УДК 621.391

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ МЕТОДІВ КІБЕРЗАХИСТУ ВІД АТАКИ TCP SYN FLOOD ТРАНСПОРТНОГО РІВНЯ

В.Є. Качан
Харківський національний університет радіоелектроніки

Abstract *– The work analyzes threats at seven layers of the Open Systems Interconnection reference model. Special attention is paid to the critical Transport Layer, one of the most desirable layers for an adversary to attack, and cyber defense techniques at this layer. The importance of protection against "Denial of Service" attacks at the Transport Layer has been analyzed and substantiated. The importance of implementing cyber defense against the Synchronize (SYN) Flood attack has been established. This attack was executed with the set parameters, and the consequences of its impact on the system were evaluated regarding CPU resource load, website availability, and request packet loss. The available protection mechanisms are implemented individually, in combinations, and a complex form. The change in quantitative and qualitative (which is the website availability) indicators for each case of using these tools is analyzed, evaluated, and compared. Based on a laboratory experiment, it was established that for the implemented conditions of the organization's network, the attack means, and protection methods, a complex method of cyber defense proved to be the best according to the given characteristics.*

Анотація – У роботі виконано аналіз загроз на семи рівнях еталонної моделі взаємодії відкритих систем. Особлива увага приділена критичному транспортному рівню, який є одним із найбажаніших рівнів для атаки з боку зловмисника, а також методикам кіберзахисту на цьому рівні. Проаналізовано й обґрунтовано важливість захисту від атак «відмова в обслуговуванні» на транспортному рівні, встановлено важливість впровадження кіберзахисту від атаки Synchronize (SYN) Flood. Впроваджено дану атаку із встановленими параметрами, оцінено наслідки її впливу на систему за показниками завантаженості ресурсів процесора, доступності веб-сайту та втрат пакетів запиту. Реалізовано доступні механізми захисту індивідуально, в комбінаціях та в комплексному вигляді, проаналізовано, оцінено та порівняно зміну кількісних та якісного (яким є доступність веб-сайту) показників для кожного випадку використання цих засобів. На основі лабораторного досліду встановлено, що для впроваджених умов мережі організації, засобів атаки та методів захисту від неї, найкраще за наведеними характеристиками показав себе комплексний метод кіберзахисту.

Вступ

Сьогодні питання захисту інформаційно-комунікаційних систем у кіберпросторі гостро постає в умовах постійного розвитку технологій обробки, передачі та зберігання інформації, яка є одним з найцінніших активів у компаніях і підприємствах. Зважаючи на це, керівникам слід все частіше замислюватись над забезпеченням її захисту, адже викрадення, знищення або втрата доступу до критичної інформації може завдати непоправних збитків і втрату авторитету.

Одним із найгостріших і найкритичніших питань кібербезпеки є забезпечення захисту від атак типу «відмова в обслуговуванні» (Denial of Service, DoS). Щороку динаміка та потужності таких атак зростають, впроваджуються нові механізми їхньої успішної реалізації, тож доцільним є використання кращих практик щодо захисту, за-

провадження таких рішень на рівні корпоративної політики безпеки і залучення спеціалістів відповідної області, а також компаній, що надають аудит і незалежну оцінку реалізованих методів, на основі якої розроблюються рекомендації із покращення систем кіберзахисту.

В даній роботі розглянуто атаки різних рівнів еталонної моделі взаємодії відкритих систем (EMBBC) та основні засоби кіберзахисту від них. Зокрема вказано на важливість захисту від атаки «відмова в обслуговуванні» на транспортному рівні, який є критичним при встановленні з'єднання та передачі даних. Розглянуто методи захисту від атаки SYN Flood, яка є однією з найпопулярніших DoS-атак транспортного рівня, проаналізовано переваги й недоліки існуючих рішень. Впроваджено доступні механізми захисту на веб-сервері Apache із застосуванням атаки на розгорнутий веб-сайт за допомогою вбудованих інструментів операційної системи (ОС) Kali Linux. На основі аналізу та порівняння рівнів завантаженості ресурсів процесора, втрат пакетів запиту та доступності веб-сайту, використання впроваджених методів захисту окремо та в комбінаціях під час виконання атаки обґрунтовано доцільність використання для наведених умов комплексного підходу, який в межах дослідження показав найкращі результати.

I. Огляд і класифікація засобів мережної безпеки в інфокомунікаційних системах

Інфокомунікаційна система (ІКС) – сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле [1]. У сучасному світі використання ІКС є невід'ємною складовою процесу роботи з інформаційними потоками, прогрес людства фактично неможливий без новітніх інфокомунікаційних технологій. Водночас із наростанням числа інформаційних систем невпинно зростає потреба у їх захисті. Так, за дослідженнями ізраїльської компанії Check Point Research, число кібератак у тиждень на корпоративні мережі зросла на 50% у 2021 році порівняно із 2020 роком [2]. На рис. 1 зображено середню кількість щотижневих кібератак на організацію, що була опитана і працює з ІКС.

Як можна побачити з рис. 1, середня кількість щотижневих атак на організацію невпинно зростає із кожним кварталом. Зважаючи на таку тенденцію, без ефективних програм кібербезпеки організації не зможуть захистити себе від кампаній зі злому даних в ІКС, що робить їх потенційною мішенню для кіберзлочинців. Кіберзагрози можуть надходити з будь-якого рівня організації, від атак соціальної інженерії до розподілених атак типу «відмова в обслуговуванні» (Distributed Denial of Service, DDoS) та вірусів-вимагачів. Такі атаки завдають серйозних фінансових втрат організаціям. На рис. 2 зображено середні щорічні втрати компаній за 2017 та 2018 роки через кіберзлочини згідно зі звітом Accenture Security [3].

Як можна побачити з рис. 2, більшість кібератак мають приріст нанесення фінансових збитків компаніям, більший за 10% за рік, а деякі – за 15%. Крім того, кіберза-

грозами, що наносять найбільший фінансовий збиток є зловмисне програмне забезпечення (ПЗ), веб-атаки та атаки типу «відмова в обслуговуванні». Через це впровадження мережних систем кіберзахисту від таких атак є першочерговим питанням у виживанні бізнесу, адже кіберзлочинці щороку лише розвивають і вдосконалюють методики і логіку використання цих атак. Мережна безпека має враховувати впровадження рішень із кіберзахисту на усіх семи рівнях EMBBC. Кожний із рівнів має певний функціонал і відповідає за різні етапи обробки даних. Вочевидь кожний рівень може бути атакований потенційним зловмисником, тож комплексна структура є запорукою побудови ефективної системи кіберзахисту. В табл. 1 наведено основні методи кіберзахисту від загроз на усіх рівнях EMBBC.

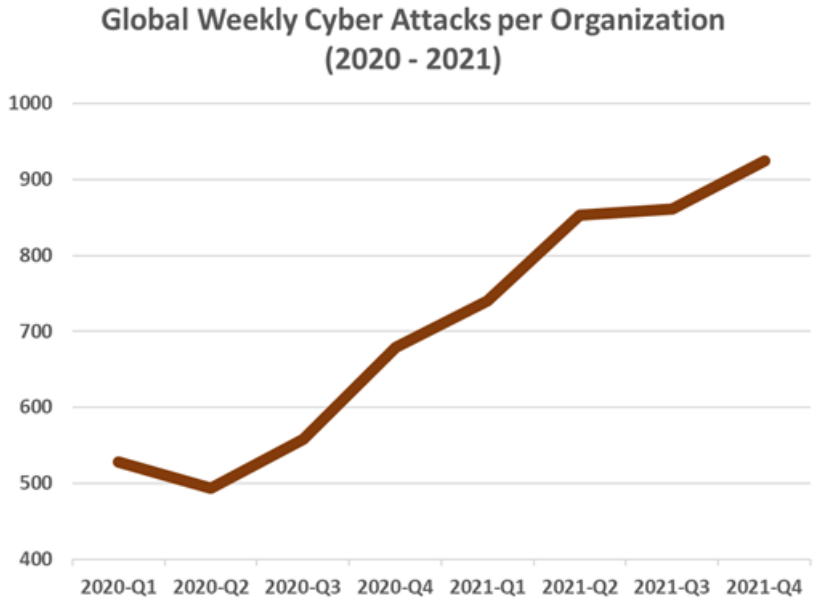

Рис. 1. Графік середньої кількості глобальних щотижневих атак на організацію за 2020-2021 роки

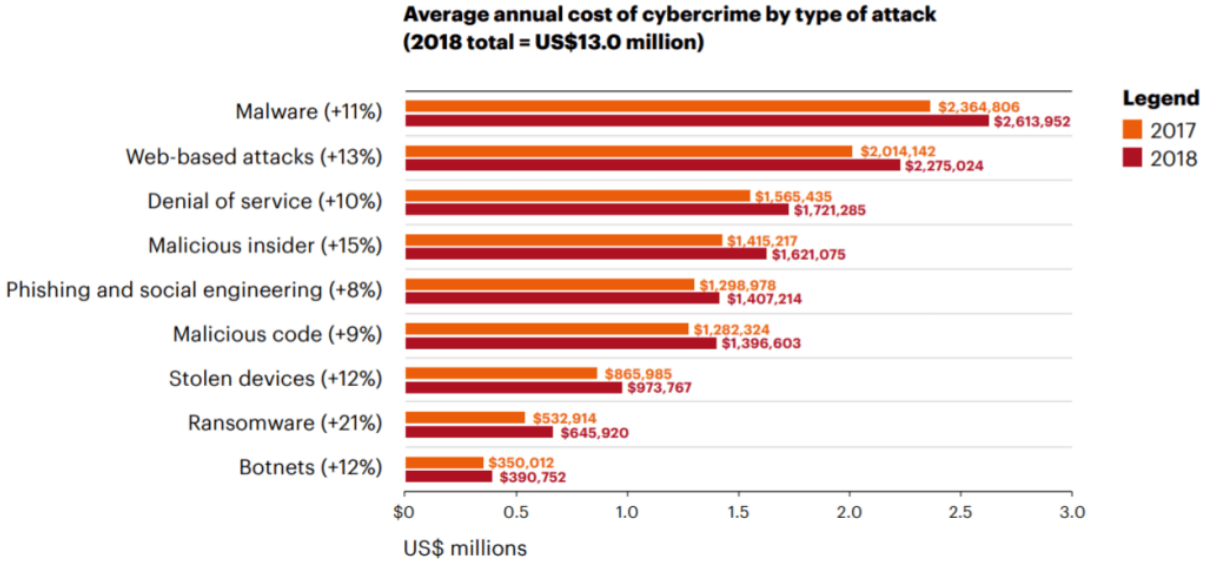

Рис. 2. Щорічні втрати компаній, розподілені по атаках

Таблиця 1. Основні загрози та засобу захисту, реалізовані на різних рівнях моделі EMBBC

Рівень EMBBC	Основні загрози	Методи кіберзахисту
Фізичний	Перешкоджання роботі обладнання, підслуховування, несанкціоноване зняття інформації	Обмеження доступу до кімнат із критичним обладнанням, використання резервних кабельних сегментів, використання мережних фільтрів і генераторів просторового зашумлення, екранування приміщення, використання FHSS та beamforming.
Канальний	DoS/DDoS, ARP-отруєння та прихована розвідка системи	Використання IDS, фільтрація трафіка і шифрування, встановлення безпеки портів, використання протоколу STP, використання VLAN, honeypot та міжмережних екранів.
Мережний	Перехоплення даних, підробка та DDoS-атаки на обладнання	Блокування невикористаних портів, служб та інтерфейсів, фільтрація та шифрування пакетів, постійне оновлення операційної системи маршрутизатора, використання брандмауера та протоколу IPSec в тунельному режимі, а не в транспортному, який є менш захищеним.
Транспортний	DDoS та сканування системи	Використання SYN cookie, блокування невикористаних портів, використання протоколу SCTP та honeypot, застосування статистичних методів виявлення DDoS [4].
Сеансовий і представницький	Несанкціонований доступ до паролів, віруси, вразливості застарілого ПЗ	Заборона несанкціонованого доступу до cookie-файлів, антивіруси, оновлення ПЗ, аудит сертифікатів SSL, зменшення невдалих спроб отримання доступу.
Прикладний	Шкідливий трафік, DDoS атаки на протоколи [5]	Комплексні рішення із моніторингом додатків, використання брандмауерів та IDS/IPS, перевірка параметрів, обмеження доступу до сервісів, використання Captcha.

Безперечно, безпекою жодного з рівнів не можна нехтувати, але особлива увага має бути приділена транспортному рівню, адже він є першим рівнем еталонної моделі на рівні хосту. Як було визначено, на цьому рівні популярними є DDoS-атаки. Особливо популярною DDoS-атакою є TCP SYN Flood. Згідно з діаграмою компанії Cloudflare [6], зображеної на рис. 3, за перший квартал 2022 року на SYN Flood припадає більше половини DoS-атак на даному рівні, що підтверджує критичну необхідність забезпечення ефективного захисту від неї.

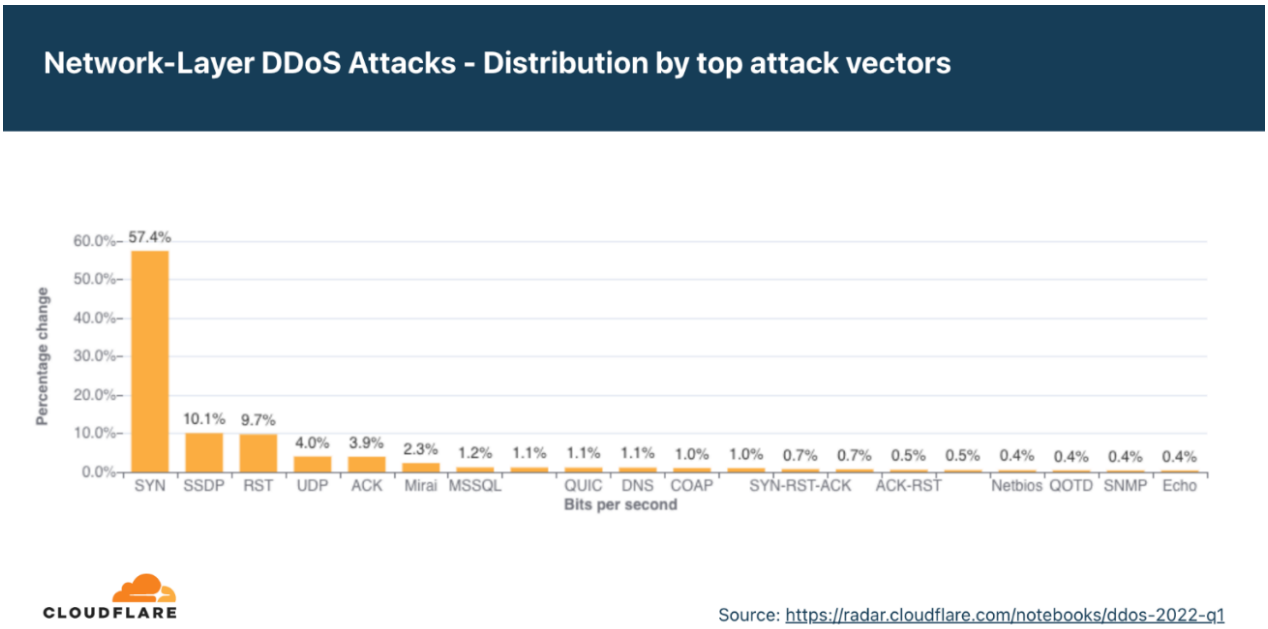

Рис. 3. Розподіл частки використання DDoS-атак мережного/транспортного рівнів

II. Аналіз методів захисту від атаки TCP SYN Flood

Сутність атаки SYN Flood полягає в тому, аби переповнити ресурси сервера шляхом заповнення пам'яті у буфері TCB (Transmission Control Block), що зберігає інформацію про «напіввідкриті» з'єднання, пакетами із прапором SYN (SYN flag), тобто прапором на встановлення з'єднання і проведення триетапного «рукостискання» TCP. Розглянемо встановлення з'єднання TCP [7] за таким «рукостисканням»:

1) Сервер перевіряє правильність TCP-прапорів, відповідаючи на них відповідно до правил протоколу, очікує на пакет із прапором SYN.

2) Коли приходить SYN-пакет, а запиту від такої адреси ще не існує, сервер відповідає пакетом із прапорами SYN та Acknowledged (ACK). На цьому етапі з'єднання переходить у буфер пам'яті протоколу TCP, має стан SYN_RECEIVED (тобто, SYN отримано) і чекає на підтвердження клієнта. Саме на цьому етапі відбувається атака SYN Flood, коли зловмисник, надсилаючи безліч SYN запитів на з'єднання, переповнює сервер кількістю пакетів, що знаходяться у стані SYN_RECEIVED, і ніколи їх не підтверджує. Коли буфер заповнюється, сервер перестає приймати легітимні запити користувачів.

3) Після надходження пакету підтвердження від клієнта із прапором ACK, сервер встановлює з'єднання, попередньо перевіряючи правильність номеру послідовності в пакеті.

Окрім переповнення буферу пам'яті сервера, він також має оброблювати кожний запит на з'єднання, надсилаючи SYN-ACK пакет у відповідь, що витрачає обчислювальні ресурси та створює навантаження на сервер. Тому можна зробити висновок, що для атаки важливо саме встановлення прапору SYN, тобто для успішної атаки використовується недолік протоколу, а саме процесу триетапного «рукостискання».

Отже, протидія атаці SYN Flood передбачає захист ресурсів системи на етапі «рукостискання» TCP. Атака TCP SYN Flood є атакою на доступність, тож головною ціллю є підвищення відмовостійкості сервера.

В табл. 2 наведено результати аналізу відомих засобів захисту від атаки TCP SYN Flood, їх переваги та недоліки.

Зазвичай найефективніша система кіберзахисту являє собою комплексне рішення, але проведення лабораторного експерименту, що включатиме в себе проведення атаки із можливістю зміни її параметрів і кількісну характеристику методів захисту на основі їх впровадження під час такої атаки, є доцільним способом оцінки ефективності впровадження комплексної системи. В даному випадку проведення дослідження можливе із доступними в ОС Linux і відкритими засобами захисту від SYN Flood, якими є обробка черги з'єднань, SYN Cookie та фільтрація пакетів. Для прийняття рішення щодо раціональності їхнього використання як результативних механізмів захисту важливо впровадити ці механізми та проаналізувати їхні показники в усіх можливих варіаціях, тобто в незалежному використанні один від одного, комбіновано попарно та у комплексному вигляді. Доступними та наочними показниками, що мають бути оцінені та порівняні, є використання ресурсів процесора під час атаки, частка втрат пакетів запиту (кількісні показники) та доступність ресурсів системи (якісний показник). Саме на основі цих, отриманих під час експерименту даних, необхідно будувати висновок щодо доцільності використання наведених рішень, зокрема, і комплексного підходу.

III. Імплементація та порівняння методів захисту від SYN Flood атаки

Об'єктом захисту було обрано веб-сервер з розгорнутим веб-сайтом, який надає доступ до нього віддаленим користувачам. Веб-сервером обрано Apache Web Server, розгорнутого на віртуальній машині із ОС Ubuntu та одним ядром процесора. Оскільки для встановлення з'єднання використовується протокол TCP, то загрози, пов'язані із порушенням роботи цього протоколу, є критичними для компанії та потребують реалізації засобів кіберзахисту, в даному випадку від атаки SYN Flood.

Атака проводилась із використанням утиліти `hping3`, вбудованої в ОС Kali Linux, яку розгорнуто на іншій віртуальній машині. Для проведення атаки виконувалась наступна команда – `sudo hping3 -S -p 80 --flood --rand-source 192.168.1.104`, в якій використано наступні параметри:

- `sudo` – виконання команди із правами root-користувача;
- `hping3` – використання утиліти `hping3` для виконання атаки SYN Flood;
- `-S` – встановлення прапору SYN в пакетах;
- `-p 80` – пакети надсилаються на порт 80;
- `--flood` – пакети надсилаються із максимальною швидкістю;
- `--rand-source` – генерування випадкових IP адрес;
- IP-адреса жертви, в даному випадку 192.168.1.104 є IP-адресою веб-серверу.

Таблиця 2. Показники системи при атаці та реалізованих методах захисту

Метод захисту	Переваги	Недоліки
SYN Cookie	Під час переповнення буферу, інформація про нові підключення оброблюється окремо, не витрачаючи місце у буфері, а старі запити не відкидаються.	Втрата параметрів TCP, що передаються в пакеті із прапором SYN, неможливість повторної передачі пакету SYN-ACK клієнту. Крім того, обчислення хеш-функцій також витрачає процесорні ресурси системи.
Обробка пакетів в черзі «напіввідкритих» з'єднань [8]	Дозволяє зменшити час перебування пакетів в стані очікування, що збільшить кількість пакетів, які оброблюються, і полегшить приймання запитів користувачів.	Є лише допоміжним заходом для протистояння атаці SYN Flood, адже атака зазвичай відбувається із значною швидкістю передачі пакетів SYN.
SYN Proxy [9]	Основний сервер не приймає навантаження, натомість це робить SYN Proxy, який надсилає серверу вже справжній, а не зловмисний запит на з'єднання.	Проксі сам має використовувати методи захисту, наприклад SYN Cookie, для встановлення з'єднання. Сам проксі-сервер може стати потенційною ціллю атаки.
SYN Authentication [10]	Даний метод не зберігає ніякої інформації про з'єднання і нічого не оброблює, натомість лише використовує правила протоколу TCP.	Користувач має двічі надсилати запити на з'єднання, що збільшує час на його встановлення.
Фільтрація пакетів із прапором SYN	Дозволяє відкидати пакети, шлях до яких не визначено, як зазвичай і відбувається.	Зловмисник, який має під контролем хости в локальній мережі або виконує атаку із власної машини, повністю обходить фільтрацію пакетів. У такому випадку використовувати цей метод недоцільно.
Кешування запитів (SYN Cache) [11]	Під час переповнення буферу, як і у випадку SYN Cookie, нові підключення не заміняють собою старі, які при цьому оброблюються, і з'єднання легітимних користувачів не відкидаються.	Витрачаються ресурси на зберігання хеш-функцій та їхнє обчислення.
Алгоритм «Три лічильники» [12]	Виокремлена обробка пакетів із використанням їхнього випадкового відкидання дозволяє заборонити з'єднання при надходженні великого числа пакетів з однієї адреси.	Атака SYN Flood зазвичай відбувається з різних IP-адрес, які не надсилають один запит багато разів, що робить метод неефективним. Також у даному методі наявна інформація про з'єднання в буфері, який може бути переповнений.

Дані параметри є стандартними для проведення цієї атаки. Зловмисником можливе встановлення спеціальних налаштувань, як-от, наприклад, максимальний розмір сегменту, але це може призвести до легшої протидії атаці шляхом виявлення нестандартних шаблонів та їхньої фільтрації.

В процесі дослідження було використано наступні інструменти моніторингу:

1) Мережний аналізатор *Wireshark*. Він використовується для наочного відображення й аналізу пакетів, їхнього вмісту, IP-адрес, міток часу тощо.

2) Утиліта *top*. Дана утиліта є вбудованою в ядро Linux і використовувалась для відображення працюючих процесів у системі і використання ними ресурсів центрального процесора (у відсотках).

3) Утиліта *ping*. Використовується для перевірки з'єднання та доступності сервера за допомогою запиту протоколу міжмережних керуючих повідомлень (Internet Control Message Protocol, ICMP), тобто так званих «луно-запитів» або «echo request».

4) Веб-браузер *Firefox*. Цей браузер є вбудованим за замовчуванням в ОС Kali Linux, він використовувався для перевірки доступності веб-сайту.

Перш за все, атаку було проведено без впровадження методів захисту із використанням кількох терміналів для ефективнішого результату. На рис. 4 зображено результат надсилання SYN-пакетів веб-серверу Apache (флудінг пакетами), їх відображено у програмі Wireshark. Як можна побачити з рис. 4, на сервер надсилаються пакети SYN, і на кожен сервер має відповісти. У полі Source IP-адреси відправника, тобто машини зловмисника, є різними, оскільки була виставлена опція генерування випадкових IP-адрес. Крім того, номер послідовності (sequence number), вказаний праворуч у параметрах, завжди нульовий, тобто кожен SYN-пакет є першим від кожного підробленого користувача і сервер має оброблювати кожний з них.

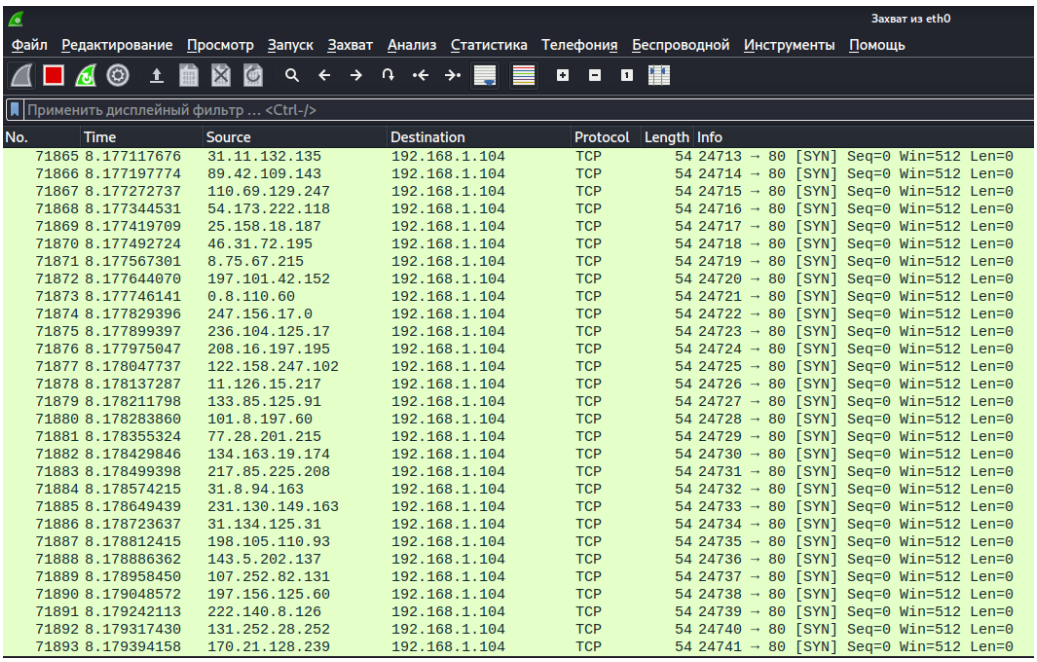

Рис. 4. Флудінг веб-серверу пакетами SYN

На рис. 5 зображено частину від усіх з'єднань, що очікують і перебувають у стані SYN_RECEIVED, тобто це «напіввідкриті» з'єднання.

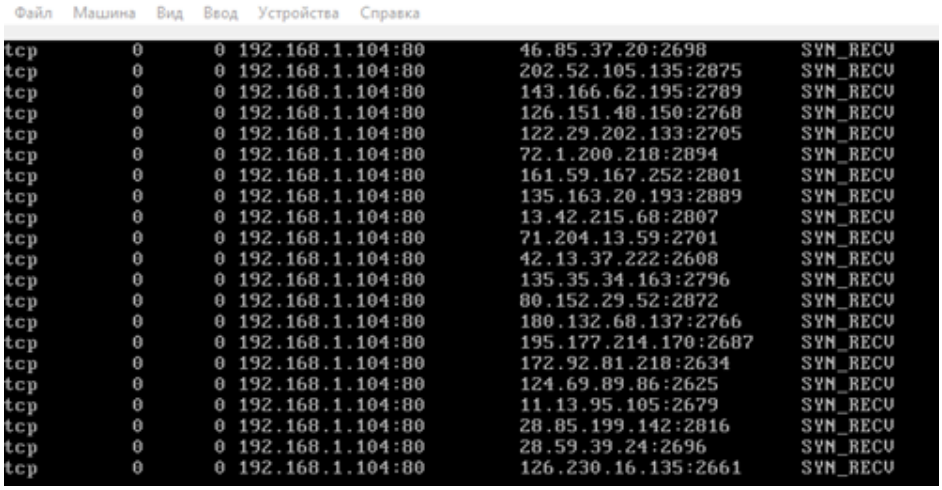

Рис. 5. Заповнений буфер пам'яті для «напіввідкритих» з'єднань

Як можна побачити з рис. 5, «напіввідкриті» з'єднання зберігаються, як і їхні IP-адреси, що згенерував зловмисник, і мають стан SYN_RECEIVED. Крім того, завантаженість процесорних ресурсів сягнула 100% під час виконання атаки.

Результатом атаки стала неможливість з'єднання з веб-сайтом на сервері. На рис. 6 зображено працюючу головну сторінку та повідомлення про помилку підключення до сайту під час атаки.

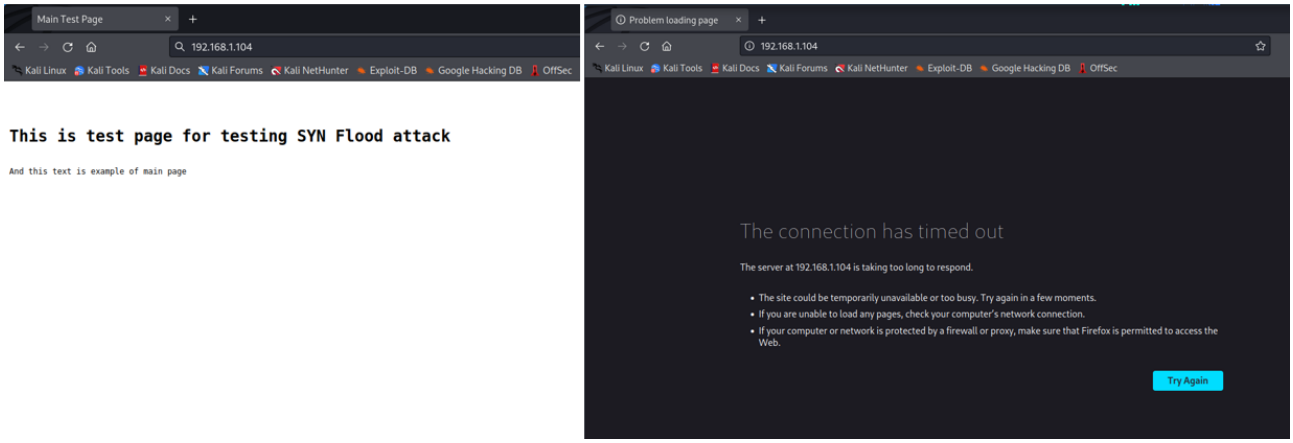

Рис. 6. Працююча сторінка та повідомлення браузера про помилку підключення під час атаки

На рис. 7 зображено результат атаки на сервер без засобів захисту за кількістю прийнятих ICMP-пакетів, тобто відповідей на «луно-запити». В даному випадку і в подальших вимірюваннях кількість запитів ICMP сягатиме приблизної кількості у 40 пакетів (на рис. 7 можна спостерігати пакети за їхнім порядковим номером, що представлений значенням icmp_seq), деяка розбіжність зумовлена тим, що програма не відображає пакети, які відкидаються.

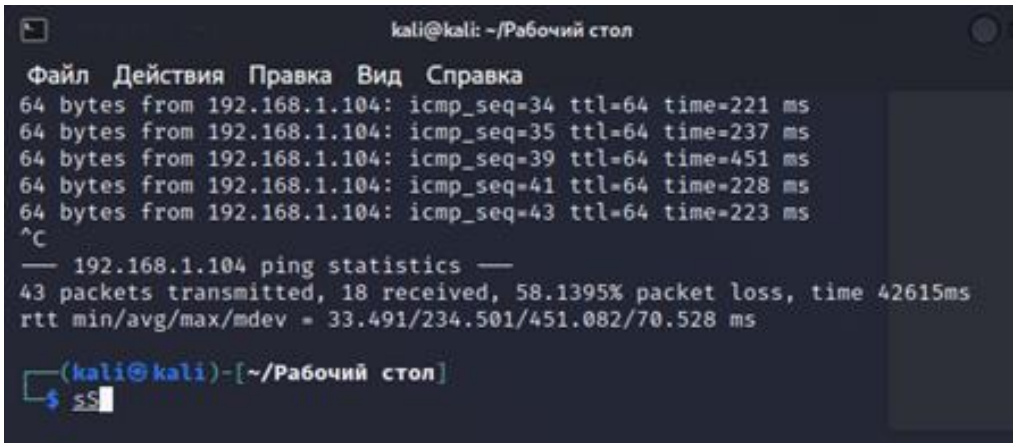

Рис. 7. Результат атаки за кількістю відповідей на ICMP-запити

Як можна побачити з рис. 7, більше половини (приблизно 58% пакетів) було втрачено, і вони не отримали відповіді. Також можна спостерігати час між відправленням запиту й отриманням відповіді, який для деяких пакетів більший за 250 мс, хоча це значення під час звичайної роботи системи зазвичай не перевищує 10 мс. Значне завантаження і втрати унеможливлюють роботу серверу, тож необхідно впроваджувати механізми захисту, що знизять ці показники і зроблять сервер доступним під час атаки.

У ОС Linux SYN Cookie реалізовано за допомогою параметру `net.ipv4.tcp_syncookies=2`. Параметр «2» означає, що SYN cookies вмикаються одразу, на відміну від параметру «1», що запускає їх лише тоді, коли буфер переповнюється. На рис. 8 зображено графік використання процесорних ресурсів у разі атаки, коли використовуються SYN Cookie. Веб-сервер хоч і під навантаженням, але дає змогу підключення справжньому користувачу. Незважаючи на це, таке навантаження є досить критичним, і виконувати будь-які інші дії на такій машині стає майже неможливим.

Як можна побачити з рис. 8, використання процесорних ресурсів при застосуванні SYN Cookies частково перевищує 60%, а середнє значення – 52,7%. Такі значення є вкрай високими для обробки запитів користувачів, тобто система є надто навантаженою. Кількість «луно-запитів», які були втрачені під час атаки із реалізацією цього методу захисту, сягнула 25%, що безперечно є кращим показником ніж без використання SYN Cookie, але, все ж таки, чверть втрачених пакетів є незадовільним результатом. Навантаження на ресурси сервера є також важливим чинником затримки з'єднання та запитів, який вплинув на відсоток пакетів, що не отримали відповідь.

Рис. 8. Графік використання процесорних ресурсів під час атаки з використанням SYN cookies

Розглянемо реалізацію методу обробки черги з'єднань. Для реалізації цієї атаки було реалізовано наступні команди:

- `sysctl -w net.ipv4.tcp_max_SYN_backlog=1000` – кількість з'єднань, що є «напіввідкритими» і зберігаються в буфері дорівнює 1000;
- `sysctl -w net.ipv4.tcp_synack_retries=3` – зменшення кількості повторних спроб підключення до трьох.

На рис. 9 показано навантаження на процесор при застосуванні цих налаштувань із різними значеннями розміру буфера та кількості повторних спроб підключення. Результатом атаки із усіма наведеними параметрами стала відсутність доступу до веб-серверу через веб-браузер.

Як можна побачити з рис. 9, суттєвої різниці при зміні параметрів не спостерігається. Для кожного випадку використання параметрів було обчислено наступні середні значення використання ресурсів процесора:

- обробка черги з'єднань (backlog=1000, retries=3) – 48,7%;
- обробка черги з'єднань (backlog=3000, retries=2) – 48,8%;
- обробка черги з'єднань (backlog=5000, retries=1) – 47,2%.

Середні значення мають незначну розбіжність, і усі вони є критично високими. Даний метод за середнім значенням використання процесорних ресурсів не суттєво відрізняється від такого ж значення у механізмі SYN Cookie.

Для кожної комбінації параметрів, наведеної на рис. 9, було проведено запити ICMP під час атаки. В табл. 3 наведено результати аналізу втрат пакетів із «луно-запитами». Як видно з табл. 3, обробка черги з'єднань навіть при різних параметрах не дала значного результату, наведений відсоток втрат приблизно на 10% відрізняється від такого ж значення при відсутності засобів захисту під час атаки.

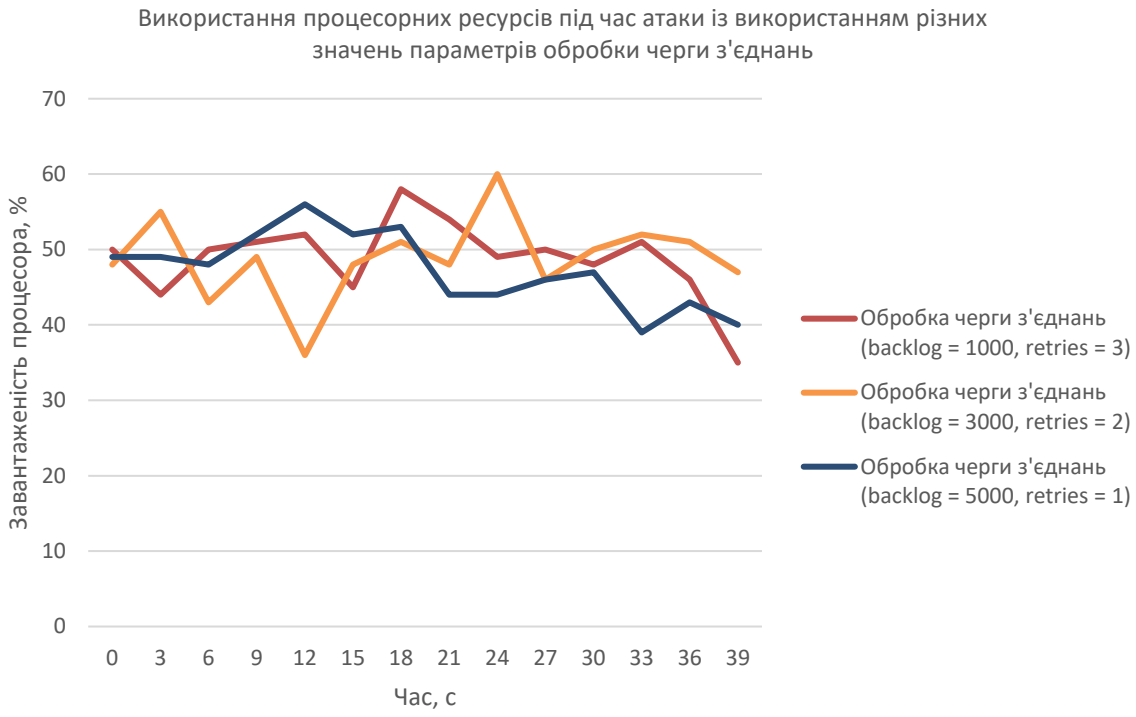

Рис. 9. Графік використання процесорних ресурсів під час атаки з обробкою черги з'єднань

Порівняно з відповідним значенням при використанні SYN Cookie цей метод значно програє в ефективності. Такі значення є вкрай незадовільними, адже майже не впливають на систему під час атаки, тобто не запроваджують той захист, що є необхідним. Для подальшого порівняння використовуватиметься значення результатів обробки з'єднань із параметрами backlog=5000 та retries = 1.

Таблиця 3. Результати втрати пакетів із луно-запитами із використанням різних параметрів обробки черги з'єднань

Параметр обробки черги з'єднань	Відсоток втрачених пакетів під час атаки
backlog = 1000, retries = 3	46,1%
backlog = 3000, retries = 2	44,4%
backlog = 5000, retries = 1	41,6%

Розглянемо реалізацію методу на основі фільтрації пакетів. В системі, що використовується, за фільтрацію відповідають параметри `net.ipv4.conf.rp_filter` та `net.ipv4.default.rp_filter`, обидва отримують значення «1».

На рис. 10 зображено графік завантаженості процесора під час атаки із використанням фільтрації відправників. Веб-сервер в результаті не втратив доступність для користувача.

Рис. 10. Графік використання процесорних ресурсів під час атаки із використанням фільтрації пакетів

Як можна побачити з рис. 10, значення завантаженості процесора сягає 50% і тримається у проміжку між 30% та 50% завантаженості. Середнє значення завантаженості становить 38,8%, що також є значною часткою, але значно меншою у порівнянні з SYN Cookie та обробкою черги з'єднань, тобто за даним показником метод фільтрації показує найкращий результат.

Частка втрачених пакетів перевірки з'єднання для даного методу сягнула 21,4%, що значно менше за відсоток, який можна побачити при відсутності механізмів захисту та при використанні обробки черги з'єднань, і становить невелику різницю порівняно із частиною втрат при використанні SYN Cookies. Хоча серед реалізованих методів захисту фільтрація пакетів дала найкращий результат, але частина втрат, як і навантаження, все одно є значними і робити висновок про те, що слід використовувати лише даний метод, який забезпечить найкращий результат у разі атаки, недоцільно.

Зважаючи на припущення щодо ефективності комплексної системи захисту, доцільним є дослідити та підтвердити або спростувати таке припущення. Перш за все, дослідження проведено із попарними комбінаціями реалізованих методів. Для усіх комбінацій веб-сайт не втратив доступність через веб-браузер.

На рис. 11 показано рівень використання процесорних ресурсів для кожної пари застосованих засобів захисту.

Рис. 11. Використання процесорних ресурсів із застосуванням комбінацій методів

Як можна побачити з рис. 11, SYN Cookie та фільтрація пакетів показали найкращий результат. Методи мають такі середні значення використання ресурсів процесора:

- SYN Cookie та обробка черги з'єднань – 33%;
- SYN Cookie та фільтрація пакетів – 23%;
- обробка черги з'єднань та фільтрація пакетів – 35%.

Судячи з отриманих середніх значень, використання методів захисту у парах дало кращі показники ніж при їхньому використанні окремо. Найкращий результат за середнім значенням має SYN Cookie та фільтрація пакетів: більше ніж на 10% нижчий за найкращий показник окремого методу, що становив 38,8%. Інші ж комбінації методів показали незначну різницю, порівняно з ним – приблизно 3-5%.

Далі було проведено дослідження з аналізу втрат пакетів. Значення рівня втрат пакетів ICMP отримало наступний розподіл:

- для SYN Cookie та обробки черги з'єднань – 25%;
- для SYN Cookie та фільтрації пакетів – 19,7%;
- для обробки черги з'єднань та фільтрації пакетів – 22,3%.

Таким чином, наведені значення втрат при попарному використання значно змінились, порівняно із методом обробки черги з'єднань, і несуттєво, порівняно із іншими реалізованими методами. Незважаючи на це, найкращий показник і тут дала комбінація механізмів SYN Cookie та фільтрації пакетів. Цей показник на даному етапі є найнижчим серед усіх досліджених, тобто попарна реалізація дала, хоч і незначний, але виграш у ефективності.

На рис. 12 наведено результати аналізу використання ресурсів при усіх реалізованих методах на одному графіку, а також використання ресурсів процесора, коли атака не відбувається. Під час атаки веб-сайт не втрачав свою доступність.

Рис. 12. Використання процесорних ресурсів із використанням трьох впроваджених методів захисту

Як видно з рис. 12, показник використання ресурсів при повній комплексній системі сягає максимум 35% і опускається майже до рівня, коли атака не відбувається. Середнє значення у даному випадку становить 17%. Такий показник використання ресурсів процесора є найкращим серед усіх досліджень, тож за даним показником повна комплексна система є найефективнішим рішенням.

Використання комплексної системи рішень призвело до найнижчих втрат запитів ICMP (близько 10%), що майже в 6 разів менше за такий же показник у разі відсутності засобів захисту.

При реалізації атаки наведені значення щодо рівня використання ресурсів процесора та втрат пакетів є задовільними, адже вплив на систему під час протидії атаці майже відсутній. Отже, припущення про найкращу ефективність саме комплексної системи підтвердилось, а показники, отримані при реалізації окремих методів, було покращено за рахунок комплексного підходу. У табл. 4 наведено структуровані результати проведеного експерименту. Як можна побачити з табл. 4, найкращим є підхід, при якому використовуються усі реалізовані механізми в комплексі. За середнім значенням завантаженості ресурсів процесора комплексне рішення є меншим майже у 6 разів за найбільше значення, яке система має під час атаки без впровадження засобів захисту, і у майже 1,5 рази менше за другий найменший показник комбінованого рішення із використанням SYN Cookie та фільтрації пакетів. Схожі результати можна спостерігати і шляхом аналізу втрат пакетів ICMP, яких майже у 6 разів менше при використанні комплексного рішення порівняно із втратами за відсутності методів захисту та майже в 2 рази менше за рішення із реалізацією фільтрації пакетів та SYN Cookie.

Таблиця 4. Показники системи при атаці та реалізованих методах захисту

№ з.п.	Засіб захисту	Середнє значення використання ресурсів процесору, %	Доступність веб-сайту через веб-браузер	Втрата пакетів запиту, %
1	-	100	Ні	58
2	SYN Cookie	52,7	Так	25
3	Обробка черги з'єднань	47,2	Ні	41,6
4	Фільтрація пакетів	38,8	Так	21,4
5	SYN Cookie та обробка черги	33	Так	25
6	SYN Cookie та фільтрація пакетів	23	Так	19,7
7	Обробка черги та фільтрація пакетів	35	Так	22,3
8	Усі методи разом	17	Так	10

Доступність веб-сайту було втрачено лише при відсутності застосування методів захисту та при використанні рішення щодо обробки черги з'єднань. На рис. 13 зображено діаграму, що показує у скільки разів кількісні показники кожного із варіантів захисту від SYN Flood є більшими за показники комплексної системи. Методи захисту зазначено згідно з нумерацією за порядком, наведеною в табл. 4.

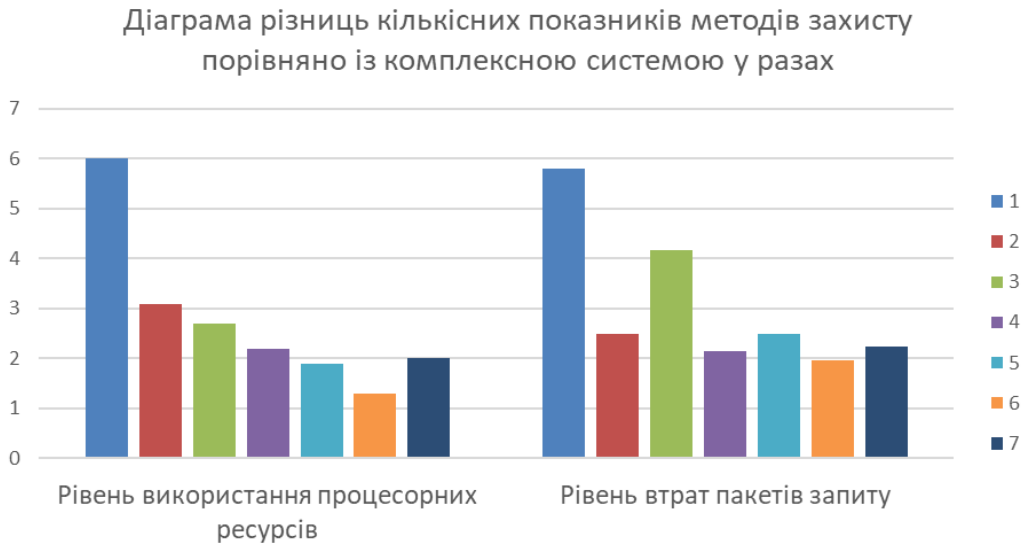

Рис. 13. Діаграма різниць кількісних показників методів захисту порівняно із комплексною системою (у разах)

Як можна побачити з рис. 13, комплексна система, розглянута в роботі, дійсно покращує кіберзахист від SYN Flood і виграє за показниками майже у кожного іншого

методу мінімум у 2 рази. Звичайно, доцільним є розширення системи кіберзахисту за рахунок інших, не реалізованих у межах даної роботи рішень, та оцінки їхніх якісних і кількісних характеристик. Крім того, дієва система захисту має враховувати не тільки функціонал транспортного, але й інших рівнів моделі EMBBC, розглядати інші види атак і методи захисту від них.

Висновки

Було проведено аналіз існуючих кіберзагроз в ІКС на транспортному рівні EMBBC. Було встановлено, що однією з найбільших загроз на усіх рівнях, і транспортному зокрема, є атаки типу «відмова в обслуговуванні», що направлені на втрату доступності ресурсів системи жертви. Обґрунтовано доцільність впровадження захисту на даному рівні від однієї з найпопулярніших DDoS-атак, а саме атаки TCP SYN Flood, доля якої серед DDoS-атак транспортного рівня становить 57,4% [6]. Проаналізовано відомі рішення щодо кіберзахисту від SYN флудінгу, розглянуто принцип їхньої роботи й ідеї, які вони в собі несуть, їхні переваги та недоліки.

У роботі реалізовано засоби захисту, які є доступними та вбудованими в ОС Linux на веб-сервері Apache, що встановлений на Ubuntu, проведено атаку за допомогою вбудованого в Kali Linux інструменту `hping3` та проаналізовано її результати. Проведено аналіз результатів ефективності вбудованих засобів захисту за показниками доступності веб-сайту під час атаки, відсотку використання процесорних ресурсів і втрат «луно-запитів», зроблено висновок щодо доцільності використання наведених механізмів кіберзахисту. За результатами лабораторного експерименту найефективнішим механізмом стала комплексна система, що містила усі реалізовані методи. Показник використання процесорних ресурсів у такої системи складав 17%, що є меншим майже у 6 разів за такий же показник при відсутності методів захисту та майже у 1,5 рази меншим ніж у другого за ефективністю рішення, реалізованого із використанням SYN Cookie та фільтрації пакетів. Аналогічно, комплексне рішення призводило до втрат на рівні 10%, що є майже у 6 разів нижчим за втрати при відсутності захисту та майже у 2 рази нижчим за рівень втрат порівняно із рішенням на основі фільтрації пакетів та SYN Cookie. Водночас доступність веб-сайту через браузер не постраждала, тобто було підтверджено ефективність такої системи.

Список літератури

1. Верховна Рада України (1994), Закон України “Про захист інформації в інформаційно-комунікаційних системах”, режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення 04.10.2022).

2. Check Point Blog (2021), “Check Point Research: Cyber Attacks Increased 50% Year over Year”, available at: https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/ (last accessed 04.10.2022).

3. The Cost Of Cybercrime (2019), “Ninth Annual Cost Of Cybercrime Study”, available at: https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf (last accessed 04.10.2022).

4. *Радівілова, Т.А., Тавалбех, М.Х., Глушаєв, Д.Я., Заіка, М.В.* (2019), "Виявлення DDoS атак статистичними методами", Третя міжнародна науково-технічна конференція "Комп'ютерні та інформаційні системи і технології", Збірник наукових праць, Харків: ХНУРЕ, С. 137. **URL**: http://openarchive.nure.ua/handle/document/8540.

5. *Shapovalova, A., Yevdokymenko, M.* (2019), "Investigation of the Impact of HTTP DoS Attacks on the Cloud Web Server", Proceedings of the International Conference on Natural Science and Technology (ICONAT 2019), Kharkiv-Ukraine, P. 19–26.

6. The Cloudflare Blog (2022), "DDoS Attack Trends for 2022 Q1", available at: https://blog.cloudflare.com/ddos-attack-trends-for-2022-q1/ (last accessed 10.10.2022).

7. Global Information Assurance Certification Paper (2002), "Syn cookies, an exploration", available at: https://www.giac.org/paper/gsec/2013/syn-cookies-exploration/103486 (last accessed 03.10.2022).

8. *Eddy, W.* (2007), TCP SYN Flooding Attacks and Common Mitigations, RFC 4987. **URL**: https://www.rfc-editor.org/rfc/rfc4987.

9. *Eddy, W.* (2006), "Defenses against TCP SYN Flooding attacks", The Internet Protocol Journal, No. 9(4), P. 2–16.

10. *Villing, J.* (2019), "Investigating TCP SYN Flood Mitigation Techniques in the Wild", Seminar IITM WS 18/19, Network Architectures and Services, P. 67–70. **DOI**: https://doi.org/10.2313/NET-2019-06-1_14.

11. *Lemon, J.* (2002), "Resisting SYN Flood DoS Attacks with a SYN Cache", Proceedings of the BSDCon 2002, P. 89–98. **URL**: https://www.usenix.org/legacy/publications/library/proceedings/bsdcon02/full_papers/lemon/lemon_html/index.html.

12. *Gavaskar, S., Surendiran, R., Ramaraj, E.* (2010), "Three counter defense mechanism for TCP SYN flooding attacks", International Journal of Computer Applications, No. 6(6), P. 12–15. **DOI**: https://doi.org/10.5120/1083-1399.