



ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

УДК 004.056.5:004.7.056.53:004.89

DOI: <https://doi.org/10.17721/ISTS.2025.10.83-95>

Юрій КРАВЧЕНКО, д-р техн. наук, проф.

ORCID ID: 0000-0002-0281-4396

e-mail: kr34@ukr.net

Київський національний університет імені Тараса Шевченка, Київ, Україна

Олена ФІСУН, асп.

ORCID ID: 0009-0009-6640-3818

e-mail: lenafi@ukr.net

Київський національний університет імені Тараса Шевченка, Київ, Україна

МЕТОД ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ ПРОГРАМНО-КЕРОВАНИХ МЕРЕЖ В УМОВАХ ВПЛИВУ КІБЕРАТАК

Вступ. В умовах стрімкого розвитку мережевих технологій архітектура Software-Defined Networking (SDN) стала основою для побудови гнучких і керованих корпоративних мереж. Проте її централізована природа створює потенційні вразливості, що можуть бути використані зловмисниками для дестабілізації управління мережею. Забезпечення функціональної стійкості SDN в умовах кібератак різної інтенсивності є складною задачею, оскільки потребує динамічної адаптації параметрів управління для запобігання переходу системи в критичні стани.

Методи. Запропоновано метод підтримання функціональної стійкості SDN на основі поєднання стохастичного моделювання та рекурентних нейронних мереж типу LSTM (Long Short-Term Memory). Модель SDN формалізовано як систему з п'ятьма можливими станами та набором інтенсивностей переходів між ними. LSTM-модуль виконує функцію адаптивного регулятора, який у процесі роботи оцінює імовірності перебування системи в різних станах і коригує окремі інтенсивності переходів із метою підтримання цільового рівня функціональної стійкості. Для навчання LSTM застосовано поєднання імітаційного та підкріплювального підходів, що дає змогу враховувати як попередньо змодельовані сценарії атак, так і поточний стан мережі.

Результати. Розроблений метод продемонстрував ефективність у підтриманні стійкого функціонування SDN за рахунок своєчасного коригування параметрів системи у разі зміни інтенсивності загроз. Імітаційне моделювання для трьох сценаріїв (низький, середній і високий рівні загрози) показало, що без корекції параметрів стійкість зберігається лише за низького рівня атак, тоді як для середнього та високого рівнів у певні моменти часу спостерігаються критичні відхилення. Застосування LSTM-контролера дозволило вчасно виявляти ці моменти й адаптивно оновлювати інтенсивності переходів, відновлюючи стійкість мережі.

Висновки. Запропонований метод забезпечення функціональної стійкості SDN на основі LSTM дає змогу створити інтелектуальну систему адаптивного управління, здатну підтримувати стабільність мережі в умовах дестабілізуючих впливів кібератак. Результати моделювання підтверджують доцільність використання нейромережевих механізмів для прогнозування станів і корекції параметрів SDN у реальному часі. У перспективі планується розширити модель для багаторівневих SDN-архітектур і дослідити вплив просторової топології на ефективність адаптивного управління.

Ключові слова: програмно-керована мережа, функціональна стійкість, кібератака, стохастичне моделювання, рекурентна нейронна мережа.

Вступ

Сучасні програмно-керовані мережі (Software-Defined Networks, SDN) відіграють ключову роль у побудові гнучких, масштабованих і керованих інфраструктур передачі даних. Проте їхня централізована архітектура робить такі мережі вразливими до різноманітних кібератак, здатних призвести до деградації або повної втрати функціональної стійкості. Забезпечення безперервного функціонування SDN в умовах змінних загроз вимагає розроблення інтелектуальних методів управління, здатних адаптивно реагувати на аномалії та підтримувати стабільний стан системи (Кравченко, & Фісун, 2025).

Загальна постановка проблеми. Відокремлення площини управління від площини передачі даних у SDN забезпечує централізоване керування мережею, гнучке маршрутизаційне планування й ефективне використання ресурсів. Водночас така архітектура створює нові вектори кібератак на контролер і мережеві пристрої, що актуалізує проблему забезпечення функціональної стійкості SDN. Стохастичний характер динаміки мережі та часові залежності між атаками і реакцією системи ускладнюють підтримання стійкості, тому доцільним є використання оптимального управління інтенсивностями переходів між станами.

Отже, суть проблеми полягає у розробленні моделі та методу адаптивного управління станами SDN, що забезпечує її функціональну стійкість у динамічних умовах кібератак і мінімізує ризики деградації мережі.

Огляд літератури. У сфері забезпечення функціональної стійкості SDN під час кібератак проведено чимало досліджень, які розглядають загальні загрози, відмовостійкість і методи виявлення атак. Наприклад в роботі (Scott-Hayward, O'Callaghan, & Sezer, 2013) узагальнено безпекові аспекти площин SDN – контролера, комутаторів і протоколу OpenFlow – та класифіковано основні сценарії атак. Перевагою роботи є систематизація векторів загроз і контрзаходів, проте вона має описовий характер і не враховує кількісне моделювання функціональної стійкості чи адаптивне управління мережею.

В огляді (Silva et al., 2015) розглянуто відмовостійкість і резервування контролерів і мережевих елементів, що створює корисну основу для побудови архітектури SDN. Водночас дослідження зосереджується переважно на

інфраструктурних рішеннях і майже не охоплює динамічне моделювання стохастичних переходів між станами мережі під час цілеспрямованих атак.

Аналітичні підходи, зокрема й дослідження (Kotenko et al., 2023), поєднують марковські моделі атак, стохастичні мережі й елементи машинного навчання для оцінювання впливу атак на функціональність SDN. Перевагою роботи є формалізація взаємозв'язку між атаками та параметрами мережі, однак питання керування інтенсивностями переходів (λ) та розроблення адаптивних стратегій управління залишаються недостатньо опрацьованими.

Дослідження із застосуванням LSTM (Long Short-Term Memory) і гібридних глибоких мереж (Sahu, Choudhury, & Misra, 2022) демонструють високу ефективність у класифікації та виявленні атак у SDN, завдяки здатності відтворювати часові залежності. Водночас вони не розглядають питання керування інтенсивностями переходів між станами мережі – ключового для підтримання її стійкості. Методи Deep Reinforcement Learning (Sun et al., 2019) показують здатність агентів адаптивно керувати маршрутизацією чи QoS, проте орієнтовані вони переважно на продуктивність, а не на збереження працездатності під час атак.

Крім того, у роботі (Chen et al., 2021) використано глибокі нейронні мережі для виявлення DDoS-атак, але без подальшого управління після детекції. Аналогічно, у (Wang, Li, & Xu, 2022) розроблено RL-модель для оптимізації трафіка, проте без урахування стійкості до атак. Аналогічно, Liu, Zhao, & Yang (2023) запропонували CNN-attention архітектуру для точнішої детекції, однак без реалізації механізмів відновлення. Автори (Alharbi et al., 2023) запропонували блокчейн-підхід до безпеки SDN, який обмежений у застосуванні в реальному часі.

Інші сучасні роботи також підтверджують актуальність проблеми. Наприклад, Chhaytli, & Persikov (2021) розглядали безпечну маршрутизацію як засіб підвищення кіберстійкості. Автори Farooq, Riaz, & Alvi (2023) визначили ключові виклики безпеки SDN, а Hoang, Nguyen, & Pham (2024) показали ефективність LSTM у прогнозуванні мережевих маршрутів. Утім, усі ці підходи зосереджені на підвищенні QoS чи безпеки окремих компонентів, але не забезпечують адаптивного управління для підтримання функціональної стійкості SDN у динамічних умовах кібератак.

Отже, наведений огляд робіт показує, що попри значну кількість досліджень у сфері стійкості та безпеки SDN, більшість із них фокусуються або на виявленні атак, або на підвищенні продуктивності мережі. Недостатньо розробленими залишаються методи, які комплексно враховували б часову динаміку станів SDN, адаптивну зміну параметрів системи та критерії функціональної стійкості під час кібератак.

Метою нашої статті є забезпечення функціональної стійкості програмно-орієнтованих мереж (SDN) в умовах дії кібератак шляхом розроблення методу адаптивного керування параметрами мережі на основі оцінювання її поточного стану та рівня загрози.

Для досягнення поставленої мети визначено такі основні завдання дослідження:

1. Проаналізувати сучасні підходи до забезпечення стійкості та безпеки SDN у контексті кібератак різної інтенсивності.
2. Формалізувати модель функціонування SDN як стохастичної системи, здатної до переходу між різними станами під впливом зовнішніх загроз.
3. Розробити метод адаптивного управління, який забезпечує підтримання заданого рівня функціональної стійкості мережі.
4. Провести імітаційне моделювання процесу зміни ймовірностей перебування SDN у різних станах за різних рівнів загроз.

Методи

Обґрунтування підходу щодо забезпечення функціональної стійкості SDN. Концептуальна структура SDN включає прикладний рівень, API, рівень керування, протокол OpenFlow та рівень даних (рис. 1) (Karakus, & Durresi, 2017). Рівень даних, представлений програмними або апаратно-програмними комутаторами, забезпечує передачу трафіка L2/L3, виконуючи отримані від контролера правила через канал керування OpenFlow. Контролер є центральним елементом, що керує мережею, формує маршрути, збирає інформацію про стан пристроїв і надає інтерфейси API для взаємодії з мережевими застосунками.

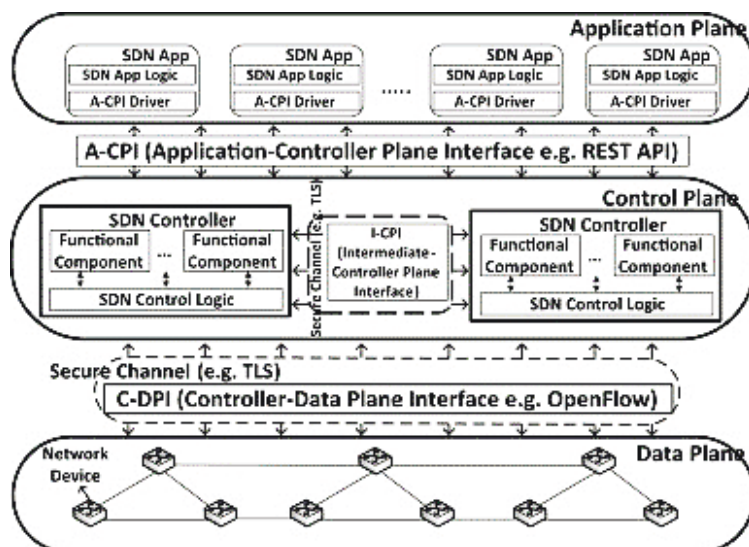


Рис. 1. Концептуальна структура SDN (Karakus, & Durresi, 2017)



Разом із перевагами, централізоване управління в SDN створює нові ризики. Основними вразливими елементами SDN є контролер, канал керування, користувацькі з'єднання та відкриті потоки комутаторів. Тому забезпечення функціональної стійкості SDN розглядають як здатність мережі підтримувати свої функції та продуктивність навіть під впливом кібератак.

Розглянемо модель функціональної стійкості SDN. Для оцінювання функціональної стійкості SDN необхідно визначити умови, за яких мережа втрачає здатність виконувати свої основні функції. Логічно її можна поділити на транспортну та локальну компоненти. Транспортну мережу вважають непрацездатною у випадку відмови або підміни контролера з метою перехоплення трафіка, виходу з ладу маршрутизаторів, що забезпечують транспортну складову, змін топології, які створюють "чорні діри" для трафіка, або порушення зв'язку між вузлами. З урахуванням цих факторів функціональну стійкість SDN із резервними комутаторами OpenFlow та контролером можна описати марковською моделлю з дискретними станами у неперервному часі, де час перебування в кожному стані підпорядковується експоненціальному закону розподілу (Kotenko et al., 2023). На рис. 2 наведено граф можливих станів системи та переходів між ними.

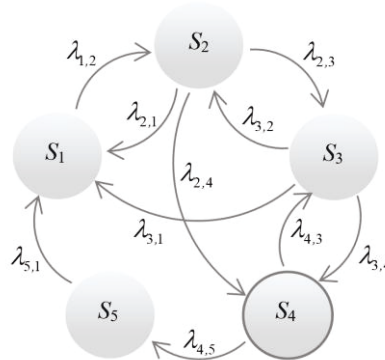


Рис. 2. Граф дискретних станів та умовних переходів в SDN

У загальному випадку для розподіленої корпоративної SDN під впливом кібератак можна виділити такі дискретні стани:

- S_1 – нормальна стійка робота мережі;
- S_2 – фаза розвідки, коли зломисник збирає інформацію про цільову інфраструктуру;
- S_3 – активні спроби реалізації атаки;
- S_4 – успішна компрометація з порушенням функціонування мережі (отримання зломисником доступу до контролера або інших критичних ресурсів);
- S_5 – відновлення після атаки (відновлення працездатності).

Ключові переходи між цими станами включають:

- λ_{12} – виникнення можливостей підключення зломисника (напр., через публічні мережі);
- λ_{21} – ухилення зломисника від атаки;
- λ_{23} – накопичення зломисником достатньої кількості розвідувальної інформації;
- λ_{24} – проведення непідготовленої атаки;
- λ_{31} – невдала атака з виявленням;
- λ_{32} – невдала атака без виявлення;
- λ_{34} – успішна компрометація;
- λ_{43} – запобігання доступу завдяки превентивним заходам;
- λ_{45} – виявлення аномалій у трафіку та поведінці пристроїв;
- λ_{51} – перезавантаження мережевих елементів із застосуванням оновлених параметрів.

Отже, початкові дані для задачі такі:

1. Граф агрегованих стійких станів SDN в умовах кібератаки $G = (S, \lambda)$ (рис. 2).

2. Набір станів SDN під час кібератаки:

$$S = (S_1, S_2, S_3, S_4, S_5). \quad (1)$$

3. Набір потоків подій, коли стани SDN змінюються в умовах кібератаки:

$$\Lambda = (\lambda_{12}, \lambda_{21}, \dots, \lambda_{ij}). \quad (2)$$

4. Вектор імовірностей початкових станів системи: $p_i(0) = (1, 0, 0, 0, 0)$.

5. Умова нормалізації:

$$\sum_{i=1}^5 p_i(t) = 1. \quad (3)$$

Інтенсивності потоку λ_{ij} є ключовим параметром, який визначає середню кількість подій, що виникають за одиницю часу. Числові значення інтенсивностей λ_{ij} можуть бути визначені на основі імітаційної моделі системи. Для аналізу динаміки переходів застосовують неперервний час $t \rightarrow \infty$, у межах якого розв'язується система лінійних диференціальних рівнянь із постійними коефіцієнтами, що відповідає опису однорідного марковського процесу.

Згідно з графом станів (рис. 2), складаємо систему диференціальних рівнянь Колмогорова з невідомими функціями $p_i(t)$ (Kravets et al., 2024):



$$\begin{aligned}\frac{\partial p_1(t)}{\partial t} &= \lambda_{51}p_5(t) + \lambda_{31}p_3(t) - \lambda_{12}p_1(t), \\ \frac{\partial p_2(t)}{\partial t} &= \lambda_{12}p_1(t) + \lambda_{32}p_3(t) - \lambda_{23}p_2(t), \\ \frac{\partial p_3(t)}{\partial t} &= \lambda_{23}p_2(t) + \lambda_{43}p_4(t) - (\lambda_{31} + \lambda_{32} + \lambda_{34})p_3(t), \\ \frac{\partial p_4(t)}{\partial t} &= \lambda_{34}p_3(t) - (\lambda_{43} + \lambda_{45})p_4(t), \\ \frac{\partial p_5(t)}{\partial t} &= \lambda_{45}p_4(t) - \lambda_{51}p_5(t), \\ \sum_{i=1}^5 p_i(t) &= 1.\end{aligned}\quad (4)$$

Кожне рівняння системи (4) відображає зміну ймовірності перебування SDN у певному стані залежно від можливих переходів між цим та іншими станами. На відміну від випадкових технічних збоїв, кібератаки мають цілеспрямований і багаторівневий характер, що може призвести до значних порушень у роботі мережі. Відтак забезпечення її функціональної стійкості передбачає не лише підвищення надійності компонентів, але й формування здатності системи своєчасно виявляти, локалізувати та нейтралізувати атаки за збереження працездатності.

Аналізуючи модель SDN, зображену на рис. 2, варто зазначити, що лише стан S_4 описує відмову системи внаслідок успішної атаки, тобто стан, якого необхідно уникнути. Тому показник функціональної стійкості доцільно визначати як сумарну ймовірність перебування системи в усіх інших станах $S_1 + S_2 + S_3 + S_5$, що характеризують її здатність зберігати працездатність за більшості типових умов.

Водночас перед оцінюванням цього показника необхідно визначити ризик кібератаки, що передбачає побудову її математичної моделі на основі вербального опису сценарію атаки.

Модель кібератаки на SDN базується на послідовності етапів, які відображають логіку дій зломисника – від збору інформації до приховування слідів. Такий підхід дозволяє описати кібератаку як послідовність станів і переходів між ними, що створює основу для математичного моделювання процесу (Kotenko et al., 2023).

Для кількісного опису цього процесу доцільно застосувати апарат *сигнальних графів*, який дає змогу подати кібератаку як сукупність взаємопов'язаних елементарних підпроцесів із певними ймовірностями та часовими характеристиками. Вузли графа відповідають станам системи, а ребра – можливим подіям чи переходам між ними. Використання правил топологічних перетворень і формули Мейсона дозволяє отримати узагальнену функцію передачі, що характеризує ймовірнісну динаміку розвитку атаки (Srikant, & Ying, 2014; Robert, 2013).

Розглянемо модель атаки "Підміна топології мережі". Щоб побудувати математичну модель кібератаки на зразок "Підміна топології мережі", подамо сценарій її реалізації у вигляді послідовності дій (табл. 1).

Таблиця 1

Сценарій кібератаки на зразок "Підміна топології мережі"

№	Опис етапу кібератаки	Позначення етапу	Час процесу	Функція розподілу часу
1	Перевірка доступності каналу зв'язку з атакованою мережею	$w(s)$	$\bar{t}_{test}$	$W(t)$
2	Обмін повідомленнями з контролером через протокол OpenFlow з одночасною підміною легітимного вузла шкідливим пристроєм	$m(s)$	$\bar{t}_{tac}$	$M(t)$
3	Передача контролеру зібраної мережевої статистики через протокол керування й аналіз отриманої відповіді	$l(s)$	$\bar{t}_{tr}$	$L(t)$
4	Зміна конфігурації мережі подачею фальшивих даних статистики	$z(s)$	$\bar{t}_{repl}$	$Z(t)$
5	Маніпулювання роботою мережі через введення контролера в оману фальшивими повідомленнями OpenFlow	$d(s)$	$\bar{t}_{re}$	$D(t)$

Наслідком атаки "підміна топології мережі" є проникнення зломисника під виглядом довіреного мережевого пристрою з використанням ідентифікаційних даних, здобутих у процесі розвідки. Опис цієї атаки за даними з табл. 1 наведено у вигляді сигнального графа (рис. 3) (Qin, Li, & Zhang, 2023).

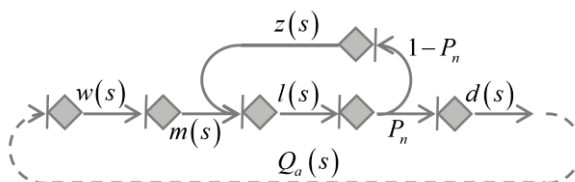


Рис. 3. Сигнальний граф для атаки "Підміна топології мережі"

Для обчислення еквівалентної функції використовують концепцію замкненого сигнального графа, що враховує наявність циклів першого та k -го порядків (Srikant, & Ying, 2014; Robert, 2013). Еквівалентна функція циклу k -го порядку

$$Q_k(k) = \prod_{i=1}^k Q_i(s). \quad (5)$$

де $Q_i(s)$ – еквівалентна функція i -го циклу першого порядку, що визначається як добуток еквівалентних функцій усіх гілок, які формують цей цикл.



Це також дає змогу застосувати топологічне рівняння Мейсона (Lu, Hsu, & Chang, 2020) для замкнених сигнальних графів із метою обчислення еквівалентної функції початкової мережевої моделі:

$$H = 1 + \sum_{k=1}^K (-1)^k Q_k(s) = 0, \quad (6)$$

де K – максимальний порядок циклів, що входять до сигнального графа.

Приєднання до сигнального графа допоміжної (фіктивної) гілки $Q_a(s) = \frac{1}{h(s)}$, де $h(s)$ позначає шукану еквівалентну функцію, дає можливість виділити та перерахувати всі цикли графа.

Цикли першого порядку

$$\frac{w(s)m(s)l(s)P_n d(s)}{h(s)}, (1 - P_n)z(s)l(s). \quad (7)$$

Оскільки в цьому сигнальному графі відсутні цикли другого та вищих порядків, рівняння (7) може бути спрощене та подане у такій формі:

$$1 - \frac{w(s)m(s)l(s)P_n d(s)}{h(s)} - (1 - P_n)z(s)l(s) = 0. \quad (8)$$

У цьому випадку еквівалентна функція набуває вигляду

$$h(s) = \frac{w(s)m(s)l(s)P_n d(s)}{1 - (1 - P_n)z(s)l(s)}. \quad (9)$$

Для визначення розрахованого відношення функції розподілу припустимо, що часові тривалості всіх елементарних процесів на ребрах графа є взаємно незалежними випадковими величинами з експоненціальним законом розподілу з параметрами

$$W(t) = 1 - e^{-wt}, M(t) = 1 - e^{-mt}, \\ L(t) = 1 - e^{-lt}, D(t) = 1 - e^{-dt}, Z(t) = 1 - e^{-zt}, \quad (10)$$

де $w = \frac{1}{\bar{t}_{test}}, m = \frac{1}{\bar{t}_{tac}}, l = \frac{1}{\bar{t}_{tr}}, d = \frac{1}{\bar{t}_{re}}, z = \frac{1}{\bar{t}_{repl}}$, а $\bar{t}_{test}, \bar{t}_{tac}, \bar{t}_{tr}, \bar{t}_{re}, \bar{t}_{repl}$ – середній час реалізації k -го етапу атаки.

Застосування перетворення Лапласа дає змогу отримати зображення функцій щільності розподілу часу виконання k -го етапу атаки. Таке зображення являє собою функцію у частотній області, отриману шляхом інтегрального перетворення Лапласа вихідної функції із часової області. Воно відображає поведінку процесу не у часі, а у спектральному вимірі, що дає змогу спростити аналіз складних систем (Amin, & Ahmad, 2022).

Зазначене перетворення визначається співвідношенням $F(s) = \int_0^\infty e^{-st} f(t) dt$, де $f(t)$ – функція в часовій області (залежність від часу t); $F(s)$ – її зображення у частотній області, отримане за допомогою перетворення Лапласа. Змінна s є комплексною і називається частотою Лапласа. Зазначений підхід дозволяє перетворювати диференціальні рівняння часової області на алгебраїчні рівняння у частотній області, що полегшує процес їхнього розв'язання. Наприклад, для експоненціальної функції $f(t) = e^{at}$, її зображення за перетворенням Лапласа матиме вигляд $F(s) = \frac{1}{s-a}$.

У нашому випадку

$$w(s) = \int_0^\infty e^{-st} d[W(t)] = \frac{w}{w+s}, \\ m(s) = \int_0^\infty e^{-st} d[M(t)] = \frac{m}{m+s}, \\ l(s) = \int_0^\infty e^{-st} d[L(t)] = \frac{l}{l+s}, \\ d(s) = \int_0^\infty e^{-st} d[D(t)] = \frac{d}{d+s}, \\ z(s) = \int_0^\infty e^{-st} d[Z(t)] = \frac{z}{z+s}. \quad (11)$$

Підставивши (10) у вираз (11), а отримані результати – у вираз (9), одержимо

$$h(s) = \frac{wmlP_n d(z+s)}{(w+s)(d+s)(m+s)[(l+s)(z+s) - (1-P_n)zl]}. \quad (12)$$

Для спрощення подальших обчислень доцільно виконати заміну окремих коефіцієнтів при змінній s у знаменнику рівняння (12), що дозволить отримати зручнішу форму для аналітичного розв'язання:

$$A = d + l + m + w + z, \\ B = mw + mz + wz + d(l + m + w + z) + l(m + w + z - (1 - P_n)z), \\ C = mwz - lw(-1 + (1 - P_n)z) + lm(w + z - (1 - P_n)z) + d(wz + m(w + z) + l(m + l + z - (1 - P_n)z)), \\ D = -lmw(-1 + (1 - P_n)z) + (mwz - lw(-1 + (1 - P_n)z) + lm(w + z - (1 - P_n)z)), \\ E = dlmwz - dlm(1 - P_n)wz. \quad (13)$$

Щоб знайти оригінал еквівалентної функції (12), скористаємося дискретною формою розкладання Гевісайда (методом розкладання на прості дробі) (Malik, & Singh, 2023):

$$h(s) = \sum_{k=1}^n \frac{f(s_k)}{\varphi'(s_k)} \cdot \frac{1}{s-s_k} = \sum_{k=1}^5 \frac{wmlP_n d(z+s_k)}{5s_k^4 + 4As_k^3 + 3Bs_k^2 + 2Cs_k + D} \cdot \frac{1}{s-s_k}, \quad (14)$$

де $\varphi'(s_k)$ – похідна знаменника (12); s_k – розкладання полюсів (корені рівняння $s^5 + As^4 + Bs^3 + Cs^2 + Ds + E = 0$); w, m, l, d, z – визначають так само, як і в (10).

Тоді

$$h(t) = L^{-1}\{h(s)\} = \sum_{k=1}^5 \frac{wmlP_n d(z+s_k)}{5s_k^4 + 4As_k^3 + 3Bs_k^2 + 2Cs_k + D} \cdot e^{s_k t}. \quad (15)$$

Оскільки отриманий вираз описує функцію щільності ймовірностей, то відповідну інтегральну функцію розподілу ймовірностей визначають як її інтеграл від нуля до поточного моменту часу:

$$F(t) = \int_0^t h(t)dt = \sum_{k=1}^5 \frac{wmlP_n d(z+s_k)}{5s_k^4 + 4As_k^3 + 3Bs_k^2 + 2Cs_k + D} \cdot \frac{1-e^{s_k t}}{(-s_k)} \quad (16)$$

Середній час $\bar{t}_{attack}$, витрачений на реалізацію кібератаки, знаходять як

$$\bar{t}_{attack} = \int_0^\infty th(t)dt = \sum_{k=1}^5 \frac{wmlP_n d(z+s_k)}{5s_k^4 + 4As_k^3 + 3Bs_k^2 + 2Cs_k + D} \cdot \frac{1}{(-s_k)^2} \quad (17)$$

Отже, було визначено інтегральну функцію розподілу та обчислено середній час $\bar{t}_{attack}$ реалізації кібератаки. Аналогічні розрахунки можна виконати для кожного типу кібератаки, що дає змогу здійснити комплексне оцінювання їхнього впливу на стійкість SDN.

Приклад реалізації моделі кібератаки на SDN. Для ілюстрації підходу розглянемо атаку "Підміна топології мережі", використавши часові показники з табл. 1 як параметри елементарних підпроцесів: $\bar{t}_{test} = 4.3$ хв, $\bar{t}_{tac} = 2.5$ хв, $\bar{t}_{tr} = 5.0$ хв, $\bar{t}_{repl} = 5.5$ хв, $\bar{t}_{re} = 3.4$ хв. Імовірність успішного перехоплення управління в SDN змінюватимемо у межах $P_n = 0.1 \dots 1.0$.

На основі вихідних даних побудовано залежності $F(t)$ та T_a , (рис. 4–5), що дозволяють визначити: імовірність $P_n(t \leq T_a)$ реалізації кібератаки за час, не більший заданого T_a ; середній час реалізації атаки; а також часову межу, яка відповідає заданому рівню загрози реалізації кібератаки.

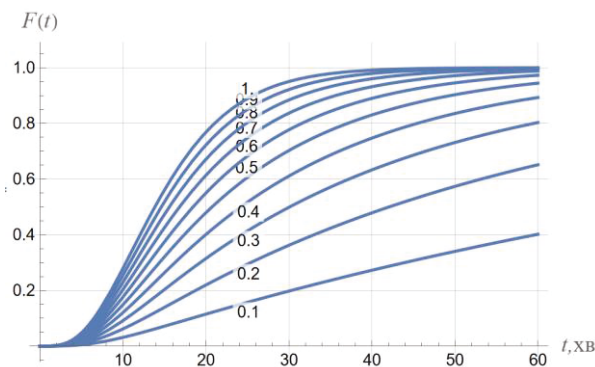


Рис. 4. Інтегральна функція розподілу ймовірності від часу реалізації кібератаки

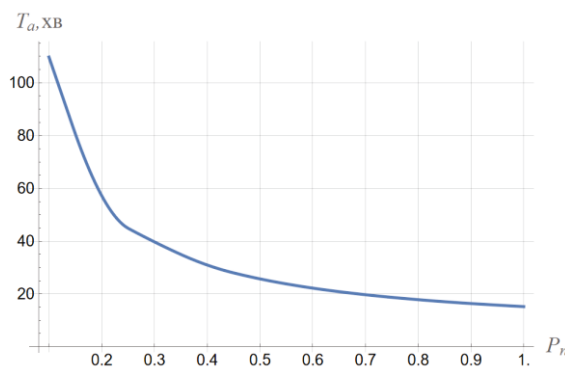


Рис. 5. Залежність середнього часу реалізації кібератаки від імовірності P_n

Аналіз побудованих залежностей (рис. 4–5) показує, що для реалізації кібератаки на зразок "Підміна топології мережі" за заданих часових характеристик етапів атаки необхідно близько 170 хв у разі ймовірності успішного перехоплення управління в SDN при $P_n = 0.1$, і приблизно 22 хв при $P_n = 0.9$. Отримані графічні залежності дають змогу оцінити, як зміна ймовірності успішного перехоплення управління в SDN у межах заданого часу впливає на функцію розподілу тривалості реалізації атаки. Спостерігається тенденція до зменшення середнього часу виконання атаки зі збільшенням значення P_n . Водночас із подальшим зростанням P_n ступінь його впливу на інтегральну функцію розподілу $F(t)$ поступово зменшується, і після досягнення певного порогу цей вплив стає незначним. Отже, отримано інтегральні функції розподілу та середній час $\bar{t}$ реалізації кібератаки, що може бути використано для аналогічних розрахунків щодо інших типів атак на SDN.

Метод оптимального управління для забезпечення функціональної стійкості SDN в умовах кібератак. Задачу забезпечення функціональної стійкості SDN в умовах деструктивного кібервпливу можна подати у вигляді задачі оптимального управління динамічною системою (4), у якій керуючі параметри $\lambda_{ij}(t)$ можуть мати безперервний або дискретний характер.

Формулювання задачі. Еволюція станів системи $p(t) = (p_1, \dots, p_5)$ описується системою звичайних диференціальних рівнянь $p'(t) = f(p(t), \lambda(t))$, що відповідає марковській моделі (4).

В межах поставленої мети – забезпечення функціональної стійкості SDN – завдання управління мережею полягає у максимізації інтегрального критерію ефективності

$$J[\lambda(\cdot)] = \int_0^T R(t)dt = \int_0^T (p_1(t) + p_2(t) + p_3(t) + p_5(t))dt \rightarrow \max_{\lambda(t)} \quad (18)$$



при обмеженнях на керування $\lambda_{ij}(t) \in [0, \lambda_{ij}^{max}]$, який відображає сумарну ймовірність перебування системи у працездатних станах протягом заданого інтервалу часу. Така постановка задачі дозволяє визначити оптимальну стратегію впливу на параметри системи з метою мінімізації наслідків кібератак і підтримання безперервності функціонування SDN.

Оскільки еволюція станів SDN характеризується часовою залежністю та наявністю "пам'яті" щодо попередніх подій – спроб кібератак і реакцій системи на них – для розв'язання задачі (18) та формування оптимального закону управління інтенсивностями переходів $\lambda_{ij}(t)$ найдоцільнішим є застосування рекурентних нейронних мереж (RNN). Цей клас моделей здатний ефективно відтворювати послідовні залежності, поєднуючи інформацію про поточний стан мережі з історією її функціонування, що дає змогу прогнозувати майбутні переходи між станами. Завдяки такій властивості RNN можуть адаптивно змінювати керуючі впливи $\lambda_{ij}(t)$ з метою максимізації інтегрального показника функціональної стійкості SDN у межах заданого часового інтервалу $[0, T]$. Це забезпечує підтримання безперервності та безпеки роботи мережі навіть за умов динамічних і непередбачуваних кібератак.

Параметризація закону управління SDN. Для практичної реалізації підходу потрібно формалізувати керування інтенсивностями переходів $\lambda_{ij}(t)$ у вигляді закону управління, який враховує поточний стан SDN та історію попередніх подій. Для цього доцільно застосувати рекурентні нейронні мережі типу LSTM, що дозволяють параметризувати закон управління як функцію від поточних спостережень і попередніх керувань.

На момент k (у час t_k) закон управління отримує вхідний вектор x_k , який зазвичай включає: поточні або апроксимовані ймовірності станів $p(t_k) = (p_1, \dots, p_5)$ (або інші метрики – ентропія потоків, лічильники аномалій тощо); поточний час t_k або нормалізований час $\frac{t_k}{T}$; попередні керування $\lambda_{ij}(t_{k-1})$; а також додаткові контекстні ознаки (стан контролера, завантаження CPU, індикатори зовнішніх загроз).

У такій концепції RNN (LSTM/GRU) потрібні тому, що вплив атак і захисних заходів має часову пам'ять: важливо врахувати темп наростання розвідки, повторні спроби чи застосовані контрзаходи. Рекурентна мережа зберігає прихований стан h_k , який акумулює цю історичну інформацію, і на його основі формує наступні значення інтенсивностей $\lambda_{ij}(t_{k+1})$.

Обґрунтування застосування мережі LSTM. LSTM – це спеціалізований тип рекурентних нейронних мереж (RNN), призначений для ефективного опрацювання послідовних даних із довготривалими залежностями. Архітектура LSTM уможливорює подолання проблеми "згасання градієнта", характерної для класичних RNN. Завдяки своїй структурі LSTM забезпечує механізм вибіркового запам'ятовування або забування інформації, що дає змогу мережі адаптивно керувати часовим контекстом (Krichen, & Mihoub, 2025).

Послідовність кроків функціонування LSTM зображено на рис. 6.

Крок 1. Визначення інформації для видалення зі стану чарунки (рис. 6а). На цьому етапі сигмоїдальний шар забування (forget gate layer) визначає, які дані зі стану чарунки C_{t-1} слід зберегти, а які – відкинути. Він аналізує вхідний вектор x_t та попередній вихід h_{t-1} , після чого для кожного елемента стану формує значення від 0 до 1: 1 – означає "повністю зберегти інформацію"; 0 – "повністю видалити":

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f). \quad (19)$$

Крок 2. Визначення нової інформації для збереження у стані чарунки (рис. 6б). На цьому етапі вхідний шар (input gate layer) із сигмоїдальною активацією визначає, які саме дані необхідно оновити. Після цього шар з активацією $\tanh$ формує новий вектор кандидатних значень $\tilde{C}_t$, які можна додати до стану чарунки для оновлення її змісту:

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i), \quad (20)$$

$$\tilde{C}_t = \tanh(W_C \cdot [h_{t-1}, x_t] + b_C). \quad (21)$$

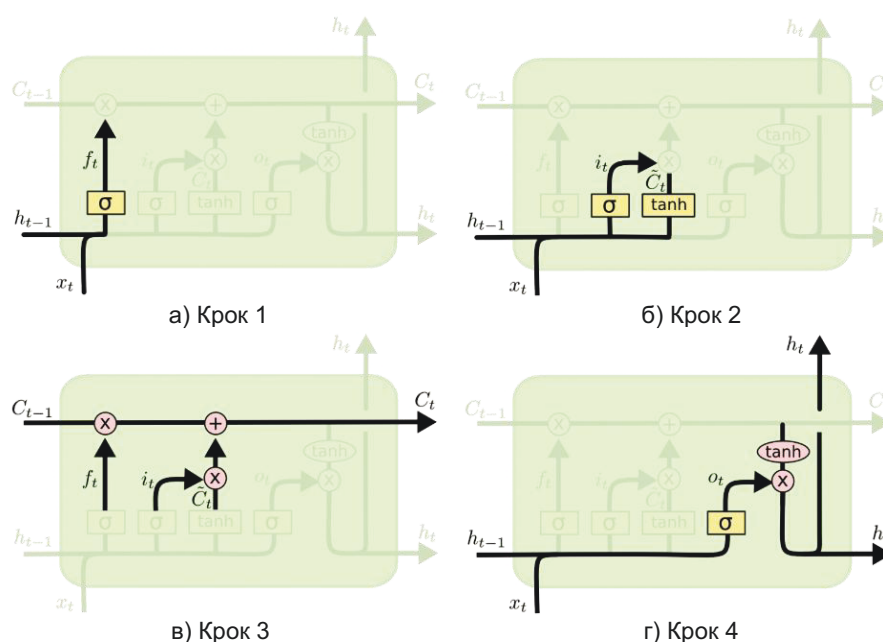


Рис. 6. Функціонування мережі LSTM (Olah, 2015)

Крок 3. Оновлення стану чарунки (рис. 6в). На цьому кроці попередній стан чарунки C_{t-1} перетворюється на новий C_t . Спочатку попередній стан множиться на f_t , що відповідає за "забуту" частину інформації. Потім до нього додається добуток Адамара $i_t \circ \tilde{C}_t$, який представляє нові кандидатні значення, зважені за ступенем їхньої важливості. У результаті формується оновлений стан чарунки C_t , що поєднує релевантну попередню інформацію з новими даними:

$$C_t = f_t \circ C_{t-1} + i_t \circ \tilde{C}_t. \quad (22)$$

Крок 4. Формування вихідного сигналу (рис. 6г). На цьому етапі визначають, яку інформацію слід передати далі. Спочатку сигмоїдальний шар o_t вирішує, які частини оновленого стану чарунки C_t потраплять на вихід. Потім значення стану проходять через функцію активації $\tanh$, що обмежує їх у межах від -1 до 1 . Отриманий результат перемножується з вихідним сигналом сигмоїдального шару, завдяки чому на виході h_t залишається лише найбільш релевантна інформація для подальшого оброблення:

$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o), \quad (23)$$

$$h_t = o_t \circ \tanh(C_t). \quad (24)$$

Застосування мереж LSTM для побудови методу оптимального управління функціональною стійкістю SDN в умовах кібератак має суттєві переваги завдяки їхній здатності моделювати часові залежності та запам'ятовувати попередні стани системи. LSTM забезпечують ефективне врахування історії динаміки атак і реакцій мережі, що дозволяє адаптивно коригувати інтенсивності переходів між станами SDN з урахуванням контексту попередніх подій.

Навчання LSTM. Для задачі забезпечення функціональної стійкості SDN в умовах кібератак найдоцільнішим є поєднання імітаційного навчання (offline learning) з подальшою онлайн-адаптацією. На першому етапі LSTM може бути попередньо натренована на симульованих сценаріях функціонування мережі, що охоплюють різні типи атак, збоїв і процесів відновлення. Такий підхід дозволяє безпечно сформувати базову політику управління інтенсивностями переходів без ризику впливу на реальну інфраструктуру. Імітаційне навчання дає змогу LSTM отримати початкові навички оптимального реагування на типові ситуації, зменшуючи час адаптації в реальних умовах.

Додатково, для підвищення ефективності процесу оптимізації може бути використаний елемент навчання з підкріпленням (RL) у контурі онлайн-адаптації. У цьому випадку LSTM отримує зворотний зв'язок у вигляді функції винагороди, що відображає рівень стійкості системи, і поступово вдосконалює свої дії. Така гібридна стратегія – "offline pretraining + online reinforcement fine-tuning" – забезпечує як безпечний старт, так і здатність до постійного самонавчання в умовах реальних кіберзагроз.

Схема управління для забезпечення функціональної стійкості SDN в умовах кібератак. Загальну схему управління SDN, побудовану на LSTM-мережі, зображено на рис. 7. Ця схема відображає роботу інтелектуального модуля управління функціональною стійкістю SDN, у якому LSTM-мережа виконує роль адаптивного прогностно-коригуючого елемента.

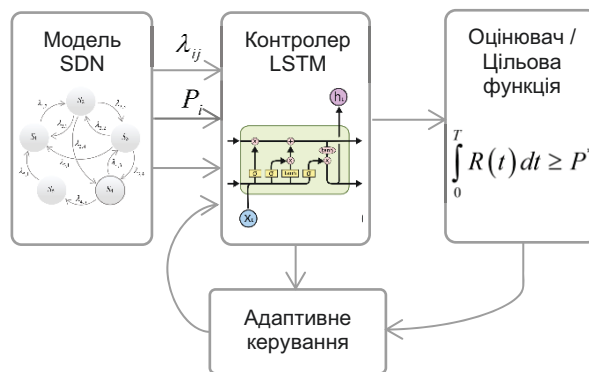


Рис. 7. Схема інтелектуалізованого управління SDN

У схемі на рис. 7 наведено:

1. Блок SDN-моделі (система станів $S_1, \dots, S_5$). Переходи між станами визначаються інтенсивностями λ_{ij} , окремі з яких ($\lambda_{12}, \lambda_{34}, \lambda_{45}, \lambda_{51}$) можуть змінюватися в часі.

2. LSTM-модуль. На вхід LSTM-модуля надходять часові ряди, що характеризують поточний стан SDN: поточні ймовірності станів ($P_1, \dots, P_5$); інтенсивності переходів λ_{ij} ; показники навантаження, затримок, аномалій трафіка; індикатори безпеки (кількість атак, типи подій тощо). LSTM, завдяки своїй пам'яті (cell state), враховує історію цих параметрів, що дозволяє відстежувати тенденції змін системи.

3. Робота LSTM-модуля управління. На основі попередніх і поточних станів LSTM-модуль прогнозує майбутню динаміку і формує керувальні дії – оновлені значення деяких інтенсивностей переходів: ($\lambda_{12}, \lambda_{34}, \lambda_{45}, \lambda_{51}$). У такий спосіб LSTM виконує оптимізацію параметрів системи, спрямовану на збереження функціональної стійкості.

4. Цільова функція (18) – це інтегральний показник стійкості, який відображає ймовірність того, що система перебуває у працездатному стані. LSTM коригує інтенсивності переходів таким способом, щоб підтримувати цей показник на рівні, що не нижчий від заданого порогу P^* .

5. Зворотний зв'язок. Отримані нові значення λ_{ij} подаються назад у модель SDN, яка еволюціонує в часі відповідно до скоригованих параметрів. Результат цього впливу знову надходить на вхід LSTM, утворюючи замкнений контур оптимального управління.



Отже, схема реалізує адаптивне управління на основі прогнозу, де LSTM безперервно навчається на поточних і минулих даних, забезпечуючи максимізацію показника функціональної стійкості SDN в умовах змінних кібератак і навантажень.

Результати

Для демонстрації запропонованого підходу розглянемо три сценарії, що відповідають низькому, середньому та високому рівням загрози кібератак (табл. 2), для яких задано відповідні значення інтенсивностей переходів λ_{ij} . Як видно з табл. 2, сценарії відрізняються співвідношеннями інтенсивностей переходів між станами. Зокрема, за низького рівня загрози спостерігається більша інтенсивність переходів до функціонально стійких станів (S_1, S_2, S_3, S_5), ніж до деградованого стану S_4 . За високого рівня загрози, навпаки, переважають переходи до стану S_4 , що відображає зростання ризику втрати стійкості. Середній рівень загрози характеризується більш збалансованими значеннями інтенсивностей переходів між усіма станами.

Таблиця 2

Початкові значення інтенсивностей переходів між станами SDN для різних сценаріїв реалізації загроз

Позначення	Рівень загрози		
	низький	середній	високий
λ_{12}	0.2	0.3	0.5
λ_{21}	0.5	0.3	0.05
λ_{23}	0.2	0.3	0.4
λ_{24}	0.05	0.3	0.15
λ_{31}	0.5	0.3	0.05
λ_{32}	0.4	0.3	0.02
λ_{34}	0.05	0.3	0.4
λ_{43}	0.5	0.3	0.05
λ_{45}	0.5	0.3	0.2
λ_{51}	0.3	0.3	0.3

Запропонований метод забезпечення функціональної стійкості SDN на основі застосування рекурентних нейронних мереж LSTM реалізується у чотири етапи:

- 1) формування початкових даних;
 - 2) отримання на основі початкових даних залежностей ймовірностей $P_1(t), \dots, P_5(t)$ перебування системи в станах $S_1, \dots, S_5$;
 - 3) запуск LSTM-модуля, прогнозування зміни $P_1(t), \dots, P_5(t)$ і визначення моментів часу, коли $P_{\text{ФС}}(t) = P_{\text{ФС}}^*$. Корекція заданих параметрів λ_{ij} шляхом визначення нових оптимальних значень λ_{ij} за деяким інтегральним максимумом $P_1(t) + P_2(t) + P_3(t) + P_5(t)$;
 - 4) оцінювання впливу скоригованих початкових даних на функціональну стійкість системи, яка досліджується.
- У результаті моделювання з використанням параметрів, наведених у табл. 2, отримано відповідні графічні залежності, подані на рис. 8–10.

З аналізу наведених графіків (рис. 8–10) видно, що за заданих інтенсивностей переходів властивість функціональної стійкості SDN, яка визначається ймовірністю перебування системи у працездатних станах $P_{\text{ФС}}$, зберігається протягом усього періоду лише за умов низького рівня загрози кібератаки. Для середнього та високого рівнів загроз ця властивість має обмежений у часі характер – близько 28 хв і 2 хв відповідно.

Як показує приклад на рис. 8, у сценарії низького рівня загрози система залишається стабільною і не потребує втручання. У випадку середнього рівня загрози (рис. 9) приблизно на 28-й хвилині спостерігається втрата стійкості $P_{\text{ФС}}(t) \leq P_{\text{ФС}}^*$, що вимагає коригування параметрів λ_{ij} . Після внесення змін до інтенсивностей переходів отримано нові значення $P_{\text{ФС}}(t)$, на основі яких побудовано оновлені залежності ймовірностей станів (рис. 11–12). Як показано на рис. 11, після регулювання у цьому сценарії спостерігається ще один момент часу – приблизно на 56-й хвилині, коли система знову переходить у критичний режим роботи. Це свідчить про необхідність повторного коригування параметрів для відновлення функціональної стійкості SDN і запобігання подальшому зниженню її працездатності.

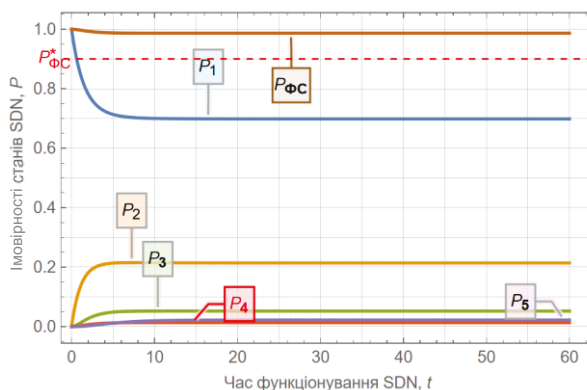


Рис. 8. Зміна ймовірностей станів SDN для низького рівня загрози атаки

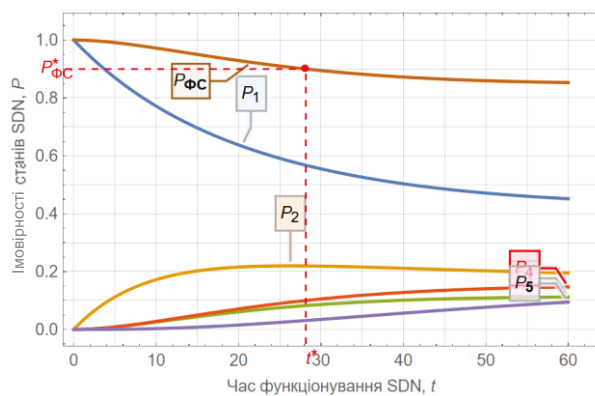


Рис. 9. Зміна ймовірностей станів SDN для середнього рівня загрози атаки

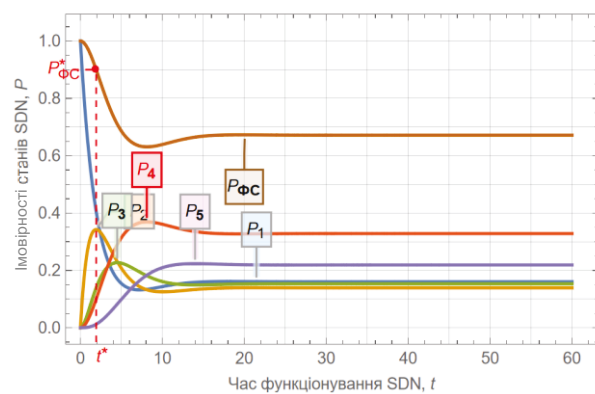


Рис. 10. Зміна ймовірностей станів SDN для високого рівня загрози атаки

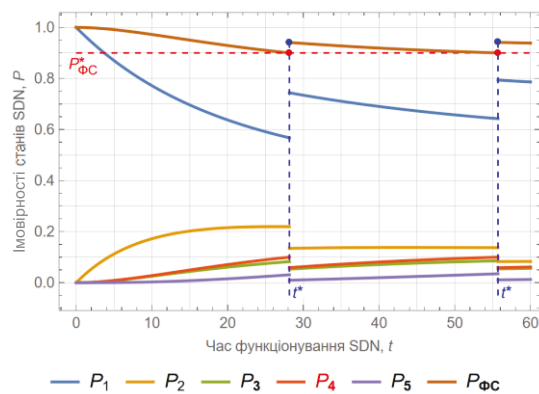


Рис. 11. Зміна ймовірностей станів SDN при середньому рівні загрози атаки з корекцією λ_{ij}

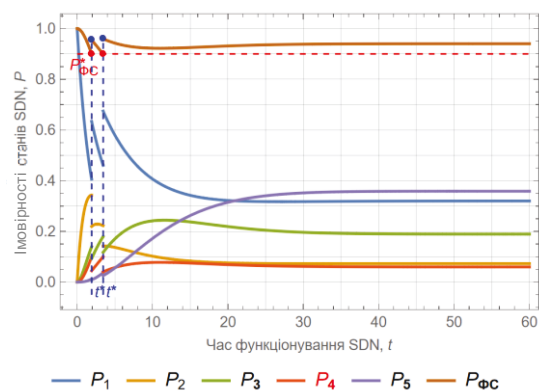


Рис. 12. Зміна ймовірностей станів SDN при високому рівні загрози атаки з корекцією λ_{ij}



У випадку сценарію з високим рівнем загрози (рис. 12) критичні стани системи спостерігаються вже на 2-й та 4-й хвилинах моделювання. Це вимагає оперативнішого втручання та корекції параметрів λ_{ij} у зазначені моменти часу, що дає змогу підтримати функціональну стійкість SDN навіть за умов інтенсивного зовнішнього впливу.

Таким чином, величина λ_{ij} зі стаціонарної стає змінною в часі $\lambda_{ij}(t)$ і підлягає корекції шляхом пошуку оптимальних значень за критерієм (18) на часовому інтервалі від t^* до t_{max} . Варто зазначити, що в наведених сценаріях (рис. 11–12) оптимізація здійснювалася не для всіх λ_{ij} , а лише для тих, що мають найбільший вплив на функціональну стійкість SDN. Зокрема: λ_{12} – ініціація розвідки та контроль підключень (вхід / доступ); λ_{34} – імовірність успішної атаки ("прорив"); λ_{45} – виявлення аномалій (перехід до відновлення); λ_{51} – швидкість відновлення системи.

Параметр λ_{12} впливає на частоту "початку проблем" – визначає частоту виникнення інцидентів: його зменшення знижує кількість атак і підвищує стабільність системи на початкових етапах роботи, що узгоджується із заходами контролю доступу та фільтрації трафіка (NAC). Параметр λ_{34} характеризує ефективність атаки, його зменшення (напр., через ізоляцію або обмеження привілеїв) безпосередньо підвищує показник стійкості $P_{FC}(t)$. Параметр λ_{45} відповідає за швидкість виявлення аномалій, чим він більший, тим швидше система реагує на загрозу. Нарешті, λ_{51} визначає темп відновлення після інциденту, його оптимізація суттєво впливає на інтегральний показник стійкості $P_{FC}(t)$.

Отже, запропонований підхід дає змогу реалізувати метод визначення рівня функціональної стійкості та побудову оптимального управління SDN в умовах кібератак. Отримані результати підтверджують ефективність моделі для оцінювання та підтримання стійкості мережі до типових кіберзагроз.

Дискусія і висновки

1. В результаті аналізу сучасних підходів до забезпечення стійкості програмно-керованих мереж (SDN) встановлено, що більшість існуючих рішень орієнтовано на виявлення атак і відновлення працездатності, проте вони не враховують часову динаміку функціональної стійкості системи. Це зумовлює необхідність розроблення методу, здатного не лише реагувати на інциденти, а й прогнозувати їхній вплив на стабільність SDN у режимі реального часу.

2. Формалізація моделі функціонування SDN як стохастичної системи, яка описується системою диференціальних рівнянь Колмогорова, дозволяє відобразити процеси переходів між станами мережі під впливом зовнішніх кібератак. Такий підхід забезпечує можливість кількісного оцінювання ймовірностей перебування SDN у функціонально стійких і нестійких станах залежно від інтенсивності атак.

3. Розроблений метод адаптивного управління, який ґрунтується на використанні рекурентної нейронної мережі LSTM для прогнозування динаміки станів SDN і коригування параметрів інтенсивностей переходів між станами системи з метою підтримання інтегрального показника функціональної стійкості, забезпечує своєчасне втручання в роботу мережі для запобігання переходу у критичний стан.

4. Результати імітаційного моделювання свідчать, що розроблена модель адекватно відображає поведінку SDN у різних умовах загроз. Для низького рівня кібератак мережа зберігає функціональну стійкість протягом усього періоду спостереження, тоді як для середнього і високого рівнів відбуваються короточасні втрати стійкості, які можуть бути компенсовані за рахунок своєчасного коригування параметрів моделі.

Отже, результати дослідження підтверджують ефективність розробленого методу забезпечення функціональної стійкості SDN в умовах кібератак і створюють основу для побудови інтелектуальних систем прогнозно-адаптивного управління мережею. У подальших дослідженнях планується розширити запропонований метод шляхом урахування просторової топології SDN і взаємодії між її підмережами, а також інтегрувати механізми глибинного навчання для підвищення точності прогнозування динаміки станів мережі. Перспективним напрямом є також розроблення адаптивного контролера, який у режимі реального часу здійснюватиме оптимізацію параметрів стійкості з урахуванням типу й інтенсивності кібератак.

Внесок авторів: Юрій Кравченко – концептуалізація, методологія, аналіз джерел, написання (перегляд і редагування); Олена Фісун – збір даних та їхня валідація, формальний аналіз, комп'ютерне моделювання, перевірка результатів, написання (оригінальна чернетка).

Джерела фінансування. Це дослідження не отримало жодного гранту від фінансової установи в державному, комерційному або некомерційному секторах.

Список використаних джерел

- Кравченко, Ю. В., & Фісун, О. С. (2025). Аналіз існуючих методів забезпечення функціональної стійкості складних систем для удосконалення комп'ютерних мереж. *Зв'язок*, 3, 29–35. <https://doi.org/10.31673/2412-9070.2025.025385>
- Alharbi, A., Alsubhi, K., Alghamdi, A., & Alotaibi, F. (2023). Blockchain-based decentralized security framework for software-defined networks. *IEEE Access*, 11, 36540–36555. <https://doi.org/10.1109/ACCESS.2023.3258792>
- Amin, M. B. M., & Ahmad, S. S. (2022). Laplace Transform for Solving System of Integro-Fractional Differential Equations of Volterra Type with Variable Coefficients and Multi-Time Delay. *Symmetry*, 14(5), 984. <https://doi.org/10.3390/sym14050984>
- Chen, Y., Zhang, L., Wang, Y., & Xu, J. (2021). Deep neural network-based anomaly detection in software-defined networking. *Computer Networks*, 195, 108180. <https://doi.org/10.1016/j.comnet.2021.108180>
- Chhaytli, Y., & Persikov, A. (2021). Cyber-resilient routing mechanisms for SDN. *Journal of Network and Computer Applications*, 187, 103097. <https://doi.org/10.1016/j.jnca.2021.103097>
- Farooq, M., Riaz, Q., & Alvi, S. (2023). Security challenges and solutions in software-defined networking: A systematic review. *Journal of Information Security and Applications*, 74, 103453. <https://doi.org/10.1016/j.jisa.2023.103453>
- Hoang, T., Nguyen, H., & Pham, Q. (2024). LSTM-based predictive routing for adaptive resource allocation in SDN environments. *Future Generation Computer Systems*, 154, 328–340. <https://doi.org/10.1016/j.future.2023.10.026>
- Karakus, M., & Durrezi, A. (2017). Quality of Service (QoS) in Software Defined Networking (SDN): A survey. *Journal of Network and Computer Applications*, 80, 200–218. <https://doi.org/10.1016/j.jnca.2016.12.019>
- Kotenko, I., Saenko, I., Privalov, A., & Laut, O. (2023). Ensuring SDN Resilience under the Influence of Cyber Attacks: Combining Methods of Topological Transformation of Stochastic Networks, Markov Processes, and Neural Networks. *Big Data Cogn. Comput.*, 7, 66. <https://doi.org/10.3390/bdcc7020066>
- Kravets, V., Kapitsa, M., Domanskyi, I., Kravets, V., Hryshechukina, T., & Zakurday, S. (2024). Devising an analytical method for solving the eighth-order Kolmogorov equations for an asymmetric Markov chain. *Eastern-European Journal of Enterprise Technologies*, 5(4(131)), 33–41. <https://doi.org/10.15587/1729-4061.2024.312971>
- Krichen, M., & Mihoub, A. (2025). Long Short-Term Memory networks: A comprehensive survey. *AI*, 6(9), 215. <https://doi.org/10.3390/ai6090215>



- Liu, X., Zhao, P., & Yang, K. (2023). Hybrid deep learning model for anomaly detection in SDN using CNN and attention mechanisms. *IEEE Transactions on Network and Service Management*, 20(2), 2331–2343. <https://doi.org/10.1109/TNSM.2023.3234456>
- Lu, W., Hsu, C., & Chang, Y. (2020). A matrix approach for analyzing signal flow graph. *Information*, 11(12), 562. <https://doi.org/10.3390/info11120562>
- Malik, A., & Singh, B. (2023). Application of Heaviside expansion method for solving fractional order differential equations in control systems. *Fractional Calculus and Applied Analysis*, 26(2), 541–562. <https://doi.org/10.1515/fca-2023-0034>
- Olah, Ch. (2015). Understanding LSTM Networks. <https://colah.github.io/posts/2015-08-Understanding-LSTMs/>
- Qin, Y., Li, H., & Zhang, D. (2023). Fault diagnosability evaluation method based on multi-signal flow graph and similarity measure. *Systems Engineering and Electronics*, 45(1), 302–312. <https://doi.org/10.12305/j.issn.1001-506X.2023.01.35>
- Robert, P. (2013). *Stochastic Networks and Queues*. Springer Science & Business Media.
- Sahu, R., Choudhury, S., & Misra, S. (2022). LSTM-based anomaly detection in software-defined networking environments. *IEEE Transactions on Network and Service Management*, 19(3), 2471–2484. <https://doi.org/10.1109/TNSM.2022.3158729>
- Scott-Hayward, S., O'Callaghan, G., & Sezer, S. (2013). SDN Security: A Survey. In *2013 IEEE SDN for Future Networks and Services (SDN4FNS)* (pp. 1–7). <https://doi.org/10.1109/SDN4FNS.2013.6702553>
- Silva, A., Smith, P., & Mauthe, A., & Schaeffer-Filho, A. (2015). Resilience support in software-defined networking: A survey. *Computer Networks*, 92, 189–207. <https://doi.org/10.1016/j.comnet.2015.09.012>
- Srikant, R., & Ying, L. (2014). *Communication Networks: An Optimization, Control, and Stochastic Networks Perspective*. Cambridge University Press.
- Sun, Y., Peng, M., Zhou, Y., Huang, Y., & Mao, S. (2019). Application of deep reinforcement learning in mobile networks: A survey. *IEEE Communications Surveys & Tutorials*, 21(4), 3133–3174. <https://doi.org/10.1109/COMST.2019.2924243>
- Wang, J., Li, Z., & Xu, T. (2022). Reinforcement learning-based adaptive traffic control in SDN. *Computer Communications*, 188, 125–135. <https://doi.org/10.1016/j.comcom.2022.02.012>

References

- Alharbi, A., Alsubhi, K., Alghamdi, A., & Alotaibi, F. (2023). Blockchain-based decentralized security framework for software-defined networks. *IEEE Access*, 11, 36540–36555. <https://doi.org/10.1109/ACCESS.2023.3258792>
- Amin, M. B. M., & Ahmad, S. S. (2022). Laplace Transform for Solving System of Integro-Fractional Differential Equations of Volterra Type with Variable Coefficients and Multi-Time Delay. *Symmetry*, 14(5), 984. <https://doi.org/10.3390/sym14050984>
- Chen, Y., Zhang, L., Wang, Y., & Xu, J. (2021). Deep neural network-based anomaly detection in software-defined networking. *Computer Networks*, 195, 108180. <https://doi.org/10.1016/j.comnet.2021.108180>
- Chhaytli, Y., & Persikov, A. (2021). Cyber-resilient routing mechanisms for SDN. *Journal of Network and Computer Applications*, 187, 103097. <https://doi.org/10.1016/j.jnca.2021.103097>
- Farooq, M., Riaz, Q., & Alvi, S. (2023). Security challenges and solutions in software-defined networking: A systematic review. *Journal of Information Security and Applications*, 74, 103453. <https://doi.org/10.1016/j.jisa.2023.103453>
- Hoang, T., Nguyen, H., & Pham, Q. (2024). LSTM-based predictive routing for adaptive resource allocation in SDN environments. *Future Generation Computer Systems*, 154, 328–340. <https://doi.org/10.1016/j.future.2023.10.026>
- Karakus, M., & Durrresi, A. (2017). Quality of Service (QoS) in Software Defined Networking (SDN): A survey. *Journal of Network and Computer Applications*, 80, 2017, 200–218. <https://doi.org/10.1016/j.jnca.2016.12.019>
- Kotenko, I., Saenko, I., Privalov, A., & Laut, O. (2023). Ensuring SDN Resilience under the Influence of Cyber Attacks: Combining Methods of Topological Transformation of Stochastic Networks, Markov Processes, and Neural Networks. *Big Data Cogn. Comput.*, 7, 66. <https://doi.org/10.3390/bdcc7020066>
- Kravchenko, Yu. V., & Fisun, O. S. (2025). Analysis of existing methods for ensuring functional resilience of complex systems for improving computer networks. *Communication*, 3, 29–35 [in Ukrainian]. <https://doi.org/10.31673/2412-9070.2025.025385>
- Kravets, V., Kapitsa, M., Domanskyi, I., Kravets, V., Hryshechukina, T., & Zakurday, S. (2024). Devising an analytical method for solving the eighth-order Kolmogorov equations for an asymmetric Markov chain. *Eastern-European Journal of Enterprise Technologies*, 5(4(131)), 33–41. <https://doi.org/10.15587/1729-4061.2024.312971>
- Krichen, M., & Mihoub, A. (2025). Long Short-Term Memory networks: A comprehensive survey. *AI*, 6(9), 215. <https://doi.org/10.3390/ai6090215>
- Liu, X., Zhao, P., & Yang, K. (2023). Hybrid deep learning model for anomaly detection in SDN using CNN and attention mechanisms. *IEEE Transactions on Network and Service Management*, 20(2), 2331–2343. <https://doi.org/10.1109/TNSM.2023.3234456>
- Lu, W., Hsu, C., & Chang, Y. (2020). A matrix approach for analyzing signal flow graph. *Information*, 11(12), 562. <https://doi.org/10.3390/info11120562>
- Malik, A., & Singh, B. (2023). Application of Heaviside expansion method for solving fractional order differential equations in control systems. *Fractional Calculus and Applied Analysis*, 26(2), 541–562. <https://doi.org/10.1515/fca-2023-0034>
- Olah, Ch. (2015). Understanding LSTM Networks. <https://colah.github.io/posts/2015-08-Understanding-LSTMs/>
- Qin, Y., Li, H., & Zhang, D. (2023). Fault diagnosability evaluation method based on multi-signal flow graph and similarity measure. *Systems Engineering and Electronics*, 45(1), 302–312. <https://doi.org/10.12305/j.issn.1001-506X.2023.01.35>
- Robert, P. (2013). *Stochastic Networks and Queues*. Springer Science & Business Media.
- Sahu, R., Choudhury, S., & Misra, S. (2022). LSTM-based anomaly detection in software-defined networking environments. *IEEE Transactions on Network and Service Management*, 19(3), 2471–2484. <https://doi.org/10.1109/TNSM.2022.3158729>
- Scott-Hayward, S., O'Callaghan, G., & Sezer, S. (2013). SDN Security: A Survey. In *2013 IEEE SDN for Future Networks and Services (SDN4FNS)* (pp. 1–7). <https://doi.org/10.1109/SDN4FNS.2013.6702553>
- Silva, A., Smith, P., & Mauthe, A., & Schaeffer-Filho, A. (2015). Resilience support in software-defined networking: A survey. *Computer Networks*, 92, 189–207. <https://doi.org/10.1016/j.comnet.2015.09.012>
- Srikant, R., & Ying, L. (2014). *Communication Networks: An Optimization, Control, and Stochastic Networks Perspective*. Cambridge University Press.
- Sun, Y., Peng, M., Zhou, Y., Huang, Y., & Mao, S. (2019). Application of deep reinforcement learning in mobile networks: A survey. *IEEE Communications Surveys & Tutorials*, 21(4), 3133–3174. <https://doi.org/10.1109/COMST.2019.2924243>
- Wang, J., Li, Z., & Xu, T. (2022). Reinforcement learning-based adaptive traffic control in SDN. *Computer Communications*, 188, 125–135. <https://doi.org/10.1016/j.comcom.2022.02.012>

Отримано редакцією журналу / Received: 05.11.25

Прорецензовано / Revised: 10.11.25

Схвалено до друку / Accepted: 19.12.25

Yurii KRAVCHENKO, DSc (Engin.), Prof.
ORCID ID: 0000-0002-0281-4396
e-mail: kr34@ukr.net
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Olena FISUN, PhD Student
ORCID ID: 0009-0009-6640-3818
e-mail: lenafi@ukr.net
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

METHOD FOR ENSURING FUNCTIONAL RESILIENCE OF SOFTWARE-DEFINED NETWORKS UNDER CYBERATTACK INFLUENCE

B a c k g r o u n d . In the context of the rapid development of network technologies, the Software-Defined Networking (SDN) architecture has become the basis for building flexible and manageable corporate networks. However, its centralized nature



creates potential vulnerabilities that can be used by attackers to destabilize network management. Ensuring functional stability of SDN under cyberattacks of varying intensity is a complex task, as it requires dynamic adaptation of control parameters to prevent the system from entering critical states.

M e t h o d s . *The paper proposes a method for maintaining functional stability of SDN based on a combination of stochastic modeling and recurrent neural networks of the LSTM (Long Short-Term Memory) type. The SDN model is formalized as a system with five possible states and a set of transition intensities between them. The LSTM module performs the function of an adaptive controller, which in the process of operation estimates the probabilities of the system being in different states and adjusts individual transition intensities in order to maintain the target level of functional stability. A combination of simulation and reinforcement approaches was used to train the LSTM, which allows taking into account both previously simulated attack scenarios and the current state of the network.*

R e s u l t s . *The developed method demonstrated its effectiveness in maintaining stable SDN operation by timely adjusting system parameters when the intensity of threats changes. Simulation modeling for three scenarios (low, medium, and high threat levels) showed that without parameter correction, stability is maintained only at a low level of attacks, while for medium and high levels, critical deviations are observed at certain points in time. The use of the LSTM controller made it possible to detect these moments in time and adaptively update the transition intensities, restoring network stability.*

C o n c l u s i o n s . *The proposed method for ensuring the functional stability of SDN based on LSTM allows creating an intelligent adaptive control system capable of maintaining network stability under the destabilizing effects of cyberattacks. The modeling results confirm the feasibility of using neural network mechanisms for predicting states and correcting SDN parameters in real time. In the future, it is planned to expand the model for multi-level SDN architectures and investigate the influence of spatial topology on the effectiveness of adaptive control.*

K e y w o r d s : *Software-Defined Network, functional stability, cyberattack, stochastic modeling, Recurrent Neural Network.*

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.