ПІДВИЩЕННЯ СТІЙКОСТІ ВІРТУАЛЬНИХ СЕРВЕРІВ ДО DDOS АТАК НА ОСНОВІ АВТОМАТИЧНОГО МАСШТАБУВАННЯ КЛАСТЕРНИХ ОБЧИСЛЮВАЛЬНИХ РЕСУРСІВ.

Робота студента
Гунька Іллі

Науковий керівник
Карпінець В.В.

МЕТА ТА АКТУАЛЬНІСТЬ РОБОТИ

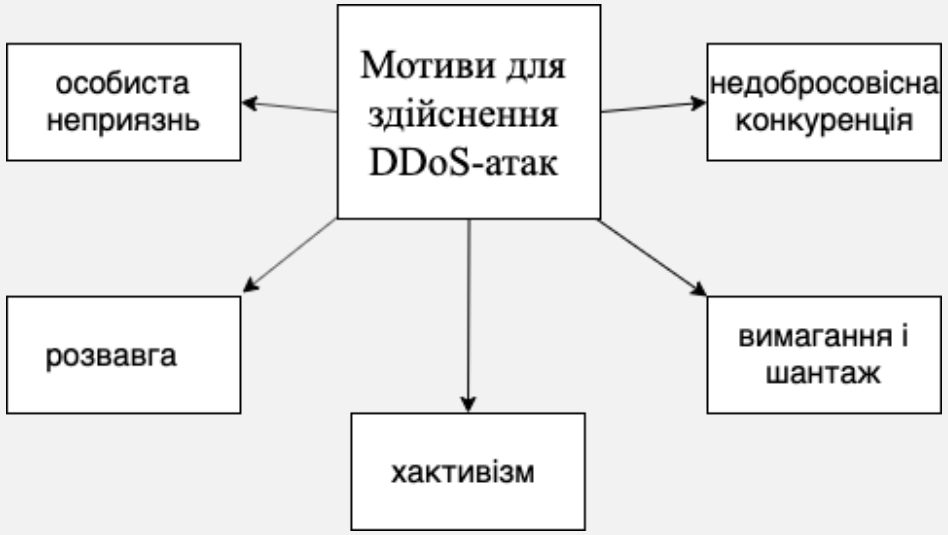
Метою роботи є розробка алгоритму і програмного додатку для покращення захисту віртуальних контейнеризованих серверів від DDoS-атак.

Робота здійснюється на прикладі розроблюваного програмного додатку.

- У зв'язку з виникненням інформаційного суспільства, зумовленим розвитком інформаційних технологій та електронної техніки, виникла суттєва загроза кібератак.
- На сьогоднішній день однією з найбільш популярних атак є DDoS-атаки. Мета DDoS-атаки – повне припинення роботи атакується сервера за рахунок подачі на нього велику кількість помилкових запитів. Середні збитки від DDoS-атак оцінюються по світу в 50 тисяч доларів для невеликих організацій і майже в 500 тис. доларів для великих підприємств.
- Усунення наслідків DDoS-атаки потребує додаткового робочого часу співробітників, відволікання ресурсів з інших проектів на забезпечення безпеки, розробки плану оновлення програмного забезпечення, модернізації обладнання тощо.
- Репутація атакованих організацій може постраждати не тільки через погану роботи сайту, а й через крадіжки персональних даних або фінансової інформації.

DDOS-АТАКА

DDoS-атака – комплекс дій, здатний повністю або частково вивести з ладу інтернет-ресурс. В якості жертви може виступати практично будь-який інтернет-ресурс, наприклад веб-сайт, ігровий сервер або державний ресурс.



DDOS-АТАКА

Найчастіше від DDoS-атак **страждають** сайти і сервера :

- великих компаній і державних установ;
- фінансових установ (банків, компаній, що управляють);
- купонних сервісів;
- медичних установ;
- платіжних систем;
- ЗМІ та інформаційних агрегаторів;
- інтернет-магазинів і підприємств електронної комерції;
- онлайн-ігор та ігрових сервісів;
- бірж криптовалюти.

DDOS-АТАКА

- Згідно з даними Corero Network Security, більш ніж дві третини всіх компаній в світі щомісяця піддаються атакам «відмови в доступі».
- Власники сайтів, які не передбачили захист сервера від DDoS-атак, можуть не тільки понести величезні збитки, але і зниження довіри клієнтів, а також конкурентоспроможності на ринку.

БОРОТЬБА ПРОТИ DDOS-АТАК

Заходи протидії DDoS-атакам можна розділити на пасивні і активні, а також на превентивні і реакційні. Нижче наведено короткий перелік **основних методів боротьби**:

- запобігання.
- відповідні заходи.
- програмне забезпечення.
- фільтрація і блекхолінг.
- зворотний DDOS
- розосередження.
- ухилення.
- активні заходи у відповідь.

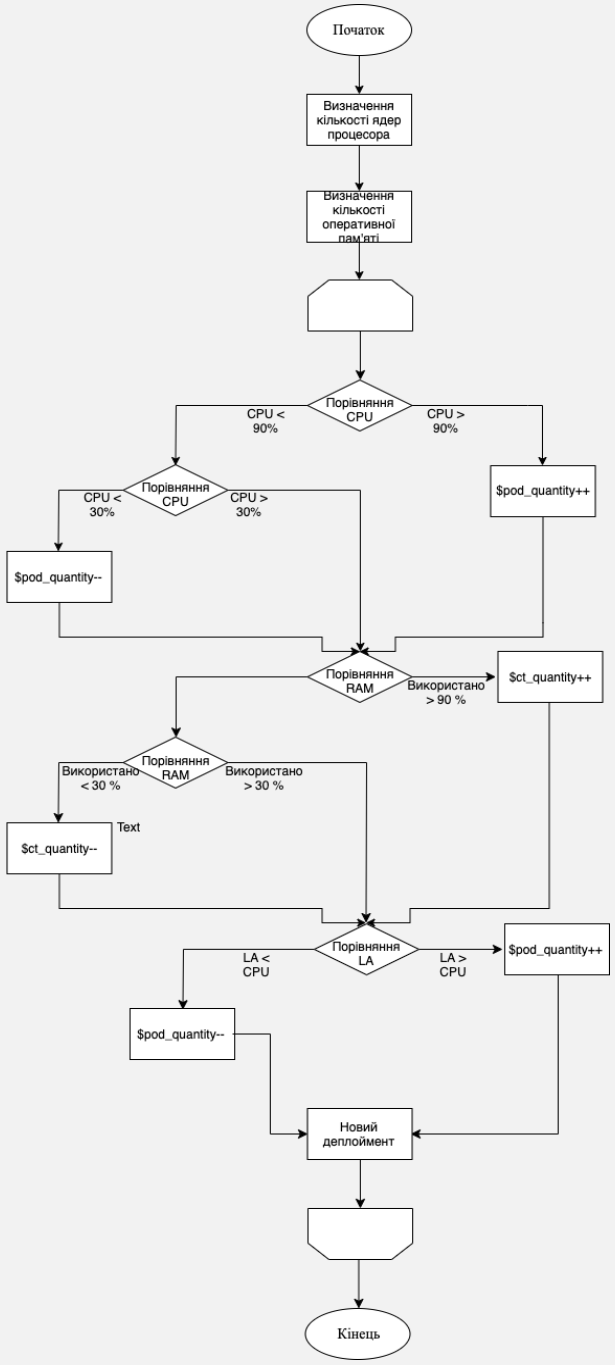
СУТЬ ЗАПРОПОНОВАНОГО МЕТОДУ

В даному випадку використовується **горизонтальне масштабування**, як таке, що легко імплементується в інфраструктуру без змін вихідного програмного коду і може бути глобально застосовано як частина вирішення проблеми DDoS атак для клієнтів хмарних хостингів.

Програмний продукт **відслідковує навантаження** різних значущих показників операційної системи і, в залежності від результатів моніторингу, **вносить зміни до інфраструктури** підвищуючи її стійкісь.

Значущими параметрами для моніторингу є наступні параметри:

- CPU;
- RAM;
- Load Average.

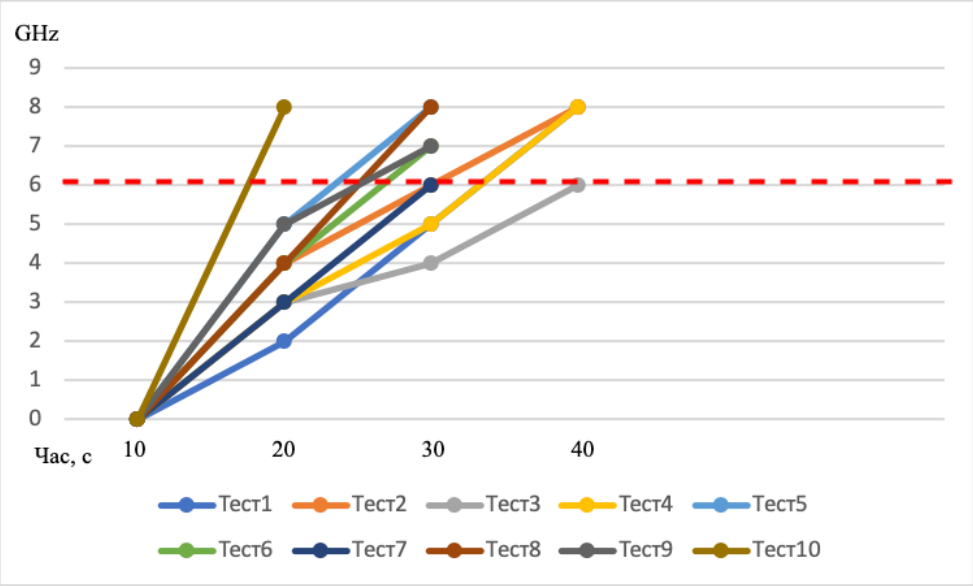

Початок
Визначення кількості ядер процесора
Визначення кількості оперативної пам'яті
Порівняння CPU
CPU < 90%
CPU > 90%
$pod_quantity++
Порівняння CPU
CPU < 30%
CPU > 30%
$pod_quantity--
Порівняння RAM
Використано > 90 %
$ct_quantity++
Порівняння RAM
Використано < 30 %
Використано > 30 %
Text
$ct_quantity--
Порівняння LA
LA < CPU
LA > CPU
$pod_quantity++
$pod_quantity--
Новий деплоймент
Кінець

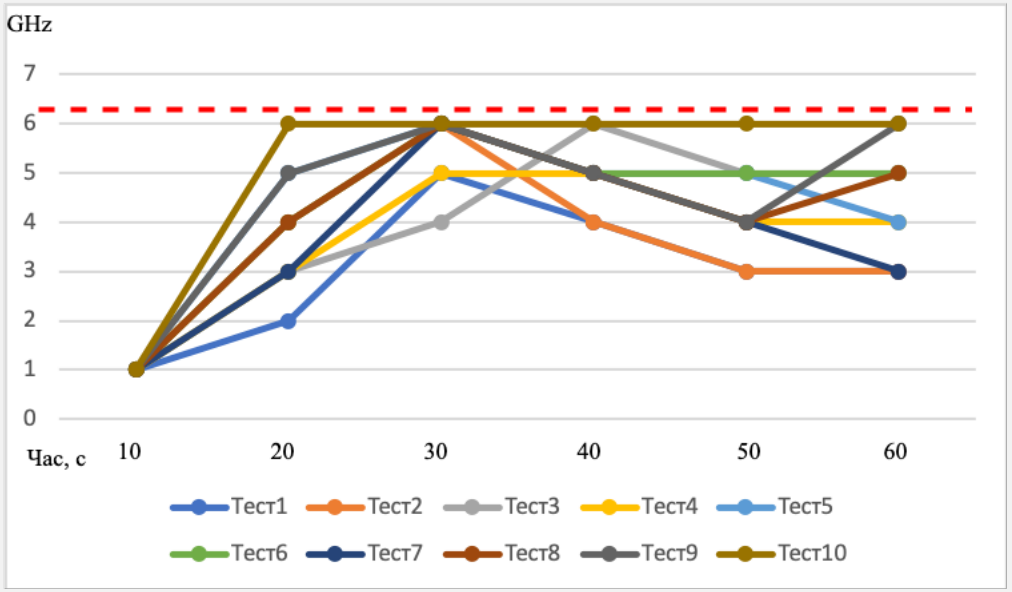
ПРИКЛАД РОБОТИ ДОДАТКУ

```
root@node78656-env-3508536 ~ $ kubectl get pods
NAME                                    READY   STATUS    RESTARTS   AGE
deploy-779878df9c-7xpk5                 1/1     Running   0          10s
deploy-779878df9c-bqr2b                 1/1     Running   2          6d23h
deploy-779878df9c-vgzsf                 1/1     Running   2          6d23h
```

```
root@node78656-env-3508536 ~ $ kubectl get pods
NAME                                    READY   STATUS    RESTARTS   AGE
deploy-779878df9c-7xpk5                 1/1     Running   0          62s
deploy-779878df9c-8zlmt                 1/1     Running   0          8s
deploy-779878df9c-bqr2b                 1/1     Running   2          6d23h
deploy-779878df9c-vgzsf                 1/1     Running   2          6d23h
```

ВИПРОБУВАННЯ





ВИСНОВОК

- Отже, у роботі був розроблений алгоритм **автоматичного масштабування** серверних кластерних ресурсів для протидії **DDoS атакам**. На основі алгоритму був розроблений і протестований програмний продукт.
- Алгоритм виконує **моніторинг** основних критично важливих для здорового функціонування сервера метрик, у разі необхідності виконує **масштабування** ресурсів без участі людини у процесі, а також повідомляє про свої дії адміністратора системи.

ДЯКУЮ ЗА УВАГУ!