УДК 004.056
DOI https://doi.org/10.32782/2663-5941/2024.5.1/09

Маруняк С.Т.
Національний університет «Львівська політехніка»

ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПРОТОКОЛАХ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ ЗА ДОПОМОГОЮ МАШИННОГО НАВЧАННЯ З ВИКОРИСТАННЯМ НАЇВНОГО КЛАСИФІКАТОРА БАЙЄСА

Сучасні мережеві інфраструктури покладаються на протоколи динамічної маршрутизації, такі як BGP (Border Gateway Protocol) та OSPF (Open Shortest Path First), для забезпечення ефективної маршрутизації даних у мережах різного масштабу. Водночас ці протоколи можуть стати об'єктом атак, що загрожують безпеці та стабільності мереж. Атаки на доступність, зокрема denial-of-service (DoS) атаки, можуть спричинити перевантаження мережевих ресурсів та відмову в наданні послуг, що становить серйозну загрозу для корпоративних та державних інфраструктур. У цій статті досліджено можливість підвищення інформаційної безпеки в протоколах динамічної маршрутизації шляхом застосування машинного навчання, зокрема наївного класифікатора Байєса. Наївний Байєс дозволяє ефективно обробляти великі обсяги даних для швидкого виявлення та ідентифікації мережевих аномалій, що забезпечує можливість своєчасного реагування на загрози в реальному часі.

Однією з ключових переваг використання наївного класифікатора Байєса є його здатність швидко навчатися на обмежених вибірках даних, що дозволяє скоротити час на підготовку моделі та забезпечити її функціональність в умовах реального часу. Крім того, цей метод машинного навчання є стійким до змін у структурі даних, що робить його особливо корисним у динамічних мережах, де дані постійно оновлюються. У статті також проаналізовано, як можна підвищити точність класифікації за допомогою додаткових технік, таких як використання евристичних правил та фільтрація шумів у даних, що робить підхід більш адаптивним і точним для захисту протоколів маршрутизації від різних видів атак.

Стаття охоплює аналіз існуючих підходів до інформаційної безпеки в мережевих протоколах динамічної маршрутизації, а також досліджує роль машинного навчання у підвищенні рівня захисту від кіберзагроз. Описано етапи розробки рішення, починаючи з аналізу вразливостей мережі, збору й обробки даних для тренування моделі, та закінчуючи валідацією результатів і впровадженням рішення у реальні мережеві інфраструктури. Особливу увагу приділено моніторингу й адаптації моделі для підтримки її актуальності та точності в умовах динамічних змін у мережевому середовищі. Також розглянуто перспективи інтеграції запропонованих рішень в існуючі мережі з мінімальними витратами на підтримку й адаптацію. Запропоноване дослідження може бути корисним фахівцям у сфері кібербезпеки, розробникам мережевих технологій, дослідникам, а також організаціям, що займаються захистом інформації у мережах критичної інфраструктури. Перспективи подальших досліджень включають оптимізацію моделей машинного навчання для кращої виявляємості складних загроз та розробку нових алгоритмів для захисту мереж від майбутніх викликів кібербезпеки.

Ключові слова: *інформаційна безпека, динамічна маршрутизація, машинне навчання, наївний класифікатор Байєса, захист даних.*

Постановка проблеми. У сучасному світі, де інформаційні технології глибоко інтегровані у всі сфери діяльності, забезпечення інформаційної безпеки є одним з найважливіших завдань. Особливе значення це має у контексті динамічних мережевих протоколів, які відіграють ключову роль у управлінні потоками даних у мережах. Традиційні методи забезпечення безпеки часто не можуть ефективно реагувати в контексті сучасних загроз, що вимагає інноваційних підходів. Одним із перспективних напрямків є використання машинного навчання для аналізу та виявлення потенційних атак на динамічну маршрутизацію. В світлі цього важливо фокусуватися на дослідженні можливостей застосування наївного класифікатора Байєса для підвищення інформаційної безпеки в протоколах динамічної маршрутизації. Метод наївного класифікатора Байєса є актуальним завдяки його здатності ефективно обробляти великі обсяги даних і забезпечувати надійність при розпізнаванні шаблонів у складних даних, що є критично важливим для мережевої безпеки.

Наївний класифікатор Байєса, який базується на застосуванні теореми Байєса, є одним з найпопулярніших алгоритмів машинного навчання, здатний швидко адаптуватися до змін у вхідних даних, що є ідеальним для систем динамічної маршрутизації. Відповідно важливо проаналізувати основні виклики, з якими зіштовхуються традиційні системи безпеки та описати методологію використання наївного класифікатора Байєса для ідентифікації аномалій у поведінці маршрутизації. Крім того важливим є питання впровадження наївного класифікатора Байєса може значно знизити ризики пов'язані з мережевими атаками, зокрема, з атаками на маршрутизацію. Все це сприятиме кращому розумінню потенціалу машинного навчання у сфері інформаційної безпеки та надасть глибше розуміння науково-практичних аспектів застосування машинного навчання для зміцнення безпеки динамічних мережевих систем.

Аналіз останніх досліджень і публікацій. Питанню посилення інформаційної безпеки в протоколах динамічної маршрутизації за допомогою машинного навчання присвячено значний масив робіт українських і закордонних дослідників. С. Сатья (S. Sathya), К. Умадеві (K. Umadevi) [1] вивчають питання розробки оптимізованого дистриб'ютивного безпечного протоколу маршрутизації з використанням динамічного розподілу ключів для підвищення безпеки в бездротових мережах. Автори намагались покращити мережеву безпеку за допомогою адаптивних технік управління ключами. А. Мудгерікар (A. Mudgerikar), Е. Бертіно (E. Bertino) [2] аналізують інтелектуальний безпечний маршрутизаційний протокол, який використовує методи безмодельного навчання з підкріпленням. Цей підхід дозволяє мережам самостійно адаптуватися до змін умов і потенційних загроз безпеці, оптимізуючи маршрутизацію в реальному часі. Л. Венкатраман (L. Venkatraman), Д. Агравал (D. Agrawal) [3] аналізує стратегії підвищення безпеки протоколів маршрутизації в мобільних ad hoc мережах (MANETs). Автори розглядають різні підходи до забезпечення цілісності, доступності та конфіденційності даних у таких мережах. Робота Х. Мудні (H. Moudni) та інші [4] зосереджена на покращенні безпеки в протоколі оптимізованої маршрутизації на основі стану зв'язків для мобільних ad hoc мереж. Автори впроваджують нові механізми захисту для зменшення вразливостей у маршрутизаційних протоколах. К. Чжу (Q. Zhu), Ж. Сонг (J. Song), Т. Басар (T. Başar) [5] аналізують питання динамічної маршрутизації в розподілених когнітивних радіомережах. Це включає стратегії, які дозволяють користувачам радіомережі ефективно адаптуватися до загроз безпеки і оптимізувати свої маршрутизаційні рішення. У проаналізованих вище дослідження в цілому розглянуто широкий спектр питань та технічних підходів у забезпеченні безпеки маршрутизації в різних типах мереж, від традиційних бездротових мереж до мобільних ad hoc і когнітивних радіомереж.

На сучасному етапі значна увага досліджень приділена покращенню маршрутизації та безпеки в різноманітних мережевих середовищах, використовуючи методи машинного навчання та глибокого навчання. У ряді досліджень висвітлено інноваційні підходи, які можуть бути використані для ефективнішої та безпечнішої маршрутизації. Дж. Надараджан (J. Nadarajan), Дж. Каліаперумал (J. Kaliyaperumal) [6] розробили алгоритм маршрутизації, який враховує якість обслуговування (QoS) та забезпечує безпеку за допомогою машинного інтелекту в мережах VANET наступного покоління. Цей алгоритм покращує надійність передачі даних та знижує затримку, що є критично важливим для систем з високими вимогами до часу реакції. М. Джонстон (M. Johnston), К. Данілов (C. Danilov), К. Ларсон (K. Larson) [7] дослідили застосування методів навчання при маршрутизації у тактичних мережах. Даний підхід дозволяє системі динамічно адаптуватися до змінних умов мережі, забезпечуючи високу надійність комунікацій. Ф. Ху (F. Hu) та інші [8] представили протокол безпечної маршрутизації для бездротових ad hoc мереж на основі глибокого навчання. Цей протокол використовує потужні можливості глибокого навчання для ідентифікації та запобігання безпековим загрозам в мережі. Ю. Йу (Y. Yu) та інші [9] запропонували схему безпеки маршрутизації на основі оцінки репутації в ієрархічних ad hoc мережах. Цей підхід дозволяє підвищити безпеку мережі через ефективне управління довірою між вузлами. Е. Геленбе (E. Gelenbe) [10] описує використання машинного навчання для маршрутизації в мережах, акцентуючи на тому, як сучасні технології можуть сприяти більш ефективному розподілу мережевого трафіку і зменшенню затримок. Висвітлені вище дослідження формують сучасний контекст розробки методів маршрутизації, що включають новітні досягнення в машинному та глибокому навчанні, надаючи потужні інструменти для забезпечення ефективності та безпеки мережевих операцій. Подані роботи також вказують на різноманітність потенційних застосувань та підходів, що можуть бути адаптовані до специфіки різних типів мереж.

В окремому масиві робіт зосереджено увагу на аспектах безпеки маршрутизації в різних типах бездротових мереж, включаючи мобільні ad hoc мережі (MANETs) і транспортні ad hoc мережі (VANETs), а також підходи до управління даними і оптимізації в системах прийняття рішень. А. Еччаахуі (A. Echchaachoui) та інші [11] описують методи асиметричного та динамічного шифрування для забезпечення безпеки маршрутизації в MANETs. Ці методики підкреслюють необхідність захисту від зовнішніх і внутрішніх загроз у динамічно змінюваних мережах. А. Амалія (A. Amalia) та інші [12] розглядають використання глибокого навчання для розробки протоколу безпечної маршрутизації, щоб уникнути атак типу «чорна діра» в VANETs. У роботі підтримано розвиток методів штучного інтелекту для забезпечення безпеки в складних і високодинамічних мережевих умовах. А. Снігуров В. Чакрян [13] вивчають особливості формування метрик маршрутизації, заснованих на ризиках інформаційної безпеки. Дослідники звертають увагу на необхідність врахування факторів інформаційної безпеки при проектуванні маршрутів у мережах. Крім того, у дослідженні [14] подано підхід до управління маршрутизацією в спеціальних бездротових телекомунікаційних мережах, що працюють в умовах інформаційної протидії. Дослідники акцентують на адаптації маршрутизаційних стратегій до постійно змінних умов зовнішнього середовища. В. Москаленко [15] описує інформаційно-екстремальне навчання системи підтримки прийняття рішень, яке включає адаптивну кластеризацію даних. Цей підхід дозволяє підвищити ефективність обробки даних і прийняття рішень в складних умовах. В. Москаленко А. Рижова [16] досліджують інтелектуальну автоматизовану систему керування, що оптимізує часові параметри аналізу вхідних даних. У цій роботі вказано на шляхи покращення процесів аналітичної обробки для забезпечення оперативного реагування на змінні умови. Огляд вищезазначених досліджень підкреслює важливість інтеграції сучасних технологічних досягнень, таких як штучний інтелект та глибоке навчання, у розвиток мережевих безпекових протоколів і систем управління даними, що адаптуються до складних і динамічних умов. Однак, питання посилення інформаційної безпеки в протоколах динамічної маршрутизації в площині машинного навчання за рахунок інструментарію наївного класифікатора Байєса недостатньо розглянуто в наявному масиві досліджень і потребує додаткового вивчення.

Постановка завдання. Метою статті є аналіз методів підвищення безпеки в мережевих протоколах динамічної маршрутизації за рахунок застосування машинного навчання, зокрема наївного класифікатора Байєса. Дане дослідження покликано сприяти розширенню науково-практичних напрацювань з виявлення та запобігання можливим атакам на маршрутизаційні протоколи (BGP, OSPF), що покликано покращити здатність мережі розпізнавати та реагувати на неавторизовані чи шкідливі зміни в маршрутизації, тим самим забезпечуючи більш високий рівень інформаційної безпеки.

Виклад основного матеріалу. Протоколи динамічної маршрутизації є важливими в сучасному мережевому середовищі завдяки їхній здатності автоматично адаптуватися до змін у мережі. Ці протоколи за своєю природою автоматично додають інформацію з підключених маршрутизаторів до таблиць маршрутизації, гарантуючи, що кожен маршрутизатор має найновішу інформацію про топологію мережі. Цей процес додатково посилюється здатністю протоколів надсилати оновлення топології щоразу, коли відбувається зміна в структурі мережі, що дозволяє маршрутизаторам відповідно налаштовувати свої таблиці маршрутизації для відображення цих змін. Відповідно динамічна адаптація полегшує використання найбільш ефективних або альтернативних шляхів для передачі даних, хоча це може призвести до потенційних перевантажень в разі керування неналежним чином. В рамках пом'якшення таких ускладнень, сучасні протоколи динамічної маршрутизації призначені для вибору маршрутів на основі мінімальної метрики або балансування трафіку між маршрутами з ідентичними метриками, таким чином оптимізуючи загальну продуктивність мережі. Цей динамічний автоматизований підхід до маршрутизації значно допомагає оптимізувати ефективність і надійність мережі, демонструючи розширені можливості протоколів динамічної маршрутизації в управлінні складними мережевими структурами.

В даному ключі важливо заглибитися в те, як конкретні протоколи, такі як BGP і OSPF, функціонують для оптимізації мережевої маршрутизації. Протокол BGP відіграє ключову роль у маршрутизації, дозволяючи інтернет-провайдерам, великим корпораціям та організаціям із загальнодоступними номерами автономної системи автономно обмінюватися інформацією про маршрутизацію без прямої залежності від постачальників послуг Інтернет-зв'язку. Ця автономія має вирішальне

значення для підтримки цілісності та ефективності архітектури глобальної маршрутизації Інтернет. З іншого боку, протокол OSPF використовує алгоритм найкоротшого шляху Дейкстри для динамічного перерахунку мережевих шляхів у відповідь на зміни топології, в такий спосіб підтримуючи безпечний і ефективний процес маршрутизації через автентифікацію змін протоколу та підтримку повної бази даних топології мережі. Завдяки використанню протоколів BGP і OSPF мережі досягають вищого ступеня масштабованості, надійності та безпеки, що є значним позитивним зрушенням у порівнянні з традиційними механізмами маршрутизації. Проте і ці протоколи мають свої особливості в контексті безпеки. Складність конфігурації протоколу OSP може призвести до помилок, які можуть бути використані зловмисниками. BGP підтримує аутентифікацію, але залишається вразливим до таких атак, як hijacking, де зловмисники можуть перенаправляти трафік через небажані маршрути.

Внутрішні вразливості протоколів маршрутизації додатково ускладнюють контекст безпеки мережевої маршрутизації. Зокрема, протокол EIGRP має вразливості через свій механізм роботи, який не враховує кількість переходів під час розрахунку маршруту. Ця особливість може бути використана зловмисниками для маніпулювання шляхами маршрутизації непомічено, що загрожує цілісності та продуктивності мережі. Окрім того, маршрутизатори Cisco, широко використовувані у мережах, мають свої специфічні вразливості. Здатність зловмисників використовувати налаштування пропускної здатності інтерфейсів та статичні параметри затримки може призвести до зниження продуктивності мережі або навіть до її повного збою, що підкреслює критичні недоліки безпеки в конфігурації цих пристроїв. У сукупності, ці вразливості підкреслюють важливість жорстких заходів безпеки та необхідність постійного моніторингу та оновлення мережевих протоколів для захисту від нових загроз.

Спираючись на основу протоколів динамічної маршрутизації в мережах, застосування машинного навчання запроваджує трансформаційний підхід до керування та оптимізації цих мереж. Машинне навчання, зокрема через його здатність прогнозувати на основі відомих властивостей, отриманих із навчальних даних, являє значний поступ в управлінні мережею. Ця здатність машинного навчання додатково доповнюється методами інтелектуального аналізу даних, які значно підвищують точність механізму навчання в мережах. Ці позитивні технологічні зрушення підкреслюють тенденцію до більш інтелектуальних, само-оптимізованих мереж, які можуть динамічно пристосовуватися до уподобань користувачів і нових проблем безпеки.

Наївний класифікатор Байєса є ключовим інструментом в машинному навчанні завдяки своїй простоті та ефективності у рішенні широкого спектру класифікаційних завдань. Алгоритм базується на теоремі Байєса, а його «наївність» полягає у припущенні, що використовувані ознаки є незалежними одна від одної. Це спрощення, хоч і може вести до неточностей, зазвичай не суттєво впливає на ефективність алгоритму у багатьох практичних застосуваннях. Широке використання цього методу у створенні специфічних функцій щільності ймовірностей (Specific Probability Density Functions – SPDF) для таких задач, як прогнозування часових рядів та використання байєсівських мереж, свідчить про його універсальність і здатність значно впливати на сферу статистичного розпізнавання образів (Statistical Pattern Recognition – SPR). Незважаючи на те, що наївний класифікатор Байєса може бути неоптимальним у сценаріях, де припущення про незалежність серйозно порушують базовий розподіл даних, його простота впровадження та низькі витрати на обчислення роблять його ефективним на ранніх стадіях розробки моделей або у програмах з обмеженими даними. Цей баланс між простотою та ефективністю забезпечує популярність наївного класифікатора Байєса і його значення у практиці машинного навчання.

У контексті динамічної маршрутизації, інтеграція специфічних практичних прикладів, таких як стохастична маршрутизація продуктивності процесу, сприяє підвищенню ефективності та надійності мережі. Розробка виявлення найкоротшого шляху (Shortest Path Discovery – SPD) та його впровадження на основі байєсівських мереж надає глибокі інсайти для оптимізації протоколів динамічної маршрутизації. Такі системи адаптуються до різних умов мережі, забезпечуючи надійніші шляхи передачі даних. Зокрема, використання SPD для прогнозування часових рядів дозволяє динамічним маршрутизаційним протоколам прогнозувати потенційні перевантаження та автоматично коригувати маршрути, зменшуючи затримки та втрати пакетів. Використання байєсівських мереж у SPD також дозволяє протоколам приймати обґрунтовані рішення, враховуючи ймовірність станів мережі, що підвищує надійність передачі даних у невизначених умовах.

Перехід до класифікаторів Байєса, особливо у контексті безпеки, зумовлений їх потенціалом для підвищення точності прогнозування та прийняття рішень у невизначених умовах. Практичне впровадження цих класифікаторів, як у випадках з послідовними тестами співвідношення ймовірностей, так і заснованими на байєсівських мережах, підкреслює їхню універсальність та ефективність у складних сценаріях безпеки. Такі методи є особливо дієвими у середовищах з невизначеним станом каналу, демонструючи, що традиційні методи розподілу потужності між передавальними антенами не завжди покращують частоту бітових помилок, що критично для забезпечення цілісності та безпеки зв'язку.

Застосування машинного навчання для динамічної маршрутизації вимагає розв'язання завдань, пов'язаних із забезпеченням конфіденційності та безпеки даних, що перетинають ці мережі. Використання технології блокчейн у цьому контексті підкреслює ефективність рішень на основі машинного навчання для динамічної маршрутизації. Однак, постійне оновлення моделей машинного навчання для адаптації до нових загроз і змін у топології мережі вимагає значних інвестицій у кваліфікацію персоналу та підтримку цих систем. Крім того, швидкі зміни мережевих конфігурацій потребують розробки моделей машинного навчання, які можуть швидко адаптуватися, мінімізуючи обчислювальні витрати та затримки.

В даному контексті сформуємо стратегію розробки та імплементації рішення на основі застосування наївного класифікатора Байєса. Стратегія розробки та імплементації рішення для підвищення інформаційної безпеки в протоколах динамічної маршрутизації за допомогою машинного навчання, зокрема через використання наївного класифікатора Байєса, охоплює декілька ключових етапів. На початковому етапі потрібно визначити цілі та вимоги до проекту. Це передбачає детальний аналіз поточної мережевої інфраструктури і виявлення можливих вразливостей у протоколах динамічної маршрутизації. Основою для цього є збір вхідної інформації через аналітичні звіти та експертні інтерв'ю. На основі цього аналізу формулюються конкретні цільові вимоги до безпеки, які будуть адресовані в проекті. Наступним кроком є збір та обробка даних. Це включає моніторинг мережевих активностей для збору даних про нормальну та аномальну поведінку у мережі. Зібрані дані підлягають попередній обробці, включаючи очищення та нормалізацію, а також виділення ознак, які будуть використані для тренування моделі. Третім етапом є розробка моделі машинного навчання. Вибір падає на наївний класифікатор Байєса через його ефективність при роботі з великими обсягами даних і хорошу швидкість реакції на зміни. Модель тренується на зібраних даних, використовуючи методики крос-валідації для забезпечення її надійності та ефективності. Після тренування моделі відбувається її тестування та валідація. Тестування здійснюється на різноманітних сценаріях атак та при нормальній мережевій поведінці для визначення її стійкості та надійності. Ефективність моделі оцінюється за допомогою таких метрик, як точність, відгук та інші. Імплементація моделі включає її інтеграцію з існуючими мережевими протоколами, забезпечення сумісності з мережевими налаштуваннями, а також автоматизацію процесів виявлення та реагування на загрози на основі результатів класифікації. Завершальними етапами є моніторинг та налагодження системи, які передбачають постійне стеження за її роботою і регулярне оновлення моделі для адаптації до нових загроз та змін у поведінці мережі. Документування всіх процесів та тренування персоналу забезпечують стійке впровадження та ефективну експлуатацію системи в реальних умовах. Така інтегрована стратегія дозволяє ефективно вирішити завдання підвищення інформаційної безпеки в протоколах динамічної маршрутизації, використовуючи переваги машинного навчання. Запропоновану стратегію розробки та імплементації узагальнено подано в табл. 1.

Ця стратегія розробки та імплементації враховує як технічні, так і управлінські аспекти впровадження машинного навчання для забезпечення безпеки в протоколах динамічної маршрутизації.

Висновки. В підсумку, протоколи динамічної маршрутизації мають критично важливу роль в сучасних мережах, демонструючи їх здатність адаптуватися до змін у мережевій топології. Протоколи, такі як BGP та OSPF забезпечують вищу стійкість та безпеку мереж, однак, все ж мають певні вразливості, які в основному виникають в процесі аутентифікації. Інші протоколи, такі як EIGRP, також мають вразливості, що можуть бути використані для маніпуляцій з маршрутами. Враховуючи ці виклики, застосування машинного навчання, зокрема наївного класифікатора Байєса, виявляється перспективним для підвищення безпеки мережі. Машинне навчання дозволяє прогнозувати і адаптувати систему до змін, забезпечуючи автоматизацію процесів виявлення та реагування на аномалії в мережі.

Таблиця 1

Стратегія розробки та імплементації рішення на основі застосування наївного класифікатора Байєса

Етап	Завдання	Інструменти
1. Визначення цілей та вимог	Аналіз поточної ситуації та визначення вимог	Аналітичні звіти, інтерв'ю з експертами
	Цільові вимоги до безпеки	Стандарти безпеки, специфікації
2. Збір та обробка даних	Збір даних	Моніторинг мережі, логи
	Попередня обробка даних	Інструменти для обробки даних, нормалізація
3. Розробка моделі	Вибір моделі	Наївний класифікатор Байєса
	Тренування моделі	Крос-валідація, тренувальні та тестувальні датасети
4. Тестування та валідація	Тестування моделі	Сценарії атак, тестування стійкості
	Оцінка ефективності	Метрики ефективності, аналіз результатів
5. Імплементація	Інтеграція з існуючими системами	Технічна інтеграція, конфігурація
	Автоматизація процесів	Автоматизаційне ПЗ, скрипти
6. Моніторинг та налагодження	Моніторинг системи	Моніторинг в реальному часі, логіка виявлення
	Адаптація та оновлення	Оновлення ПЗ, адаптація до нових загроз
7. Документування та підтримка	Розробка документації	Керівництва для користувачів, технічна документація
	Навчання персоналу	Тренінги, семінари

Джерело: результат авторського аналізу

Запропонована стратегія розробки та імплементації рішення для підвищення інформаційної безпеки в протоколах динамічної маршрутизації з використанням наївного класифікатора Байєса є досить комплексною. В рамках даної стратегії першочергово проводиться детальний аналіз існуючої мережевої інфраструктури, де ідентифікуються потенційні вразливості, що дозволяє визначити конкретні цілі та вимоги до проекту. Після цього відбувається збір та попередня обробка даних, зокрема очищення та нормалізація, щоб виділити ознаки для тренування моделі. Розробка моделі машинного навчання включає вибір наївного класифікатора Байєса, який ефективно працює з великими обсягами даних і забезпечує швидку адаптацію до змін. Модель проходить ретельне тестування в різних сценаріях для оцінювання її стійкості та точності. Після цього відбувається її інтеграція в існуючі мережеві протоколи, що забезпечує сумісність і автоматизацію процесів виявлення та реагування на загрози. Завершальні етапи включають моніторинг та налагодження системи, що дозволяє їй адаптуватися до нових викликів, а також документацію всіх процесів і навчання персоналу для забезпечення стійкого впровадження та ефективної експлуатації системи в реальних умовах. Такий інтегрований підхід підкреслює важливість комплексності в інформаційній безпеці і використання переваг машинного навчання для покращення захисту динамічної маршрутизації.

Стратегія імплементації має враховувати не лише технічні, але й управлінські аспекти впровадження таких технологій, включаючи навчання персоналу та постійний моніторинг системи для адаптації до нових загроз та змін у поведінці мережі, що підкреслює комплексний підхід до підвищення безпеки в протоколах динамічної маршрутизації.

Майбутні дослідження мають сконцентруватися на аналізі особливості розробки та впровадження стратегії посилення безпеки у мережевих протоколах динамічної маршрутизації в площині машинного навчання.

Список літератури:

1. Sathya S.S., Umadevi K. An optimized distributed secure routing protocol using dynamic rate aware classified key for improving network security in wireless sensor network. *Journal of Ambient Intelligence & Humanized Computing/ Journal of Ambient Intelligence and Humanized Computing*. 2020. №12(7). P. 7165–7171.

2. Mudgerikar A., Bertino E. Intelligent Security Aware Routing: Using Model-Free Reinforcement Learning. *2023 32nd International Conference on Computer Communications and Networks (ICCCN)*. P. 1–10. DOI: 10.1109/ICCCN58024.2023.10230195

3. Venkatraman L., Agrawal D. P. Strategies for enhancing routing security in protocols for mobile ad hoc networks. *Journal of Parallel and Distributed Computing*. 2013. №63(2). P. 214–227.

4. Moudni H., Er-Rouidi M., Faouzi H., Mouncif H., Hadadi B.E. Enhancing security in optimized link state routing protocol for mobile ad hoc networks. *Ubiquitous Networking*. Springer. 2017. pp. 107–116.

5. Zhu Q., Song J.B., Başar T. Dynamic Secure Routing Game in Distributed Cognitive Radio Networks. *2011 IEEE Global Telecommunications Conference – GLOBECOM 2011*. P. 1–6. URL: https://researchr.org/publication/ZhuSB11 (date of appeal: 01.10.2024).

6. Nadarajan J., Kaliyaperumal J. QOS aware and secured routing algorithm using machine intelligence in next generation VANET. International *Journal of System Assurance Engineering and Management*. 2021. №1. P. 1–15.

7. Johnston M.R., Danilov C.B., Larson, K. A Reinforcement Learning Approach to Adaptive Redundancy for Routing in Tactical Networks. *MILCOM 2018 – 2018 IEEE Military Communications Conference (MILCOM)*. P. 267–272.

8. Hu F., Chen B., Shi D., Zhang X., Zhang H., Pan M. Secure Routing Protocol in Wireless Ad Hoc Networks via Deep Learning. *2020 IEEE Wireless Communications and Networking Conference (WCNC)*. P. 1–6. DOI: 10.1109/WCNC45663.2020.9120545

9. Yu Y., Guo L., Wang X., Liu C. Ruting security scheme based on reputation evaluation in hierarchical ad hoc networks. *Computer Networks*. 2010. №54(9). P. 1460–1469.

10. Gelenbe E. Machine Learning for Network Routing. *Mediterranean Conference on Embedded Computing*. 2020 9th Mediterranean Conference On Embedded Computing (MECO). Budva, Montenegro, 2020. P. 1–18.

11. Echchaachoui A., Choukri A., Habbani A., Elkoutbi M. Asymmetric and dynamic encryption for routing security in MANETs. *2014 International Conference on Multimedia Computing and Systems (ICMCS)*. P. 825–830.

12. Amalia A., Pramitarini Y., Perdana R. H. Y., Shim K., An B. A Deep-Learning-Based secure routing protocol to avoid blackhole attacks in VANETs. *Sensors*. 2023. №23(19). P. 8224.

13. Снегуров А., Чакрян А. Особливості формування метрики маршрутизації, що засновані на ризиках інформаційної безпеки. *Радіоелектроніка та молодь XXI століття* : XVII міжнародний молодіжний форум : Збірник тез доповідей. Харків, 2013. С. 226–227.

14. Снігуров А., Чакрян А. 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.

15. Москаленко В.В. Інформаційно-екстремальне навчання системи підтримки прийняття рішень з адаптивною кластеризацією даних. *Вісник Сумського державного університету*. 2012. № 3. С. 110–124.

16. Москаленко В., Рижова А. Інтелектуальна автоматизована система керування з оптимізацією часових параметрів аналізу вхідних даних. *Вісник Сумського державного університету*. 2013. №3. С. 7–14.

Maruniak S.T. ENHANCING INFORMATION SECURITY IN DYNAMIC ROUTING PROTOCOLS WITH THE HELP OF MACHINE LEARNING USING A NAIVE BAYES CLASSIFIER

Modern network infrastructures rely on dynamic routing protocols, such as BGP (Border Gateway Protocol) and OSPF (Open Shortest Path First), to provide efficient data routing in networks of varying scale. At the same time, these protocols can become the object of attacks that threaten the security and stability of networks. Availability attacks, including denial-of-service (DoS) attacks, can cause network resource overload and denial of service, posing a serious threat to corporate and government infrastructures. This article investigates the possibility of increasing information security in dynamic routing protocols by applying machine learning, in particular, a naive Bayes classifier. Naive Bayes enables efficient processing of large volumes of data for rapid detection and identification of network anomalies, enabling timely response to real-time threats.

One of the key advantages of using a naive Bayes classifier is its ability to quickly learn on limited data samples, which allows to reduce the time to prepare the model and ensure its functionality in real-time conditions. In addition, this machine learning method is robust to changes in the data structure, which makes it particularly useful in dynamic networks where data is constantly updated. The paper also analyzes how the classification accuracy can be improved using additional techniques, such as the use of heuristic rules and noise filtering in the data, which makes the approach more adaptive and accurate for protecting routing protocols against various types of attacks.

The article covers the analysis of existing approaches to information security in dynamic routing network protocols, and also explores the role of machine learning in increasing the level of protection against cyber threats. The stages of solution development are described, starting with the analysis of network vulnerabilities, collecting and processing data for model training, and ending with the validation of the results and the implementation of the solution in real network infrastructures. Special attention is paid to the monitoring and adaptation of the model to maintain its relevance and accuracy in the conditions of dynamic changes in the network environment. The prospects of integrating the proposed solutions into existing networks with minimal costs for support and adaptation are also considered. The proposed study can be useful to cyber security specialists, network technology developers, researchers, and organizations involved in information protection in critical infrastructure networks. Prospects for further research include optimizing machine learning models for better detection of complex threats and developing new algorithms to protect networks from future cyber security challenges.

Key words: *information security, dynamic routing, machine learning, naive Bayes classifier, data protection.*