Груба В. В.,
курсантка 4-го курсу,
Харківський національний
університет внутрішніх справ
(м. Кам'янець-Подільський, Україна)

Калякін С. В.,
старший викладач кафедри протидії
кіберзлочинності,
Харківський національний
університет внутрішніх справ
(м. Кам'янець-Подільський, Україна)

ІННОВАЦІЙНИЙ МЕТОД FIREWALL PHASE-SHIFT OBFUSCATION (FPO) У СИСТЕМАХ МЕРЕЖЕВОГО ЗАХИСТУ

Міжмережеві екрани з моменту свого виникнення зазнали значної еволюції. Перші системи, створені наприкінці 1980-х – на початку 1990-х років, працювали на основі простих списків контролю доступу (ACL), які забезпечували фільтрацію трафіку за IP-адресами та портами . Ці механізми виявлялися дієвими лише у випадку однорідних мереж із низьким рівнем кіберзагроз, якими тоді характеризувалося мережеве середовище [2].

У 2000-х роках сталося впровадження станового (stateful) фільтрування, яке дозволило брандмауерам аналізувати контекст з'єднань та підтримувати таблиці станів [2]. Це суттєво ускладнило встановлення несанкціонованих з'єднань, однак проблема статичності політик залишилася невирішено.

Подальший розвиток мережевих технологій спричинив появу міжмережевих екранів нового покоління (Next Generation Firewalls або NGFW), що об'єднують функції фільтрації даних, глибинного аналізу пакетів (Deep Packet Inspection, DPI), системи виявлення та запобігання вторгненням (IDS/IPS), а також розширених аналітичних модулів [1]. Такі інтегровані рішення стали ключовими інструментами у протидії складним кіберзагрозам, особливо в контексті захисту військових та урядових інформаційних систем.

Однак, незважаючи на високий рівень технологічності, NGFW залишаються здебільшого реактивними системами, орієнтованими на ідентифікацію загроз і блокування атак після їх виявлення або на основі визначених сигнатур [2]. У контексті зростаючих викликів, пов'язаних із гібридними загрозами, така модель має суттєві обмеження. Зловмисники отримують можливість здійснювати розвідку, адаптуватися до поточного стану захисних механізмів і готувати атаку, спираючись на прогнозовані зміни конфігурацій системи.

Таким чином, статична архітектура стає передбачуваною й зменшує ефективність захисту. Для вирішення цієї проблеми запропоновано метод Firewall Phase-shift Obfuscation, що передбачає перехід від статичної моделі до

динамічної. У цій моделі конфігурація системи змінюється у часовому вимірі, що істотно підвищує її стійкість до адаптивних кібератак.

Забезпечення інформаційної та кібербезпеки набуває особливого значення в контексті формування ефективної системи державної безпеки, особливо в умовах триваючої збройної агресії проти України та ескалації глобальних гібридних загроз [4]. Сучасні воєнні конфлікти дедалі частіше переносяться у кіберпростір, де об'єктами атак стають елементи критичної інфраструктури держави, що піддаються технічно складним та масштабним кібернетичним атакам. Одним із фундаментальних засобів забезпечення захисту в умовах подібних загроз залишаються міжмережеві екрани (firewalls) — комплексні програмно-апаратні рішення, спрямовані на контроль і фільтрацію мережевого трафіку відповідно до встановлених політик безпеки [2].

Традиційні фаєрволи зазвичай базуються на статичних наборах правил, що досить ефективно запобігають стандартним мережевим вторгненням [1]. Однак вони виявляються значно менш дієвими проти динамічних та розподілених атак. Сучасні зловмисники активно використовують методи аналізу мереж, сканування портів, атаки типу SYN flood і евристичні алгоритми для обходу систем фільтрації. Такі підходи дозволяють швидко ідентифікувати відкриті сервіси, адаптуватися до політик захисту фаєрволів і знаходити слабко захищені сегменти мережевої інфраструктури [3]. Подібна діяльність становить серйозну загрозу для військових структур і державних установ, які залежать від власних комунікаційних мереж у зоні бойових дій або під час виконання заходів із забезпечення безпеки.

У сучасних умовах гібридної війни актуалізується необхідність розробки та впровадження динамічних і адаптивних методів забезпечення мережевої безпеки, спрямованих на ускладнення функціонування розвідувальних та атакувальних засобів противника [5]. У цьому аспекті пропонується метод Firewall Phase-shift Obfuscation (FPO), що представляє собою новаторський підхід до управління конфігураційними параметрами міжмережевого екрану. Основу методу становить принцип фазового зсуву конфігурацій у часових інтервалах, який покликаний забезпечити підвищену ефективність системи кіберзахисту за умов постійної змінюваності загроз.

Основний принцип методу полягає у регулярному оновленні ключових конфігураційних параметрів міжмережевого екрану згідно з наперед заданим фазовим розкладом. До таких характеристик можуть належати:

- набір відкритих портів;
- часові вікна доступу до окремих служб;
- сигнатури систем виявлення вторгнень;
- маршрути внутрішнього трафіку та правила NAT;
- налаштування журналювання та оповіщення.

Фазовий графік генерується за допомогою алгоритмічного підходу, використовуючи псевдовипадкові послідовності або криптографічні генератори [3]. Це забезпечує динамічну зміну мережевого середовища з плином часу, створюючи для потенційного зловмисника непередбачуваність щодо поточного

стану системи. Такий метод суттєво знижує шанси на успішне прогнозування мережевої поведінки, ускладнює сканування та підготовку до можливих атак.

Метод фазового зсуву в мережевій безпеці базується на принципах інформаційної асиметрії та стохастичних процесів. У класичних сценаріях атакувальник здатен детерміновано аналізувати функціонування мережевої системи, визначаючи її закономірності. Однак якщо параметри системи динамічно змінюються з часом, спостереження для зловмисника перетворюється на складний марковський стохастичний процес, де ймовірність переходу між станами залишається для нього невідомою. З точки зору системного аналізу, фазовий зсув призводить до зміни фаз у часопросторовому представленні системи, що змушує атакувальника і захисника діяти у відмінних інформаційних просторах. Завдяки цьому захисник отримує можливість контролювати моменти переходів системи між станами, тоді як атакувальник залишається без точних даних про теперішній чи майбутній стан системи [3].

У контексті гібридних загроз ця модель набуває особливої ваги, адже противники часто застосовують автоматизовані фреймворки для розвідки та атак, які орієнтовані на стабільність конфігурацій. Проте, якщо конфігурація динамічно змінюється, скрипти розвідки стають неактуальними ще до того, як завершується процес збору даних [1]. Додатково, фазовий зсув можна розглядати як практичну адаптацію принципу невизначеності у сфері кіберзахисту. Завдяки цьому підходу захисна система навмисно створює для зловмисника ситуацію інформаційного дисбалансу. Така стратегія не лише ускладнює планування атаки, але й значно збільшує її вартість, що забезпечує перевагу для безпекових структур і зміцнює їхню позицію в умовах сучасних викликів [1].

У міжнародній практиці концепція динамічної зміни конфігурацій отримала подальший розвиток у рамках підходу Moving Target Defense (MTD). Ця стратегія, яка активно розвивається в країнах НАТО та Європейського Союзу, спрямована на створення умов, за яких зловмисник змушений функціонувати в середовищі постійної невизначеності [3;4]. Водночас оборонна сторона бере під контроль і активно маніпулює поверхнею атаки, мінімізуючи ризики та підвищуючи ефективність захисту.

Метод FPO слід розглядати як один із прикладів впровадження концепції MTD у системах мережевого захисту. На відміну від складних комерційних рішень, цей підхід вирізняється гнучкістю та здатністю до адаптації під різні рівні мережевої інфраструктури, що робить його особливо актуальним для використання у військових структурах, правоохоронних органах і державних установах [3].

Метод Firewall Phase-shift Obfuscation є перспективним напрямом розвитку систем мережевого захисту в умовах гібридних загроз. Його впровадження дозволяє:

- зробити мережеве середовище динамічним та непередбачуваним;
- знизити ефективність технік розвідки та автоматизованих атак;
- підвищити рівень захищеності без значних фінансових витрат;

- інтегрувати сучасні концепції MTD у діяльність суб’єктів сектору безпеки.

Перспективні дослідження можуть бути зосереджені на розробці математичних моделей фазових діаграм, оптимізації параметрів часових інтервалів зсуву, а також створенні алгоритмів автоматизованого управління фазами на основі детального аналізу поведінкових характеристик мережевого трафіку. Зазначений підхід має потенціал суттєвого підвищення рівня кіберстійкості критично важливої інфраструктури, водночас сприяючи розвитку адаптивних систем державної безпеки.

Список використаних джерел:

1. Pfaff B., Pettit J., Koponen T., Jackson E., Zhou A., Rajahalme J. «The Design and Implementation of Open vSwitch» — Oakland, 2015. — P. 117–130.: https://www.usenix.org/system/files/conference/nsdi15/nsdi15-paper-pfaff.pdf (дата звернення: 08.10.2025).
2. Cisco. «Firewall Best Practices for Network Security» — Cisco Systems, 2023: https://sec.cloudapps.cisco.com/security/center/resources/firewall_best_practices (дата звернення: 10.10.2025).
3. Jajodia S., Ghosh A., Subrahmanian V., Swarup V., Wang C., Wang X. «Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats» — New York: Springer, 2011. — 332 p.: https://content.e-bookshelf.de/media/reading/L-3946645-db0f56e1f7.pdf (дата звернення: 08.10.2025).
4. National Institute of Standards and Technology (NIST). «Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1» — Gaithersburg, MD: NIST, 2018: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf (дата звернення: 09.10.2025).