МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ УНІВЕРСИТЕТ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

МАТЕРІАЛИ КОНФЕРЕНЦІЇ
(зимовий форум)

Одеса, Україна, 14 листопада 2025 р.

Одеса
2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
INTERNATIONAL UNIVERSITY

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2025)

Odesa, Ukraine, November 14, 2025

Conference Proceedings
(winter forum)

Odesa
2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ УНІВЕРСИТЕТ

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ПТІКІ'2025)

Одеса, Україна, 14 листопада 2025 р.

Матеріали конференції
(зимовий форум)

Одеса
2025

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2025): Conference Proceedings (winter forum). Odesa : International university, 2025, 101 p.

DOI:

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2025): Матеріали конференції (зимовий форум). Одеса : Міжнародний університет, 2025, 101 с.

Збірка містить праці Міжнародної конференції з інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова

КІВАЛОВ С.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.

Співголови

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

Члени організаційного комітету

БЕРКМАН Л.Н. – д.т.н., проф., Державний університет телекомунікацій, м.Київ, Україна.
КЛИМАШ М.М. – д.т.н., проф., Національний університет «Львівська політехніка», м.Львів, Україна.
ЛЕМЕШКО А. В. – д.т.н., проф., Харківський національний університет радіоелектроніки, м. Харків, Україна.
РОЗЕНВАССЕР Д.М. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.
РИХЛІК А. – к.т.н., Лодзький технічний університет, м.Лодзь, Польща
СЕМЕНКО А.І. – д.т.н., проф ., Національний авіаційний університет, Київ, Україна.
СІМЕНС Е. – д.т.н., проф., Анхальтський університет прикладних наук, м.Кетен, Німеччина.
СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.
СУНДУЧКОВ К.С. – д.т.н., проф., Національний авіаційний університет, м. Київ, Україна.

РЕДАКЦІЙНИЙ КОМІТЕТ

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.
РОЗЕНВАССЕР Д.М. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

КОМІТЕТ МІЖНАРОДНИХ ЗВ’ЯЗКІВ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
ГЛОБА Л. С . – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ВЧЕНИЙ СЕКРЕТАР

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.
ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

ТЕХНІЧНО-ПРОГРАМНИЙ КОМІТЕТ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.
ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

СЕКЦІЇ

СЕКЦІЯ 1. ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.
ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

СЕКЦІЯ 2. КОМП'ЮТЕРНІ НАУКИ ТА КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

МІРОШНИК М.А. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.
РУСУ О.П. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

СЕКЦІЯ 3. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

ЛУНТОВСЬКИЙ А.О. – д.т.н., проф., Державна академія Саксонії «Беруфсакадемія», м. Дрезден, Німеччина.
ЙОНА Л.Г. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
МАНЬКО Д.Г. – д.ю.н., проф., Міжнародний університет, м.Одеса, Україна.

СЕКЦІЯ 4. ЕЛЕКТРОННІ КОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.
ЛЕМЕШКО А.В. – д.т.н., проф., Харківський національний університет радіоелектроніки, м. Харків, Україна.
ПЕДЯШ В.В. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

СЕКЦІЯ 5. ІНФОРМАТИКА ТА ПРОГРАМУВАННЯ В ОСВІТІ

КУЧАЙ О.В. - д.п.н., проф., Національний університет біоресурсів і природокористування України.
ЖИГУЛІН О.А. – д.е.н., проф., Міжнародний університет, Одеса, Україна
ГОРБАЧОВ В.Е. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

ЗМІСТ

СЕКЦІЯ 1. ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Русу О.П., Цуркан Л.Л. Програмне забезпечення для розрахунку перетворювачів напруги комп'ютерного обладнання 10

Жигулін О.А., Шестаков М.М. Інформаційні технології у забезпеченні сталого розвитку бізнесу 12

Азовський А.І. Педяш В.В. Програмна реалізація нейромережевих моделей для автоматизованого аналізу текстових даних 14

СЕКЦІЯ 2. КОМП'ЮТЕРНІ НАУКИ ТА КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Стрелковська І.В., Салоїд В.О. Сплайн-апроксимація розпізнавання жестів рук на базі OpenCV 18

Стрелковська І.В., Стоянов І.А. Дослідження мережевого трафіку хмарних сервісів та CDN-платформ 22

Баранюк Е.О. Розробка ігрового застосунку в жанрі city builder 27

Беседа О.Д. Розробка інтелектуальної мобільної платформи з функцією відстеження об'єктів 28

Дудко І.А. Дослідження системи розпізнавання жестів з використанням Mobilenet для задач комп'ютерного зору 30

Нікольський В.В., Лорткіпанідзе Р. Розподілена система моніторингу навколишнього середовища на базі LoRaWAN 34

Колесник О.В. Розробка інтелектуальної системи детекції зображень 37

Крупецький К.А., Русу О.П. Цифрове керування імпульсними перетворювачами напруги в комп'ютерному обладнанні 39

Горбачов В.Е., Яровий Д.О. Дослідження параметрів датчиків температури у цифрових сенсорних мережах 42

СЕКЦІЯ 3. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

Перчеклій Д.В. Дослідження інтеграції технології блокчейн у платіжні системи 45

Петков Є.І. Принципи роботи DoS, DDoS атак та засоби захисту проти них 48

Бєліков Д.В. Дослідження методів захисту від соціально-інженерних загроз 51

Чебанюк О.Д., Динін Б.І. Розробка та реалізація високопродуктивної системи для агрегації та аналізу метрик криптовалютних ринків у реальному часі 53

Тімофєєв О.О. Формальні методи аналізу вразливостей систем електронного документообігу 56

Головатюк К.В., Григор'єва Т.І. Оптимізація процесів інформаційних технологій при атаках фішингу із застосуванням нечіткої логіки 60

Проценко М.М. Порівняльне дослідження методів тестування безпеки LLM-коду: SAST, DAST, graph-based та синтез гібридного підходу 63

Лавров А.В. Стан та перспективи розвитку електронних платежів в Україні 66

Onatskyi Oleksii, Zharova Oksana. Comparative analysis of homomorphic properties of asymmetric cryptosystems RSA and Paillier 68

Петков Євген Ігорович.
Аспірант, спеціальність 125 Кібербезпека та захист інформації,
Міжнародний університет
yepetkov@gmail.com
Науковий керівник
Йона Лариса Григорівна, к.т.н.,
Завідувач, доцент кафедри комп'ютерної інженерії та інноваційних технологій
Факультету кібербезпеки, програмної інженерії та комп'ютерних наук
Міжнародного університету
yonalarisa66@gmail.com

ПРИНЦИПИ РОБОТИ DOS, DDOS АТАК ТА ЗАСОБИ ЗАХИСТУ ПРОТИ НИХ

Анотація. *Дослідження розглядає загальні принципи роботи DoS, DDoS атак, методи виявлення та засоби захисту проти них.*

У сучасному цифровому середовищі захист інформаційних систем є ключовим елементом роботи будь-якої організації. Серед найпоширеніших і найсерйозніших загроз для стабільності серверів та мереж виділяються DoS (Denial of Service) та DDoS (Distributed Denial of Service) атаки. Їхня основна мета — вивести ресурс із строю, зробити його недоступним для користувачів, завдати фінансових втрат або пошкодити репутацію компанії.

DoS-атаки (Denial of Service) базуються на принципі перевантаження ресурсів цільової системи, що призводить до її недоступності для легітимних користувачів. Атакуючий генерує величезну кількість запитів або трафіку, спрямованого на сервер, мережевий пристрій чи додаток, перевищуючи їхню пропускну здатність або обчислювальні можливості. Це може бути досягнуто шляхом надсилання пакетів SYN без завершення TCP-з'єднання (SYN-флуд), надмірного використання протоколів ICMP (наприклад, ping-флуд), або експлуатації вразливостей у програмному забезпеченні. Внаслідок цього сервер витрачає всі доступні ресурси на обробку шкідливого трафіку, не залишаючи можливостей для обслуговування реальних запитів, що й забезпечує відмову в обслуговуванні. Приклад DoS-атаки зображено на рис.1.

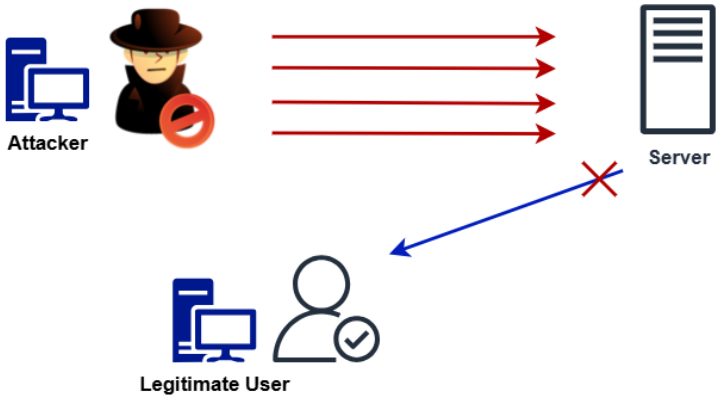

Рисунок 1 – Принцип роботи DoS-атаки

DDoS-атаки (Distributed Denial of Service) базуються на принципі розподіленого перевантаження ресурсів цільової системи за рахунок великої кількості заражених пристроїв, об'єднаних у ботнет. Зловмисник, або так званий ботмайстер, інфікує тисячі чи навіть мільйони комп'ютерів, смартфонів та IoT-пристроїв шкідливим програмним забезпеченням, після чого Сервер Керування (Command and Control Server) одночасно активує їх для створення потужного потоку трафіку на адресу жертви. Такий трафік може бути об'ємним (наприклад, UDP-flood або DNS-ампліфікація), спрямованим на рівень додатків (HTTP-flood із GET чи POST-запитами) або поєднувати кілька методів одночасно. Завдяки розподіленій природі атаки обсяг шкідливих запитів значно перевищує можливості звичайної DoS-атаки, що ускладнює їхнє фільтрування й блокування, часто призводячи до повної недоступності сервера або мережі для справжніх користувачів.

Для виявлення DoS та DDoS-атак, можуть використовуватись методи:

- Моніторинг трафіку. Постійне відстеження в реальному часі обсягу запитів і трафіку в мережі, або на серверне обладнання. Атака виявляється при аномальному сплеску (наприклад, зростання трафіку на 300% від базового рівня). Використовуються такі протоколи як NetFlow/ sFlow (аналіз потоків пакетів) та SNMP (моніторинг стану пристроїв), разом із системами моніторингу.
- Аналіз логів подій. Перегляд серверних і мережевих логів на наявність підозрілих IP-адрес, геолокацій або повторюваних шаблонів (наприклад, масові запити з однієї підмережі). Використовуються SIEM-системи (Splunk, ELK), які збирають, корелюють і аналізують логи з різних джерел.
- Сигнатурний аналіз. Порівняння вхідного трафіку з базою відомих сигнатур атак (наприклад, SYN-флуд, HTTP-флуд). Ефективний проти типових, раніше зафіксованих векторів атак. Тут можуть використовуватись IDS/IPS (Intrusion Detection System, Intrusion Prevention System - системи виявлення та запобігання вторгнень), які аналізують трафік у реальному часі, виявляють аномалії (наприклад, надмірну кількість півз'єднань) і можуть автоматично блокувати шкідливі джерела або обмежувати трафік.

Засоби захисту від DoS/DDoS-атак вимагають багатошарового підходу, що охоплює різні рівні та ділянки IT-інфраструктури. На мережевому рівні розгортаються апаратні та програмні фаєрволи (як NGFW – Next Generation Filrewalls), разом із системами виявлення та запобігання вторгнень (IDS/IPS), які аналізують сигнатури атак і блокують аномальний трафік; балансувальники навантаження (наприклад, F5 Big-IP, NGINX, HAProxy) розподіляють запити між серверами та автоматично відсікають підозрілі джерела. На рівні транспортної мережі провайдера ефективні техніки BGP FlowSpec, а також blackhole routing для перенаправлення шкідливого трафіку в «чорну діру». Хмарні рішення (Cloudflare, Akamai, AWS Shield Advanced, Azure DDoS Protection) забезпечують глобальну мережу розподілення трафіка (CDN - Content Delivery Network), а також хмарні Анти-DDoS сервіси, де трафік очищається від атак до надходження на кінцевий сервер замовника; вони здатні витримувати атаки об'ємом у сотні Gbps/Tbps. На рівні додатків може застосовуватись WAF (Web Application Firewall), який фільтрує HTTP/HTTPS-запити, блокуючи шкідливі та надмірні запити; функції rate limiting та throttling обмежують кількість запитів з однієї IP (наприклад, не більше 100 запитів/хв), а CAPTCHA та JavaScript-челенджі відсіюють ботів. Додатково можуть впроваджуватись чорні та білі списки IP, геоблокування (дозвіл трафіку лише з певних країн), резервні канали зв'язку через кількох провайдерів, а також регулярне оновлення ПЗ, патчинг вразливостей (CVE) і навчання персоналу — все це разом створює стійку систему захисту, здатну виявляти, зменшувати вплив та відновлюватися після DoS/DDoS-атак будь-якої складності.

Висновок. DoS і DDoS-атаки становлять одну з найсерйозніших загроз для стабільності та безпеки будь-якої IT-інфраструктури. Їх небезпека полягає в тому, що вони відносно прості у реалізації, але водночас надзвичайно складні для повного запобігання та нейтралізації. Навіть короткочасна атака може призвести до зупинки бізнес-процесів, фінансових та репутаційних втрат компанії. Однак завдяки розвитку сучасних технологій — таких як хмарні платформи з вбудованими механізмами безпеки, системи інтелектуального аналізу мережевого трафіку, а також алгоритми машинного навчання для виявлення аномалій — сьогодні можливо суттєво підвищити ефективність захисту. Важливо використовувати гібридний підхід до кіберзахисту, який поєднує різні методи моніторингу, фільтрації та реагування на атаки. Такий багаторівневий захист дозволяє своєчасно виявляти DoS і DDoS-атаки та мінімізувати їхній вплив.

Література

1. Тези всеукраїнської науково-практичної конференції студентів, аспірантів та молодих учених «Екзистенційні виклики освіти, науки, безпеки та здоров’я в сучасних умовах: пошуки молодих вчених». Петков Є.І. «Аналіз поточного стану криптографічних протоколів». URL: http://catalog.liha-pres.eu/index.php/liha-pres/catalog/book/372.
2. Петков Є. І. Типи спуфінг атак та засобів захисту в локальних мережах / Є. І. Петков // Передові технології в інформаційно-комунікаційній інженерії (ATICE'2025) : матеріали Міжнародної конференції / за заг ред. С. В. Ківалова ; Міжнародний університет. Одеса : Видавничий дім «Гельветика», 2025. С. 85-90. URL: https://hdl.handle.net/11300/30133; DOI: 10.32837/11300.30133
3. Cloudflare’s 2025 Q2 DDoS threat report. URL: https://blog.cloudflare.com/ddos-threat-report-for-2025-q2/.
4. Cloudflare’s 2025 Q1 DDoS Threat Report. URL: https://blog.cloudflare.com/ddos-threat-report-for-2025-q1/.
5. Cloudflare. What is a DDoS attack? URL: https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/.
6. Fortinet. What Is The Difference Between DoS Attacks And DDoS Attacks? URL: https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos.
7. AWS. DDoS Attack Protection. URL: https://aws.amazon.com/shield/ddos-attack-protection/.
8. F5. F5 DDoS Protection: Recommended Practices. URL: https://www.f5.com/pdf/products/ddos-protection-recommended-practices.pdf.

Бєліков Дмитро Вячеславович
Міжнародний університет