ЗАТВЕРДЖУЮ
Перший проректор Державного університету інформаційно-комунікаційних технологій
член-кореспондент НАН України,
доктор технічних наук, професор,
лауреат Державної премії України в галузі науки і техніки,
Заслужений діяч науки і техніки України
_____ Олександр КОРЧЕНКО
"22" травня 2025 року

ВИСНОВОК

міжкафедрального семінару кафедри Технічних систем кіберзахисту Державного університету інформаційно-комунікаційних технологій про наукову новизну, теоретичне та практичне значення результатів дисертаційної роботи
Поночовного Петра Михайловича на тему: "Система протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси", поданої на здобуття наукового ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека

Витяг
з протоколу № 16 засідання кафедри Технічних систем кіберзахисту
від "22" травня 2025 року

Присутні: Головуючий на засіданні – директор Навчально-наукового інституту кібербезпеки та захисту інформації, д.т.н., професор Іванченко Євгенія Вікторівна.
З кафедри Технічних систем кіберзахисту:
завідувач кафедри – д.т.н., професор Туровський Олександр Леонідович;
професор кафедри – к.т.н., доцент Пепа Юрій Володимирович;
доцент кафедри – к.е.н. Аверічев Ігор Миколайович;
старший викладач кафедри – Рижаков Микола Миколайович
Запрошені:
- *з кафедри Управління кібербезпекою та захистом інформації:*
завідувач кафедри – д.е.н., професор Легомінова Світлана Володимирівна;
професор кафедри – д.т.н., професор Савченко Віталій Анатолійович;
доцент кафедри – к.т.н., доцент Щавінський Юрій Віталійович;
- *з кафедри Систем та технологій кібербезпеки:*
завідувач кафедри – д.т.н., професор Гайдур Галина Іванівна;
професор кафедри – д.т.н., професор Казмірчук Світлана Володимирівна;
доцент кафедри – доктор філософії за спеціальністю 125 Кібербезпека та захист інформації Марченко Віталій Вікторович;

Вхідний ДУІКТ № 700
«26» 06 2025 р.

завідувач кафедри – д.т.н., професор, завідувач кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і архітектури, академік Української академії наук Хлапонін Юрій Іванович;

професор кафедри – к.т.н., професор кафедри технічного захисту інформації, факультету комп'ютерних наук та технологій, Державного некомерційного підприємства "Державний Університет "Київський Авіаційний Інститут" Іванченко Ігор Сергійович;

завідувач кафедри – к.т.н., доцент, завідувач Кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка. Складанний Павло Миколайович

Всього присутніх – 14 осіб. серед присутніх 7 докторів технічних наук та 5 кандидатів технічних наук.

ПОРЯДОК ДЕННИЙ:

Обговорення дисертаційної роботи аспіранта кафедри Технічних систем кіберзахисту Державного університету інформаційно-комунікаційних технологій Поночовного Петра Михайловича на тему: "Система протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси", поданої на здобуття ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека.

Дисертація виконана на кафедрі Технічних систем кіберзахисту Державного університету інформаційно-комунікаційних технологій. Тема дисертаційної роботи затверджена в новій редакції та призначено наукових керівників:

кандидат технічних наук, професор кафедри Технічних систем кіберзахисту Пепа Юрій Володимирович;

кандидат технічних наук, доцент кафедри технічного захисту інформації, факультету комп'ютерних наук та технологій, Державного некомерційного підприємства "Державний Університет "Київський Авіаційний Інститут" Іванченко Ігор Сергійович на засіданні Вченої ради Державного університету інформаційно-комунікаційних технологій (протокол № 1 від 19.12.2024 року).

СЛУХАЛИ: доповідь про дисертаційну роботу Поночовного Петра Михайловича "Система протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси", подану на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека.

ПОНОЧОВНИЙ П.М.: Шановні Голово, члени міжкафедрального семінару, присутні! Вашій увазі пропонується доповідь за дисертаційною роботою на тему: "Система протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси ".

Актуальність дисертаційної роботи зумовлена зростаючою кількістю низькошвидкісних HTTP DDoS-атак, відсутністю ефективних інструментів

виявлення, вразивістю доступності веб-ресурсів, потребою в адаптивних системах із використанням ШІ. На слайді 3 за допомогою таблиці 3.1 представлено різницю між простою DDoS-атакою та низькошвидкісною DDoS-атакою. З цієї таблиці ми бачимо, що низькошвидкісні DDoS-атаки маскуються під легітимний трафік на відміну від простої DDoS-атаки, яка перенавантажує систему. В ході дослідження було проведено аналіз DDoS захисних систем. Результати показані на на слайді 4 в таблиці 4.1. Аналіз DDoS систем дозволив зробити висновки що більша частина систем не фільтрує низькошвидкісний трафік. Представлені таблиці дали можливість сформувати мету, предмет та об'єкт дослідження.

Метою роботи є зниження ефективності впливу низькошвидкісних HTTP DDoS-атак на веб-ресурси..

Об'єктом процес захисту веб-ресурсу від низькошвидкісних HTTP DDoS-атак.

Предметом дослідження є системи захисту веб-ресурсів від низькошвидкісних HTTP DDoS-атак.

Основним науковим завданням дослідження є:

- проаналізувати системи захисту від низькошвидкісних HTTP DDoS-атак та їх ефективності;
- розробити модель упередження низькошвидкісних HTTP DDoS-атак на кінцевого користувача для запобігання кіберінцидентам в кіберпросторі;
- розробити метод раннього виявлення та захисту від низькошвидкісних HTTP DDoS-атак шляхом аналізу обробки пакетних груп;
- розробити систему протидії низькошвидкісним HTTP DDoS-атакам на веб-ресурси, яка враховує аномалії в пакетах для підвищення ефективності захисту від низькошвидкісних HTTP DDoS-атак;
- провести експериментальне дослідження розробленої системи протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси.

Наукова новизна запропонованого підходу полягає у:

вперше розроблено модель упередження низькошвидкісних HTTP DDoS-атак на кінцевого користувача, яка за рахунок виявлення аномального потоку, алгоритму фільтрації трафіку, модуля пам'яті, дозволить передувати та протидіяти низькошвидкісним HTTP DDoS-атакам на рівні кінцевого користувача;

вперше розроблено метод раннього виявлення та захисту від низькошвидкісних HTTP DDoS-атак, який за рахунок умов фільтрації трафіку, а саме обмеження кількості запитів з одного IP/підмережі, блокування трафіку з регіонів, де немає клієнтів, тривалості запиту, дає можливість зменшити навантаження на сервер від 40 до 60 % і підтримати цілісність системи;

вперше розроблено систему протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси з урахуванням аномалій в пакетах, яка за рахунок розроблених моделі та методу, дає можливість упередженню та

покращенню захисту від низькошвидкісних HTTP DDoS-атак на 73% завдяки комбінації аналізу пакетних груп та динамічних особливостей.

Таким чином, у дисертаційній роботі обґрунтовано теоретико-методичні засади та розроблено систему протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси. Дана система складається з:

- моделі упередження низькошвидкісних HTTP DDoS-атак з використанням штучного інтелекту;
- алгоритму фільтрації трафіку;
- модуля виснаження пам'яті при DDoS-атаці.

Складові даної моделі дають можливість покращити рівень захищеності від низькошвидкісних HTTP DDoS-атак на 73%.

Доповідь закінчено. Дякую за увагу!

По завершенню доповіді Поночовному Петру Михайловичу присутніми були поставлені такі запитання:

1. Чому низькошвидкісні HTTP DDoS-атаки важко виявити?
2. Які основні цілі низькошвидкісних HTTP DDoS-атак?
3. Чому традиційні методи захисту неефективні проти таких атак?
4. У чому полягає наукова новизна дослідження?
5. Які особливості пакетів використовуються в моделі упередження?
6. Які алгоритми фільтрації трафіку запропоновано?
7. кі результати експериментів показали ефективність системи?
8. Які переваги має запропонована система порівняно з існуючими (наприклад, Cloudflare)?
9. Як оцінюється ймовірність успіху DDoS-атаки в розробленій моделі?
10. Які практичні сфери застосування результатів дослідження?
11. Які технології використовувались для навчання ШІ?
12. Які обмеження має запропонована система?
13. Які показники використовувались для оцінки ефективності системи?
14. Які публікації та апробації супроводжували дослідження?
15. Де вже впроваджені результати дослідження?

На всі питання були дані вичерпні відповіді.

СЛУХАЛИ: відгук наукового керівника кандидата технічних наук, доцента, Пепу Юрія Володимировича про дисертаційну роботу аспіранта Поночовного Петра Михайловича на тему: "Система протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси", подану на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека.

ПЕПА Ю.В.: Дисертаційна робота Поночовного Петра Михайловича "Система протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси" виконана у межах плану науково-дослідних робіт Державного університету інформаційно-комунікаційних технологій МОН України за темою "Шляхи підвищення ефективності захисту командно-телеметричної інформації

безпілотних літальних апаратів" (№ держ. реєстрації 0123U100244, ДУІКТ, м. Київ).

У процесі підготовки дисертації Петро Поночовний проявив себе як самостійний, наполегливий, відповідальний і високоерудований науковець, здатний формулювати та ефективно вирішувати складні наукові завдання. Він володіє сучасними методами наукових досліджень, аналітичними підходами, а також комунікаційними та іншими професійними компетентностями, що дозволяють йому логічно і послідовно представляти результати власних досліджень, публікувати їх у вітчизняних та міжнародних наукових виданнях, брати участь у наукових дискусіях, демонструючи вміння аргументовано обґрунтовувати та відстоювати власні наукові досягнення.

Автором дослідження коректно визначено мету, завдання, об'єкт і предмет дослідження. У процесі виконання дисертаційної роботи ефективно застосовано комплексний захист із застосуванням ШІ, теорії ймовірностей, метод аналізу шляхом тестування розробленої системи на серверах розгорнутих на різних платформах. Такий підхід забезпечив не лише формулювання та теоретичне обґрунтування наукової новизни отриманих результатів, а й їх практичну реалізацію, що визначило значущість дослідження для розв'язання проблеми захисту від низькошвидкісних HTTP DDoS-атак на веб-ресурси.

У ході виконання дисертаційної роботи автором досягнуто мети роботи – зниження ефективності впливу низькошвидкісних HTTP DDoS-атак на веб-ресурси. Отримані результати мають важливе практичне значення для спеціалістів у сфері кібербезпеки, інформаційної безпеки, аудиту інформаційних систем, а також можуть бути використані в навчальних програмах із підвищення обізнаності співробітників.

За результатами дисертаційних досліджень опубліковано 20 наукових праць. Основні наукові результати викладені в 9 наукових статтях опублікованих у спеціалізованих фахових виданнях, затверджених наказом МОН України. Матеріали виступів на наукових та науково-практичних конференціях опубліковано у 12 збірниках тез доповідей.

Основні наукові та прикладні результати дисертаційної роботи, що виносяться на захист, отримані автором особисто. З наукових праць, які опубліковані у співавторстві, використано лише ті положення, ідеї та висновки, які є результатом власного дослідження здобувача.

Робота є самостійно виконаним науковим дослідженням, що відповідає принципам академічної доброчесності та не містить некоректних запозичень. Вона повністю відповідає спеціальності 125 Кібербезпека, за якою подається до захисту.

Дисертаційна робота Поночовного Петра Михайловича є завершеним науковим дослідженням, яке здійснює вагомий внесок у розвиток теоретичних і прикладних аспектів інформаційної безпеки, зокрема у сфері захисту веб-ресурсів від низькошвидкісних HTTP DDoS-атак. Запропоновані автором науково-методичні підходи сприяють удосконаленню систем захисту веб-ресурсів від низькошвидкісних HTTP DDoS-атак, підвищенню рівня захищеності користувачів та забезпеченню стійкості організацій до впливу

низькошвидкісних HTTP DDoS-атак. Дослідження виконане на високому науковому рівні, підтверджує наукову зрілість, ґрунтовну підготовку та високу компетентність здобувача в галузі кібербезпеки.

Вважаю, що дисертаційна робота повністю готова до захисту, а її автор заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 Кібербезпека.

Призначені рецензенти:

к.т.н., доцент кафедри Управління кібербезпекою та захистом інформації Щавінський Юрій Віталійович; д.т.н., професор кафедри Систем та технологій кібербезпеки Казмірчук Світлана Володимирівна загалом позитивно оцінили дисертаційну роботу, відзначивши її високу актуальність, теоретичну значущість та практичну цінність. Особливу увагу було приділено науковій новизні, обґрунтованості результатів і систематизованому підходу до вирішення поставленої проблеми.

Зокрема, **доктор технічних наук, професор, професор кафедри Систем та технологій кібербезпеки Казмірчук Світлана Володимирівна** відзначила високий науковий рівень дисертаційної роботи Поночовного Петра Михайловича та її актуальність у контексті сучасних викликів кібербезпеки.

Загальний аналіз дисертації дозволив зробити наступні висновки:

1. Ознайомлення зі змістом дисертаційної роботи підтверджує логічність її побудови, чіткість наукової аргументації, а також обґрунтованість висновків і рекомендацій, сформульованих автором самостійно.

2. Структура роботи відповідає визначеній меті та поставленому науковому завданню. Дисертація ґрунтується на положеннях інформаційної безпеки, теорії ризиків, аналізу DDoS-захисних систем, теорії математичного моделювання, що забезпечує її теоретичну глибину. Актуальність дослідження підтверджується проведеним аналізом DDoS-захисних систем, де за певними ознаками ми бачимо, що потрібність створення системи протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси є актуальним і важливим для зниження ефективності впливу низькошвидкісних DDoS-атак на веб-ресурси.

3. Автором сформульовано оригінальні наукові рішення, які стосуються створення ефективної системи протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси. Все це втілено в представленій моделі упередження низькошвидкісних HTTP DDoS-атак з використанням ШІ. Дана модель фільтрує вхідний трафік за певними особливостями. Отримані результати мають значний практичний потенціал для підвищення кіберстійкості веб-ресурсів.

4. Дисертаційне дослідження є самостійною науковою працею, що не містить некоректних запозичень. Опубліковані результати досліджень відображають основні положення наукової новизни та відповідають вимогам до дисертацій за спеціальністю 125 Кібербезпека.

Позитивно оцінюючи положення дисертаційного дослідження Поночовного П.М., **Казмірчук С.В.** звернула увагу на певні аспекти, що можуть бути уточнені або розширені:

1. У роботі приділено значну увагу технічним аспектам виявлення та протидії атакам, однак аналіз специфіки саме низькошвикісних (low-rate/low-and-slow) HTTP DDoS-атак та їх відмінностей від класичних DDoS потребує поглиблення. Було б корисно детальніше розглянути конкретні механізми формування таких атак (наприклад, використання повільних HTTP-запитів, атак на серверні сесії, цілеспрямоване вичерпання окремих ресурсів) та їхній вплив на ефективність обходу традиційних систем захисту.

2. У роботі детально досліджено основні принципи функціонування пропонованої системи. Однак варто було б глибше проаналізувати вплив динамічно змінюваних умов мережевого середовища, таких як різкий ріст легального трафіку, сезонні коливання навантаження чи зміни у топології мережі, на точність виявлення саме низькошвидкісних атак та ймовірність хибної класифікації.

3. Дослідження має значний прикладний потенціал, проте було б корисно детальніше розглянути питання практичної інтеграції розробленої системи в існуючу інфраструктуру захисту веб-ресурсів (наприклад, разом із WAF, CDN або традиційними DDoS-миттцями), а також визначити конкретні вимоги до апаратних ресурсів, масштабованості та керованості системи в різних середовищах експлуатації.

Наведені зауваження стосуються переважно питань подальшого розвитку дослідження та не впливають на його загальну наукову та практичну значущість. Робота є завершеним дослідженням, що робить вагомий внесок у розвиток методів виявлення та нейтралізації складних для детектування низькошвидкісних HTTP DDoS-атак, спрямованих на веб-ресурси, та підвищення стійкості інформаційних систем до них. За рівнем наукової аргументації, методологічного підходу та практичної значущості висновків, дисертація відповідає вимогам, які висуваються до досліджень на здобуття наукового ступеня доктора філософії за спеціальністю 125 Кібербезпека. Робота виконана державною мовою, *з дотриманням норм та правил академічної доброчесності.*

Кандидат технічних наук, доцент кафедри Управління кібербезпекою та захистом інформації Щавінський Юрій Віталійович охарактеризував дисертаційну роботу як ґрунтовне наукове дослідження високого рівня, що відображає актуальні виклики у сфері кібербезпеки, зокрема проблему протидії складним для детектування низькошвидкісним (low-rate) HTTP DDoS-атакам на веб-ресурси. Робота містить чітке теоретичне обґрунтування, новітні підходи до аналізу векторів атак та практичні рішення щодо їх нейтралізації. Наукові результати дослідження мають важливе значення для розвитку систем захисту веб-інфраструктури та практичного впровадження в організаціях різного профілю.

Разом із позитивною оцінкою дисертації, рецензент висловив окремі зауваження та наголосив на аспектах для подальшого дослідження:

1. Універсальність системи: Запропонований механізм виявлення low-rate атак орієнтований на загальні принципи функціонування веб-серверів. Доцільно було б перевірити його ефективність у різних середовищах, наприклад, при захисті веб-застосунків з інтенсивним API-трафіком, високонавантажених e-commerce платформ або систем з динамічним контентом, де шаблони легального трафіку суттєво відрізняються.

2. Часова динаміка атак: У роботі аналізуються переважно "стаціонарні" сценарії атак. Варто глибше дослідити вплив часових факторів (тривалість атаки, варіативність інтервалів між запитами, адаптація до сезонних навантажень) на стійкість системи до довготривалих та адаптивних low-rate DDoS, що імітують поведінку легальних користувачів.

3. Оптимізація роботи системи: Дослідження фокусується на алгоритмах детектування, проте потребує поглибленого аналізу ефективності різних стратегій реагування (наприклад, динамічне регулювання QoS, селективне обмеження трафіку, інтеграція з механізмами автоматизованого блокування). Було б корисним з'ясувати оптимальні параметри калібрування системи для мінімізації false positive у реальних умовах експлуатації.

Загалом, рецензована робота підготовлена на високому науковому рівні, вирізняється системністю, новизною технічних рішень та практичною цінністю отриманих результатів, виконана *з дотриманням норм академічної доброчесності*. Це дає підстави оцінити її позитивно та рекомендувати до захисту на здобуття наукового ступеня доктора філософії за спеціальністю 125 Кібербезпека.

Рецензентами відзначено, що дисертаційна робота відповідає встановленим вимогам щодо наукової новизни, теоретичної та практичної значущості, а також може бути рекомендована до спеціалізованої вченої ради для попереднього розгляду та захисту на здобуття наукового ступеня доктора філософії.

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертаційної роботи Поночовного Петра Михайловича на тему "Система протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси", поданої на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека

Актуальність теми дослідження. Сучасні зловмисники все частіше використовують низькошвидкісні HTTP DDoS-атаки, які важко виявити через їхню схожість із легальним трафіком. Такі атаки націлені на довгострокове паралізування веб-ресурсів, що становить загрозу для доступності критичних сервісів (наприклад, електронних урядів або фінансових платформ).

Дослідженням підходів до виявлення та прогнозування низькошвидкісних DDoS-атак займаються як закордонні, так і вітчизняні вчені. Спеціалізація, аналіз поведінки мережевого трафіку, методи виявлення повільних DDoS-атак, Лукова-Чуйко Н.В.. Базова модель параметрів для побудування систем виявлення атак, Корченко А.О.. Класифікація DDoS-атак, включаючи низькоінтенсивні методи, Mirkovic J., & Reiher P.. Механізми виявлення атак на основі часових характеристик трафіку, S. M. Specht, R. B. Lee. Розробка алгоритмів для ідентифікації "повільних" атак на веб-сервери, D. Kagir. Аналіз вразливостей HTTP/HTTPS-протоколів до DDoS із низькою швидкістю, Asosheh A., & Ranezani N.. Дослідження, комбінація машинного навчання та сигнатурного аналізу для блокування DdoS-атак, Douligeris C., & Mitrokotsa A.. Розробка моделі системи виявлення кіберзагроз з підтримкою та оновленням правил виявлення атаки О. Шпур. Системи моніторингу на основі аналізу сесійних даних HTTP, K. Salah. Дослідження механізмів "shrew attacks" та їх впливу на веб-інфраструктуру, A. Kuzmanovic. Вплив перехоплення HTTPS на безпеку, V. Paxson.

Аналіз робіт вітчизняних і зарубіжних авторів дає змогу зробити висновок, що на сьогодні проблема низькошвидкісних HTTP DDoS-атак досліджена вкрай недостатньо.

Низькошвидкісні HTTP DDoS-атаки порушують роботу серверів, що призводить до втрат доходів, репутаційних збитків та порушення функціонування інфраструктури. Забезпечення стабільності веб-ресурсів є пріоритетом для організацій, які працюють з великою кількістю користувачів.

Існуючі системи захисту часто не розрізняють низькошвидкісні DDoS-атаки та звичайний трафік, що призводить до запізнілого реагування або помилкових блокувань. Це створює потребу в спеціалізованих рішеннях, орієнтованих на аналіз поведінки користувачів та аномалій у HTTP-запитах.

Традиційні методи блокування DDoS (наприклад, блокування лишень за IP) неефективні проти низькошвидкісних атак, які використовують розподілені джерела та імітують легальних користувачів. Необхідність у розумних алгоритмах, здатних навчатися на нових типах загроз, робить тему дослідження критично важливою для кібербезпеки.

Тому розробка системи протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси є актуальною науковою задачею.

Зв'язок роботи з науковими програмами, планами, темами, грантами.

Дисертаційна робота виконана відповідно до планів наукової і науково-технічної діяльності Державного університету інформаційно-комунікаційних технологій в рамках науково-дослідної роботи "Шляхи підвищення ефективності захисту командно-телеметричної інформації безпілотних літальних апаратів" (№ держ. реєстрації 0123U100244, ДУІКТ, м. Київ).

Мета і завдання дослідження.

Метою дослідження є зниження ефективності впливу низькошвидкісних HTTP DDoS-атак на веб-ресурси.

Для досягнення поставленої мети автором виконано наступні *окремі завдання дослідження*:

проведено аналіз існуючих систем захисту від низькошвидкісних HTTP DDoS-атак та їх ефективності, визначено їх основні недоліки та обмеження;

розроблено модель упередження низькошвидкісних HTTP DDoS-атак на кінцевого користувача для запобігання кіберінцидентам в кіберпросторі;

розроблено метод раннього виявлення та захисту від низькошвидкісних HTTP DDoS-атак шляхом аналізу обробки пакетних груп, забезпечено уніфікацію для інтеграції в модель;

розроблено систему протидії низькошвидкісним HTTP DDoS-атакам на веб-ресурси, яка враховує аномалії в пакетах для підвищення ефективності захисту від низькошвидкісних HTTP DDoS-атак;

проведено експериментальне дослідження розробленої системи протидії низькошвидкісним HTTP DDoS-атак на веб-ресурси.

Об'єкт дослідження – процес захисту веб-ресурсу від низькошвидкісних HTTP DDoS-атак.

Предмет дослідження – системи захисту веб-ресурсів від низькошвидкісних HTTP DDoS-атак.

Методи дослідження.

Ґрунтуються за допомогою визначення груп пакетів в часовому вікні. Це надає можливість створити особливості, за допомогою яких забезпечується раннє виявлення та захисту від низькошвидкісних HTTP DDoS-атак. Достовірність наукових результатів, висновків та рекомендацій, викладених у дисертаційній роботі, обґрунтовано коректним використанням математичного апарату, моделюванням на обчислювальних пристроях, а також аналізом впливу низькошвидкісних HTTP DDoS-атак на ймовірність успішних DDoS-атак.

Результати теоретичних досліджень були підтверджені результатами симуляцій та експериментального моделювання в умовах різних сценаріїв оцінок захищеності.

Наукова новизна дослідження:

Вперше розроблено модель упередження низькошвидкісних HTTP DDoS-атак на кінцевого користувача, яка за рахунок виявлення аномального потоку, алгоритму фільтрації трафіку, модуля пам'яті, дозволить передувати та

протидіяти низькошвидкісним HTTP DDoS-атакам на рівні кінцевого користувача.

Вперше розроблено метод раннього виявлення та захисту від низькошвидкісних HTTP DDoS-атак, який за рахунок умов фільтрації трафіку, а саме обмеження кількості запитів з одного IP/підмережі, блокування трафіку з регіонів, де немає клієнтів, тривалості запиту, дає можливість зменшити навантаження на сервер від 40 до 60 % і підтримати цілісність системи.

Вперше розроблено систему протидії низькошвидкісним HTTP DDoS-атакам на веб-ресурси з урахуванням аномалій в пакетах, яка за рахунок розроблених моделі та методу, дає можливість упередженню та покращенню захисту від низькошвидкісних HTTP DDoS-атак на 73% завдяки комбінації аналізу пакетних груп та динамічних особливостей.

Практичне значення.

Практичне значення одержаних результатів полягає в тому, що розроблений алгоритм роботи системи захисту серверів, який складається з адаптивної моделі ШІ для виявлення аномалій низькошвидкісних HTTP DDoS-атак, який на ввідміну від існуючих методів виявлення низькошвидкісних HTTP DDoS-атак враховує вище згадані особливості і на 73% краще блокує низькошвидкісні HTTP DDoS-атаки.

Особистий внесок здобувача. Дисертація є самостійною науковою працею, в якій висвітлені власні ідеї і розробки автора, що дозволили вирішити поставлені завдання. Робота містить теоретичні та методичні положення і висновки, сформульовані дисертантом особисто. Використані в дисертації ідеї, положення чи гіпотези інших авторів мають відповідні посилання і використані лише для підкріплення ідей здобувача.

Роботи, що опубліковані в співавторстві, де в дисертаційній роботі використано тільки результати дослідження, що були отриманні виключно здобувачем. У роботах, опублікованих в співавторстві, автором: методика виявлення мережевих вторгнень і ознак комп'ютерних атак на основі емпіричного підходу; технологія забезпечення кібербезпеки хмарного середовища на базі рішення Cisco Cloudlock; оцінка якості системи моніторингу технічного стану телекомунікаційних мереж спеціального призначення; виявлення DDoS-атаки на високошвидкісну мережу: опитування; модель упередження низькошвидкісних HTTP DDoS атак на кінцевого користувача; метод раннього виявлення та захисту від мінливих DDoS атак на основі аналізу обробки пакетних груп; реалізація системи захисту серверів з урахуванням аномалій в пакетах; модель трансформації на основі штучного інтелекту з елементами захисту від DDoS -атак.

Апробація результатів дослідження.

Основні результати дисертаційної роботи були представлені та обговорені на міжнародних науково-технічних та науково-практичних конференціях: «Штучний інтелект та інтелектуальні системи AIIS`2023 XXIII міжнар. наук.-тех. конф.» (м. Київ, 2023), «Математика. Інформаційні технології. Освіта XIII міжнар. наук.-практ. конф.» (м. Луцьк, 2024), «ITSec-2024: Безпека інформаційних технологій: матеріали XIII міжнар. наук.-тех. конф.» (м. Львів, 2024), «Сучасні

аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії II міжнар. наук.-практ. конф.» (м. Київ, 2024), «TTSIIT – 2025 The IV International Conference on Emerging Technology Trends on the Smart Industry and the Internet of Things» (Ukraine - Iraq – Poland, 2025), «ITSec-2025: Безпека інформаційних технологій: матеріали XIV міжнар. наук.-тех. конф.» (м. Тернопіль, 2025).

Публікації. За результатами дисертаційних досліджень опубліковано 21 наукових працях. Основні наукові результати викладені в 9 наукових статтях опублікованих у спеціалізованих фахових виданнях, затверджених наказом МОН України. Матеріали виступів на наукових та науково-практичних конференціях опубліковано у 12 збірниках тез доповідей.

Список опублікованих праць за темою дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Лук'яненко Т.Ю. (Lukyanenko T. Yu.), Поночовний П.М. (Ponochovnyy P. M.), Легомінова С.В. (Lehominova S. V.), Методика виявлення мережевих вторгнень і ознак комп'ютерних атак на основі емпіричного підходу // *Сучасний захист інформації*, 2022. – № 2. – 15-21. Режим доступу: https://doi.org/10.31673/2409-7292.2022.021521

2. Опанасенко М.І., Поночовний П.М., Технологія забезпечення кібербезпеки хмарного середовища на базі рішення Cisco Cloudlock // *Сучасний захист інформації*, 2023. – № 1. – С.72-78. Режим доступу: https://doi.org/10.31673/2409-7292.2023.010010

3. Прокопенко А.Г., Лаврінець К.Г., Поночовний П.М., Оцінка якості системи моніторингу технічного стану телекомунікаційних мереж спеціального призначення // *Зв'язок*, 2024. – № 4. – С.19-23. Режим доступу: https://doi.org/10.31673/2412-9070.2024.041923

4. Савченко В.А., Поночовний П.М., Аверічев І.М. Виявлення DDOS-атаки на високошвидкісну мережу: опитування. // *Прикладні проблеми комп`ютерних наук, безпеки та математики*. Луцьк: Волинський національний університет імені Лесі Українки, 2024. №3. – С.71-76. Режим доступу: https://apcssm.vnu.edu.ua/index.php/Journalone/article/view/127

5. Поночовний П.М. Модель упередження низькошвидкісних HTTP DDoS атак на кінцевого користувача // Електронне фахове наукове видання *Кібербезпека: освіта, наука, техніка.* Київ: Київський столичний університет імені Бориса Грінченка, 2024. Том 2 № 26. – С.291-304. Режим доступу: https://doi.org/10.28925/2663-4023.2024.26.695

6. Поночовний П.М., Іванченко І.С. Метод раннього виявлення та захисту від мінливих DDoS атак на основі аналізу обробки пакетних груп // *Наукові записки ДУІКТ* – 2024. No2. – С.153-164. Режим доступу: https://doi.org/10.31673/2786-8362.2024.027035

7. Поночовний П.М., Пепа Ю.В. Реалізація системи захисту серверівз урахуванням аномалій в пакетах // *Вимірювальна та обчислювальна техніка в*

технологічних процесах, 2025, №2. м. Хмельницький – С.44-51. Режим доступу: https://doi.org/10.31891/2219-9365-2025-81-6

8. Рижаков М.М., Поночовний П.М. Модель трансформації на основі штучного інтелекту з елементами захисту від DDoS-атак // *Прикладні проблеми комп'ютерних наук, безпеки та математики.* 2025, №4 м. Луцьк – С. 14-32. Режим доступу: https://apcssm.vnu.edu.ua/index.php/Journalone/article/view/128

9. Поночовний П.М., Пепа Ю.В. Реалізація захисту серверів з нестандартними обліковими записами в пакетній системі // *Український журнал досліджень інформаційної безпеки.* 2025, Том 26, №2. м. Київ С. 270-277. Режим доступу: https://doi.org/10.18372/2410-7840.26.20018

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Поночовний П.М. Інформаційна безпека сьогодні// II Всеукраїнської науково-практичної конференції пам'яті академіка Академії наук вищої освіти, професора Анатолія Володимировича Касперського, 29 червня, Київ, 2022 р – С. 77 – 79, покликання на матеріал: https://enpuir.npu.edu.ua/bitstream/handle/123456789/37971/book_2022.pdf?sequence=1&isAllowed=y

2. Поночовний П.М. Впровадження систем штучного інтелекту у сфери безпеки і оборони, науки і освіти, економіки, медицини // С34 Системи та засоби штучного інтелекту: тези доповідей Міжнародної наукової молодіжної школи. – Київ: ІПШІ «Наука і освіта», 2023. – С. 30-33. Режим доступу: https://www.ipai.net.ua/docs/AIIS-2023-school.pdf

3. Поночовний П.М. Використання штучного інтелекту в освіті // IV Всеукраїнська науково-практична конференція «Модернізація змісту професійної освіти в умовах євроінтеграції України – 2024», 2024, м. Київ – С.437-439. Режим доступу: https://drive.google.com/file/d/18Jhvyz_tMht0tu7wjcuRpeXN86R3ony4/view

4. Пепа Ю.В., Поночовний П.М., Вплив сторонніх факторів на обробку сигналів // XIII Міжнародна науково-практична конференція «Математика. Інформаційні технології. Освіта, 2024, м. Луцьк – с.157-159. Режим доступу: https://drive.google.com/file/d/16GSq2WkNNsnEs6KRBkfCGdcYCKwi1bwO/view

5. Поночовний П.М., Ігор Аверічев І.М., Критерії виявлення повільних DDoS-атак // XIII Міжнародна науково-технічна конференція ITSec-2024 Безпека інформаційних технологій, 2024, м. Львів – с.175-176. Режим доступу: https://drive.google.com/file/d/1N1orbCGW37_pIRTzbHWuEgO3M8lw9B6r/view?usp=drive_link

6. Пепа Ю.В., Поночовний П.М., Інтегральне оцінювання стійкості систем управління // Науково-практична конференція «Перспективи та проблематика Інтелектуальних систем», 2024, м. Київ – с.3-4. Режим доступу: https://duikt.edu.ua/uploads/p_2661_35995256.pdf

7. Поночовний П.М., Пепа Ю.В., "Захист освітнього сервера від повільних DDoS-атак" // IV Всеукраїнська науково-практична конференція

пам'яті академіка Академії наук вищої освіти, професора Анатолія Володимировича Касперського «Актуальні проблеми та перспективи розвитку фундаментальних, прикладних, загальнотехнічних та безпекових наук», 2024, м. Київ – с.159 – 162. Режим доступу: https://drive.google.com/file/d/1zYSEg2O2x88H3_NHh27EFyTwjRg7mGt6/view

8. Поночовний П.М. "Кіберзагрози в епоху цифровізації: моделювання та захист від DDoS-атак" // Всеукраїнська науково-практична конференція «Актуальні проблеми безпеки інформаційно-телекомунікаційних систем», 2024, м. Київ – с.85 – 86. Режим доступу: https://duikt.edu.ua/uploads/p_2661_93669247.pdf

9. Куліш Є.О., Поночовний П.М., Пепа Ю.В. Оцінка ефективності систем раннього виявлення DDoS-атак // Всеукраїнська науково-практична конференція «Актуальні проблеми безпеки інформаційно-телекомунікаційних систем», 2024, м. Київ – с.17 – 20. Режим доступу: https://duikt.edu.ua/uploads/p_2661_93669247.pdf

10. Поночовний П.М., Іванченко І.С. Експериментальне дослідження системи реалізації захисту серверів з урахуванням аномалій в пакетах // II міжнародна науково-практична конференція «Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії», 2024, м. Київ – С. 173 – 177. Режим доступу: https://duikt.edu.ua/uploads/p_2661_99635945.pdf

11. Yuriy PEPA, Petro PONOCHOVNYI, Oleksandr LEVKUSHA METHOD FOR DETERMINING VULNERABILITIES TO DDOS ATTACKS ON CONTENT MANAGEMENT SYSTEMS // The IV International Conference on Emerging Technology Trends on the Smart Industry and the Internet of Things "TTSIIT - 2025", KYIV NATIONAL UNIVERSITY OF CONSTRUCTION AND ARCHITECTURE -30-31 січня 2025, Ukraine-Iraq-Poland C. – 95-100. Режим доступу: https://drive.google.com/file/d/145aOtud0A7zl4N9RKXiFyt9iMLKYsMt_/view

12. Поночовний П.М. Автоматизоване реагування на кіберінциденти за допомогою ШІ: міф чи реальність сучасних SOC? // XIIV Міжнародна науково-технічна ITSec-2025 Безпека інформаційних технологій, 2025, м. Тернопіль – с.156-159. Режим доступу: https://drive.google.com/file/d/14lB_f2ShfCzvJqOWsu7gt-Bf5JNqzDgx/view?usp=sharing

Структура та обсяг дисертації.

Дисертаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел із 145 найменувань на 17 сторінках. Загальний обсяг роботи становить 183 сторінки, серед яких 132 сторінки основного тексту, 68 малюнків, 16 таблиць.

Характеристика особистості здобувача.

Поночовний Петро Михайлович у 2016 році закінчив Національний педагогічний університет імені М.П. Драгоманова та отримав диплом Магістра за спеціальністю «Технологічна освіта» та здобув кваліфікацію магістра технологічної освіти; викладача вищого навчального закладу; вчителя

технологій, креслення та профільного навчання, основний напрям за кваліфікацією (8.0110301 Технологічна освіта; спеціалізація – Інформаційні технології та захист інформаційних ресурсів). У 2021 році вступив до аспірантури Державного університету телекомунікацій, м. Київ, Україна, за спеціальністю 125 Кібербезпека. 19 грудня 2024 року протокол №1 на засіданні Вченої Ради Державного університету інформаційно-комунікаційних технологій було затверджено у новій редакції тему дисертаційної роботи Поночовного Петра Михайловича "Система протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси".

Під час виконання дисертаційної роботи Поночовний П.М. провів ґрунтовне дослідження, спрямоване на аналіз сучасного стану проблематики, заявленої у дисертації. Було чітко визначено об'єкт, предмет, мету та завдання дослідження, обґрунтував актуальність теми та обрано відповідні методи для досягнення поставлених цілей. Здобувач Петро Поночовний приймав безпосередню участь під час постановки наукових завдань, планування та виконання експериментів, а також обговорення отриманих результатів. Проявив себе як відповідальний, дисциплінований та ініціативний дослідник, здатний працювати як самостійно, так і в команді. Продемонстрував високий рівень теоретичної підготовки, володіє сучасними методами дослідження, аналітичними інструментами та практичними навичками. Системно підходить до вирішення наукових завдань, критично оцінює результати власної роботи, виявляє наполегливість у досягненні поставлених цілей. Постійно вдосконалює свої знання, прагнучи підвищити рівень наукової обґрунтованості та практичної значущості отриманих результатів.

Оцінка мови та стилю дисертації. Дисертація виконана фаховою українською мовою, текстове подання матеріалу відповідає стилю науково-дослідної літератури.

Рецензенти рекомендують: відповідно до **п.15** Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12 січня 2022р. №44, ***пропонується такий склад разової ради:***

Голова ради:

Іванченко Євгенія Вікторівна, доктор технічних наук, професор, Лауреат Національної премії України ім. Бориса Патона, директор Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.

Рецензенти:

Казмірчук Світлана Володимирівна, доктор технічних наук, професор, професор кафедри Систем та технологій кібербезпеки Навчально-наукового

інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.

Щавінський Юрій Віталійович, кандидат технічних наук, доцент, доцент кафедри Управління кібербезпекою та захистом інформації Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.

Офіційні опоненти:

Хлапонін Юрій Іванович, доктор технічних наук, професор, академік Української академії наук, завідувач кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і архітектури.

Складанний Павло Миколайович, кандидат технічних наук, доцент, завідувач Кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка.

У результаті попередньої експертизи дисертації **Поночовного Петра Михайловича** і повноти публікації основних результатів дослідження.

УХВАЛЕНО:

1. Затвердити висновок про наукову новизну, теоретичне та практичне значення результатів дисертації Поночовного Петра Михайловича на тему "Система протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси".

2. Констатувати, що за актуальністю, степенем наукової новизни, обґрунтованістю, науковою та практичною цінністю здобутих результатів дисертація Поночовного П.М. відповідає спеціальності 125 Кібербезпека та вимогам **Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах),** затвердженого постановою Кабінету Міністрів України від 23 березня 2016 р. № 261, пп. **6, 7, 8 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії,** затвердженого постановою Кабінету Міністрів України від 12 січня 2022 р. № 44.

3. Рекомендувати дисертацію Поночовного П.М. на тему "Система протидії упередження низькошвидкісних HTTP DDoS-атак на веб-ресурси" до захисту на здобуття ступеня доктора філософії у разовій спеціалізованій вченій раді за спеціальністю 125 Кібербезпека.

4. Рекомендувати вченій раді Державного університету інформаційно-комунікаційних технологій затвердити склад разової спеціалізованої вченої ради:

Голова ради:

Іванченко Євгенія Вікторівна, доктор технічних наук, професор, Лауреат Національної премії України ім. Бориса Патона, директор Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.

інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.

Щавінський Юрій Віталійович, кандидат технічних наук, доцент, доцент кафедри Управління кібербезпекою та захистом інформації Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.

Офіційні опоненти:

Хлапонін Юрій Іванович, доктор технічних наук, професор, академік Української академії наук, завідувач кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і архітектури.

Складанний Павло Миколайович, кандидат технічних наук, доцент, завідувач Кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка.

Результати голосування щодо рекомендації до захисту дисертації Поночовного Петра Михайловича:

"За" – 14

"Проти" – немає

"Утримались" – немає

Додаток: Презентація Поночовного Петра Михайловича на 24 стор.

Головуючий на засіданні –
Директор Навчально-наукового інституту
кібербезпеки та захисту інформації Євгенія ІВАНЧЕНКО

Секретар засідання Микола РИЖАКОВ