UDC 004.056.53:510.644

Лахно Валерій Анатолійович
доктор технічних наук, професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки,
Національний університет біоресурсів і природокористування України
ORCID: http://orcid.org/0000-0001-9695-4543
E-mail: lva964@nubip.edu.ua

Касаткін Дмитро Юрійович
кандидат педагогічних наук, доцент, завідувач кафедри комп'ютерних систем, мереж та кібербезпеки,
Національний університет біоресурсів і природокористування України
ORCID: https://orcid.org/0000-0002-2642-8908
E-mail: d.kasatkin@nubip.edu.ua

НЕЧІТКО-ЛОГІЧНА МОДЕЛЬ ОЦІНЮВАННЯ СТАНУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІД ЧАС DDOS-АТАК

Аннотація. *Запропоновано нечітко-логічну модель оцінювання стану інформаційної системи (ІС) під час DDoS-атак. Модель базується на використанні системи лінгвістичних змінних, які описують критичні параметри мережевого трафіку та характеристик функціонування ІС. Для формування оцінки поточного ризику застосовано нечіткий висновок типу Мамдані з подальшою дефазифікацією методом центра ваги. Проведено імітаційний експеримент, який реалізовано у середовищі Python із використанням бібліотеки scikit-fuzzy. Отримані результати підтвердили, що запропонована модель адекватно відображає залежність інтегрального ризику від зміни параметрів навантаження, забезпечує безперервність оцінювання та чутливість до критичних комбінацій факторів трафіку. Отримані результати дають підставу розглядати розроблену модель як базис синтезу модуля моніторингу стану ІС.*

Ключові слова: *DDoS-атака, нечітка логіка, модель ризику, інформаційна система, нечіткий висновок Мамдані, оцінювання стану, моніторинг безпеки*.

Вступ. Під час функціонування корпоративних інформаційних систем (ІС) з високим рівнем інтеграції та навантаженням виникає потреба у безперервному контролі їхнього технічного та інформаційного стану. Також виникає завдання виявлення і оцінювання наслідків DDoS-атак, коли потік запитів формується з великої кількості джерел, а класичні сигнатурні та порогові методи не дають можливостей своєчасно розпізнати перехід системи до критичного стану [1, 2]. У подібних умовах стандартні метрики продуктивності або ізольовані показники безпеки не відображають реального ступеня деградації системи, оскільки мають нечіткі границі між нормальними та атиповими режимами. Практичний досвід експлуатації мережевої інфраструктури показав, що поведінка ІС під навантаженням DDoS-типу описується не лише кількісними параметрами трафіку. Її також описують якісними співвідношеннями між показниками, а саме інтенсивністю запитів, пропускною здатністю каналів, часткою втрат пакетів, затримками обробки транзакцій тощо [3, 4]. Зміна навіть одного з цих факторів може не мати суттєвого впливу на ІС. Проте їх комбінація створить ситуацію, коли система втратить стійкість до подальшого навантаження. Подібні залежності складно формалізувати аналітично. Але вони піддаються опису засобами нечіткої логіки [5]. Використання нечітко-логічного підходу для оцінювання стану ІС під час DDoS-атак дасть змогу інтегрувати різнорідні параметри у єдину узагальнену оцінку ризику. На відміну від детермінованих методів, нечітка модель дозволить врахувати неповноту та неточність вхідних даних, а також суб'єктивні експертні знання, отримані з практики адміністрування систем захисту.

Саме тому, у даній роботі запропоновано нечітко-логічну модель оцінювання стану інформаційної системи під час DDoS-атак. Модель базується на сукупності лінгвістичних

DOI: 10.31548/itees.2025.02.056
ISSN 3083-7502

змінних, що відображають параметри мережевого трафіку та внутрішніх процесів обробки даних. Результатом є інтегрована оцінка ризику порушення працездатності ІС.

Постановка проблеми. Інформаційні системи (ІС) постійно стикаються із ситуацію, коли мережеві потоки та інтенсивність запитів постійно змінюється. А під час DDoS-атак ІС опиняються в умовах перевантаження. Проблема полягає у відсутності інтегрованих моделей, здатних оцінювати поточний стан ІС за множиною взаємопов'язаних параметрів трафіку та внутрішніх характеристик системи з урахуванням нечітких меж між нормальним і критичним станом ІС. Отже виникає потреба синтезу моделі оцінювання поточного стану ІС на основі системи нечітких правил.

Аналіз актуальних досліджень. Аналіз наукових джерел засвідчив зростання інтересу до використання методів нечіткої логіки для виявлення та нейтралізації DDoS-атак. Зокрема у статтях [1, 2] систематизовано методи виявлення DDoS-атак у високошвидкісних мережах. Автори наголосили, що сигнатурні та статистичні підходи поступаються за ефективністю інтелектуальним методам аналізу, зокрема заснованим на нечітких моделях прийняття рішень.

Перші практичні підходи до застосування нечіткої логіки у задачі виявлення DDoS-атак розглянуто у дослідженні Shiaeles S. N. та ін. [3]. Автори реалізували систему на основі нечітких оцінювачів трафіку й довели придатність нечітких правил для ідентифікації відхилень у мережевих потоках. Подальший розвиток цього напряму представлено у роботі [4]. Автори розробили метод виявлення та відновлення роботи бездротових сенсорних мереж із використанням нечітких параметрів, які характеризували інтенсивність DDoS атак.

Вагомий внесок у систематизацію методів нечіткої логіки при виявленні DDoS атак зробили Javaheri D. зі співавторами у [5]. В цих роботах автори виконали порівняльний аналіз сучасних моделей виявлення аномалій трафіку та класифікацію підходів на основі типу нечіткого висновку. Автори підкреслили, що, нечіткі системи демонстрували під час досліджень стійкість до змін характеристик мережевого середовища та забезпечували гнучке налаштування параметрів оцінювання працездатності мережі. У [6] Almseidin M. та інші співавтори колеги запропонували нечітку систему висновку для виявлення DDoS-атак. Система базувалася на інтеграції вхідних метрик трафіку, а отримані результати підтвердили ефективність нечіткого висновку для підвищення точності детекції при низькому рівні хибнопозитивних спрацьовувань системи нечіткого висновку.

У [7] Petkovic M. та інші співавтори досліджували ефективність нечіткого методу Такеґі–Суґено–Канґ (TSK) у поєднанні з моделлю оцінювання ентропії трафіку. Автори довели, що запропонований у статті метод забезпечив високу чутливість до низько інтенсивних DDoS атак порівняно з традиційними статистичними методами.

Lin H., Wu C., та Masdari M. у [8] узагальнили релевантні схеми виявлення аномалій. Автори наголосили на доцільності застосування гібридних методів виявлення DDoS атак. Зокрема методів та моделей, у яких нечітка логіка поєднувалася з машинним навчанням для зменшення похибки класифікації.

Інтеграційні рішення для виявлення DDoS атак розглянуті у роботах [9, 10]. У статтях автори використовували апарат нечіткої логіки як керуючий модуль для системи класифікаторів у середовищі Apache Spark. Додатково у [9] Almotiri S. H. представив нечітку модель кількісного оцінювання стійкості мережі до DDoS-атак на основі методу TOPSIS.

Загалом проведений аналіз засвідчує, що використання нечіткої логіки у завданнях виявлення та оцінювання стану інформаційних систем під час DDoS-атак забезпечує підвищення точності та стійкості механізмів захисту. Проте, більшість проаналізованих досліджень зосереджена на задачах детекції, тоді як питання формалізації нечітко-логічних моделей оцінювання поточного стану інформаційних систем під час DDoS атак залишилися недостатньо розробленими, що визначило актуальність подальших досліджень у цьому напрямі.

Метою статті є розробка та апробація нечітко-логічної моделі оцінювання стану ІС під час DDoS-атак, яка забезпечує інтегроване відображення впливу основних параметрів мережевого трафіку та характеристик продуктивності системи на її поточний рівень ризику.

Матеріали і методи дослідження. Метою побудови моделі є формування інтегрованої оцінки поточного стану ІС під час дії DDoS-атак з урахуванням параметрів трафіку, характеристик мережевого середовища та показників деградації продуктивності. Для цього запропоновано використати нечітко-логічний підхід, який дозволить формалізувати експертні знання про залежності між множиною факторів та якісною оцінкою стану ІС.

Як вхідні дані моделі використовуємо часткові параметри стану ІС, які характеризують потік запитів, поведінку мережевих протоколів, пропускну здатність каналів ІС, затримки обробки та інші індикатори, які реагують на DDoS-навантаження. Для кожного параметра визначено універсум значень та відповідні лінгвістичні терми, наведені у табл. 1.

Таблиця 1 – База нечітких правил типу Мамдані для оцінювання поточного стану ІС під час дії DDoS-атак з урахуванням параметрів трафіку

Позначення	**Опис параметра**	**Універсум**	**Лінгвістичні терми**
y_1	Показник поточних ризиків	[0,1]	некритична (нкр), критична (кр)
y_2	Прийнятний рівень інформаційного ризику	[0,1]	прийнятний (пр), неприйнятний (нп)
y_3	Інтенсивність потоку кадрів (запитів)	[10,6000] кадр/с	немає (н), незначна (нк), середня (ск), велика (вк)
y_4	Пропускна спроможність каналу	[10,100] Мбіт/с	низька (нпс), середня (спс), висока (впс)
y_5	Кількість спроб доступу до середовища	[0,1]	зафіксовані (зф), незафіксовані (нф)
y_6	Час очікування обслуговування транзакції	[0.001, 0.01] с	неприйнятний (нп), середній (ср), нормальний (н)
y_7	Довжина IP-пакету	[1,65529] байт	низька (н), нижче критичної (нкр), критична (кр), вище критичної (вкр)
y_8	Кількість великих IP-пакетів (Ping of Death)	[0,1]	мала (м), середня (с), велика (в)
y_9	Кількість HTTP-запитів	[0,1]	мала (м), середня (с), велика (в)
y_{10}	Частка TCP-пакетів	[0,1]	мала (м), середня (с), велика (в)
y_{11}	Частка UDP-пакетів	[0,1]	мала (м), середня (с), велика (в)
y_{12}	Частка ICMP-пакетів	[0,1]	мала (м), середня (с), велика (в)
y_{13}	Ознаки SQL-ін’єкції	[0,1]	виявлені (в), частково невиявлені (чв), невиявлені (нв)
y_{14}	Міжкадровий інтервал	[10,100] біт	малий (м), середній (с), великий (в)

Для кожного терма T_i визначаємо функцію належності $\mu_{T_i}(y_i)$, яка відображатиме ступінь, з яким значення параметра (y_i) відповідатиме відповідному лінгвістичному опису. Як

DOI: 10.31548/itees.2025.02.056
ISSN 3083-7502

базові типи функцій належності використовуємо трикутні та трапецієподібні функції, що забезпечать інтерпретованість та простоту обчислень.

Нечітко-логічна модель сформує оцінку (Y^*) поточного стану ІС на основі системи правил виду:

$$R_k\text{: } якщо\ y_3\ є \text{ велика } та\ y_6\ є \text{ неприйнятний, } то\ Y^*\ є \text{ критичний.}$$

Загальну систему нечітких рівнянь, що відповідають дереву висновку, подамо у вигляді:

$$\mu_{Y^*}(x) = \max_k \min_i \mu_{T_i}(y_i),$$

де $\mu_{T_i}(y_i)$ – функції належності вхідних змінних до відповідних термів;

операції $\left(\max_k\right)$ та $\left(\min_i\right)$ відповідають логічним операціям **АБО** та **І** у системі нечіткого висновку типу Мамдані [11].

У процесі дефазифікації для отримання числової оцінки рівня ризику застосовувався метод центра ваги [8]:

$$Y^* = \frac{\int x \cdot \mu_{Y^*}(x)dx}{\int \mu_{Y^*}(x)dx}.$$

Результат (Y^*) інтерпретуємо як ступінь критичності стану ІС у діапазоні [0,1]. Значення, близькі до 0, відповідають нормальному режиму. Значення, близькі до 1, відповідно, критичному стану внаслідок DDoS-навантаження.

Базу правил сформовано експертним шляхом на основі практичних спостережень поведінки ІС під час атак. Типові приклади правил:

- якщо інтенсивність запитів велика і час обслуговування неприйнятний – то стан системи критичний;
- якщо пропускна спроможність висока і інтенсивність кадрів середня – то стан системи нормальний;
- якщо кількість ICMP-пакетів велика і міжкадровий інтервал малий – то система перебуває у потенційно небезпечному стані.

Отже, модель надала змогу об’єднати різнорідні показники в єдину метрику ризику, яка характеризувала реальний стан ІС у момент часу (t).

Результати дослідження та їх обговорення. Для оцінювання працездатності запропонованої нечітко-логічної моделі проведено імітаційний експеримент (рис. 1 і рис. 2), спрямований на дослідження поведінки оцінки стану ІС під час зміни основних параметрів DDoS-навантаження. Експеримент реалізовано у середовищі Python (Google Colab) з використанням бібліотеки scikit-fuzzy, яка забезпечила реалізацію бази правил типу Мамдані та процедуру дефазифікації методом центру ваги.

У моделі використовувались дві вхідні змінні – інтенсивність запитів (y_3) та затримка обслуговування транзакцій (y_6), а також одна вихідна змінна – інтегральний рівень ризику (Y^*), який відображав узагальнений стан ІС у діапазоні [0,1]. Вибір саме цих параметрів зумовлений тим, що в реальних умовах саме вони мають найбільший вплив на деградацію продуктивності ІС.

Для кожної змінної побудовано набір функцій належності трикутного або трапецієподібного типу. Це забезпечило просту інтерпретацію експертних знань. Зокрема, інтенсивність трафіку описано трьома термами – «низька», «середня» і «висока»; затримка – «нормальна», «середня», «критична»; рівень ризику – «нормальний», «підвищений», «критичний». Базу правил сформовано таким чином, щоб відобразити типові залежності між параметрами мережевого навантаження та станом системи.

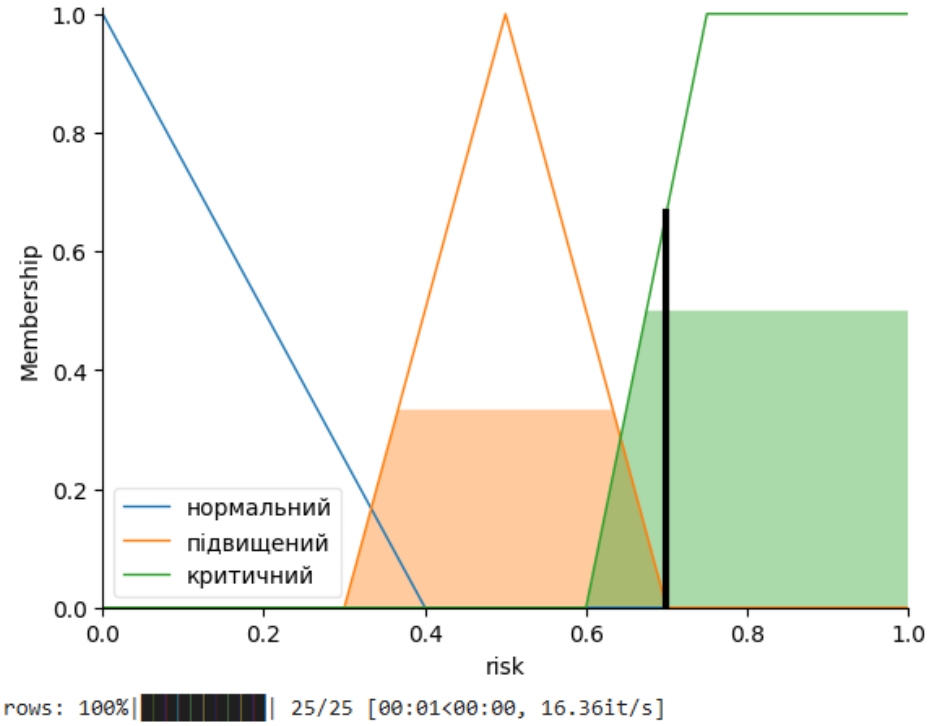

Рисунок 1 – Оцінка стану ризику

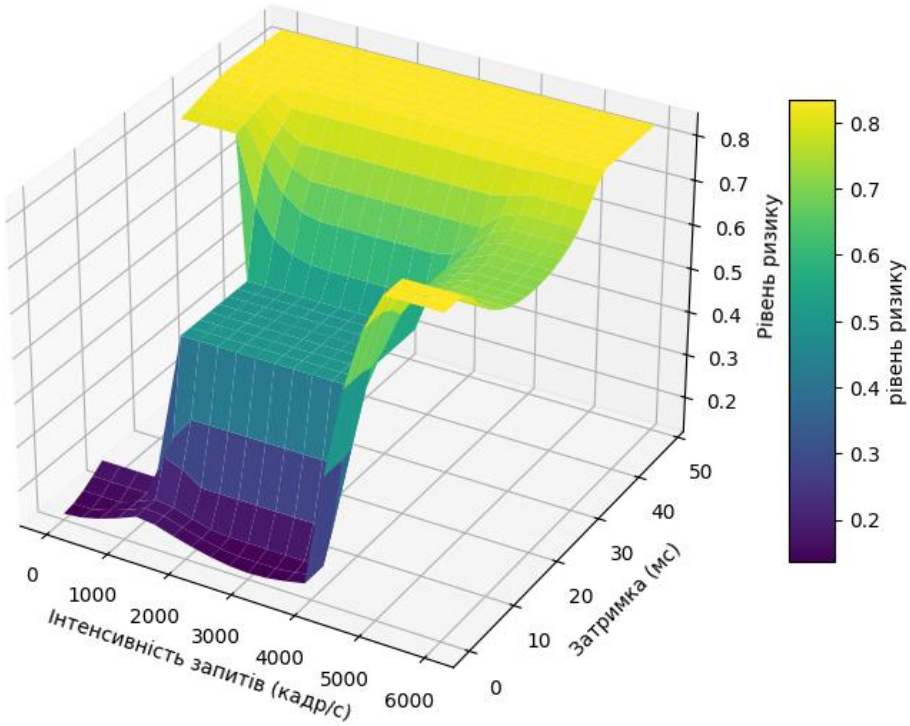

Рисунок 2 – Оцінка стану ризику у вигляді поверхні

Під час моделювання проведено дискретне сканування простору вхідних параметрів у діапазонах [0, 6000] кадр/с для трафіку та [0, 50] мс для затримки. Для кожної комбінації значень обчислювалась відповідна величина ризику (Y^*). Отримані результати подано у вигляді поверхні нечіткого висновку, яка характеризує залежність рівня ризику від обох вхідних параметрів. Аналіз поверхні показав, що модель демонструє плавну зміну

DOI: 10.31548/itees.2025.02.056
ISSN 3083-7502

інтегральної оцінки при зростанні навантаження та затримки, без різких стрибків, що свідчить про коректну роботу процедури нечіткого висновку.

Типова точка експерименту, що відповідає інтенсивності запитів 4200 кадр/с і затримці 30 мс, дала значення інтегрального ризику ($Y^* = 0{,}76$). Це відповідало критичному стану системи, коли ресурси серверів близькі до вичерпання, а затримка обробки транзакцій перевищує прийнятні межі. У діапазоні середніх навантажень (2000–3000 кадр/с) ризик залишається у межах 0,4–0,55. При низьких інтенсивностях і коротких затримках (до 1000 кадр/с, <10 мс) оцінка ризику стабільно не перевищує 0,2. А отже ІС система функціонує у нормальному режимі. Результати імітаційного експерименту підтверджують, що запропонована нечітко-логічна модель адекватно відображає залежність інтегрального ризику від мережевих параметрів, забезпечує безперервність оцінювання та стійкість до варіацій вхідних даних. Це дозволяє розглядати її як основу для побудови модуля моніторингу стану ІС у режимі реального часу.

Вважаємо, що подальші дослідження доцільно спрямувати на розширення бази правил з урахуванням характеристик різних типів атак (UDP flood, HTTP flood, ICMP flood), а також на інтеграцію нечітко-логічного ядра з алгоритмами машинного навчання для автоматичного коригування функцій належності залежно від поточних даних моніторингу ІС.

Висновки. Запропоновано нечітко-логічну модель оцінювання стану інформаційної системи під час DDoS-атак, що дозволило формалізувати залежність між параметрами мережевого трафіку, затримками обслуговування транзакцій та інтегральним рівнем ризику. Основні результати дослідження можна узагальнити так. Розроблено систему лінгвістичних змінних, що описують критичні характеристики ІС під час DDoS-навантаження, зокрема інтенсивність запитів, пропускну здатність каналів, затримку обслуговування, частку протокольних пакетів та інші індикатори аномалій. Сформовано базу нечітких правил типу Мамдані, що відображає експертні знання про вплив комбінацій параметрів на стан ІС. Проведено імітаційний експеримент, який підтвердив адекватність запропонованої моделі. Продемонстровано плавний характер зміни інтегрального ризику залежно від інтенсивності навантаження та затримки обробки, без різких стрибків і розривів у результатах. Встановлено критичні області функціонування ІС, у яких поєднання високої інтенсивності запитів і збільшення затримки призводило до переходу системи у нестійкий стан. Отримані значення ризику добре узгоджуються з реальною поведінкою корпоративних ІС під час DDoS-інцидентів. Практична значущість моделі полягає у потенціалі її інтеграції до систем моніторингу безпеки як модуля оцінювання стану ІС у реальному часі.

Список використаних джерел

1. Savchenko, V., Ponochovnyi, P., & Averichev, I. (2024). Vyiavlennia DDoS-ataky na vysokoshvydkisnu merezhu: Opytuvannia [Detection of a DDoS attack on a high-speed network: A survey]. Prykladni Problemy Kompiuternykh Nauk, Bezpeky ta Matematyky [Applied Problems of Computer Science, Security and Mathematics], 3, 71–81.
2. Shevchenko, S., Zhdanova, Yu., Skladannyi, P., & Petrenko, T. (2024). Nechitki kohnityvni karty yak instrument vizualizatsii stsenariiv reahuvannia na intsydenty v systemakh bezpeky [Fuzzy cognitive maps as a tool for visualizing incident response scenarios in security systems]. Kiberbezpeka: Osvita, Nauka, Tekhnika [Cybersecurity: Education, Science, Technique], 2(26), 417–429. https://doi.org/10.28925/2663-4023.2024.26.707.
3. Shiaeles, S. N., Katos, V., Karakos, A. S., & Papadopoulos, B. K. (2012). Real time DDoS detection using fuzzy estimators. Computers & Security, 31(6), 782–790. https://doi.org/10.1016/j.cose.2012.06.002.
4. Pajila, P. B., Julie, E. G., & Robinson, Y. H. (2022). FBDR-fuzzy based DDoS attack detection and recovery mechanism for wireless sensor networks. Wireless Personal Communications, 122(4), 3053–3083. https://doi.org/10.21203/rs.3.rs-217674/v1.

5. Javaheri, D., Gorgin, S., Lee, J. A., & Masdari, M. (2023). Fuzzy logic-based DDoS attacks and network traffic anomaly detection methods: Classification, overview, and future perspectives. Information Sciences, 626, 315–338. https://doi.org/10.1016/j.ins.2023.01.067.
6. Almseidin, M., Al-Sawwa, J., Alkasassbeh, M., & Alweshah, M. (2023). On detecting distributed denial of service attacks using fuzzy inference system. Cluster Computing, 26(2), 1337–1351. https://doi.org/10.1007/s10586-022-03657-5.
7. Petković, M., Bašičević, I., Kukolj, D., & Popović, M. (2018). Evaluation of Takagi-Sugeno-Kang fuzzy method in entropy-based detection of DDoS attacks. Computer Science and Information Systems, 15(1), 139–162. https://doi.org/10.2298/CSIS160905039P.
8. Lin, H., Wu, C., & Masdari, M. (2022). A comprehensive survey of network traffic anomalies and DDoS attacks detection schemes using fuzzy techniques. Computers and Electrical Engineering, 104, 108466. https://doi.org/10.1016/j.compeleceng.2022.108466.
9. Almotiri, S. H. (2024). Improving network resilience against DDoS attacks: A fuzzy TOPSIS-based quantitative assessment approach. Heliyon, 10(22), Article e40018. https://doi.org/10.1016/j.heliyon.2024.e40413.
10. Alsirhani, A., Sampalli, S., & Bodorik, P. (2019). DDoS detection system: Using a set of classification algorithms controlled by fuzzy logic system in Apache Spark. IEEE Transactions on Network and Service Management, 16(3), 936–949. https://doi.org/10.1109/TNSM.2019.2929425.
11. Imamguluyev, R. (2025). Detection and prevention of cyber attacks based on fuzzy logic and deep learning. In International Conference on Intelligent and Fuzzy Systems (pp. 402–409). Springer. https://doi.org/10.1007/978-3-031-97992-7_45.

Lakhno Valerii
Doctor of Technical Sciences, Professor, Professor of the Department of Computer Systems, Networks and Cybersecurity,
National University of Life and Environmental Sciences of Ukraine
ORCID: http://orcid.org/0000-0001-9695-4543
E-mail: lva964@nubip.edu.ua

Kasatkin Dmytro
PhD of Pedagogical Sciences, Associate Professor, Head of the Department of Computer Systems, Networks and Cybersecurity,
National University of Life and Environmental Sciences of Ukraine
ORCID: https://orcid.org/0000-0002-2642-8908
E-mail: d.kasatkin@nubip.edu.ua

A FUZZY-LOGICAL MODEL FOR ASSESSING THE STATUS OF AN INFORMATION SYSTEM DURING DDOS ATTACKS

Abstract. *A fuzzy-logical model for assessing the state of an information system (IS) during DDoS attacks is proposed. The model is based on the use of a system of linguistic variables that describe critical parameters of network traffic and the operational characteristics of the IS. To form an assessment of the current risk, Mamdani-type fuzzy inference was applied, followed by defuzzification using the centre-of-gravity method. A simulation experiment was conducted, implemented in the Python environment using the scikit-fuzzy library. The results obtained confirmed that the proposed model adequately reflects the dependence of the integral risk on changes in load parameters, ensures continuity of assessment and sensitivity to critical combinations of traffic factors. The results obtained provide grounds for considering the developed model as a basis for the synthesis of an IS status monitoring module.*

Keyword*: DDos Attack, Fuzzy Logic, Risk Model, Information System, Mamdani Fuzzy Inference, State Assessment, Security Monitoring.*