DOI: https://doi.org/10.36910/6775-2524-0560-2024-55-16
УДК: 004.7
Маруняк Станіслав Тарасович, аспірант
http://orcid.org/0009-0006-0635-512X
Національний університет «Львівська Політехніка», м. Львів, Україна

ВИЯВЛЕННЯ ТА ПОМ'ЯКШЕННЯ ВРАЗЛИВОСТЕЙ БЕЗПЕКИ В ПРОТОКОЛАХ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ: ПОТОЧНІ ВИКЛИКИ ТА РІШЕННЯ

Маруняк С.Т. Виявлення та пом'якшення вразливостей безпеки в протоколах динамічної маршрутизації: поточні виклики та рішення. У сучасному світі, де цифрова інфраструктура стає все більш комплексною та взаємопов'язаною, динамічна маршрутизація відіграє ключову роль у підтримці ефективності та гнучкості мережевих систем. Метою статті є визначення актуального стану безпекових вразливостей у протоколах динамічної маршрутизації, що застосовуються в мережевих системах, та запропонувати комплексну стратегію зниження ризиків з використанням можливостей штучного інтелекту. Стаття розглядає різні протоколи динамічної маршрутизації, такі як OSPF, IS-IS, BGP, та EIGRP, їх особливості та сфери застосування в залежності від конкретних потреб та вимог до мережевого середовища. Особлива увага приділяється вибору між цими протоколами з урахуванням факторів, таких як масштабування, гнучкість управління та наявність специфічного обладнання. Акцентовано, що безпека динамічної маршрутизації залишається вразливою до різноманітних загроз через недоліки в аутентифікації, масштабуванні, розподілі навантаження та можливості фальсифікації маршрутизаційної інформації. Наголошено на значенні комплексного підходу до забезпечення безпеки, включаючи застосування сучасних методів аутентифікації, оновлення програмного забезпечення, моніторинг мережі та використання шифрування. Окремо висвітлено роль штучного інтелекту в ідентифікації та пом'якшенні загроз, що відкриває нові перспективи для підвищення безпеки мережевих інфраструктур. Підкреслено необхідність неперервного розвитку та інвестицій в кібербезпеку, а також потребу в стійкій увазі до безпеки на рівні маршрутизаційних протоколів для ефективного протистояння кіберзагрозам. Запропоноване дослідження може бути корисним фаховим дослідникам, аналітикам, бізнесу. Подальші дослідження фокусуватиметься на детальному аналізі впливу штучного інтелекту на виявлення та пом'якшення вразливостей безпеки в протоколах динамічної маршрутизації.
Ключові слова: протоколи динамічної маршрутизації; безпека мережі; вразливості мережі; заходи безпеки; штучний інтелект у кібербезпеці.

Maruniak S. **Detecting and mitigating security vulnerabilities in dynamic routing protocols: current challenges and solutions.** In the modern world, where digital infrastructure is becoming increasingly complex and interconnected, dynamic routing plays a key role in maintaining the efficiency and flexibility of network systems. The purpose of the article is to determine the current state of security vulnerabilities in dynamic routing protocols used in network systems and to propose a comprehensive risk mitigation strategy using artificial intelligence capabilities. The article discusses various dynamic routing protocols, such as OSPF, IS-IS, BGP, and EIGRP, their features and applications depending on specific needs and requirements for the network environment. Particular attention is paid to the choice between these protocols, taking into account factors such as scalability, management flexibility, and the availability of specific equipment. It is emphasized that the security of dynamic routing remains vulnerable to various threats due to shortcomings in authentication, scaling, load balancing, and the possibility of falsifying routing information. The importance of an integrated approach to security is emphasized, including the use of modern authentication methods, software updates, network monitoring, and encryption. The role of artificial intelligence in identifying and mitigating threats is highlighted, which opens up new prospects for improving the security of network infrastructures. The need for continuous development and investment in cybersecurity, as well as the need for sustained attention to security at the level of routing protocols to effectively counter cyber threats, is emphasized. The proposed research can be useful for professional researchers, analysts, and businesses. Further research will focus on a detailed analysis of the impact of artificial intelligence on the detection and mitigation of security vulnerabilities in dynamic routing protocols.
Keywords: dynamic routing protocols; network security; network vulnerabilities; security measures; artificial intelligence in cybersecurity.

Вступ. В останні роки, зі зростанням глобальної інформаційної мережі, важливість надійних і безпечних протоколів динамічної маршрутизації стає все більш виразною. Ці протоколи, які є ключовими компонентами мережевої інфраструктури, забезпечують визначення та оптимізацію шляхів передачі даних між вузлами в складних і динамічно змінюваних мережевих середовищах. Однак, разом з технологічним прогресом зростає і кількість потенційних загроз для цих протоколів, що робить питання їх безпеки особливо актуальним. Відповідно постає нагальна потреба аналізу сучасних викликів, пов'язаних з вразливостями безпеки в протоколах динамічної маршрутизації, і вивчення ефективних методів їх виявлення та пом'якшення. Важливо розглянути різні аспекти безпеки динамічної маршрутизації, включаючи ідентифікацію потенційних загроз, аналіз ризиків, а також розробку і впровадження механізмів захисту, що можуть ефективно протистояти виявленим вразливостям. Особлива увага приділяється новітнім дослідженням і розробкам у цій галузі, з акцентом на інноваційні підходи та технології, які обіцяють значне покращення захисту протоколів динамічної маршрутизації. Важливо проаналізувати існуючі рішення, їх переваги та недоліки, а

також висвітлити перспективні напрямки досліджень, спрямовані на забезпечення більшої стійкості мережевої інфраструктури до зовнішніх і внутрішніх загроз. У контексті стрімкого розвитку цифрових технологій, питання безпеки динамічної маршрутизації набуває особливої актуальності. Від ефективного виявлення та пом'якшення вразливостей безпеки залежить не лише стабільність роботи окремих мереж, але й безпека цілих систем, від корпоративних мереж до глобального Інтернету. Відповідно розробка та впровадження новітніх методів захисту є ключовою для забезпечення цілісності, доступності та конфіденційності інформації в сучасному цифровому світі. В силу цього важливо поглибити розуміння поточного стану безпеки протоколів динамічної маршрутизації, визначити основні виклики та вказати на можливі шляхи їх вирішення. Відповідно це допоможе ефективніше протидіяти загрозам і підвищити рівень захищеності мережевої інфраструктури.

Огляд попередніх досліджень. Проблематиці виявлення та зниження ризиків безпеки в динамічних протоколах маршрутизації присвячено ряд робіт українських і іноземних дослідників. В роботі Sakthivel T., Chandrasekaran R. [1] пропонують комбіноване рішення, що інтегрує методи шифрування та аутентифікації для захисту мережі від атак, важливою особливістю є використання фіктивних пакетів для протидії атакуючим вузлам, що дозволяє підвищити надійність передачі даних у мережі. Chen I. та ін. [2] зосереджуються на розробці системи DTN, яка може бути застосована для безпечної маршрутизації. Автори представляють модель, яка адаптується до змінних умов мережі та використовує різноманітні параметри, такі як історія взаємодії та поведінка вузлів, для визначення надійності маршрутів. Цей підхід допомагає покращити безпеку та ефективність маршрутизації в DTN, зменшуючи ризики, пов'язані з маршрутизацією через потенційно ненадійні вузли. Korir F., Cheruiyot W. [3] здійснюють аналіз безпекових викликів протоколів маршрутизації в мережах MANET. Автори аналізують різні типи атак, з якими можуть зіткнутися протоколи маршрутизації MANET, та надають огляд існуючих рішень для захисту цих мереж. Стаття важлива тим, що надає систематизований огляд викликів безпеки та способів їхнього подолання, що може слугувати основою для розробки нових, більш ефективних рішень для захисту MANET. Mohanapriya M., Krishnamurthi I. [4] зосереджуються на протоколі DSR, модифікуючи його з використанням механізмів оцінки, щоб ефективно виявляти та ізолювати зловмисні вузли. Цей підхід покликаний підвищити безпеку та надійність маршрутизації в бездротових мережах. Alnumay W., Ghosh U. [5] розглядають методи забезпечення безпеки при маршрутизації та передачі даних в мобільних мережах.

Автори пропонують комплексний підхід до захисту мережі, який включає алгоритми аутентифікації, шифрування та інтеграції безпеки на рівні маршрутизації. Цей підхід дозволяє забезпечити конфіденційність, цілісність та доступність даних у мережах без центрального керування. Younes O. [6] пропонує модифіковану версію протоколу DHCP, яка націлена на протидію атакам в локальних мережах LAN. Автор аналізує поширені види атак на DHCP, такі як DoS, та пропонує методи їх нейтралізації через вдосконалення процедур аутентифікації та верифікації. Song W. та ін. [7] аналізують вразливості в дизайні маршрутизаторів процесорних інтерконектів, які можуть бути використані для проведення атак на архітектуру обчислювальних систем. Автори вказують на специфічні вразливі місця в дизайні маршрутизаторів і пропонують рекомендації щодо їх усунення або мінімізації ризиків.

Поміж українських досліджень в даній царині виділяється ряд робіт. Снігуров А., Чакрян В. [8] розглядають специфіку маршрутизації в спеціалізованих безпровідних телекомунікаційних мережах, що працюють в умовах активної інформаційної протидії. Автори пропонують підхід до управління маршрутизацією, який забезпечує підвищену надійність та безпеку передачі даних за рахунок адаптивної зміни маршрутів в залежності від поточної обстановки в мережі. Єременко О., Андрушко Д. [9] вивчають моделі маршрутизації для мереж, яка дозволяє підвищити ефективність та надійність передачі даних за рахунок використання шляхів, що перетинаються не лише в межах окремих вузлів, але й на різних рівнях мережевої архітектури. Кулаков Ю. та ін. [10] аналізують спосіб організації маршрутизації в MPLS мережах, який забезпечує підвищену безпеку передачі даних. Автори розглядають механізми багато-шляхової маршрутизації та їх застосування для захисту від потенційних загроз у безпровідних мережах. Бабенко Т. [11] зосереджується на аналізі мережевого трафіка з метою виявлення DoS атак. Автор пропонує використання ентропії трафіка як одного з індикаторів, що дозволяє вчасно виявити та відреагувати на спроби DoS атак, тим самим підвищуючи загальний рівень безпеки мережі.

Аналіз попередніх досліджень показав різноманітність підходів та стратегій, що використовуються для підвищення безпеки в бездротових мережах. З одного боку, інноваційні методи, такі як використання фіктивних пакетів, динамічне управління довірою, адаптивна маршрутизація в умовах інформаційних протидій, механізми оцінки довіри, спрямовані на ідентифікацію та ізоляцію зловмисних вузлів, демонструють широкий розвиток безпекових викликів та важливість адаптивності у захисті сучасних мережевих інфраструктур. З іншого боку, розробка та впровадження вдосконалених протоколів, які здатні протистояти специфічним атака вказує на необхідність постійного оновлення безпекових механізмів та методів аналізу мережевого трафіку. Сукупність досліджень підкреслює значення комплексного підходу до забезпечення безпеки, що об'єднує криптографічні методи, системи довіри, аутентифікацію та алгоритми адаптивної маршрутизації. Це не лише сприяє захисту від існуючих загроз, але й створює основу для розробки стійких до майбутніх викликів мережевих систем. Такий інтегрований підхід важливий для розробки надійних та безпечних мережевих інфраструктур, здатних адаптуватися до змінних умов та витримувати нові форми кібератак. Однак, питання комплексного підходу до ефективних методів їх пом'якшення, враховуючи можливості штучного інтелекту недостатньо досліджена та потребує додаткового вивчення.

Мета статті – проаналізувати сучасний стан вразливостей безпеки в протоколах динамічної маршрутизації, які використовуються в комп'ютерних мережах і запропонувати комплексну стратегію пом'якшення з урахуванням потенціалу штучного інтелекту.

Виклад основного матеріалу. Кібербезпека перебуває в стадії стрімкого розвитку, що обумовлено постійно зростаючими загрозами в інтернет-просторі та збільшенням кількості цифрових даних. За даними Statista [12], обсяг світового ринку рішень в царині кібербезпеки, який станом на 2023 р. становив 166,2 млрд дол США, продовжуватиме зростати високими темпами й досягне 273,5 млрд дол США до 2028 р.. Сервісам кібербезпеки представляють найбільший сегмент на даному ринку з обсягом близько 88 млрд дол США на 2023 р., що складає приблизно 53% світових ринку. Найбільший дохід на ринку кібербезпеки у 2023 р. – у США з 72 млрд дол США. В даному ключі провідні позиції також займають Китай і Великобританія із показниками у 14 млрд дол США і 10 млрд дол США відповідно. Ключовими гравцями, представленими на ринку є Broadcom, Cisco, IBM, Microsoft, Palo Alto Network.

Аналіз існуючих протоколів динамічної маршрутизації відіграє ключову роль у розумінні процесів передачі даних у сучасних комп'ютерних мережах. Динамічна маршрутизація, яка дозволяє мережам автоматично пристосовуватися до змін, використовує різноманітні протоколи, кожен з яких має свої особливості та сфери застосування. Розглянемо ключові з них. Одним з найпопулярніших протоколів є OSPF, який являє собою протокол стану каналу з відкритим стандартом. Цей протокол забезпечує ефективну маршрутизацію на основі стану каналів і підтримує розділення мереж на зони для кращого масштабування. Втім, OSPF вимагає значних ресурсів обчислення та пам'яті, що може стати проблемою в великих мережах. Протокол IS-IS працює за принципом маршрутизації стану каналу, тобто найкоротший шлях до сусіднього вузла обчислюється на основі топологічної карти мережі, яку будує кожен маршрутизатор цієї мережі. Пакети IS-IS не вразливі до атак типу IP spoofing і DDoS, оскільки це протокол канального рівня моделі OSI, а не IP-орієнтований протокол. Протокол BGP дозволяє обмін маршрутною інформацією між різними автономними системами. BGP забезпечує масштабування та гнучкість, але його налаштування та оптимізація вимагають високого рівня знань та можуть бути ускладнені ризиком неправильної конфігурації. Протокол EIGRP використовує алгоритми для ефективного визначення найкращого шляху і підтримує навантажувальне балансування. Хоча EIGRP став відкритим стандартом у 2013 році, даний протокол переважно асоціюється з обладнанням Cisco і може не бути оптимальним вибором для великих мереж. Кожен з цих протоколів сприяє розвитку динамічної маршрутизації, маючи свої специфічні переваги та обмеження. Вибір протоколу маршрутизації залежить від специфічних вимог до мережі, її розміру, а також необхідності масштабування та гнучкості. Важливо оцінити всі ці фактори в рамках забезпечення надійної та ефективної передачі даних. Зведені результати аналізу за основними характеристиками найбільш використовуваних протоколів динамічної маршрутизації подамо в таблиці 1.

Звернімо увагу, що кожен з цих протоколів має унікальні особливості та відповідає на певні вимоги мережі. Вибір між ними залежить від специфіки мережевого середовища, вимог до масштабування, гнучкості управління та наявності обладнання.

В рамках аналізу вразливості протоколів динамічної маршрутизації, ми стикаємося з низкою потенційних ризиків, що можуть відкрити мережеві системи загрозам безпеки. Ці протоколи, які лежать в основі автоматизації маршрутизації даних в комп'ютерних мережах, виявляються вразливими для різноманітних атак.

Перш за все, недостатня аутентифікація учасників у процесі маршрутизації створює можливість для несанкціонованого доступу до маршрутизаційної інформації, дозволяючи атакуючим модифікувати або перехоплювати дані. Це стає особливо небезпечним, коли атакуючі надсилають підроблені маршрутизаційні оновлення, ефективно перенаправляючи трафік через мережі під своїм контролем або створюючи маршрутизаційні петлі, що може спричинити збої у роботі мережі.

Таблиця 1. Основні характеристики найбільш використовуваних протоколів динамічної маршрутизації [13]

Характеристики	*OSPF*	*IS-IS*	*BGP*	*EIGRP*
Розробник	DEC/IETF	DEC/IETF	IETF	Cisco Systems
Тип	Відкритий стандарт	Відкритий стандарт	Відкритий стандарт	Відкритий стандарт
Метрики	Вартість шляху	Вартість шляху	Політики, префікси, атрибути	Затримка, пропускна здатність, надійність, навантаження, MTU
Масштабування	Добре	Добре	Відмінне	Добре
Основне застосування	Великі корпоративні мережі	Великі провайдерські мережі	Міждоменна маршрутизація в Інтернеті	Внутрішньої та зовнішньої маршрутизації в мережах Cisco

Проблеми з масштабуванням і розподілом навантаження також мають бути враховані в даному контексті враховувати. Велика кількість оновлень маршрутизації або навмисно створені маршрутизаційні петлі можуть перевантажити обладнання, викликаючи затримки або втрату пакетів. Недоліки в реалізації протоколів, такі як переповнення буферу в програмному забезпеченні маршрутизаторів, відкривають шлях для атак, спрямованих на виконання довільного коду або отримання несанкціонованого доступу до систем. Механізми експлуатації цих вразливостей різноманітні та включають атаки типу MitM, де атакуючі можуть перехоплювати, переглядати або змінювати передані дані. Атаки типу DoS, засновані на надсиланні великої кількості фальсифікованих маршрутизаційних повідомлень, можуть вивести з ладу маршрутизатори або знизити продуктивність мережі. Крім того, модифікація маршрутизаційної інформації дозволяє атакуючим перенаправляти чутливі дані через контрольовані ними мережі, підвищуючи ризики їх перехоплення та аналізу. Захист від таких вразливостей вимагає багаторівневого підходу до безпеки, що включає застосування сучасних методів аутентифікації, регулярне оновлення програмного забезпечення маршрутизаторів, моніторинг мережі для виявлення аномального трафіку та використання шифрування для захисту переданих даних. Такий підхід допомагає зміцнити стійкість мережі до атак і забезпечити надійну передачу даних.

Динамічна маршрутизація є ключовою для ефективності та гнучкості сучасних мережевих інфраструктур, проте безпека цих протоколів зазнає постійних випробувань через різноманітні вразливості. Розглядаючи конкретні вразливості та їх наслідки, стає можливим розробити стратегії для підвищення безпеки мереж. Виділимо основні вразливості та наслідки. По-перше, це *фальсифікація маршрутизаційної інформації*. Однією з найсерйозніших вразливостей є можливість фальсифікації маршрутизаційної інформації. Атакуючі можуть анонсувати неправильні маршрути, внаслідок чого трафік буде неналежним чином перенаправлений через атакуючого, що дозволяє здійснювати атаки MitM. Наслідки можуть включати втрату конфіденційності, цілісності даних та доступності сервісу. По-друге, це *ризик успішних DoS атак*. Механізми маршрутизації можуть бути

використані для виклику відмов в обслуговуванні, коли система або мережа стає перевантаженою або повністю недоступною для легітимних користувачів через масові фальсифіковані оновлення маршрутів. По-третє, це *використання недоліків у реалізації*. Слабкі місця у реалізації конкретних маршрутизаторів або протоколів можуть дозволити виконання довільного коду або злам обладнання, що призводить до втрати управління над мережевими компонентами.

Відповідно дані вразливості та їх наслідки потребують інструментарію для їх пом'якшення. Виділимо основні стратегії пом'якшення. Дані стратегії подано на рисунку1.

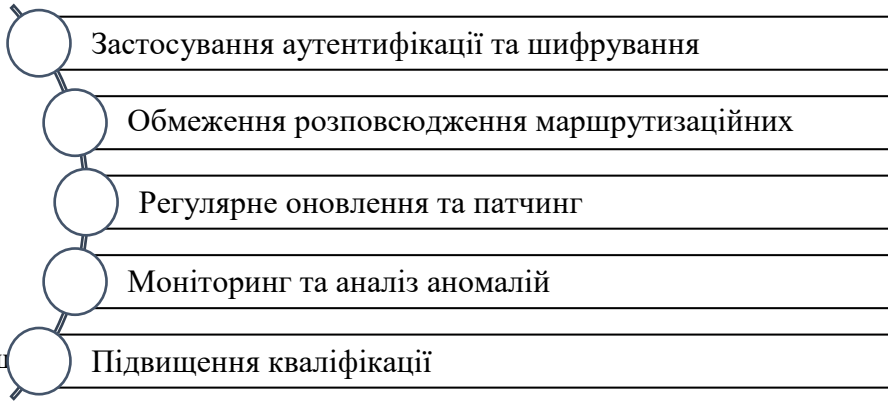

Рис. 1 – Основні стратегії пом'якш маршрутизації [14-16]

Розглянемо в більших деталях виділені стратегії пом'якшення:

Застосування аутентифікації та шифрування: використання технологій аутентифікації та шифрування для маршрутизаційних оновлень забезпечує захист від несанкціонованого доступу та модифікації. Наприклад, протоколи BGP і OSPF з захищеними з'єднаннями, можуть значно знизити ризик фальсифікації маршрутизаційної інформації;

Обмеження розповсюдження маршрутизаційних оновлень: встановлення політик, які обмежують розповсюдження маршрутизаційних оновлень від ненадійних джерел або до критично важливих частин мережі, допомагає запобігти несанкціонованому перенаправленню трафіку;

Регулярне оновлення та патчинг: оскільки багато вразливостей виникають через недоліки в програмному забезпеченні, регулярне оновлення маршрутизаторів та іншого мережевого обладнання є критично важливим. Виробники часто випускають патчі та оновлення для виправлення виявлених вразливостей;

Моніторинг та аналіз аномалій: активний моніторинг мережевого трафіку та аналіз аномалій можуть допомогти виявити незвичайну активність, яка може вказувати на спробу експлуатації вразливостей маршрутизації. Використання систем SIEM та IDS може бути корисним у цьому контексті.

Підвищення кваліфікації: ріст обізнаності та тренінг персоналу щодо потенційних вразливостей та загроз також є важливою складовою стратегії безпеки. Знання про те, як вразливості можуть бути експлуатовані та як їх можна запобігти, допомагає зміцнити загальну безпеку мережі.

Застосування цих стратегій дозволяє зміцнити безпеку мережі, знизити ризики, пов'язані з вразливостями динамічної маршрутизації, гарантувати надійність та доступність мережевих сервісів. Зауважимо, що найбільшу ефективність дані стратегії матимуть за їх комплексного застосування.

В рамках даної комплексної стратегії важливо використати потенціал штучного інтелекту. Виявлення та пом'якшення вразливостей безпеки в протоколах динамічної маршрутизації за допомогою штучного інтелекту є суттєвим для забезпечення надійності та ефективності мережевої інфраструктури. Використання штучного інтелекту у цій сфері відкриває нові можливості для аналізу поведінки мережі в реальному часі, виявляючи незвичайну активність, яка може свідчити про атаки або внутрішні збої. Штучний інтелект допомагає прогнозувати потенційні вразливості, засновуючись на аналізі історичних даних, що дозволяє вжити профілактичних заходів до того, як ці слабкі місця стануть критичними. Завдяки алгоритмам машинного навчання можливо розробити системи адаптивної маршрутизації, які здатні самостійно реагувати на атаки, змінюючи маршрути трафіку для забезпечення безперервності обслуговування. Ці системи також можуть

вдосконалювати політики безпеки, аналізуючи їхню ефективність та рекомендуючи зміни, щоб адаптуватися до постійно змінюваного ландшафту кіберзагроз. Штучний інтелект також відіграє ключову роль у створенні симуляційних моделей мережі, які дозволяють проводити навчання та тестування оборонних стратегій в контрольованих умовах. Це сприяє глибшому розумінню потенційних загроз і ефективності різних підходів до захисту мережі. Впровадження штучного інтелекту у захист протоколів динамічної маршрутизації вимагає від організацій забезпечити високу точність обробки даних, адаптивність до нових загроз і гладку інтеграцію з наявними мережевими рішеннями. Важливим аспектом є знаходження балансу між автоматизацією, що її пропонує штучний інтелект, та контролем з боку людини, що покликано гарантувати, що системи діятимуть в межах визначених політик безпеки та етичних норм.

Висновки. В підсумку, динамічна маршрутизація, яка дозволяє мережам автоматично пристосовуватися до змін, використовуючи різноманітні протоколи – такі як OSPF, IS-IS, BGP, EIGRP – є ключовою для забезпечення ефективності та гнучкості сучасних мережевих інфраструктур. Кожен з цих протоколів має свої особливості та сфери застосування, вибір між якими залежить від специфіки мережевого середовища, вимог до масштабування, гнучкості управління та наявності обладнання.

Однак, безпека цих протоколів зазнає постійних випробувань через різноманітні вразливості, які можуть бути експлуатовані атаками, спрямованими на недоліки в аутентифікації, масштабуванні, розподілі навантаження, а також через можливість фальсифікації маршрутизаційної інформації. Відтак, застосування комплексного підходу до безпеки, який включає застосування сучасних методів аутентифікації, регулярне оновлення програмного забезпечення, моніторинг мережі, використання шифрування та підвищення кваліфікації персоналу, стає критично важливим для забезпечення надійності та доступності мережевих сервісів.

Отримані результати підкреслюють не лише важливість неперервного розвитку та інвестицій у кібербезпеку на глобальному рівні, але й необхідність постійної уваги до безпеки на рівні протоколів маршрутизації та мережевих інфраструктур, щоб адекватно протистояти зростаючим кіберзагрозам. Окремим блоком даної комплексної стратегії має стати застосування потенціалу штучного інтелекту для виявлення загроз і їх пом'якшення. Подальші перспективи досліджень передбачають детальне вивчення впливу штучного інтелекту на виявлення вразливостей безпеки в протоколах динамічної маршрутизації та їх пом'якшення.

Список бібліографічного опису

1. Sakthivel T., Chandrasekaran R. A dummy Packet-Based hybrid security framework for mitigating routing misbehavior in Multi-Hop wireless networks. *Wireless Personal Communications*. 2018. №101(3). P. 1581–1618.
2. Chen I., Bao F., Chang M., Cho J. Dynamic trust management for delay tolerant networks and its application to secure routing. *IEEE Transactions on Parallel and Distributed Systems*. 2014. №25(5). P. 1200–1210.
3. Korir F., Cheruiyot W. A survey on security challenges in the current MANET routing protocols. *Global Journal of Engineering and Technology Advances*. 2022. №12(1). P. 78–91.
4. Mohanapriya M., Krishnamurthi I. Trust based DSR routing protocol for mitigating cooperative black hole attacks in ad hoc networks. *Arabian Journal for Science and Engineering*. 2013. №39(3). P. 1825–1833.
5. Alnumay W., Ghosh U. Secure routing and data transmission in mobile ad hoc networks. *International Journal of Computer Networks and Communications*. 2014. №6(1). P. 111–127.
6. Younes O. A secure DHCP protocol to mitigate LAN attacks. *Journal of Computer and Communications*. 2016. №4(1). P. 39–50.
7. Song W., Kim J., Lee J., Abts D. Security Vulnerability in Processor-Interconnect Router Design. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. 2014. P. 1–11.
8. Снігуров А., Чакрян В. Підхід до управління маршрутизацією в безпроводових телекомунікаційних мережах спеціального призначення, функціонуючих в умовах інформаційної протидії. *Захист інформації і безпека інформаційних систем* : ІІ міжнародна наук.-техн.конф. : Збірник тез доповідей. Львів, 2013. С. 16–17.
9. Єременко О., Андрушко Д. Модель маршрутизації в телекомунікаційній мережі з використанням шляхів, що перетинаються за вузлами. *Вісник Національного університету «Львівська політехніка» серія: «Радіоелектроніка та телекомунікації»*. 2015. №818. С. 181–188.
10. Кулаков Ю., Лукашенко В., Левчук А. Спосіб організації безпечної багатошляхової маршрутизації в безпроводовій мережі MPLS. *Вісник Національного Авіаційного Університету*. 2012. Т. 50. № 1. С. 101–105.
11. Бабенко Т. Дослідження ентропії мережевого трафіка як індикатора DDOS-атак. *Науковий вісник Національного гірничого університету*. 2013. №2. С. 86–89.
12. Statista. Cybersecurity: Market Data & Analysis 2023. URL: https://www.statista.com/study/124902/cybersecurity-report/ (дата доступу: 08.04.2024).

13. Cisco. Dynamic Routing Protocols: OSPF, EIGRP, RIPv2, IS-IS, BGP. URL: https://community.cisco.com/t5/networking-knowledge-base/dynamic-routing-protocols-ospf-eigrp-ripv2-is-is-bgp/ta-p/4511577 (дата доступу: 08.04.2024).
14. Australian Government. Australian Signals Directorate. Strategies to Mitigate Cyber Security Incidents. URL: https://www.cyber.gov.au/sites/default/files/2023-03/PROTECT%20-%20Strategies%20to%20Mitigate%20Cyber%20Security%20Incidents%20–%20Mitigation%20Details%20%28February%202017%29.pdf (Дата доступу: 08.04.2024).
15. Cisco. General Design Considerations for Secure Networks. URL: https://www.ciscopress.com/articles/article.asp?p=174313&seqNum=5 (Дата доступу: 08.04.2024).
16. CSRIC. Network Reliability and Security Risk Reduction. URL: https://www.fcc.gov/file/13925/download (дата доступу: 08.04.2024)

References:

17. Sakthivel T., Chandrasekaran R. A dummy Packet-Based hybrid security framework for mitigating routing misbehavior in Multi-Hop wireless networks. *Wireless Personal Communications*. 2018. №101(3). P. 1581–1618.
18. Chen I., Bao F., Chang M., Cho J. Dynamic trust management for delay tolerant networks and its application to secure routing. *IEEE Transactions on Parallel and Distributed Systems*. 2014. №25(5). P. 1200–1210.
19. Korir F., Cheruiyot W. A survey on security challenges in the current MANET routing protocols. *Global Journal of Engineering and Technology Advances*. 2022. №12(1). P. 78–91.
20. Mohanapriya M., Krishnamurthi I. Trust based DSR routing protocol for mitigating cooperative black hole attacks in ad hoc networks. *Arabian Journal for Science and Engineering*. 2013. №39(3). P. 1825–1833.
21. Alnumay W., Ghosh U. Secure routing and data transmission in mobile ad hoc networks. *International Journal of Computer Networks and Communications*. 2014. №6(1). P. 111–127.
22. Younes O. A secure DHCP protocol to mitigate LAN attacks. *Journal of Computer and Communications*. 2016. №4(1). P. 39–50.
23. Song W., Kim J., Lee J., Abts D. Security Vulnerability in Processor-Interconnect Router Design. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. 2014. P. 1–11.
24. Снігуров А., Чакрян В. Підхід до управління маршрутизацією в безпроводових телекомунікаційних мережах спеціального призначення, функціонуючих в умовах інформаційної протидії. *Захист інформації і безпека інформаційних систем* : II міжнародна наук.-техн.конф. : Збірник тез доповідей. Львів, 2013. С. 16–17.
25. Єременко О., Андрушко Д. Модель маршрутизації в телекомунікаційній мережі з використанням шляхів, що перетинаються за вузлами. *Вісник Національного університету «Львівська політехніка» серія: «Радіоелектроніка та телекомунікації»*. 2015. №818. С. 181–188.
26. Кулаков Ю., Лукашенко В., Левчук А. Спосіб організації безпечної багатошляхової маршрутизації в безпроводовій мережі MPLS. *Вісник Національного Авіаційного Університету*. 2012. Т. 50. № 1. С. 101–105.
27. Бабенко Т. Дослідження ентропії мережевого трафіка як індикатора DDOS-атак. *Науковий вісник Національного гірничого університету*. 2013. №2. С. 86–89.
28. Statista. Cybersecurity: Market Data & Analysis 2023. URL: https://www.statista.com/study/124902/cybersecurity-report/ (дата доступу: 08.04.2024).
29. Cisco. Dynamic Routing Protocols: OSPF, EIGRP, RIPv2, IS-IS, BGP. URL: https://community.cisco.com/t5/networking-knowledge-base/dynamic-routing-protocols-ospf-eigrp-ripv2-is-is-bgp/ta-p/4511577 (дата доступу: 08.04.2024).
30. Australian Government. Australian Signals Directorate. Strategies to Mitigate Cyber Security Incidents. URL: https://www.cyber.gov.au/sites/default/files/2023-03/PROTECT%20-%20Strategies%20to%20Mitigate%20Cyber%20Security%20Incidents%20–%20Mitigation%20Details%20%28February%202017%29.pdf (Дата доступу: 08.04.2024).
31. Cisco. General Design Considerations for Secure Networks. URL: https://www.ciscopress.com/articles/article.asp?p=174313&seqNum=5 (Дата доступу: 08.04.2024).
32. CSRIC. Network Reliability and Security Risk Reduction. URL: https://www.fcc.gov/file/13925/download (дата доступу: 08.04.2024)