $K_P \in \{0;1\}$.

При цьому в формулі (3.24) пропонується вибрати $C_{scale} = 16$. Це пояснюється тим, що зменшення коефіцієнта масштабування призводить до зменшення впливу стандартних значень метрики EIGRP, та зростання впливу на неї параметрів РІБ. При цьому максимальне значення коефіцієнта масштабування повинно бути рівним 256, а ступінь, в яку він зводиться, повинен бути цілочисельним, щоб спростити розрахунки. Цим критеріям задовольняють три вирази: 16^2, 4^4, 2^8, де $C_{scale} \in \{2;4;16\}$. Для збереження максимальної рівноваги впливу стандартних параметрів розрахунку метрики і параметрів РІБ, потрібно вибрати $\mathbf{max}(C_{scale} \in \{2;4;16\})$, яким є значення 16.

Для того щоб враховувати тільки один з параметрів $R_{p_{i,j}}$ чи $P_{m,дост.}$ у формулі розрахунку метрики EIGRP (3.24) застосуємо умову (3.18).

Також коефіцієнт K_R відіграє важливу роль в формулі (3.24), так, якщо $K_R = 1$ та параметри РІБ враховуються в метриці, то розрахунки проводяться за вдосконаленою формулою, а якщо $K_R = 0$, то формула (3.24) набуває виду формули (3.23), що є стандартною формулою розрахунку метрики для протоколу EIGRP.

3.3. Висновки по третьому розділу

1. В даному розділі представлена моделі одношляхової та багатошляхової динамічної маршрутизації. Також представлені вдосконалені моделі вирішення завдання вибору оптимального шляху для таких ПДМ як: RIP, OSPF, EIGRP, особливістю яких є врахування РІБ в формулах розрахунку метрик для зазначених протоколів.
2. Для вибору вдосконалених формул для протоколів: RIP, OSPF, EIGRP, було запропоновано декілька варіацій формул для яких були побудовані графіки. Вдосконалені формули для кожного з протоколів вибрані відповідно до критеріїв врахування РІБ в формулах розрахунку метрики, які описані в підрозділі 1.5.
3. Усі вдосконалені формули розрахунку метрики для кожного з досліджуваних ПДМ враховують як стандартні параметри, які описані у відповідних стандартах протоколів, так і РІБ або РНД ПП як окремі параметри формули.
4. В кожній удосконаленій формулі розрахунку метрики для відповідних ПДМ одночасно враховується лише один з параметрів ризику: РІБ, що розраховується на основі оцінки вразливостей маршрутизаторів та ЕММ, або РНД ПП.
5. Недоліком удосконаленої метрики для протоколу RIP є малий розкид метрики в залежності від параметрів ризику. Це може призвести до того, що два шляхи передачі ПП, які мають різні метрики, розраховані за стандартною формулою, можуть мати однакову вихідну метрику при розрахунках за удосконаленою формулою. Що в свою чергу може призвести до перемаршрутизації ПП по не ефективним шляхам. Дана проблема залишається невирішеною.
6. Недоліком удосконаленої метрики для протоколу OSPF є помноження стандартних параметрів метрики на додатковий коефіцієнт масштабування, який збільшує розкид метрики в залежності від значень

параметрів ризику. Це може призвести до перевищення максимально допустимого значення метрики для протоколу OSPF, та, як наслідок, до того, що деякі шляхи передачі будуть вважатися недосяжними і не будуть приймати участь в процесі маршрутизації ПП. Для запобігання виникнення даної проблеми запропоновано задавати вручну адміністратором ТКМ вартість КЗ, які мають в 4369 разів меншу ПРЗД ніж КЗ з найбільшою ПРЗД в ТКМ, який приймає участь в процесах динамічної маршрутизації за допомогою OSPF.

7. Недоліком удосконаленої метрики для протоколу EIGRP є недостатня кількість досліджень взаємодії з такими параметрами метрики як: надійність та завантаженість КЗ в шляху передачі ПП, так як дані параметри стандартно не враховуються в формулі розрахунку метрики та активуються адміністратором ТКМ за допомогою окремих коефіцієнтів.

РОЗДІЛ 4
КІЛЬКІСНИЙ АНАЛІЗ МОДЕЛЕЙ ТА МЕТОДІВ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ ПОТОКУ ПАКЕТІВ З УРАХУВАННЯМ ВИМОГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У попередніх трьох розділах представлені дослідження, які розробити модель динамічної маршрутизації ПП шляхом вдосконалення формул розрахунку метрики для таких ПДМ, як: RIP, OSPF, EIGRP, враховуючи не тільки стандартні параметри метрики, а і параметри РІБ.

В даному розділі наводиться кількісний аналіз (КА) запропонованих моделей та методів.

4.1. Умови та вихідні данні для проведення кількісного аналізу

Для проведення КА створена топологія, на основі якої проводилися експерименти для кожного з протоколів динамічної маршрутизації, досліджуваних в роботі: RIP, OSPF, EIGRP.

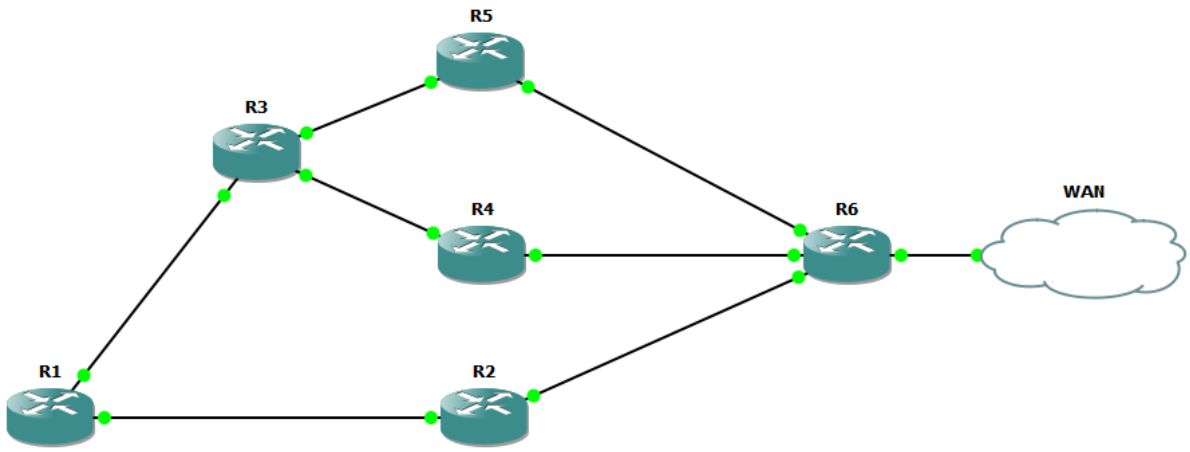


Рис. 4.1. Топологія мережі для проведення кількісного аналізу

На рис. 4.1 представлена топологія досліджуваної ТКМ. В рамках досліджуваної топології елементи R1-R6 – є стандартними маршрутизаторами, хмара WAN – емулює вузол-отримувач ПП. Пропускні спроможності всіх КЗ в досліджуваній топології однакові та дорівнюють 100 мбіт/с. КЗ між R6 та хмарою WAN також має ПРЗД 100 мбіт/с.

В ТКМ передається ПП SFTP. Інтенсивність вхідного ПП в ТКМ дорівнює $\lambda = 60$ мбіт/с. При цьому завантаженість центральних процесорів кожного з маршрутизаторів однакова і дорівнює 20%. За формулою (2.15) розрахуємо параметр залишкової ПРЗД: $\beta_{обс.} = 40$ мбіт/с.

ПП передається з маршрутизатора R1 у WAN. В такому випадку в ТКМ існують наступні шляхи передачі ПП:

- від R1 до WAN:
  - $p_1 \in [R1, R2, R6, WAN]$;
  - $p_2 \in [R1, R3, R4, R6, WAN]$;
  - $p_3 \in [R1, R3, R5, R6, WAN]$;
- від R2 до WAN:
  - $p_4 \in [R2, R6, WAN]$;
- від R3 до WAN:
  - $p_5 \in [R3, R4, R6, WAN]$;
  - $p_6 \in [R3, R5, R6, WAN]$;
- від R4 до WAN:
  - $p_7 \in [R4, R6, WAN]$;
- від R5 до WAN:
  - $p_8 \in [R5, R6, WAN]$.

ПДМ формують шляхи, які не мають петель, тобто, ПП не відправляється тому вузлу, з якого він прийшов. Тому, в розглянутому прикладі (при передачі ПП від R1 до WAN), шляхи p_4, p_7, p_8 не мають альтернатив і не будуть розглядатися.

Розрахуємо ЙСД ПП по досліджуваним шляхам за $t = 150$ мс, використовуючи математичну модель, представлену в пункті 2.2.2:

- $P_{p_1, дост.}(t) = P_{p_5, дост.}(t) = P_{p_6, дост.}(t) = 0{,}938,$
- $P_{p_2, дост.}(t) = P_{p_3, дост.}(t) = 0{,}849.$

Параметр R_{θ_i} є постійним для заданої ТКМ і буде змінюватися тільки в разі її фізичного переналаштуванні. Тому цей параметр можна вважати спільним для всіх наступних експериментів з даної топологією. Нижче наведені результати розрахунку нормованого параметра R_{θ_i}, отримані за допомогою імітаційного моделювання в пакеті MATLAB: $R_{\theta_{R1}} = 0{,}3077$, $R_{\theta_{R2}} = 0{,}3571$, $R_{\theta_{R3}} = 0{,}3571$, $R_{\theta_{R4}} = 0{,}3077$, $R_{\theta_{R5}} = 0{,}3077$, $R_{\theta_{R6}} = 0$, $R_{\theta_{WAN}} = 0{,}2174$.

Слід зазначити, що вузол WAN знаходиться поза рамками заданої ТКМ, тому параметр $R_{\theta_{WAN}}$ враховуватися не буде, так само, як і не будуть враховуватися інші параметри РІБ віддаленої ТКМ.

Слід описати те, як маршрутизатори в ТКМ будуть послідовно приймати рішення про маршрутизації ПП за певним шляхами. ПП починає передаватися з вузла R1, який приймає перше рішення про вибір шляху в заданій ТКМ. Маршрутизатор R1 знає метрики для шляху p_1, а також для одного з маршрутів p_2, p_3. Тобто маршрутизатор R1 приймає рішення на основі знання двох величин: метрики M_{p_1}, і однієї з метрик M_{p_2}, M_{p_3}. Маршрутизатор R1 виберемо той шлях, у якого метрика найменша. У разі вибору шляху p_1 ПП передаються далі на маршрутизатор R2, який має лише один шлях передачі ПП до WAN – p_4. У разі ж, якщо маршрутизатор R1 вибере шлях передачі ПП до WAN, який проходить через маршрутизатор R3, то на цьому етапі маршрутизатор R3 також повинен зробити свій вибір яким шляхом він відправить ПП далі. Він також вибере шлях з меншою метрикою. Далі маршрутизатори R4 і R5 мають лише по одному безальтернативного шляху, незалежно від того, який шлях вибере маршрутизатор R3, подальший шлях передачі пакетів буде визначений.

Слід зазначити, що протокол OSPF будує повну карту ТКМ, тому маршрутизатор R1 буде знати про всі три шляхи передачі ПП до WAN p_1, p_2, p_3, і вибере той, у якого метрика виявиться меншою. При використанні протоколів RIP та EIGRP маршрутизатор R1 буде знати лише два шляхи передачі ПП: p_1, а також один з шляхів p_2, p_3.

Також в цьому розділі необхідно буде розраховувати при яких значеннях РІБ буде відбуватися перемаршрутизація ПП, для цього будемо використовувати формули, що наведені нижче:

1. Для протоколу RIP

$$R \geq \mathbf{log}_{15}\left(\left(M_{other} + k_{rr}\right) \cdot 2 - M_{old}\right), \tag{4.1}$$

де k_{rr} – коефіцієнт який визначає умови пошуку, при $k_{rr} = 0$ буде знайдено мінімальне значення РІБ для балансування ПП між двома шляхами, так як вони будуть мати однакову метрику, та при $k_{rr} = 1$ буде знайдено мінімальне значення РІБ, при якому буде відбуватися повна перемаршртизація ПП за новим шляхом.

M_{other} – метрика не оптимального шляху та за яким може відбутися маршрутизація ПП у разі виконання наведеної умови, при цьому даний параметр розраховується за удосконаленою формулою розрахунку метрики (3.17);

M_{old} – метрика поточного оптимального шляху, що розраховується за стандартною формулою розрахунку метрики для ПДМ RIP.

2. Для протоколу OSPF

$$R \geq \mathbf{log}_{C_{scale}}\left(\frac{M_{other} + k_{rr}}{M_{old}}\right), \tag{4.2}$$

де C_{scale} – коефіцієнт масштабування для удосконаленої формули розрахунку метрики ПДМ OSPF, при цьому $C_{scale} = 256$.

k_{rr} – коефіцієнт який визначає умови пошуку, при $k_{rr} = 0$ буде знайдено мінімальне значення РІБ для балансування ПП між двома шляхами, так як вони будуть мати однакову метрику, та при $k_{rr} = 1$ буде знайдено мінімальне значення РІБ, при якому буде відбуватися повна перемаршртизація ПП за новим шляхом.

M_{other} – метрика не оптимального шляху та за яким може відбутися маршрутизація ПП у разі виконання наведеної умови, при цьому даний параметр розраховується за удосконаленою формулою розрахунку метрики (3.17);

M_{old} – метрика поточного оптимального шляху, що розраховується за стандартною формулою розрахунку метрики для ПДМ RIP.

3. Для протоколу EIGRP

$$R \geq log_{C_{scale}} \left(\frac{M_{other} + k_{rr}}{body} \right) - 1, \tag{4.3}$$

де C_{scale} – коефіцієнт масштабування для удосконаленої формули розрахунку метрики ПДМ EIGRP, при цьому $C_{scale} = 16$;

k_{rr} – коефіцієнт який визначає умови пошуку, при $k_{rr} = 0$ буде знайдено мінімальне значення РІБ для балансування ПП між двома шляхами, так як вони будуть мати однакову метрику, та при $k_{rr} = 1$ буде знайдено мінімальне значення РІБ, при якому буде відбуватися повна перемаршртизація ПП за новим шляхом.

M_{other} – метрика не оптимального шляху та за яким може відбутися маршрутизація ПП у разі виконання наведеної умови, при цьому даний параметр розраховується за удосконаленою формулою розрахунку метрики (3.17);

$body$ – стандартна формула розрахунку метрики ПДМ EIGRP (3.23), але без перемноження на C_{scale}, тобто

$$body = \left[\left(K_1 \cdot B_{min}^{p} + \frac{K_2 \cdot B_{min}^{p}}{256\text{-}L_{max}^{p}} + K_3 \cdot \frac{D_{sum}^{p}}{10} \right) \cdot \frac{K_5}{K_4 + R_{min}^{p}} \right],$$

де B_{min}^{p} – найменше значення зваженого показника ПРЗД в шляху p;

L_{max}^{p} – найбільша завантаження одного з КЗ в шляху p;

D_{sum}^{p} – сумарна затримка в шляху, мкс;

R_{min}^{p} – найменша надійність одного з КЗ в шляху p.

4.1.1. Кількісний аналізу удосконаленої моделі динамічної маршрутизації з використанням метрики протоколу RIP

Для проведення аналізу використовується топологія, що представлена на рис. 4.1.

Виходячи з формули (3.17), якщо параметр $K_{RIP} = 0$, то формула розрахунку метрики протоколу RIP набуває стандартний вид, а метрики шляхів, в такому випадку будуть наступними:

$$M_{p_1} = 2,\ M_{p_2} = 3,\ M_{p_3} = 3,\ M_{p_5} = 2,\ M_{p_6} = 2.$$

Виходячи з вище представлених метрик видно, що маршрутизатор R1 вибере шлях p_1 для передачі ПП до WAN.

Для того, щоб провести аналіз удосконаленої моделі з урахуванням параметру РІБ, що розраховується на основі метрик NIST CVSS, встановимо наступні коефіцієнти $K_{CVSS} = 1$ и $K_\theta = 0$, при цьому $K_p = 0$. Використаємо табл. К.1 та знайдемо нові значення метрик шляхів з урахуванням того, що R_{CVSS} на всіх маршрутизаторах дорівнює нулю:

$$M_{p_1}=1,\ M_{p_2}=2,\ M_{p_3}=2,\ M_{p_5}=1,\ M_{p_6}=1.$$

За формулою (4.1) знайдемо мінімально прийнятне значення (з округленням до однієї тисячної) параметра РІБ, яке призведе до перемаршрутизації ПП:

$$R \geq \mathbf{log}_{15}((2)\cdot 2-2)=0{,}256, \text{ при } k_{rr}=0;$$

$$R \geq \mathbf{log}_{15}((2+1)\cdot 2-2)=0{,}512, \text{ при } k_{rr}=1.$$

Знайдемо значення $R_{CVSS_{R2}}$ при якому буде відбуватися перемашрутизація ПП, при тому що R_{CVSS} на всіх інших маршрутизаторах ТКМ дорівнює нулю. Так як РІБ розраховується як середнє значення параметрів РІБ на всіх маршрутизаторах в заданому шляху, то $R_{CVSS_{R2}}=0{,}512\cdot 3=1{,}536$ при $k_{rr}=1$, що не є можливим, тобто повна перемаршрутизація ПП неможлива за даних умов, та $R_{CVSS_{R2}}=0{,}256\cdot 3=0{,}768$ при $k_{rr}=0$, що означає, що при $R_{CVSS_{R2}}=0{,}768$ можливе балансування ПП між двома або більшою кількістю шляхів. В даному випадку при $R_{CVSS_{R2}}=0{,}768$ балансування ПП буде відбуватися за шляхами p_1, p_2, p_3 рівномірно.

Знайдемо залежність захищеності ПП та ЙСД ПП. При цьому тут і далі по тексту під захищеністю ПП, яку позначимо як S, будемо мати на увазі величину зворотну РІБ шляху передачі, тобто $S=1-R$.

На графіку на рис. 4.2 зображено випадок, коли $k_{rr}=0$ та $R_{CVSS_{R2}}=0{,}768$. При використанні вдосконаленого моделі маршрутизації ПП балансується між доступними шляхами, що дозволило підвищити захищеність ПП приблизно на 4%. При цьому ЙСД зменшилася приблизно на 9%.

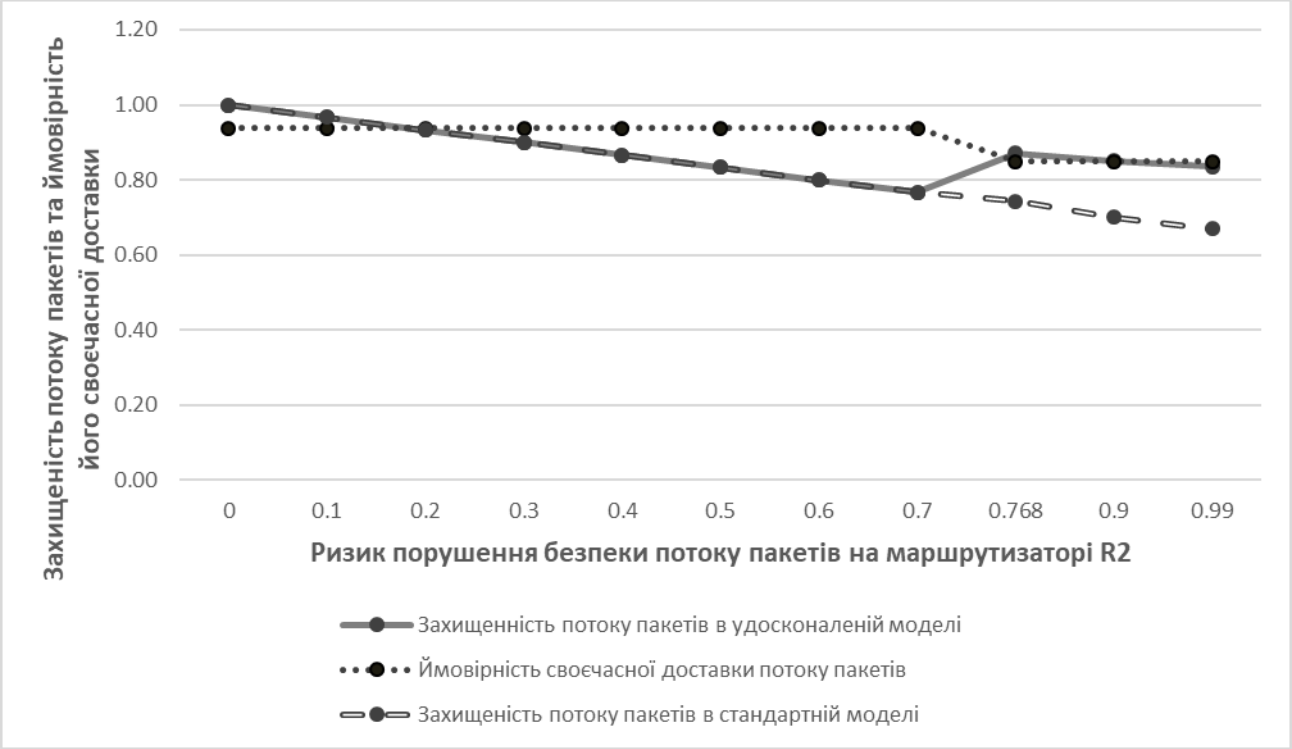


Рис. 4.2. Залежність ймовірності своєчасної доставки і захищеності потоку пакетів від ризику інформаційної безпеки потоку пакетів на маршрутизаторі R2 для протоколу RIP

Розглянемо інший випадок, коли: $K_{CVSS} = 0,\ K_\theta = 1,$ та $K_p = 0.$ У такому випадку РІБ розраховується лише на основі ЕММ. Перерахуємо метрики шляхів:

$$M_{p_1} = 5, M_{p_2} = 5, M_{p_3} = 5, M_{p_5} = 5, M_{p_6} = 5.$$

В такому випадку ПП буде рівномірно балансуватися між усіма можливими шляхами. За даних значень метрик механізму PBR не буде знати за яким зі шляхів передавати довірливий та приорітетний ПП. Для вирішення цієї проблеми пропонується вибирати для шкідливого ПП шлях з меншим середнім значенням ЕММ по всім маршрутизаторам даного шляху (з меншим РІБ, який розраховується на основі ЕММ), в даному випадку $R_{\theta_{p1}} < R_{\theta_{p2}}$ та $R_{\theta_{p1}} < R_{\theta_{p3}}$, тобто, буде вибраний шлях p_1. Таке розв'язання не є оптимальним, тому що довірливий та

приорітетний ПП буде передаватися за шляхами p_2 та p_3, які мають більшу затримку.

У випадку, коли: $K_{CVSS} = 0,\ K_\theta = 0,$ та $K_p = 1,$ РІБ буде розраховуватися як РНД ПП. Припустимо, що максимально можлива затримка пакетів становить 150 мс. Перерахуємо метрики шляхів:

$$M_{p_1} = 1,\ M_{p_2} = 2,\ M_{p_3} = 2,\ M_{p_5} = 1,\ M_{p_6} = 1,$$

в такому випадку, весь ПП буде як і раніше проходити за шляхом p_1.

Припустимо, що інтенсивність вхідного ПП постійна $\lambda = 60$ мбіт/с, а завантаженість ЦПМ на маршрутизаторі R2 становить 20%. При цьому на маршрутизаторі R2 поступово збільшується споживання ресурсів ЦПМ, внаслідок роботи шкідливого процесу, що призводить до зменшення інтенсивності обробки ПП даним маршрутизатором. Також на маршрутизаторах задані наступні параметри: $R_{CVSS_{R1}} = 0{,}2,$ $R_{CVSS_{R2}} = 0{,}2,$ $R_{CVSS_{R3}} = 0{,}4,$ $R_{CVSS_{R4}} = 0{,}55,$ $R_{CVSS_{R5}} = 0{,}5,$ $R_{CVSS_{R6}} = 0{,}2.$ На рис. 4.3 представлена залежність ЙСД ПП при використанні стандартної і вдосконаленої моделей маршрутизації для протоколу RIP від завантаженості ЦПМ маршрутизатора R2.

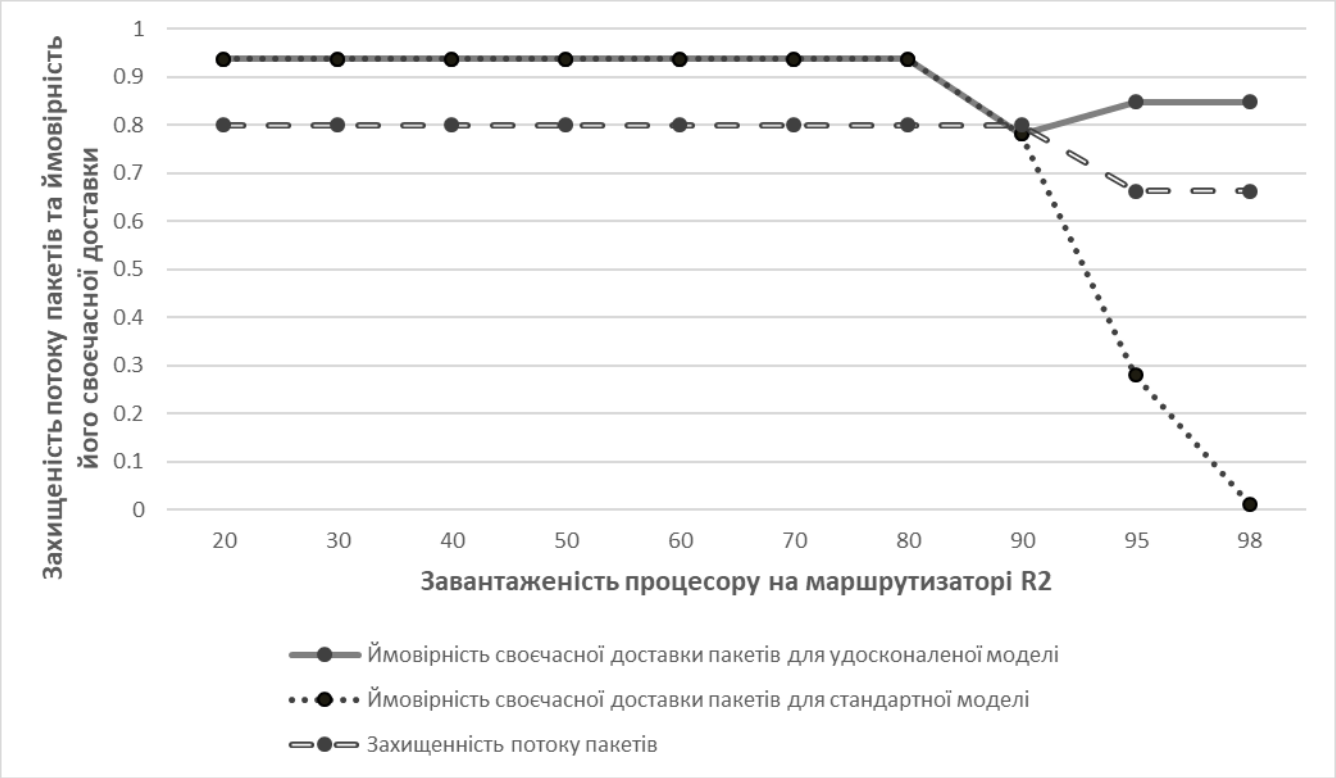


Рис. 4.3. Залежність ймовірності своєчасної доставки і захищеності трафіку від завантаженості процесора на маршрутизаторі R2 для протоколу RIP

Як видно з рис. 4.3 перемаршрутизація ПП відбувається при $L_{CPU,R2} = 95$. При використанні вдосконаленої моделі маршрутизації для протоколу RIP ПП повністю перемаршрутизується через маршрутизатор R3, що дозволило підвищити ЙСД приблизно на 14%. При цьому захищеність ПП зменшилася також приблизно на 14%.

4.1.1.1. Проблема врахування параметрів маршрутиазторів, які одночасно входять до обох шляхів, для яких проводиться розрахунок метрики

Також для протоколу RIP можливий варіант повної перемаршрутизації ПП, наприклад при $R_{CVSS_{R1}} = R_{CVSS_{R6}} = 1$ та $R_{CVSS_i} = 0$ для усіх інших маршрутизаторів, в такому випадку метрики будуть наступні:

$$M_{p_1} = 4, M_{p_2} = 3, M_{p_3} = 3, M_{p_5} = 2, M_{p_6} = 2.$$

Перемаршрутизація можлива, тому що обидва маршрутизатора R1 та R6 входять у кожний маршрут, а так як РІБ розраховується як середнє значення РІБ на всіх маршрутиазторах в заданому шляху. Так як в шляху p_1 менше маршрутизаторів ніж в маршрутах p_2 та p_3, то РІБ для p_1 дорівнює 0,666(6), а для p_2 та p_3 дорівнює 0,5. Повна перемаршрутизація ПП при даних параметрах з однієї сторони не збільшує захищеність ПП, в той же час призводить до зменшення ЙСД ПП.

Така ж проблема виникає при розрахунку середньої ЕММ заданого шляху передачі. Наприклад, для параметрів, які описані в підрозділі 4.1, $R_{\theta_{p1}} = 0{,}2216$ та $R_{\theta_{p2}} = R_{\theta_{p3}} = 0{,}2431$, а в разі, якщо враховуються лише унікальні маршратизатори кожного зі шляхів, то $R_{\theta_{p1}} = 0{,}3571$ та $R_{\theta_{p2}} = R_{\theta_{p3}} = 0{,}3324$.

Дану проблему можливо вирішити, якщо при розрахунках альтернативних шляхів для заданого шляху не враховувати РІБ маршрутизаторів, які входять в обидва шляхи. Тоді РІБ буде розраховуватися в залежності від унікальних параметрів кожного зі шляхів. В той же час даний метод підвищує складність запропонованої моделі і може стати предметом подальших досліджень.

4.1.2. Кількісний аналізу удосконаленої моделі динамічної маршрутизації з використанням метрики протоколу OSPF

Для проведення аналізу використовується топологія, що представлена на рис. 4.1.

Для проведення аналізу вибиремо $B_{ref} = 10^8$, так як максимальна ПРЗД усіх КЗ, наведених на рис. 4.1, дорівнює 100 мбіт/с.

Розрахуємо метрики шляхів для протоколу OSPF за формулою (3.19):

$$M_{p_1} = 3,\ M_{p_2} = 4,\ M_{p_3} = 4,\ M_{p_5} = 3,\ M_{p_6} = 3.$$

Виходячи з вище представлених метрик видно, що маршрутизатор R1 вибере шлях p_1 для передачі ПП в WAN.

Розглянемо випадок, коли: $K_{CVSS} = 1$ и $K_\theta = 0,$ при цьому $K_p = 0.$ Розрахуємо метрики маршрутів для протоколу OSPF з урахуванням того, що параметр R_{CVSS} на всіх вузлах дорівнює нулю:

$$M_{p_1} = 3, M_{p_2} = 4, M_{p_3} = 4, M_{p_5} = 3, M_{p_6} = 3.$$

За формулою (4.2) знайдемо мінімально прийнятне значення (з округленням до однієї тисячної) параметра РІБ, яке призведе до перемаршрутізації ПП:

$$R \geq \mathbf{log}_{256}\left(\frac{4}{3}\right) = 0,052\text{, при } k_{rr} = 0;$$

$$R \geq \mathbf{log}_{256}\left(\frac{4+1}{3}\right) = 0,092\text{, при } k_{rr} = 1.$$

При тому що R_{CVSS_i} на всіх маршрутизаторах ТКМ, крім R2, дорівнює нулю, то балансування ПП за маршрутами p_1, p_2, p_3 відбудеться при $R_{CVSS_{R2}} = 0,052 \cdot 3 = 0,156,$ а повна перемаршрутизація відбудиться при $R_{CVSS_{R2}} = 0,092 \cdot 3 = 0,276.$

На графіку на рис. 4.4 зображено залежність захищенності ПП та його ЙСД від РІБ на маршрутизаторі R2. Використання вдосконаленого моделі маршрутизації дозволило підвищити захищеність ПП приблизно на 14%, при цьому ЙСД зменшилася приблизно на 8%.

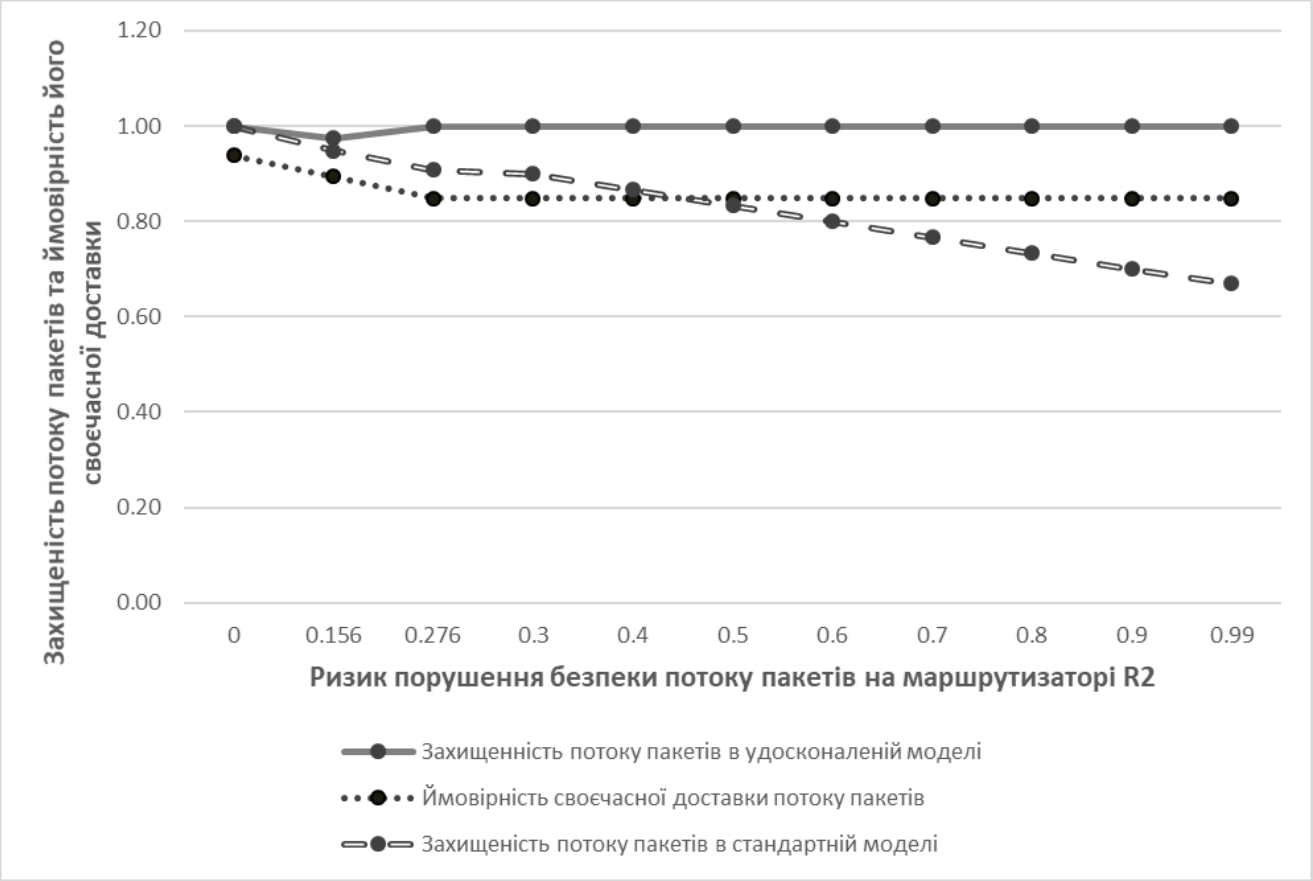


Рис. 4.4. Залежність ймовірності своєчасної доставки і захищеності потоку пакетів від ризику інформаційної безпеки потоку пакетів на маршрутизаторі R2 для протоколу OSPF

Так саме, як і для протоколу RIP, при $R_{CVSS_{R1}} = R_{CVSS_{R6}} = 1$ та $R_{CVSS_i} = 0$ для усіх інших маршрутизаторів, відбувається повна перемаршртиузація ПП, при цьому не підвищується захищеність ПП, але зменшується ЙСД ПП. Детальніше проблема і метод її вирішення описані в підпункті 4.1.1.1.

Розглянемо інший випадок, коли: $K_{CVSS} = 0,\ K_\theta = 1,$ та $K_p = 0.$ У такому випадку РІБ розраховується лише на основі ЕММ. Перерахуємо метрики шляхів:

$$M_{p_1} = 224,\ M_{p_2} = 265,\ M_{p_3} = 265,\ M_{p_5} = 224,\ M_{p_6} = 224.$$

В такому випадку довірливий та приорітетний ПП буде передаватися по першому шляху.

У випадку, коли: $K_{CVSS} = 0,\ K_\theta = 0,$ та $K_p = 1,$ РІБ буде розраховуватися як РНД ПП. Припустимо, що максимально можлива затримка пакетів становить 150 мс. Перерахуємо метрики шляхів:

$$M_{p_1} = 4,\ M_{p_2} = 9,\ M_{p_3} = 9,\ M_{p_5} = 4,\ M_{p_6} = 4,$$

в такому випадку, весь ПП буде як і раніше проходити за шляхом p_1.

Припустимо, що інтенсивність вхідного ПП постійна $\lambda = 60$ мбіт/с, а завантаженість ЦПМ на маршрутизаторі R2 становить 20%. При цьому на маршрутизаторі R2 поступово збільшується споживання ресурсів ЦПМ, внаслідок роботи шкідливого процесу, що призводить до зменшення інтенсивності обробки ПП даним маршрутизатором. Також на маршрутизаторах задані наступні параметри: $R_{CVSS_{R1}} = 0,2,$ $R_{CVSS_{R2}} = 0,2,$ $R_{CVSS_{R3}} = 0,4,$ $R_{CVSS_{R4}} = 0,55,$ $R_{CVSS_{R5}} = 0,5,$ $R_{CVSS_{R6}} = 0,2.$ На рис. 4.5 представлена залежність ЙСД ПП при використанні стандартної і вдосконаленої моделей маршрутизації для протоколу OSPF від завантаженості ЦПМ маршрутизатора R2.

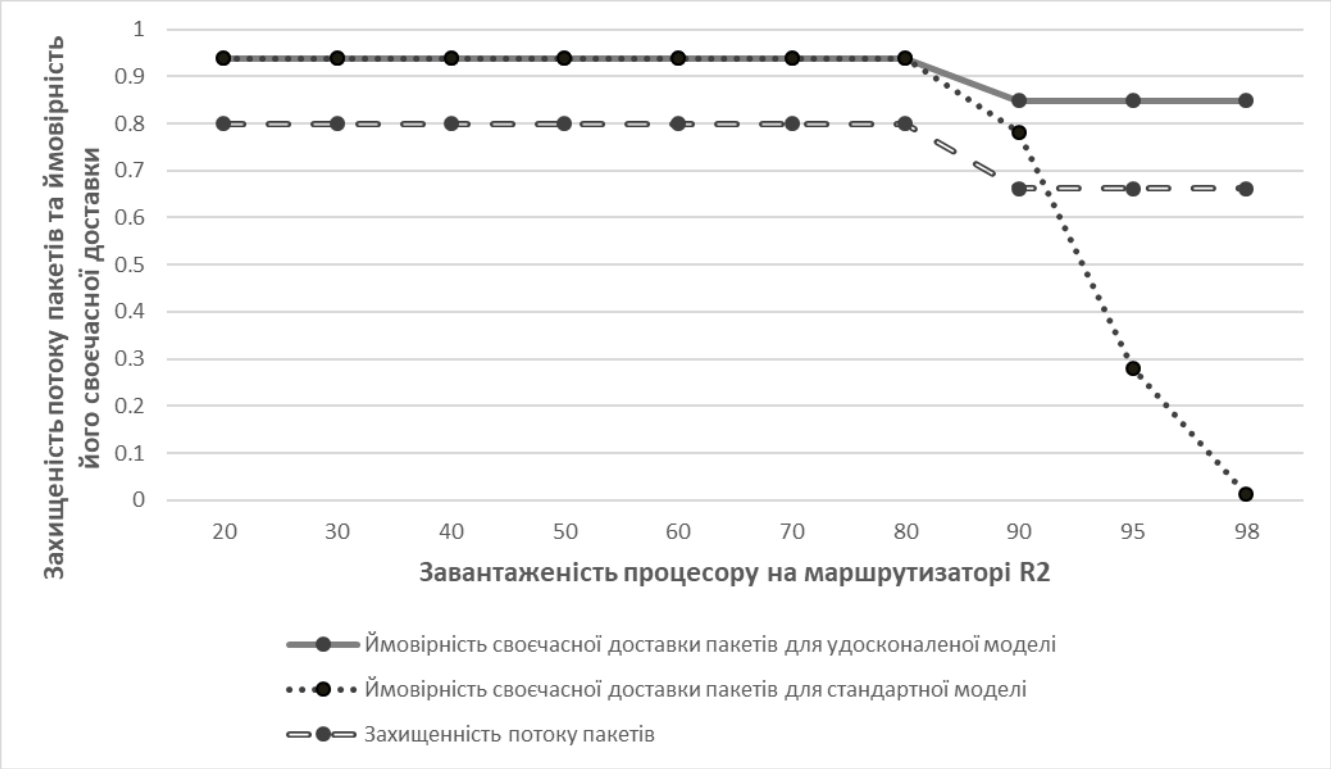


Рис. 4.5. Залежність ймовірності своєчасної доставки і захищеності трафіку від завантаженості процесора на маршрутизаторі R2 для протоколу OSPF

Як видно з рис. 4.5 перемаршрутизація ПП відбувається при $L_{CPU,R2} = 90$. При використанні вдосконаленої моделі маршрутизації для протоколу OSPF ПП повністю перемаршрутизується через маршрутизатор R3, що дозволило підвищити ЙСД приблизно на 14%. При цьому захищеність ПП зменшилася також приблизно на 14%.

4.1.3. Кількісний аналізу удосконаленої моделі динамічної маршрутизації з використанням метрики протоколу EIGRP

Для проведення аналізу використовується топологія, що представлена на рис. 4.1.

Розрахуємо метрики шляхів для протоколу EIGRP за формулою (3.23):

$$M_{p_1} = 33280, M_{p_2} = 35840, M_{p_3} = 35840, M_{p_5} = 33280, M_{p_6} = 33280.$$

Виходячи з вище представлених метрик видно, що маршрутизатор R1 вибере шлях p_1 для передачі ПП в WAN.

Розглянемо випадок, коли: $K_{CVSS}=1$ и $K_\theta=0,$ при цьому $K_p=0.$ Розрахуємо метрики маршрутів для протоколу OSPF з урахуванням того, що параметр R_{CVSS_i} на всіх вузлах дорівнює нулю:

$$M_{p_1}=2080,\ M_{p_2}=2240,\ M_{p_3}=2240,\ M_{p_5}=2080,\ M_{p_6}=2080.$$

За формулою (4.3) знайдемо мінімально прийнятне значення (з округленням до однієї десятитисячної) параметра РІБ, яке призведе до перемаршрутізації ПП:

$$R\geq \mathbf{log}_{16}\left(\frac{2240}{130}\right)-1=0{,}0267,\ \text{при}\ k_{rr}=0;$$

$$R\geq \mathbf{log}_{256}\left(\frac{2240+1}{130}\right)=0{,}0269,\ \text{при}\ k_{rr}=1.$$

При тому що R_{CVSS_i} на всіх маршрутизаторах ТКМ, крім R2, дорівнює нулю, то балансування ПП за маршрутами p_1, p_2, p_3 відбудеться при $R_{CVSS_{R2}}=0{,}0267\cdot 3=0{,}0801,$ а повна перемаршрутизація відбудиться при $R_{CVSS_{R2}}=0{,}0269\cdot 3=0{,}0807.$ Різниця між РІБ в десятитисячній долі не є суттєвою, тому використаємо операцію округлення до тисячної та запишему умову повної перемаршрутизації ПП як $R_{CVSS_{R2}}=0{,}081.$

На графіку на рис. 4.6 зображено залежність захищенності ПП та його ЙСД від РІБ на маршрутизаторі R2. Використання вдосконаленого моделі маршрутизації дозволило підвищити захищеність ПП приблизно на 13%, при цьому ЙСД зменшилася приблизно на 9%.

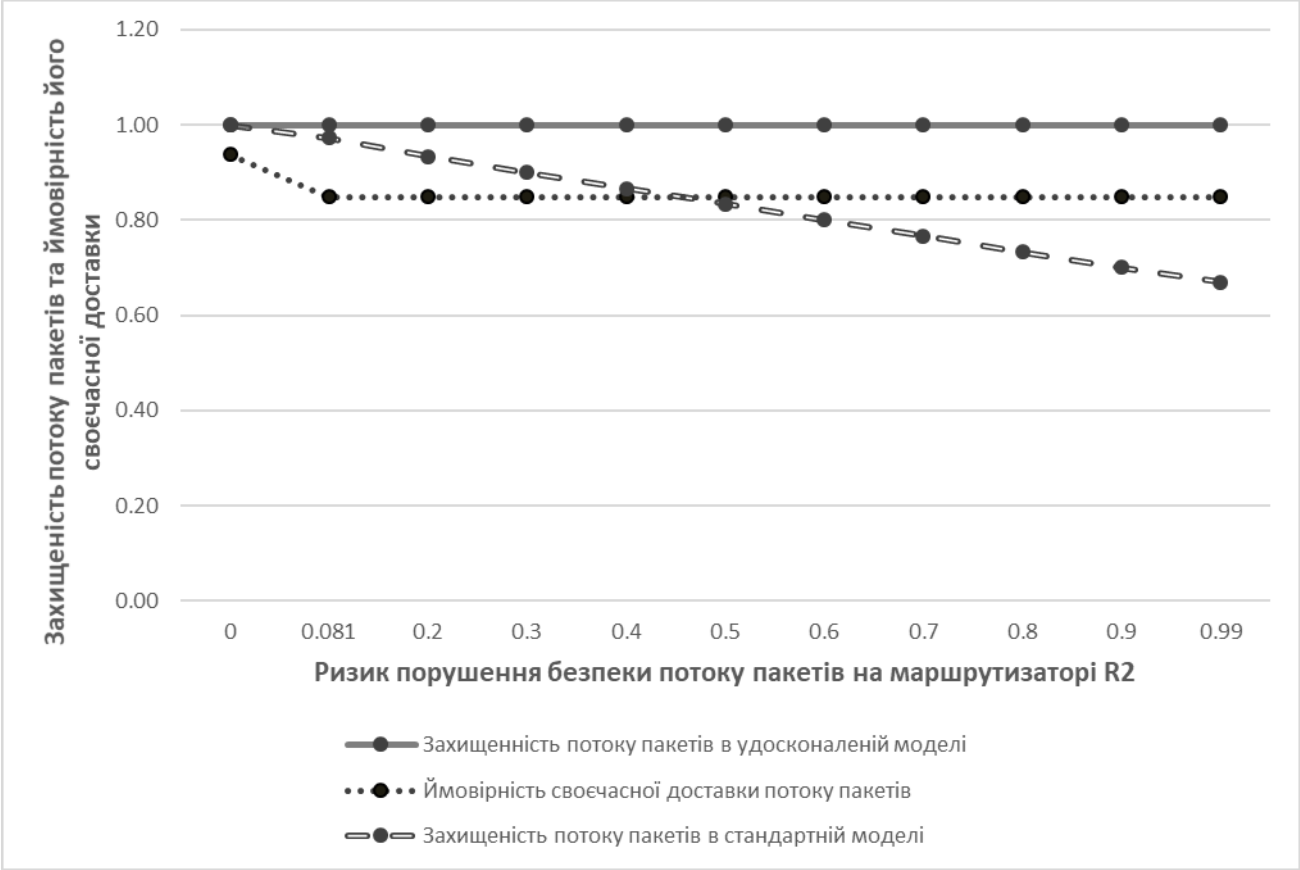


Рис. 4.6. Залежність ймовірності своєчасної доставки і захищеності потоку пакетів від ризику інформаційної безпеки потоку пакетів на маршрутизаторі R2 для протоколу EIGRP

Так саме, як і для протоколів RIP та OSPF, при $R_{CVSS_{R1}} = R_{CVSS_{R6}} = 1$ та $R_{CVSS_i} = 0$ для усіх інших маршрутизаторів, відбувається повна перемаршртиузація ПП, при цьому не підвищується захищеність ПП, але зменшується ЙСД ПП. Детальніше проблема і метод її вирішення описані в підпункті 4.1.1.1.

Розглянемо інший випадок, коли: $K_{CVSS} = 0,\ K_\theta = 1,$ та $K_p = 0.$ У такому випадку РІБ розраховується лише на основі ЕММ. Перерахуємо метрики шляхів:

$$M_{p_1} = 18003,\ M_{p_2} = 18264,\ M_{p_3} = 18264,\ M_{p_5} = 18003,\ M_{p_6} = 18003.$$

В такому випадку довірливий та приорітетний ПП буде передаватися по p_1.

У випадку, коли: $K_{CVSS} = 0,\ K_\theta = 0,$ та $K_p = 1,$ РІБ буде розраховуватися як РНД ПП. Припустимо, що максимально можлива затримка пакетів становить 150 мс. Перерахуємо метрики шляхів:

$$M_{p_1} = 2470,\ M_{p_2} = 3404,\ M_{p_3} = 3404,\ M_{p_5} = 2470,\ M_{p_6} = 2470,$$

в такому випадку, весь ПП буде як і раніше проходити за шляхом p_1.

Припустимо, що інтенсивність вхідного ПП постійна $\lambda = 60$ мбіт/с, а завантаженість ЦПМ на маршрутизаторі R2 становить 20%. При цьому на маршрутизаторі R2 поступово збільшується споживання ресурсів ЦПМ, внаслідок роботи шкідливого процесу, що призводить до зменшення інтенсивності обробки ПП даним маршрутизатором. Також на маршрутизаторах задані наступні параметри: $R_{CVSS_{R1}} = 0{,}2,$ $R_{CVSS_{R2}} = 0{,}2,$ $R_{CVSS_{R3}} = 0{,}4,$ $R_{CVSS_{R4}} = 0{,}55,$ $R_{CVSS_{R5}} = 0{,}5,$ $R_{CVSS_{R6}} = 0{,}2.$ На рис. 4.7 представлена залежність ЙСД ПП при використанні стандартної і вдосконаленої моделей маршрутизації для протоколу OSPF від завантаженості ЦПМ маршрутизатора R2.

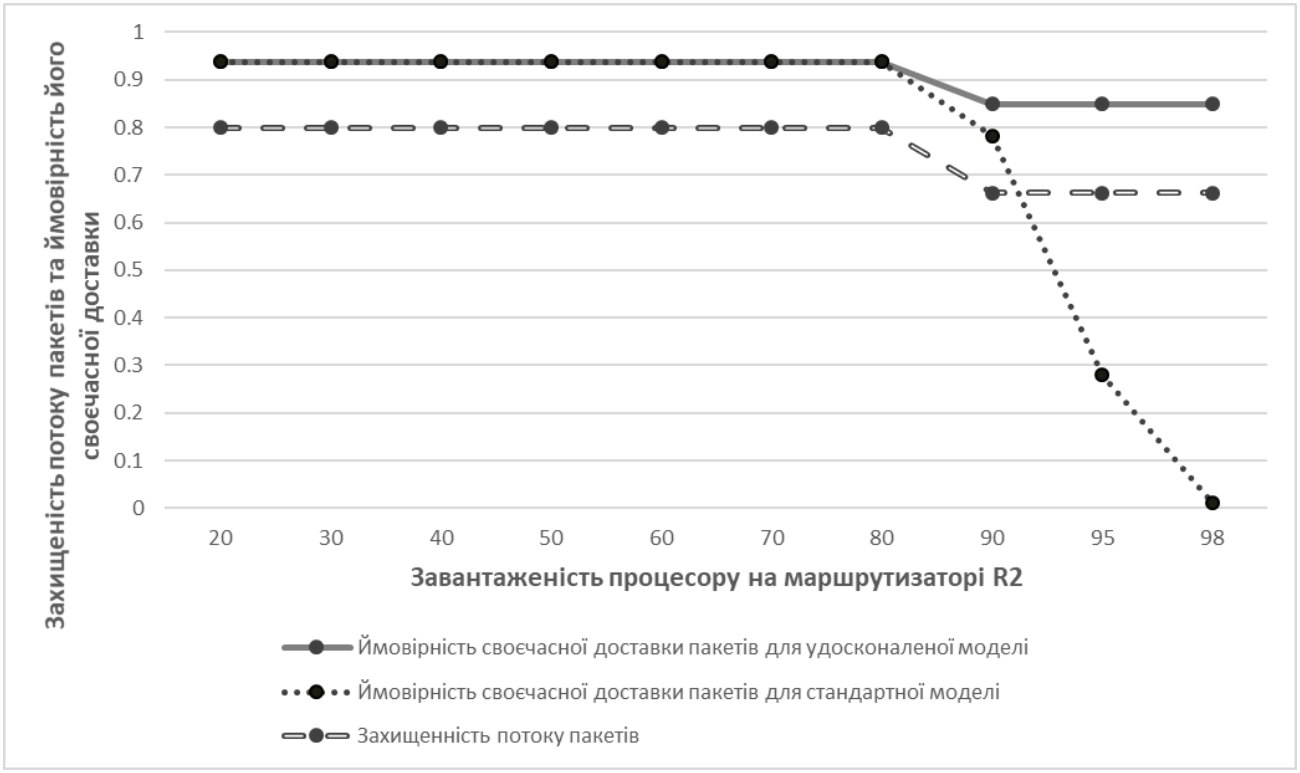


Рис. 4.7. Залежність ймовірності своєчасної доставки і захищеності трафіку від завантаженості процесора на маршрутизаторі R2 для протоколу EIGRP

Як видно з рис. 4.7 перемаршрутизація ПП відбувається при $L_{CPU,R2} = 90$. При використанні вдосконаленої моделі маршрутизації для протоколу EIGRP ПП повністю перемаршрутизується через маршрутизатор R3, що дозволило підвищити ЙСД приблизно на 15%, при цьому захищеність ПП зменшилася також приблизно на 14%.

4.1.4. Кількісний аналіз удосконаленої моделі маршрутизації для протоколів: RIP, OSPF, EIGRP, у разі зміни параметрів мережі

У разі зміни в топології, що наведена на рис. 4.1, або параметрів ТКМ, які наведені в підрозділі 4.1, можуть змінитися вихідні значення параметрів удосконаленою моделі маршрутизації. Розглянемо декілька прикладів у разі зміни ПРЗД КЗ в заданій ТКМ.

Якщо ПРЗД усіх КЗ в заданій ТКМ буде знижена зі 100 мбіт/с до 10 мбіт/с, та об’єм ПП, що передається в ТКМ також буде знижено пропорційно, то це не призведе до зміни будь-яких параметрів РІБ. В такому випадку подібна зміна буде мати наступні наслідки для ПДМ:

1. Для метрики протоколу RIP – ніяких, так як розрахунку метрики для даного протоколу інваріантні до ПРЗД КЗ ТКМ, параметри та методи розрахунку якого залишаються незмінними.
2. Для метрики протоколу OSPF – ніяких, хоча метрики шляхів и залежать від ПРЗД КЗ в ТКМ, але розрахунки вартості кожного з них залежить від параметру B_{ref}, а так як ПРЗД усіх КЗ в ТКМ однакова, то, згідно з удосконаленою моделлю, параметр B_{ref} також пропорційно зменшиться у 10 разів, що призведе до аналогічних вихідних параметрів метрик шляхів, як і до зміни ПРЗД КЗ.
3. Єдиний протокол в якому буде змінено метрики шляхів – це EIGRP, вони стануть в 10 разів більші. Але, так як зростання метрики для всіх шляхів буде однаково пропорційним, а також пропорційним як для стандартної так і для удосконаленої моделей, то на подальші розрахунки це не вплине.

Така сама ситуація спостерігається, якщо збільшити пропускні здатності усіх КЗ у 10 разів. Єдиною різницею буде те, що, в даному випадку, метрика протоколу EIGRP буде пропорційно в 10 разів меншою.

Саме тому пропонується змінити пропускні здатності КЗ ТКМ не пропорційно. В такому випадку КЗ R1-R2, R2-R6, R6-WAN – мають ПРЗД 100 мбіт/с, а усі інші КЗ – 10 мбіт/с. Тоді: $R_{\theta_{R1}} = 0{,}3978$, $R_{\theta_{R2}} = 0{,}457$, $R_{\theta_{R3}} = 0{,}2825$, $R_{\theta_{R4}} = 0{,}2135$, $R_{\theta_{R5}} = 0$, $R_{\theta_{R6}} = 0{,}0556$, $R_{\theta_{WAN}} = 0{,}0556$. На вхід ТКМ подається ПП з інтенсивністю 4 мбіт/с та передається від R1 до WAN. ЙСД ПП для $t = 150$ мс: $P_{p_1,дост.}(t) = 1$, $P_{p_2,дост.}(t) = 0{,}00358$, $P_{p_3,дост.}(t) = 0{,}00358$, $P_{p_5,дост.}(t) = 0{,}023$, $P_{p_6,дост.}(t) = 0{,}023$.

З урахуванням вказаних параметрів у разі використання метрик протоколу EIGRP не може відбутися перемаршрутизація ПП за будь-яких значень РІБ, шлях p_1 завжди буде оптимальним.

Так як метрика протоколу RIP не залежить від ПРЗД каналів зв'язків ТКМ, то, в даному випадку, розрахунки залишаться такими ж як у пункті 4.1.1. Тобто при $R_{CVSS_{R2}} = 0{,}768$ відбудеться балансування ПП між усіма шляхами. Також при заданих параметрах існує проблема, яка описана в підпункті 4.1.1.1. При цьому захищеність ПП зростає на 4%, але ЙСД ПП знижується майже в 280 разів.

При зростанні навантаження на ЦПМ маршрутизатора R2 до $L_{CPU,R2} = 96\,\%$ ЙСД ПП для p_1 зменшується до $P_{p_1,дост.}(t) = 0{,}012$, метрики для шляхів p_1, p_2 та p_3 стають однаковими та дорівнюють 8, що призводить до балансування ПП по всім доступним шляхам. При цьому ЙСД ПП зменшується приблизно на 35%.

У разі використання метрики протоколу OSPF перемаршрутизація відбувається лише якщо $R_{CVSS_{R1}} = R_{CVSS_{R2}} = R_{CVSS_{R6}} = 1$, тоді $M_{p_1} = 768$, а $M_{p_2} = M_{p_3} = 640$. При цьому захищеність ПП зростає на 50%, але ЙСД ПП зменшується приблизно у 280 разів. Подібна проблема перемаршрутизації і метод її вирішення описані в підпункті 4.1.1.1.

Основною проблемою перемаршрутизації для даних випадків є те, що шляхи p_2 та p_3 мають ПРЗД КЗ 10 мбіт/с, що в десять разів менше ніж в шляху p_1 так саме як і у порівнянні з інтенсивністю вхідного ПП, що може призвести до переповнення буферу пакетами та до їх відкидання. Так як в даній роботі розглядаються потокові моделі динамічної маршрутизації, то обмеження (3.2) призведе до неможливості знаходження оптимального шляху передачі ПП, чи до маршрутизації ПП по прийнятному за ПРЗД шляху але з більшою величиною РІБ.

З наведених розрахунків можна зробити висновок, що удосконалена модель є чутливою до неоднорідності ПРЗД каналів зв'язків в ТКМ.

4.2. Висновки до четвертого розділу

1. На основі кількісного аналізу удосконалених моделей маршрутизації з використанням метрик таких протоколів як RIP, OSPF, EIGRP, можна зробити висновок, що при однакових пропускних здатностях каналів зв'язків в ТКМ запропонована модель демонструє зростання захищеності ПП чи ЙСД ПП в залежності від задачі, що вирішується.
2. Недоліком даної моделі можна вважати те, що у разі неоднорідності ПРЗД каналів зв'язків ТКМ використання запропонованих моделей може призвести до маршрутизації ПП за шляхом з достатньою ПРЗД, але з більшою величиною РІБ. Дана проблема може бути вирішена за допомогою використання нерівномірного балансування навантаження за шляхами нерівнозначної вартості, що дасть змогу передавати частину ПП за шляхом з меньшим значенням РІБ, не призводячи при цьому до перенавантаження КЗ. Вирішення даної проблеми може стати однією з подальших задач автора дисертаційної роботи.
3. В заданій ТКМ удосконалена модель динамічної маршрутизації з використанням метрики протоколу RIP продемонструвала підвищення захищеності ПП на 4% при зменшенні ЙСД ПП на 9%, та підвищення ЙСД ПП на 14% при зниженні захищеності ПП на 14%; з використанням метрики 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%; з використанням метрики протоколу EIGRP – зростання захищеності ПП на 13% при зменшенні ЙСД ПП на 9%, та зростання ЙСД ПП на 15% при зменшенні захищеності на 14%.
4. Одна з проблем удосконаленою моделі полягає в тому, що при попарному розрахунку РІБ шляхів враховується параметри РІБ на маршрутизаторах які входять обидва шляхи одночасно. Це призводить до збільшення впливу кількості маршрутизаторів в шляху на значення РІБ та до того, що потенційно більш небезпечний шлях передачі ПП буде мати меншій

середній РІБ шляху, ніж шлях передачі з меншими ризиками. Дану проблему пропонується вирішити шляхом врахування параметрів РІБ лише тих маршрутизаторів, які є унікальними для кожного з шляхів відповідно. Дане удосконалення може стати однією з задач для подальших досліджень по темі дисертаційної роботи.

ВИСНОВКИ ПО ДИСЕРТАЦІЙНІЙ РОБОТІ

В процесі вирішення поставленої наукової задачі розроблені моделі та методи підвищення ІБ ПП, що маршрутизується в ТКМ, шляхом врахування РІБ вузлів мережі як додаткового критерію вибору оптимального шляху 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 (кількість маршрутизаторів в шляху, інтенсивність вхідного ПП, інтенсивність обробки ПП маршрутизаторами та завантаженість ЦПМ на маршрутизаторах). В статичному методі ризик розраховується на основі параметрів метрик вразливостей NIST CVSS v2 та ЕММ, в динамічному – на основі ймовірності своєчасної доставки ПП.
2. Для розрахунку ЕММ запропоновано використовувати параметри ПРЗД 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 на 486,2%.
3. Проведено аналіз впливу різних методів розрахунку 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 СКВ: 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%.
4. Проведено аналіз впливу завантаженості ЦПМ маршрутизаторів в заданому шляху передачі на процес маршрутизації ПП. В ході аналізу виявлено, що при реалізації DoS атаки для створення завантаженості ЦПМ

на 1% достатньо передавати ПП з інтенсивністю 0,0112 мбіт/с, для стандартного ж ПП (при передачі по протоколу SFTP) – необхідна інтенсивність зростає до 3,0684 мбіт/с.

5. Розроблено модель 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 ПРЗД 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 кожен з маршрутизаторів, шляхом використання прямого та зворотного перетворення Лапласа на перемноженні зображень щільностей розподілу часу обслуговування ПП кожним з маршрутизаторів в заданому шляху. Пропонується використовувати дану модель для знаходження РНД ПП вузлу-отримувачу.
6. Розроблено моделі одношляхової та багатошляхової маршрутизації ПП в ТКМ, новизною яких є врахування РІБ разом з базовими параметрами в формулах розрахунку метрик шляхів 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 або своєчасної доставки транзитного ПП.
7. Проведено аналіз методів врахування РІБ шляху в формулах розрахунку метрик таких ПДМ як RIP, OSPF, EIGRP. В результаті аналізу вибрані методи, які демонструють зростаючу експоненційну залежність вихідного покажчику метрики від РІБ шляху, та в яких більші значення РІБ збільшують значення метрики, РІБ не призводить до випадків, коли метрика дорівнює нулю, а також в метриці враховуються стандартні параметри для відповідних ПДМ.

8. Проведено кількісний аналіз запропонованих моделей з використанням метрик таких ПДМ як RIP, OSPF, EIGRP. За результатами аналізу в заданій ТКМ в умовах роботи 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%; 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%; протоколу EIGRP – зростання захищеності ПП на 13% при зменшенні ЙСД ПП на 9%, та зростання ЙСД ПП на 15% при зменшенні захищеності на 14%.
9. На основі кількісного аналізу удосконалених моделей виявлено, що моделі коректно працюють в ТКМ, в яких усі КЗ мають однакову ПРЗД. При цьому в ТКМ, в яких існують КЗ з різною ПРЗД використання удосконалених моделей може призвести до перемаршрутизації ПП по не ефективним шляхам зі значними втратами ЙСД (для заданої ТКМ приблизно на 280%), або ж до випадків, коли інтенсивність вхідного ПП перевищує інтенсивність з якою може передаватися ПП по вибраному шляху, що призведе до часткового відкидання пакетів.
10. В ході кількісного аналізу було виявлено, що метод розрахунку РІБ шляху на основі статичних параметрів може призводити до некоректної оцінки при порівнянні РІБ двох або більше шляхів. Проблема полягає в тому, що РІБ різних шляхів 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. Цю проблему можливо вирішити шляхом виключення з розрахунку РІБ параметрів маршрутизаторів, які входять в обидва або більшу кількість шляхів, при порівнянні РІБ між ними. В той же час даний метод підвищує складність запропонованої моделі і може стати предметом подальших досліджень за темою дисертаційної роботи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Sharma V. IPv6 and IPv4 Security Challenge Analysis and Best-Practice Scenario / V. Sharma // International Journal of Advanced of Networking and Applications. – 2010. – Т. 1. – № 4. – С. 258-269.
2. Yoo H.S. A Study on the Connectivity of IPv6 to IPv4 Domains and Its Security Issues / H.S. Yoo, Cagalaban G.A., S.H. Kim // International Journal of Advanced Science and Technology. – 2009. – Т. 10. – 1-10.
3. Ullrich J. IPv6 Security: Attacks and Countermeasures in a Nutshell [Електронний ресурс] / J. Ullrich, K. Krombholz, H. Hobel [та ін.] // Offensive Technologies : 11th USENIX Workshop : Тези доп. – Сан Диего, 2014. – С. 11. – Режим доступу : https://www.usenix.org/system/files/conference/woot14/woot14-ullrich.pdf
4. Aswal M.S. Threats and Vulnerabilities in Wireless Mesh Networks / M.S. Aswal, P. Rawat, T. Kumar // International Journal of Recent Trends in Engineering. – 2009. – Т. 2. – № 4. – С. 155-158.
5. Yau P.W. Security Vulnerabilities in Ad Hoc Networks / P.W. Yau, C.J. Mitchell // Communication Theory and Applications : 7th International Symposium : Тези доп. – Амблсайд, 2003. – С. 99-104.
6. Nadeem A. A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks / Nadeem A., Howarth M.P. // IEEE communications surveys & tutorials. – 2013. – Т. 15. – № 4. – С. 2027-2045.
7. Waichal S. Router Attacks-Detection and Defense Mechanisms / S. Waichal, B.B. Meshram // International Journal of Scientific & Technology Ressearch. – 2013. – Т. 2. – № 6. – С. 145-149.
8. Wang F. On the vulnerabilities and protection of OSPF routing protocol / F. Wang, S.F. Wu // Computer Communications and Networks : 7th International Conference : Тези доп. – Лафейет, 1998. – С. 148-152.

9. Murphy S. RFC 4272: BGP Security Vulnerabilities Analysis [Електронний ресурс] / S. Murphy // Request for comments. – 2006. – Режим доступу : https://tools.ietf.org/html/rfc4272.html
10. Nordström O. Beware of BGP attacks / O. Nordström, C. Dovrolis // ACM SIGCOMM Computer Communication Review. – 2004. – Т. 34. – №. 2. – С. 1-8.
11. Butler K. A survey of BGP security issues and solutions / K. Butler, T.R. Farley, P. McDaniel [та ін.] // Proceedings of the IEEE. – 2010. – Т. 98. – № 1. – С. 100-122.
12. Cisco : Vulnerability Statistics [Електронний ресурс] // CVE Details: The ultimate security vulnerability datasource. – 2017. – Режим доступу : https://www.cvedetails.com/vendor/16/Cisco.html
13. Cisco Security : Cisco Security Advisory and Alerts // Cisco Systems. – 2017. – Режим доступу : https://tools.cisco.com/security/center/publicationListing.x?resourceIDs=2096,210631,209961,211571,202356&apply=1,1,1,1,1&totalbox=5&pt0=Cisco&cp0=2096&pt1=Cisco&cp1=210631&pt2=Cisco&cp2=209961&pt3=Cisco&cp3=211571&pt4=Cisco&cp4=202356&limit=100#~FilterByProduct
14. El-Semary A.M. New trends in secure routing protocols for wireless sensor networks [Електронний ресурс] / A.M. El-Semary, M.M. Abdel-Azim // International Journal of Distributed Sensor Networks. – 2013. – Т. 9. – № 5. – С. 16, – Режим доступу : http://dsn.sagepub.com/content/9/5/802526.full.
15. Кулаков Ю.А. Безопасная многопутевая маршрутизация в беспроводных сетях большой размерности / Ю.А. Кулаков, В.В. Лукашенко, А.В. Левчук // Захист інформації. – 2011. – Т. 13. – № 2(51). – С. 5-10.
16. Кулаков Ю.А. Разработка и моделирование процесса безопасной многопутевой передачи информации в мобильных сетях / Ю.А. Кулаков, А.В. Коган, А.А. Пирогов // Вісник Національного технічного університету України. – 2011. – № 54. – С. 145-149.

17. Еременко А.С. Потоковая модель многопутевой маршрутизации по непересекающимся путям в телекоммуникационной сети / А.С. Еременко // Проблеми телекомунікацій. – 2015. – № 1(16). – С. 85-93.
18. Кулаков Ю.А. Алгоритм разделения и сборки секретного сообщения для многопутевой маршрутизации в беспроводных сетях / Ю.А. Кулаков, А.В. Коган, А.А. Пирогов // Вісник Національного технічного університету України. – 2012. – № 57. – С. 46-50.
19. Wadbude D. An efficient secure AODV routing protocol in MANET / D. Wadbude, V. Richariya // International Journal of Engineering and Innovative Technology – 2012. – Т. 1. – С. 274-279.
20. Ganesh S. Efficient and secure routing protocol for wireless sensor networks through SNR based dynamic clustering mechanisms / S. Ganesh, R. Amutha // Journal of Communications and Networks. – 2013. – Т. 15. – № 4. – С. 422-429.
21. Khan S. Cross layer secure and resource-aware on-demand routing protocol for hybrid wireless mesh networks / S. Khan, J. Loo // Wireless Personal Communications. – 2012. – Т. 62. – № 1. – С. 201-214.
22. Лемешко А.В. Усовершенствование модели безопасной маршрутизации сообщения с оптимальной балансировкой числа его фрагментов по непересекающимся маршрутам / А.В. Лемешко, А.С. Еременко // Захист інформації. – 2015. – Т. 17. – № 2. – С. 135-142.
23. Єременко О.С. Модель маршрутизації в телекомунікаційній мережі з використанням шляхів, що перетинаються за вузлами / О.С. Єременко, Д.В. Андрушко // Вісник Національного університету «Львівська політехніка» серія: «Радіоелектроніка та телекомунікації». – 2015. – № 818. – С. 181–188.
24. Yeremenko O. Enhanced Flow-based Model of Multipath Routing with Overlapping by Nodes Paths / O. Yeremenko // Problems of

Infocommunications. Science and Technology (PIC S&T-2015): Second International IEEE Conference : Тези доп. – Харків, 2015. – С. 42-45.

25. Кулаков Ю.А. Спосіб організації безпечної багатошляхової маршрутизації в безпроводовій мережі MPLS / Ю. Кулаков, В. Лукашенко, А. Левчук // Вісник Національного Авіаційного Університету. – 2012. – Т. 50. – № 1. – С. 101-105.
26. Кулаков Ю.А. Организация на основе теории игр многопутевой безопасной передачи информации / Ю.А. Кулаков, В.В. Лукашенко, А.В. Коган // Реєстрація, зберігання і обробка даних. – 2012. – Т. 14. – № 1. – С. 85-90.
27. Aggarwal A. Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs / A. Aggarwal, Gandhi S., Chaubey N. [та ін.] // Advanced Computing & Communication Technologies (ACCT) : 2014 Fourth International Conference : Тези доп. – Рогтак, 2014. – С. 432-438.
28. Matam R. Provably Secure Routing Protocol for Wireless Mesh Networks / R. Matam, S. Tripathy // IJ Network Security. – 2014. – Т. 16. – № 3. – С. 168-178.
29. Duan J. TSRF: A trust-aware secure routing framework in wireless sensor networks [Електронний ресурс] / J. Duan, D. Yang, H. Zhu [та ін.] // International Journal of Distributed Sensor Networks. – 2014. – С. 14, – Режим доступу : http://dsn.sagepub.com/content/10/1/209436.full
30. Mahmoud M.M.E.A. Secure and reliable routing protocols for heterogeneous multihop wireless networks / M.M.E.A. Mahmoud, X. Lin, X. Shen // IEEE Transactions on Parallel and Distributed Systems. – 2015. – Т. 26. – № 4. – С. 1140-1153.
31. Li S. Adaptive and secure load-balancing routing protocol for service-oriented wireless sensor networks / S. Li, S. Zhao, X. Wang [та ін.] // IEEE Systems Journal. – 2014. – Т. 8. – № 3. – С. 858-867.
32. Irissappane A.A. Secure routing in wireless sensor networks via POMDPs / A.A. Irissappane, J. Zhang, Oliehoek F.A. [та ін.] // Artificial Intelligence :

25th International Joint Conference : Тези доп. – Буенос-Айрес, 2015. – С. 2617-2623.

33. Grover S. FSR: Ferry-based Secure Routing Algorithm for Delay Tolerant Networks / S. Grover, S.A. AdityaPancholi // International Journal Of Engineering And Computer Science. – 2014. – С. 6104-6108.
34. Mehra M. Energy Efficient Secure Routing Protocol (EESRP) in Wireless Sensor Network / M. Mehra, P. Dabas // International Journal for Innovative Research in Science and Technology. – 2015. – Т. 2. – № 3. – С. 29-33.
35. Paramasivan B. Development of a secure routing protocol using game theory model in mobile ad hoc networks / B. Paramasivan, M.J.V. Prakash, M. Kaliappan // Journal of Communications and Networks. – 2015. – Т. 17. – № 1. – С. 75-83.
36. Kaliappan M. Enhancing secure routing in mobile ad hoc networks using a dynamic bayesian signaling game model / M. Kaliappan, B. Paramasivan // Computers and Electrical Engineering. – 2015. – Т. 41. – С. 301-303.
37. Abazeed M. A review of secure routing approaches for current and next-generation wireless multimedia sensor networks [Електронний ресурс] / M. Abazeed, K. Saleem, A. Derhab [та ін.] // International Journal of Distributed Sensor Networks. – 2015. – Т. 11 – № 10 – Режим доступу : http://dsn.sagepub.com/content/11/10/524038.full
38. Diwan D. Security Mechanism in RIPv2, EIGRP and OSPF for Campus Network - A Review / D. Diwan, V.K. Narang, A.K. Singh // International Journal of Computer Science Trends and Technology (IJCST). – 2017. – Т. 5. – №2. – С. 399-404.
39. Nakibly G. Persistent OSPF Attacks / G. Nakibly, A. Kirshon, D. Gonikman // Network & Distributed System Security Conference (NDSS'12) : 19th Annual Conference : Тези доповіді. – 2012. – С. 12, – Режим доступу : https://www.internetsociety.org/sites/default/files/01_3.pdf
40. Shaparia J. A proposed algorithm for securing OSPF with using Symmetric key and Encryption techniques based on Image / J. Shaparia, S. Chauhan //

International Journal for Scientific Research & Development (IJSRD). – 2013. – Т. 1. – №2. – С. 349-352.

41. Li H. Secure Routing in Wired Networks and Wireless Ad Hoc Networks / H. Li, Z. Chen, X. Qin [та ін.] // Univ. of Kentucky, Department of Computer Science. – 2002. – С. 1-34, – Режим доступу : http://web.cse.msstate.edu/~ramkumar/N3-Pilate.pdf
42. Sangroha D. Analyzer Router: An Approach to Detect and Recover from OSPF Attacks / D. Sangroha, V. Gupta // International Symposium on Security in Computing and Communication. – Springer Berlin Heidelberg. – 2014. – С. 370-378.
43. Ghourabi A. Honeypot Router for Routing Protocols Protection / A. Ghourabi, T. Abbes, A. Bouhoula // Risks and Security of Internet and Systems : International Conference : Тези доповіді. – 2009. – С. 127-130.
44. Global revenue from telecommunications equipment from 2005 to 2016 (in billion euro) [Електронний ресурс] // Statista - The Statistics Portal. – 2017. – Режим доступу : https://www.statista.com/statistics/268631/worldwide-revenue-from-telecommunications-equipment-since-2005/
45. Internet of Things - Statistics & Facts [Електронний ресурс] // Statista - The Statistics Portal. – 2017. – https://www.statista.com/topics/2637/internet-of-things/
46. 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.
47. 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 : II міжнародна наук.-техн.конф. : Тези доп. – Львів, 2013. – С. 16-17.

48. 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 : Тези доп. – Харків, 2013. – Т. 4. – С. 220-221.
49. 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 : Тези доп. – Харків, 2013. – Т. 4. – С. 224-225.
50. 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 : Тези доп. – Хакрів, 2013. – Т. 4. – С. 226-227.
51. 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 : Тези доп. – Севастопіль, 2013. – С. 470-471.
52. 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 : Тези доп. – Севастопіль, 2013. – С. 484-485.
53. 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 : Тези доп. – Львів, 2013. – С. 339-340.
54. 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 (PIC S&T-2013) : Сборник научных трудов первой международной научно-практической конференции : Тези доп. – Хакрів, 2013. – С. 81-84.

55. 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.
56. 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 : Тези доп. – Львів, 2014. – С. 578-580.
57. 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.
58. 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 (PIC S&T-2014) : First International IEEE Conference : Тези доп. – Харків, 2014. – С. 186-187.
59. 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.
60. 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.
61. 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 : Тези доп. – Харків, 2015. – Т. 4. – С. 132-133.

62. Snihurov A. Improvement of EIGRP Protocol Routing Algorithm Based on Information Security Metrics / A. Snihurov, V. Chakrian // Problems of Infocommunications. Science and Technology (PIC S&T-2015): Second International IEEE Conference : Тези доп. – Харків, 2015. – С. 263-265.
63. 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.
64. 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.
65. Snihurov 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 : Тези доп. – Львов, 2016. – С. 537-539.
66. 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.
67. Пат. 107617 Україн, 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.

68. Malkin G. RFC 2453: RIP version 2 [Електронний ресурс] / G. Malkin // Request for Comments. – 1998. – С. 39. – Режим доступу : https://tools.ietf.org/html/rfc2453
69. Malkin G. RFC 2080: RIPng for ipv6 [Електронний ресурс] / G. Malkin, R. Minnear // Request for Comments. – 1997. – С. 19. – Режим доступу : https://tools.ietf.org/html/rfc2080
70. Moy J. RFC 2328: OSPF version 2 [Електронний ресурс] / J. Moy // Request for Comments. – 1998. – С. 244. – Режим доступу : https://tools.ietf.org/html/rfc2328
71. Coltun R. RFC 5340: OSPF for IPv6 [Електронний ресурс] / R. Colturn, D. Ferguson, J. Moy [та ін.] // Request for Comments. – 2008. – С. 94. – Режим доступу : https://tools.ietf.org/html/rfc5340
72. Savage D. RFC 7868: Enhanced Interior Gateway Routing Protocol [Електронний ресурс] / D. Savage, J. Ng, S. Moore [та ін.] // Request for Comments. – 2016. – С. 80. – Режим доступу : https://tools.ietf.org/html/rfc7868
73. Atkinson R. RFC 4822: RIPv2 Cryptographic Authentication [Електронний ресурс] / R. Atkinson, M. Fanto // Request for Comments. – 2007. – С. 22. – Режим доступу : https://tools.ietf.org/html/rfc4822
74. Bhatia M. RFC 7474: Security Extension for OSPFv2 When Using Manual Key Management [Електронний ресурс] / M. Bhatia, S. Hartman, D. Zhang [та ін.] // Request for Comments. – 2015. – С. 14. – Режим доступу : https://tools.ietf.org/html/rfc7474
75. Указ Президента України від 27.09.1999 №1229/99 «Про Положення про технічний захист інформації в Україні» // Офіційний вісник України, 15.10.1999, № 39, стор. 28, код акту 11180/199.
76. Закон Верховної Ради України від 05.07.1994 №80-94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах» // Відомості Верховної Ради України, 02.08.1994, № 31, стаття 286.

77. Проект «Концепція інформаційної безпеки України» // Міністерство Інформаційної Політики України. – 2015. – Режим доступу : http://mip.gov.ua/done_img/d/30-project_08_06_15.pdf
78. Scarfone K. NIST Special Publication 800-94 Guide to intrusion detection and prevention systems (IDPS) [Електронний ресурс] / K. Scarfone, P. Mell // National Institute of Standards and Technology. – 2007. – Режим доступу : http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf
79. Scarfone K. NIST Special Publication 800-94 Revision 1 (Draft) Guide to intrusion detection and prevention systems (IDPS) [Електронний ресурс] / K. Scarfone, P. Mell // National Institute of Standards and Technology. – 2012. – Режим доступу : http://csrc.nist.gov/publications/drafts/800-94-rev1/draft_sp800-94-rev1.pdf
80. Kiravuo T. A survey of ethernet lan security / T. Kiravuo, M. Sarela, J. Manner // Communications Surveys & Tutorials. – 2013. – Т. 15. – № 3. – С. 1477-1491.
81. Catalyst 2960-X Switch Security Configuration Guide, Cisco IOS Release 15.0(2)EX [Електронний ресурс] // Cisco Systems. – 2013. – 468 с. – Режим доступу : http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/security/configuration_guide/b_sec_152ex_2960-x_cg.pdf
82. Shashank S. Cisco Guide to Harden Cisco IOS Devices [Електронний ресурс] / S. Shashank // Cisco Systems – 2016. – Режим доступу : http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html
83. Horowitz M. Security Checklist [Електронний ресурс] / M. Horowitz // routersecurity.org. – 2016. – Режим доступу : http://routersecurity.org/checklist.php
84. Diver S. Information Security Policy - A Development Guide for Large and Small Companies [Електронний ресурс] / S. Diver // SANS Institute Reading Room. – 2006. – Режим доступу : https://www.sans.org/reading-

room/whitepapers/policyissues/information-security-policy-development-guide-large-small-companies-1331

85. Router and Switch Security Policy [Електронний ресурс] // SANS Institute. – 2014. – Режим доступу : http://www.ipcert.it/media/kunena/attachments/484/Router_and_switch_security_policy.pdf
86. Sample Policies [Електронний ресурс] // www.dmoz.org. – Режим доступу : https://www.dmoz.org/Computers/Security/Policy/Sample_Policies
87. Elky S. An Introduction to Information System Risk Management [Електронний ресурс] / S. Elky // SANS Institute Reading Room. – 2006. – С. 15. – Режим доступу : https://www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management-1204
88. Peltier T.R. Information security risk analysis / T.R. Peltier // CRC press. – 2005. – С. 344.
89. Landoll D.J. The security risk assessment handbook: A complete guide for performing security risk assessments / D.J. Landoll // CRC Press. – вид. 2. – 2005. – С. 456.
90. Mell P. The common vulnerability scoring system (CVSS) and its applicability to federal agency systems [Електронний ресурс] / P. Mell, K. Scarefone, S. Romanosky // National Institute of Standards and Technology. – 2007. – 23 с. – Режим доступу : https://www.first.org/cvss/cvss-v2-guide.pdf
91. SecTools.Org: Top 125 Network Security Tools [Електронний ресурс] // SecTools.Org. – Режим доступу : http://sectools.org/tag/vuln-scanners
92. About CVE [Електронний ресурс] // cve.mitre.org: Common Vulnerabilities and Exposures. – Режим доступу : https://cve.mitre.org/about/
93. Common Vulnerability Scoring System v3.0: Specification Document [Електронний ресурс] // www.first.org: Forum of Incident Response and Security Teams. – Режим доступу : https://www.first.org/cvss/specification-document

94. Common Vulnerability Scoring System v3.0: User Guide [Електронний ресурс] // www.first.org: Forum of Incident Response and Security Teams. – Режим доступу : https://www.first.org/cvss/user-guide
95. Common Vulnerability Scoring System v3.0: Examples [Електронний ресурс] // www.first.org: Forum of Incident Response and Security Teams. – Режим доступу : https://www.first.org/cvss/examples
96. Common Vulnerability Scoring System v3.0: Calculator [Електронний ресурс] // www.first.org: Forum of Incident Response and Security Teams. – Режим доступу : https://www.first.org/cvss/calculator/3.0
97. Додонов А.Г. Живучесть информационных систем. / А.Г. Додонов, Д.В. Ландэ. – К. : Наук. думка, 2011. — 256 с.
98. Зубок В.Ю. Аналіз впливу топології на ефективність та вразливість в глобальних комп‘ютерних мережах / В.Ю. Зубок // Information Technology and Security. – 2012. – № 2. – С. 17-25.
99. No G. An efficient and reliable DDoS attack detection using a fast entropy computation method / G. No, I. Ra // 9-th International Symposium on Communications and Information Technology (ISCIT'09) : Тези доп. – Інчхон, 2009. – С. 1223-1228.
100. No G. Adaptive DDoS detector design using fast entropy computation method / G. No, I. Ra // Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS) – 5th International Conference : Тези доп. – Сеул, 2011. – С. 86-93.
101. Popovskyy V. Entropy Methods for DDoS Attacks Detection in Telecommunication Systems / V. Popovskyy, V. Skibin // Problems of Infocommunications. Science and Technology (PIC S&T-2014) : First International IEEE Conference : Тези доп. – Харків, 2014. – С. 182-185.
102. Бабенко Т.В. Дослідження ентропії мережевого трафіка як індикатора DDOS-атак / Т.В. Бабенко // Науковий вісник Національного гірничого університету. – 2013. – № 2. – С. 86-89.

103. Rakićević A. Comparison of moving averages for trading trends: the case of the belgrade stock exchange / A. Rakićević, R. Končarević, B. Petrović // SymOrg – XIV International Symposium : Тези доп. – Златібор, 2014. – С. 688-695.
104. Ehlers J.F. Nonlinear Ehlers Filters / J.F. Ehlers // Technical Analysis of Stocks & Commodities. – 2001. – Т. 19. – № 4. – С. 25-34.
105. Understanding Cisco Express Forwarding (CEF) [Електронний ресурс] // Cisco Systems. – 2006. – Режим доступу : http://www.cisco.com/c/en/us/support/docs/routers/12000-series-routers/47321-ciscoef.html
106. Cisco Express Forwarding Overview [Електронний ресурс] // Cisco Systems. – 2014. – Режим доступу : http://www.cisco.com/c/en/us/td/docs/ios/12_2/switch/configuration/guide/fswtch_c/xcfcef.html
107. Performance Tuning Basics [Електронний ресурс] // Cisco Systems. – 2007. – Режим доступу : http://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-121-mainline/12809-tuning.html
108. Troubleshooting High CPU Utilization [Електронний ресурс] // Cisco Systems – 2016. – Режим доступу : http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/troubleshooting/cpu_util.html
109. Sarabjeet S.C. Impact of Network Address Translation on Router Performance [Електронний ресурс] / S.C. Sarabjeet // VirginiaTech Digital Library and Archives. – 2003. – С. 45, – Режим доступу : https://theses.lib.vt.edu/theses/available/etd-10062003-170440/unrestricted/thesis.pdf
110. Paredes-Farrera M., Fleury M., Ghanbari M. Router response to traffic at a bottleneck link [Електронний ресурс] / M. Paredes-Farrera, M. Fleury, M. Ghanbari // Research Infrastructures for the DEvelopment of NeTworks & COMmunities (TRIDENTCOM) : 2nd International Conference : Тузисы док. – Барселона, 2006. – С. 4, – Режим доступу : https://www.res

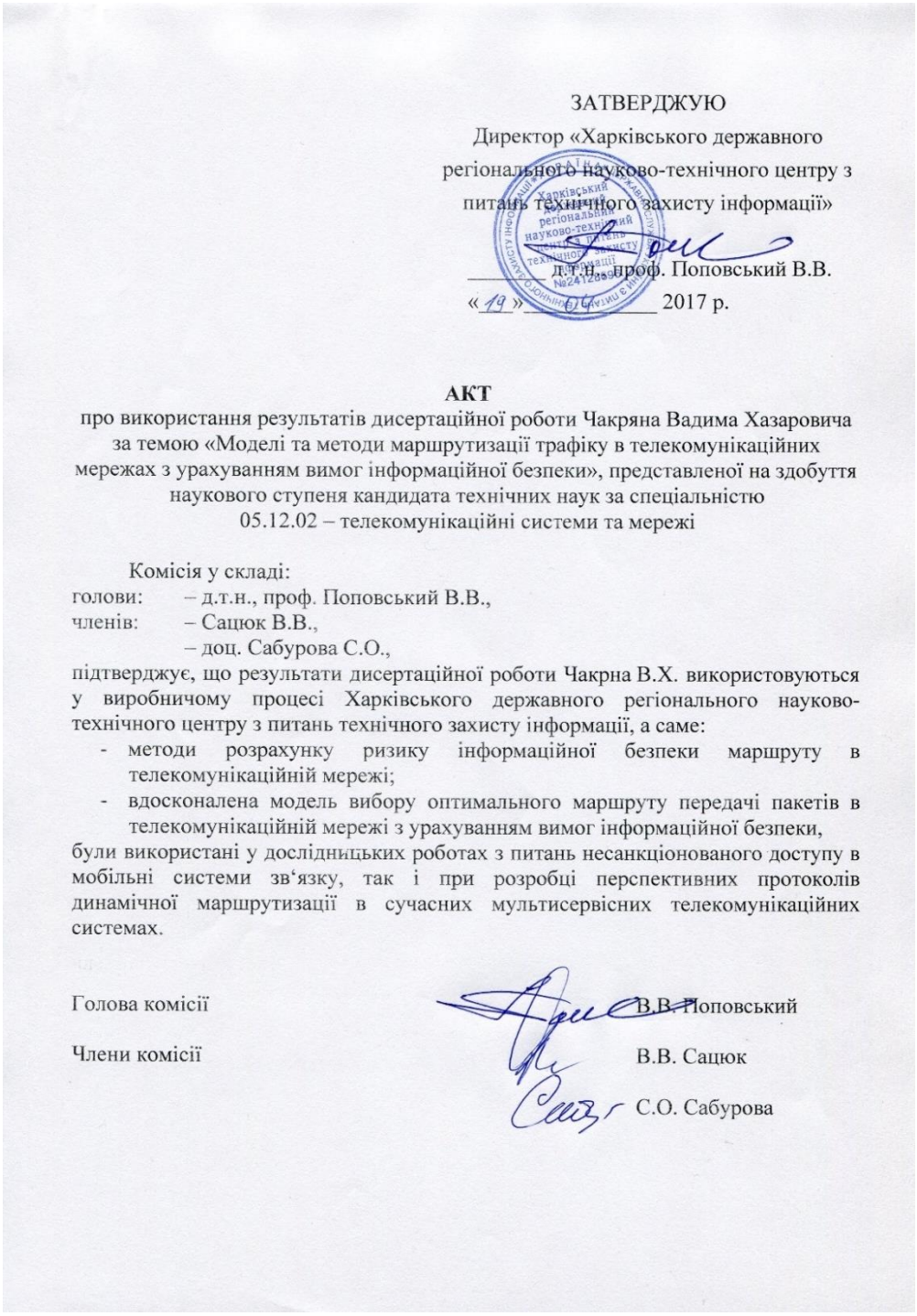
earchgate.net/publication/220864499_Router_response_to_traffic_at_a_bottleneck_link

111. Bobyshev A., DeMar P., Lamore D. Affects of dynamic ACL (Access Control List) loading on performance of Cisco routers [Електронний ресурс] / A. Bobyshev, P. DeMar, D. Lamore // Computing in High Energy Physics : Тези доп. – Мумбаї, 2006. – С. 3, – Режим доступу : http://cd-docdb.fnal.gov/0012/001260/002/dynamic_ACL_Paper.pdf
112. Troubleshooting High CPU Utilization on Cisco Routers [Електронний ресурс] // Cisco Systems. – 2016. – Режим доступу : http://www.cisco.com/c/en/us/support/docs/routers/10000-series-routers/15095-highcpu.html
113. Sharad A. Impact of BGP Dynamics on Router CPU Utilization / A. Sharad, C. Chen-Nee, B. Supratik [та ін.] // International Workshop on Passive and Active Network Measurement – Springer Berlin Heidelberg, 2004. – С. 278-288.
114. Troubleshooting High CPU Utilization Due to Interrupts [Електронний ресурс] // Cisco Systems. – 2016. – Режим доступу : http://www.cisco.com/c/en/us/support/docs/routers/7500-series-routers/41120-highcpu-interrupts.html
115. Troubleshooting High CPU Utilization due to Processes [Електронний ресурс] // Cisco Systems. – 2008. – Режим доступу : http://www.cisco.com/c/en/us/support/docs/routers/7500-series-routers/41180-highcpu-processes.html
116. Troubleshooting High CPU Caused by the BGP Scanner or BGP Router Process [Електронний ресурс] // Cisco Systems. – 2015. – Режим доступу : http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/107615-highcpu-bgp.html
117. High CPU Utilization in Exec and Virtual Exec Processes [Електронний ресурс] // Cisco Systems. – 2008. – Режим доступу : http://www.cisco.com/c/en/us/support/docs/routers/7500-series-routers/41100-highcpu-exec.html

118. Troubleshooting High CPU Utilization Caused by the HyBridge Input Process on Routers With ATM Interfaces [Електронний ресурс] // Cisco Systems – 2005. – Режим доступу : http://www.cisco.com/c/en/us/support/docs/asynchronous-transfer-mode-atm/ip-over-atm/10448-hybridge.html
119. Troubleshooting High CPU Utilization in IP Input Process [Електронний ресурс] // Cisco Systems. – 2006. – Режим доступу : http://www.cisco.com/c/en/us/support/docs/routers/7500-series-routers/41160-highcpu-ip-input.html
120. IP Simple Network Management Protocol (SNMP) Causes High CPU Utilization [Електронний ресурс] // Cisco Systems. – 2014. – Режим доступу : http://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/7270-ipsnmphighcpu.html
121. Сухоруков Ю.С. Динамика ситуационных конфликтов / В кн. Дружинин В.В., Конторов Д.С., Конторов М.Д. – Введение в теорию конфликта // М. : Радио и связь. – 1989. – С. 280-285.
122. Методические основы формирования модели конфликта [Текст] / Ю.Л. Козирацкий, М.Л. Паринов, С.В. Петренков [та ін.] // Телекоммуникации. – 2011. – № 4. – С. 2-7.
123. Козирацкий Ю.Л. Модель процесса возникновения и протекания конфликта информационных средств разных видов [Текст] / Ю.Л. Козирацкий, С.А. Будников, Д.Б. Островский [та ін.] // Радиотехника. – 2011. – № 8. – С. 6-11.
124. Клейнрок Л. Теория массового обслуживания / Л. Клейнорк. – М. : Машиностроение, 1979. – 432 с.
125. Поповский В.В. Обзор и сравнительный анализ основных моделей и алгоритмов многопутевой маршрутизации в мультисервисных телекоммуникационных сетях / В.В. Поповский, А.В. Лемешко, Л.И. Мельникова [та ін.] // Прикладная радиоэлектроника. – 2005. – Т. 4. – № 4. – С. 372-382.

126. Лемешко А.В. Анализ решений задач однопутевой и многопутевой маршрутизации многопотокового трафика в телекоммуникационных сетях / А.В. Лемешко, Т.В. Вавенко // Системи обробки інформації. – 2011. – № 8. – С. 224-228.
127. Gallager R.G. A minimum delay routing algorithm using distributed computation / R.G. Gallager // IEEE Transactions on Communications. – 1977. – Т. 25. – № 1. – С. 73-85.
128. Лемешко А.В. Модель многопутевой QoS-маршрутизации в мультисервисной телекоммуникационной сети / А.В. Лемешко, О.А. Дробот // Радиотехника: Всеукр. межвед. науч.-техн. сб. – 2006. – № 144. – С. 16-22.
129. IEEE Std 802.3bm-2015. IEEE Standard for Ethernet - Amendment 3: Physical Layer Specifications and Management Parameters for 40 Gb/s and 100 Gb/s Operation over Fiber Optic Cables [Електронний ресурс] // IEEE Standards Association. – 2015. – Режим доступу : https://standards.ieee.org /findstds/standard/802.3bm-2015.html
130. Multicast Boundaries [Електронний ресурс] // Microsoft Technet. – Режим доступу: https://technet.microsoft.com/en-us/library/cc957926.aspx
131. How Does Unequal Cost Path Load Balancing (Variance) Work in IGRP and EIGRP? [Електронний ресурс] // Cisco Systems. – 2009. – Режим доступу : http://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/13677-19.html
132. Adomnicăi C. Routing protocols behaviour under bandwidth limitation / C. Adomnicăi // International Conference on Information and Computer Networks. – 2012. – Т. 27. – С. 52-57.
133. Prabhu A. CEF Polarization [Електронний ресурс] / A. Prabhu, S. Singh, S. Dhodapkar // Cisco Systems. – 2013. – Режим доступу : http://www.cisco.com/c/en/us/support/docs/ip/express-forwarding-cef/116376-technote-cef-00.html

ДОДАТОК А
АКТИ ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЙНИХ ДОСЛІДЖЕНЬ



ЗАТВЕРДЖУЮ
Директор «Харківського державного регіонального науково-технічного центру з питань технічного захисту інформації»
_____ д.т.н., проф. Поповський В.В.
«19» 04 2017 р.

АКТ
про використання результатів дисертаційної роботи Чакряна Вадима Хазаровича за темою «Моделі та методи маршрутизації трафіку в телекомунікаційних мережах з урахуванням вимог інформаційної безпеки», представленої на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі

Комісія у складі:
голови: – д.т.н., проф. Поповський В.В.,
членів: – Сацюк В.В.,
– доц. Сабурова С.О.,
підтверджує, що результати дисертаційної роботи Чакрна В.Х. використовуються у виробничому процесі Харківського державного регіонального науково-технічного центру з питань технічного захисту інформації, а саме:

- методи розрахунку ризику інформаційної безпеки маршруту в телекомунікаційній мережі;
- вдосконалена модель вибору оптимального маршруту передачі пакетів в телекомунікаційній мережі з урахуванням вимог інформаційної безпеки,

були використані у дослідницьких роботах з питань несанкціонованого доступу в мобільні системи зв'язку, так і при розробці перспективних протоколів динамічної маршрутизації в сучасних мультисервісних телекомунікаційних системах.

Голова комісії В.В. Поповський
Члени комісії В.В. Сацюк
С.О. Сабурова

Рис. А.1. Акт впровадження результатів дисертаційних досліджень у Харківському державному регіональному науково-технічному центрі з питань технічного захисту інформації

ЗАТВЕРДЖУЮ
Ректор Харківського національного
університету радіоелектроніки

В.В. Семенець

«11» 04 2017 р.

АКТ
про впровадження в навчальний процес
Харківського національного університету радіоелектроніки
результатів дисертаційної роботи аспіранта кафедри інфокомунікаційної інженерії
Чакряна Вадима Хазаровича
на тему «Моделі та методи маршрутизації трафіку з урахуванням вимог інформаційної безпеки»

Комісія у складі: завідувача кафедрою інфокомунікаційної інженерії професора д.т.н. Поповського В.В., декана факультету інфокомунікацій, доцента кафедри інфокомунікаційної інженерії к.т.н. Снігурова А.В., професора кафедри інфокомунікаційної інженерії д.т.н. Лемешко О.В., доцента кафедри інфокомунікаційної інженерії к.т.н. Єременко О.С., підтверджує, що результати дисертаційної роботи Чакряна В.Х. на тему «Моделі та методи маршрутизації трафіку з урахуванням вимог інформаційної безпеки» використовуються в навчальному процесі Харківського національного університету радіоелектроніки на кафедрі інфокомунікаційної інженерії, а саме:

1. Наукові положення і результати дисертаційної роботи були використані при підготовці лекційних матерілів із дисципліни «Безпека інформації в інформаційно-комунікаційних системах», яка читається на кафедрі інфокомунікаційної інженерії для студентів спеціальності 125 «Кібербезпека».

2. Програмний комплекс, що реалізовує методи динамічної маршрутизації з урахуванням вимог інформаційної безпеки покладено в основу лабораторних робіт з курсу «Безпека інформації в інформаційно-комунікаційних системах».

В.В. Поповський

А.В. Снігуров

О.В. Лемешко

О.С. Єременко

Рис. А.2. Акт впровадження результатів дисертаційних досліджень у Харківському національному університеті радіоелектроніки

ЗАТВЕРДЖУЮ
Директор Державного підприємства
“Центральне конструкторське бюро “ПРОТОН”
к.т.н.
О.І. ВОТЯКОВ
« 15 » 03 2017 р.

ДЕРЖАВНЕ ПІДПРИЄМСТВО "ЦЕНТРАЛЬНЕ КОНСТРУКТОРСЬКЕ БЮРО "ПРОТОН" №14309408 УКРАЇНА

АКТ

про використання результатів дисертаційних досліджень
Чакряна Вадима Хазаровича

Комісія у складі: голови – головного інженера-головного конструктора ДП “ЦКБ “Протон” к.т.н. Білокурова О.О., членів комісії: головного наукового співробітника ДП “ЦКБ “Протон” к.т.н. Голобородько Ю.М., начальника науково-дослідного відділу ДП “ЦКБ “Протон” Смілика В.І., начальника науково-дослідної лабораторії ДП “ЦКБ “Протон” Веселовського Ю.А. склала дійсний акт в тому, що при розробці системи мережевого обміну Пристрою радіомоніторингу КХ діапазону Р-677 УИДЯ.466948.006 (прийнятий на озброєння Збройних Сил України наказом Міністра оборони України № 323 від 07.07.2015р.) використані наступні наукові результати дисертаційної роботи здобувача кафедри інфокомунікаційної інженерії Чакряна Вадима Хазаровича:

- математична модель динамічної маршрутизації трафіку з урахуванням вимог інформаційної безпеки. Модель дає можливість визначення найбезпечнішого шляху передачі інформації в мережі на основі критерію якість-безпека;

Рис А.3. Перший аркуш акта впровадження результатів дисертаційних досліджень у Державному підприємстві «Центральне конструкторське бюро «ПРОТОН»

- метод вибору оптимального шляху передачі трафіку для протоколу динамічної маршрутизації RIP. Метод дозволяє обирати найбільш безпечний шлях в інформаційній мережі.

- метод врахування ризиків інформаційної безпеки у формулі розрахунку метрики протоколу динамічної маршрутизації EIGRP. Метод дозволяє знаходити оптимальний маршрут передачі трафіку в мережі на основі критерію якість-безпека.

Використання результатів наукових досліджень Чакряна В.Х. дозволило підвищити інформаційну безпеку транзитних даних в інформаційній мережі в процесі динамічної маршрутизації трафіку.

ГОЛОВА КОМІСІЇ

Головний інженер-головний конструктор
к.т.н. О.О. Білокуров

ЧЛЕНИ КОМІСІЇ:

ГНС к.т.н. Ю.М. Голобородько

Начальник НДВ В.І. Смілик

Начальник НДЛ Ю.А. Веселовський

Рис А.4. Другий аркуш акта впровадження результатів дисертаційних досліджень у Державному підприємстві «Центральне конструкторське бюро «ПРОТОН»

ДОДАТОК Б
ТИПОЛОГІЯ АТАК ПО ЇХ ФУНКЦІОНАЛЬНОМУ ПРИЗНАЧЕННЮ

Таблиця Б.1

Типи атак на процес маршрутизації по їх функціональному призначенню

№	Атаки	*DoS*	*RR*
1	Атака на процес виявлення маршрутизатора в IPv6	–	+
2	Атака на SLAAC в IPv6	–	+
3	Атака на процес виявлення MAC адреси в IPv6	–	+
4	Атака на процес виявлення дублювання IPv6 адрес	+	–
5	Впровадження підробленого DHCP сервера	–	+
6	Маніпуляція оновленнями ПДМ	–	+
7	Атака на переповнення кеш-пам'яті маршрутизатора	+	–
8	Здійснення DoS за допомогою ICMP протоколу	+	–
9	Наводнення IPv6 RA пакетами	+	–
10	Здійснення DoS атаки за допомогою CGA	+	–
11	DoS атака шляхом маніпуляції параметром MTU	+	–
12	DoS атака шляхом зміни TTL і CHL полів пакету	+	–
13	Виснаження адрес на DHCP сервері	+	–
14	Атаки шляхом наводнення ТКМ пакетами	+	–
15	Атаки на переповнення буфера	+	–
16	Атаки можливі шляхом проникнення на мережевий вузол з правами адміністратора	+	+
17	Порушення фізичного середовища передачі ПП	+	–

Де в табл. Б.1:

№ – порядковий номер атаки;

DoS – атаки на доступність;

RR – атаки перенаправлення.

ДОДАТОК В
ПАРАМЕТРИ БАЗОВИХ МЕТРИК СТАНДАРТУ NIST CVSS V2

Таблиця В.1

Параметри базових метрик стандарту NIST CVSS v2

Значення	Опис	Числова характеристика
Вектор доступу		
Потребується локальний доступ (Л)	зловмисникові потрібен безпосередній фізичний доступ до об'єкта, на якому розташована вразливість	0,395
Можливий доступ із суміжної мережі (СмМ)	зловмисникові потрібен доступ в межах однієї локальний мережі (одного широкомовного домену) з уразливим об'єктом	0,646
Можливий доступ з будь-якої мережі (М)	зловмисник може експлуатувати уразливість віддалено з будь-якої ділянки мережі, в тому числі через Інтернет	1,0
Автентифікація		
Множинна (М)	зловмисник повинен зробити більше однієї процедури автентифікації для експлуатації вразливості	0,45
Одинична (О)	зловмиснику досить одного разу автентифікуватися для експлуатації вразливості	0,56
Відсутня (В)	зловмисникові не потрібно проходити процедуру автентифікації для експлуатації вразливості	0,704
Складність доступу		
Складна (Ск)	Існує ряд жорстких обмежень, наприклад, експлуатація можливо тільки в дуже короткий проміжок часу, або вимагає застосування соціальної інженерії, при якій зловмисник може бути легко впізнаний	0,35
Середня (Ср)	Існують деякі обмеження доступу, наприклад, підключення до уразливому пристрою можливо тільки з певних вузлів, або вразливе пристрій повинен функціонувати з нестандартними налаштуваннями	0,61

Продолжение таблицы В.1

Значення	Опис	Числова характеристика
Легка (Л)	Немає особливих умов для доступу до вразливості, наприклад, коли система доступна багатьом користувачам одночасно або коли вразлива конфігурація працює на безлічі вузлів мережі	0,71
Збиток конфіденційності		
Відсутній (В)	Можливість порушення конфіденційність інформації відсутня	0,0
Частковий (Ч)	Існує значна можливість, однак обмежене розголошення чутливої інформації	0,275
Повний (П)	Існує можливість повного розкриття секретної інформації	0,66
Збиток цілісності		
Відсутній (В)	Можливість порушення цілісності інформації відсутня	0,0
Частковий (Ч)	Існує можливість часткової модифікації даних або системних файлів	0,275
Повний (П)	Існує можливість модифікації будь-яких даних системи	0,66
Збиток доступності		
Відсутній (В)	Можливість порушення доступності ресурсу відсутня	0,0
Частковий (Ч)	Існує можливість зниження продуктивності або виведення з ладу деяких функцій системи	0,275
Повний (П)	Існує можливість повного виведення з ладу системи	0,66

ДОДАТОК Г

ПРИКЛАД ПРОГРАМНОГО КОДУ ДЛЯ РОЗРАХУНКУ ЕФЕКТИВНОСТІ МАРШРУТИЗАТОРА МЕРЕЖІ, ЩО РЕАЛІЗОВАНИЙ У MATLAB

```
clc; clear all;
%% опис основних параметрів
% 'r' – ПП, що поступає в ТКМ [мбіт/с]
r = 1;
% "c" – ПРЗД КЗ [мбіт/с]
%              R1<->R2,  R1<->R3, R2<->R4, R2<->R5, R3<->R2, R3<->R4, R4<->R5, R5<->WAN
bandwidth = [ 100;         100;         100;         100;         100;         100;         100;         100;
                100;         100;         100;         100;         100;         100;         100;         100;];
c = bandwidth;

% розрахунок затримки в КЗ
for i=1:1:length(bandwidth)
   if ( bandwidth(i) == 1 && bandwidth(i) < 100 )
      delay(i) = 10000
   end
   if ( bandwidth(i) > 1 && bandwidth(i) < 100 )
      delay(i) = 100
   end
   if ( bandwidth(i) >= 100 && bandwidth(i) < 1000 )
      delay(i) = 10
   end
   if ( bandwidth(i) >= 1000 )
      delay(i) = 1
   end
end

% розрахунок метрик КЗ
for i=1:1:length(bandwidth)
   metric(i) = ( (10^8 / (bandwidth(i)*10^3)) + delay(i) ) * 256
end
f = metric;

%% опис з'єднань вузлів ТКМ між собою
%       inverse direction   |   reverse direction   WAN
Aeq = [ 1  1  0  0  0  0  0  0  0  0  0 -1  0 -1       0  0
          -1  0  1  1  1  0  0 -1  0 -1  0  0 -1  1       0  0
           0 -1  0  0 -1  1  0  0  0  0 -1  1  1  0       0  0
           0  0 -1  0  0 -1  1  0 -1  1  1  0  0  0       0  0
           0  0  0 -1  0  0 -1  1  1  0  0  0  0  0       1 -1
           0  0  0  0  0  0  0  0  0  0  0  0  0  0      -1  1];
beq = [1; 0; 0; 0; 0; -1];

A = [r 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
      0 r 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
```

```
        0 0 r 0 0 0 0 0 0 0 0 0 0 0 0
        0 0 0 r 0 0 0 0 0 0 0 0 0 0 0
        0 0 0 0 r 0 0 0 0 0 0 0 0 0 0
        0 0 0 0 0 r 0 0 0 0 0 0 0 0 0
        0 0 0 0 0 0 r 0 0 0 0 0 0 0 0
        0 0 0 0 0 0 0 r 0 0 0 0 0 0 0
        0 0 0 0 0 0 0 0 r 0 0 0 0 0 0
        0 0 0 0 0 0 0 0 0 r 0 0 0 0 0
        0 0 0 0 0 0 0 0 0 0 r 0 0 0 0
        0 0 0 0 0 0 0 0 0 0 0 r 0 0 0
        0 0 0 0 0 0 0 0 0 0 0 0 r 0 0
        0 0 0 0 0 0 0 0 0 0 0 0 0 r 0
        0 0 0 0 0 0 0 0 0 0 0 0 0 0 r];
b = c;

%% розрахунок базової ефективності мережі
d = 0;
E = 0;

for k=1:1:length(beq)
   for i=1:1:length(beq)
      beqi = zeros(1,length(beq));
      beqi(k) = 1;
      beqi(i) = -1;
      if (i ~= k)          % не враховується випадок, коли відправник та отримувач однакові
         [x,fval] = bintprog(f,A,b,Aeq,beqi) % 'fval' - метрики; 'x' – шлях в бінарній формі
         d = d + fval;    % розрахунок загальної довжини ТКМ
      end
   end
end

routers = length(beq);
E = ( (1 / routers*(routers-1)) ) * (1 / d);       % розрахунок базової ефективності ТКМ

%% розрахунок ефективності мережі в разі атаки та видалення одного з вузлів «i»
di = zeros(1,length(beq));
Ei = zeros(1,length(beq));
Vi = zeros(1,length(beq));

for j=1:1:length(beq)
   % всі КЗ видаленого вузла – повинні бути рівні нулю
   Aeqi = Aeq;
   bi = b;
   for cols=1:1:length(Aeqi)
      if (Aeqi(j, cols) ~= 0)     % "j" – кількість вузлів ТКМ (зовнішній цикл)
         Aeqi(:, cols) = 0;
         bi(cols) = 0;
      end
   end

   for k=1:1:length(beq)
```

```
      for i=1:1:length(beq)
         beqi = zeros(1,length(beq));
         beqi(k) = 1;
         beqi(i) = -1;
         if (i ~= k)       % не враховується випадок, коли відправник та отримувач однакові
            [x,fval] = bintprog(f,A,bi,Aeqi,beqi); % 'fval' - метрики; 'x' – шлях в бінарній формі
            if (fval ~= inf)
               di(j) = di(j) + fval;    % розрахунок загальної довжини мережі за відсутності вузла «i»
            end
         end
      end
   end

   routersi = length(beqi)-1;
   Ei(j) = ( 1 / (routersi*(routersi-1)) ) * ( 1 / di(j) );          % розрахунок ефективності мережі за
відсутності вузла «i»
   % Розрахунок ЕММ вузла «i»
   Vi(j) = (E - Ei(j)) / E;
end

% процедура нормалізації
Xscale = E/max(Ei)
for i=1:1:length(Ei)
   Vweightedi(i) = (E - Xscale*Ei(i)) / E;
end

% відображення результату на екрані
Vweightedi
```

ДОДАТОК Д
ОЦІНКА ЙМОВІРНОСТІ СВОЄЧАСНОЇ ДОСТАВКИ ПОТОКУ ПАКЕТІВ ОТРИМУВАЧУ ПРИ РІЗНІЙ ЗАВАНТАЖЕНОСТІ ПАКЕТАМИ МАРШРУТИЗАТОРІВ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

Таблиця Д.1

Оцінки ЙСД ПП за 2 с при рівномірній завантаженості маршрутизаторів пакетами, де $\rho = 0{,}7$

$N_{i,DoS}$	p_i	$P1_{дост.}$	$P2_{дост.}$
1	1,2,3,5,6	0,000	0,849
2	1	0,982	0,994
3	1	0,982	0,994
4	1	0,982	0,994
5	2,3,5,6	0,849	0,715
6	3,5	0,991	0,957
7	2	0,957	0,994
8	3,5	0,991	0,957
9	3	0,991	0,994
10	4	0,997	0,977
11	4	0,997	0,977
12	4	0,997	0,977
13	4,6	0,997	0,849
14	4	0,997	0,977

Таблиця Д.2

Оцінки ЙСД ПП за 2 с при рівномірній завантаженості маршрутизаторів пакетами, де $\rho = 0{,}8$

$N_{i,DoS}$	p_i	$P1_{дост.}$	$P2_{дост.}$
1	1,2,3,5,6	0,000	0,567
2	1	0,850	0,882
3	1	0,850	0,882
4	1	0,850	0,882
5	2,3,5,6	0,567	0,371
6	3,5	0,897	0,728
7	2	0,728	0,882
8	3,5	0,897	0,728

Продовження таблиці Д.2

$N_{i,DoS}$	p_i	$P1_{дост.}$	$P2_{дост.}$
9	3	0,897	0,882
10	4	0,935	0,813
11	4	0,935	0,813
12	4	0,935	0,813
13	4,6	0,935	0,567
14	4	0,935	0,813

Таблиця Д.3

Оцінки ЙСД ПП за 2 с при рівномірній завантаженості маршрутизаторів пакетами, де $\rho = 0{,}9$

$N_{i,DoS}$	p_i	$P1_{дост.}$	$P2_{дост.}$
1	1,2,3,5,6	0,000	0,143
2	1	0,359	0,304
3	1	0,359	0,304
4	1	0,359	0,304
5	2,3,5,6	0,143	0,053
6	3,5	0,420	0,188
7	2	0,188	0,304
8	3,5	0,420	0,188
9	3	0,420	0,304
10	4	0,451	0,266
11	4	0,451	0,266
12	4	0,451	0,266
13	4,6	0,451	0,143
14	4	0,451	0,266

Таблиця Д.4

Оцінки ЙСД ПП за 2 с при рівномірній завантаженості маршрутизаторів пакетами, де $\rho = 0{,}95$

$N_{i,DoS}$	p_i	$P1_{дост.}$	$P2_{дост.}$
1	1,2,3,5,6	0,000	0,019
2	1	0,083	0,041
3	1	0,083	0,041
4	1	0,083	0,041
5	2,3,5,6	0,019	0,003
6	3,5	0,097	0,022

Продовження таблиці Д.4

$N_{i,DoS}$	p_i	$P1_{дост.}$	$P2_{дост.}$
7	2	0,022	0,041
8	3,5	0,097	0,022
9	3	0,097	0,041
10	4	0,100	0,038
11	4	0,100	0,038
12	4	0,100	0,038
13	4,6	0,100	0,019
14	4	0,100	0,038

Де в табл. Д.1-Д.4:

$N_{i,DoS}$ – номери вузлів, що вийшли з ладу;

p_i – номери шляхів, що вийшли з ладу;

$P1_{дост.}$ – ЙСД ПП до вузла-отримувача №1;

$P2_{дост.}$ – ЙСД ПП до вузла-отримувача №2.

ДОДАТОК Е
ЗАЛЕЖНІСТЬ ЗНАЧЕННЯ МЕТРИКИ ШЛЯХУ ПЕРЕДАЧІ ВІД РИЗИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ПРОТОКОЛУ RIP

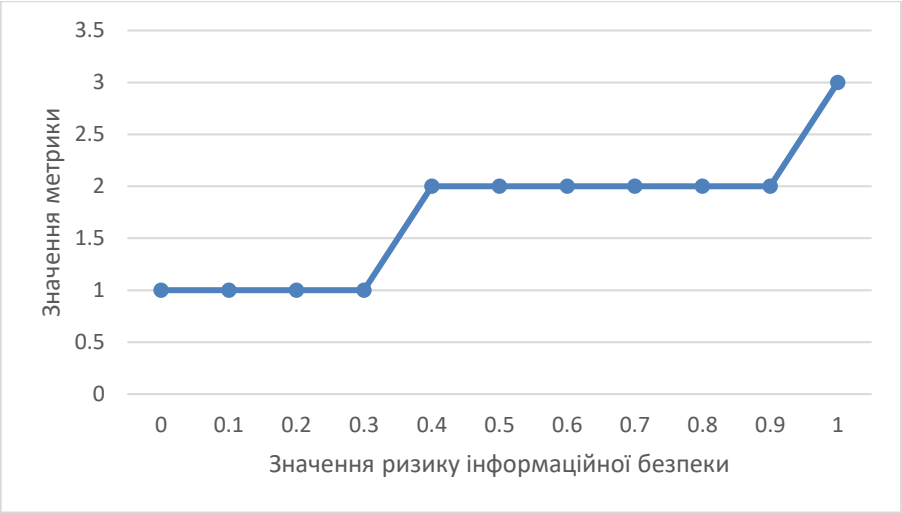


Рис. Е.1. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.6)

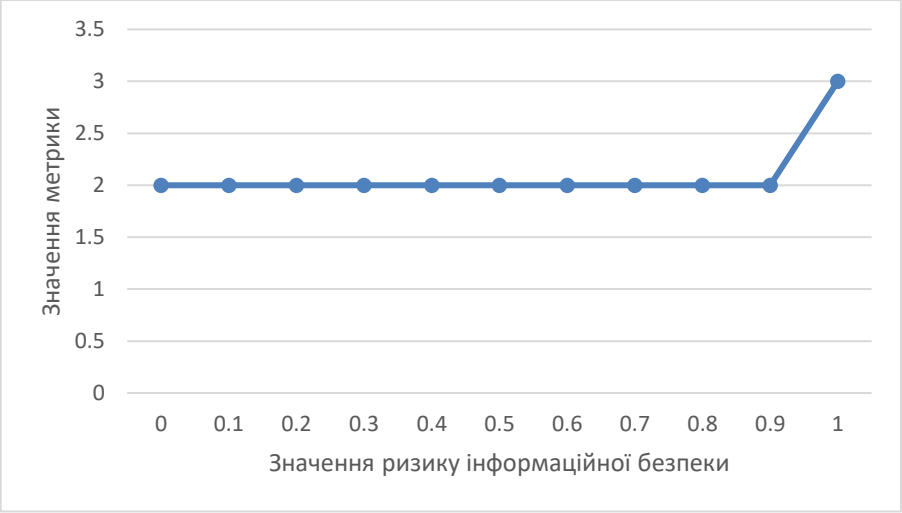


Рис. Е.2. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.7)

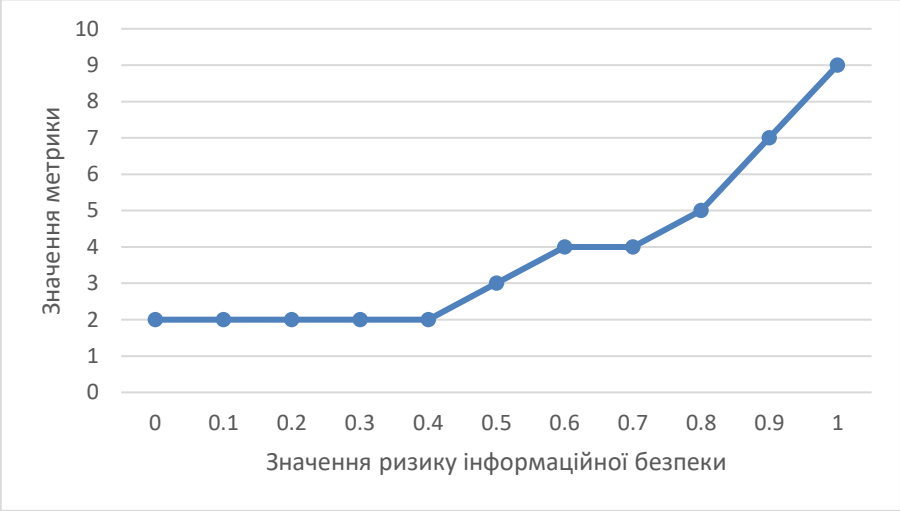


Рис. Е.3. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.8)

Рис. Е.4. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.9)

Рис. Е.5. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.10)

Рис. Е.6. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.11)

Рис. Е.7. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.12)

Рис. Е.8. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.13)

Рис. Е.9. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.14)

Рис. Е.10. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.15)

ДОДАТОК Ж
ЗАЛЕЖНІСТЬ ЗНАЧЕННЯ МЕТРИКИ ШЛЯХУ ПЕРЕДАЧІ ВІД РИЗИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ПРОТОКОЛУ OSPF

Рис. Ж.1. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.6)

Рис. Ж.2. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.7)

Рис. Ж.3. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.8)

Рис. Ж.4. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.9)

Рис. Ж.5. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.10)

Рис. Ж.6. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.11)

Рис. Ж.7. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.12)

Рис. Ж.8. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.13)

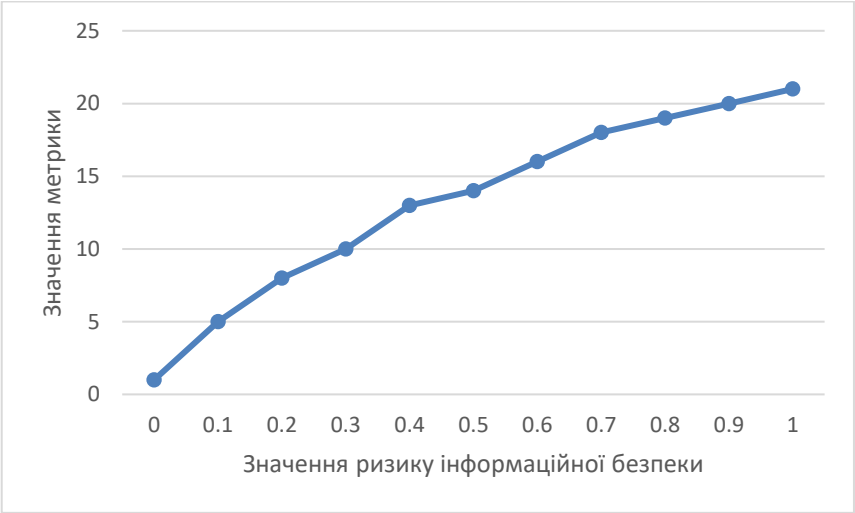


Рис. Ж.9. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.14)

Рис. Ж.10. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.15)

Таблиця Ж.1

Залежність метрики шляху OSPF з урахуванням РІБ від початкового значення метрики без урахування РІБ для формули (3.7) – варіант А, формули (3.10) – варіант Б, та формули (3.13) – варіант В відповідно.

	$M=2$			$M=8$			$M=32$			$M=128$		
	А	Б	В	А	Б	В	А	Б	В	А	Б	В
$R=0$	1	0	1	4	0	1	16	2	1	64	8	1
$R=0{,}1$	1	0	1	4	0	1	16	2	1	64	10	1
$R=0{,}2$	1	0	1	4	0	1	17	3	2	65	13	2
$R=0{,}3$	1	0	1	4	1	1	17	4	2	66	18	4
$R=0{,}4$	1	0	1	5	1	2	18	6	4	67	24	6
$R=0{,}5$	1	0	1	5	2	2	18	8	5	69	32	11
$R=0{,}6$	1	0	1	5	2	3	20	10	8	73	42	18
$R=0{,}7$	1	0	1	6	3	4	21	13	11	78	55	29
$R=0{,}8$	1	1	1	6	4	5	24	18	16	88	73	48
$R=0{,}9$	1	1	1	7	6	6	27	24	22	103	97	78
$R=1$	2	2	2	8	8	8	32	32	32	128	128	128

ДОДАТОК И
ЗАЛЕЖНІСТЬ ЗНАЧЕННЯ МЕТРИКИ ШЛЯХУ ПЕРЕДАЧІ ВІД РИЗИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ПРОТОКОЛУ EIGRP

И.1. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.11) при $x = 256$

И.2. Залежність метрики шляху передачі від ризику інформаційної безпеки для формули (3.12) при $x = 16$

ДОДАТОК К
ПРИКЛАДИ РОЗРАХУНКУ МЕТРИКИ ПРОТОКОЛУ RIP В ЗАЛЕЖНОСТІ ВІД ПАРАМЕТРА РИЗИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Таблиця К.1

Метрика ПДМ RIP в залежності від параметру РІБ

Кількість ретрансляцій пакету	Параметр РІБ $R_{p_{i,j}}$										
	0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1
$Hops = 1$	1	1	1	1	1	2	3	3	4	6	8
$Hops = 2$	1	1	1	2	2	2	3	4	5	6	8
$Hops = 3$	2	2	2	2	2	3	4	4	5	7	9
$Hops = 4$	2	2	2	3	3	3	4	5	6	7	9
$Hops = 5$	3	3	3	3	3	4	5	5	6	8	10
$Hops = 6$	3	3	3	4	4	4	5	6	7	8	10
$Hops = 7$	4	4	4	4	4	5	6	6	7	9	11
$Hops = 8$	4	4	4	5	5	5	6	7	8	9	11
$Hops = 9$	5	5	5	5	5	6	7	7	8	10	12
$Hops = 10$	5	5	5	6	6	6	7	8	9	10	12
$Hops = 11$	6	6	6	6	6	7	8	8	9	11	13
$Hops = 12$	6	6	6	7	7	7	8	9	10	11	13
$Hops = 13$	7	7	7	7	7	8	9	9	10	12	14
$Hops = 14$	7	7	7	8	8	8	9	10	11	12	14
$Hops = 15$	8	8	8	8	8	9	10	10	11	13	15

ДОДАТОК Л
СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ ТА ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ 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 : II міжнародна наук.-техн.конф. : Тези доп. – 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 : Тези доп. – Хакрів, 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 : Тези доп. – Хакрів, 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 : Тези доп. – Хакрів, 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 : Тези доп. – Севастопіль, 2013. – С. 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 : Тези доп. – Севастопіль, 2013. – С. 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 : Тези доп. – Львів, 2013. – С. 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 : Тези доп. – Хакрів, 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 : Тези доп. – Львів, 2014. – С. 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 : Тези доп. – Хакрів, 2014. – С. 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 : Тези доп. – Хакрів, 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 : Тези доп. – Хакрів, 2015. – С. 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 : Тези доп. – Львів, 2016. – С. 537-539.
22. Пат. 107617 Україн, 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.