ISSN 2076-1546
УДК 004.4 DOI: 10.46972/2076-1546.2024.27.05

В. В. Охрімчук, І. А. Охрімчук

АНАЛІЗ ЗАСОБІВ МОДЕЛЮВАННЯ МЕРЕЖ ЩОДО МОЖЛИВОСТІ ЇХ ВИКОРИСТАННЯ ДЛЯ ПРАКТИЧНОЇ ПІДГОТОВКИ ФАХІВЦІВ ІЗ КІБЕРБЕЗПЕКИ

Незважаючи на наявні системи інформаційної безпеки, ключовим аспектом ефективного кіберзахисту залишається рівень підготовки персоналу, відповідального за кібербезпеку. Сьогодні підготовка фахівця з кібербезпеки повинна ґрунтуватися на всебічному вивченні сучасних інформаційних технологій, механізмів і шаблонів проведення кібератак, способів протидії їм та включати як теоретичну, так і практичну складові. Встановлено, що найбільш поширеною практикою у провідних навчальних та наукових установах світу й України щодо здійснення практичної підготовки фахівців із кібербезпеки є створення та розгортання складних програмно-апаратних комплексів – кіберполігонів, але це вимагає витрати значних ресурсів. Тому програмні засоби емуляції і симуляції комп'ютерних мереж стають альтернативою отримання початкових практичних навичок із кібербезпеки.

У статті проаналізовано три найпопулярніші безкоштовні інструменти для симуляції та емуляції комп'ютерних мереж: Cisco Packet Tracer, GNS3 і EVE-NG – щодо можливості їх використання для практичної підготовки фахівців із кібербезпеки. У результаті аналізу встановлено, що Cisco Packet Tracer, орієнтований на користувачів-початківців, забезпечує симуляцію мережевих пристроїв виключно компанії Cisco, дозволяє налаштовувати базові протоколи та відпрацьовувати основи кіберзахисту. GNS3 за своїм функціоналом дещо переважає Cisco Packet Tracer, емулює реальні образи операційних систем і підтримує роботу з багатьма вендорами мережевих пристроїв, що робить його корисним для складних навчальних завдань. Крім того, GNS3 надає можливість відтворювати сценарії кібератак, а інтегрований мережевий аналізатор Wireshark дозволяє здійснювати моніторинг трафіку та аналізувати вплив кібератаки на систему. У свою чергу, EVE-NG – потужна платформа для емуляції мереж, яка за своїми функціональними можливостями дуже близька до GNS3. Вона також забезпечує широку підтримку обладнання і надає можливості для розгортання складних мережевих топологій. Проте основною особливістю EVE-NG є її клієнт-серверна архітектура, що дозволяє багатокористувацький формат роботи.

Отже, Cisco Packet Tracer, GNS3 та EVE-NG доповнюють один одного в процесі отримання практичних навичок із кібербезпеки на різних рівнях навчання. Використання всіх трьох інструментів у навчальних програмах дозволить формувати комплексні знання і практичні навички, необхідні для ефективного захисту критичної інформаційної інфраструктури від кібератак.

***Ключові слова**: кібербезпека; кіберзахист; кібератака; емулятор; симулятор; віртуалізація; Cisco; GNS3; EVE-NG.*

Постановка проблеми в загальному вигляді. У сучасному світі, де інформаційні технології інтегровані в усі сфери життя, кібербезпека є ключовим пріоритетом для державних установ, бізнесу та приватних осіб. Такі щоденні кіберзагрози, як: кібератаки на комп'ютерні мережі, викрадення та шифрування даних, а також використання шкідливого програмного забезпечення (ПЗ) – вимагають удосконалення чинних і розроблення новітніх механізмів кіберзахисту. Однак, незважаючи на досягнуті результати фахівців та науковців у галузі кібербезпеки зі створення систем інформаційної безпеки, ключовим аспектом ефективного кіберзахисту залишається рівень підготовки персоналу, відповідального за кібербезпеку.

Сьогодні підготовка фахівця з кібербезпеки повинна ґрунтуватися на всебічному вивченні сучасних інформаційних технологій, механізмів та шаблонів проведення кібератак, способів протидії їм та включати як теоретичну, так і практичну складові.

У світі є достатньо велика кількість установ, що займаються моніторингом, класифікацією та накопиченням відомостей про кіберзагрози. Кожна така організація надає, як правило, відкритий доступ до своїх власних баз кіберзагроз, тому отримання теоретичних знань про них та шляхи їх усунення в сучасному інформаційному суспільстві не є проблемою.

Проте досить гостро постає питання отримання практичних навичок. Передусім це пов'язано із великим різноманіттям топологій комп'ютерних мереж, їх функціональним призначенням, особливостями комутації та маршрутизації в них пакетів, наявністю значної кількості як мережевого, так і кінцевого обладнання з різними операційними системами (ОС) тощо. Тому для відпрацювання практичних питань необхідно створювати мініатюрні моделі реальних комп'ютерних мереж, що з урахуванням викладеного вище є важко реалізовуваним процесом. Інший шлях – використовувати програмні засоби симуляції та емуляції роботи комп'ютерних мереж.

Аналіз останніх досліджень і публікацій. У результаті аналізу доступних джерел [1–6] встановлено, що найбільш поширеною практикою в провідних навчальних і наукових установах світу та України щодо здійснення практичної підготовки фахівців із кібербезпеки є створення й розгортання складних програмно-апаратних комплексів – кіберполігонів. Вони дозволяють проводити наукові дослідження в галузі кібербезпеки, підвищувати ефективність практичної підготовки фахівців із кібербезпеки, відпрацьовувати питання кіберзахисту об'єктів із критичною інформаційною інфраструктурою, а також проводити дво- й багатосторонні навчання та тренування з елементами відпрацювання дій в умовах комплексних кібервпливів.

Незважаючи на всі позитивні внески від кіберполігонів в практичну підготовку фахівців із кібербезпеки, їх створення потребує значних фінансових витрат, а також вимагає наявності висококваліфікованого персоналу для підтримки. Крім того, оскільки кіберполігон, як зазначалося раніше, – це складний програмно-апаратний комплекс, то допуск до практичної роботи на ньому слід здійснювати тільки після отримання базових практичних навичок із забезпечення кібербезпеки. А розгортання таких комплексів для отримання базових практичних навичок є не тільки недоцільним, а й не цільовим. Тому й постає питання, де майбутньому фахівцю отримати первинні практичні навички.

Вирішити цю проблему можливо за допомогою програмних засобів симуляції та емуляції комп'ютерних мереж.

Формулювання завдання дослідження. Сьогодні системні адміністратори, мережеві інженери для отримання практичних навичок із налаштування та адміністрування мереж використовують спеціалізовані програмні засоби емуляції та симуляції роботи комп'ютерних мереж. У світі є достатньо велика кількість вендорів спеціалізованого ПЗ, призначеного для отримання первинних навичок із налаштування мереж та управління ними. Проте далеко не всі вони можуть бути використані для практичного навчання фахівців із кібербезпеки.

Метою статті є аналіз найбільш поширених симуляторів та емуляторів комп'ютерних мереж, оцінювання їх функціональних можливостей, визначення переваг і недоліків, а також встановлення можливості їх використання для отримання первинних практичних навичок із забезпечення кібербезпеки.

Виклад основного матеріалу. Усе спеціалізоване ПЗ, яке використовується для віртуалізації роботи мереж, можна поділити на два типи: симулятори та емулятори [7, 8].

Емулятори – це ПЗ, яке дозволяє імітувати поведінку ОС та обладнання реального пристрою. Вони зазвичай набагато повніші й точніші порівняно із симуляторами, але часто вимагають більше ресурсів комп'ютера. Емулятори використовують для тестування застосунків на різних платформах (наприклад, *Android* на *Windows* або *iOS* на *macOS*). Емулятори можуть бути повільнішими через додатковий шар абстракції, але вони зазвичай надійніші для перевірки реальної взаємодії програм з ОС [8, 9].

Симулятори – це ПЗ, яке також дозволяє імітувати поведінку ОС, але вони, як правило, працюють на вищому рівні – програми. Вони зазвичай менш ресурсоємні, але можуть не забезпечувати 100% точності порівняно з реальними пристроями.

Симулятори частіше використовують для тестування застосунків на різних версіях ОС та роздільних здатностях екрана. Вони зазвичай швидші внаслідок прямішого доступу до ресурсів комп'ютера, але менш точні, оскільки не імітують повністю реальних умов роботи на пристрої [8, 9].

Незважаючи на велике різноманіття наявних на ринку програмних засобів моделювання комп'ютерних мереж, для порівняльного аналізу ми обрали найбільш популярні на сьогодні безкоштовні симулятори та емулятори: *Cisco Packet Tracer, GNS*3 та *EVE-NG*. Розглянемо кожний із них окремо, визначимо особливості їх використання, переваги та недоліки.

Cisco Packet Tracer (*CPT*) – це програмний симулятор роботи мережі, розроблений компанією *Cisco,* який дозволяє користувачам створювати мережеві топології та імітувати сучасні комп'ютерні мережі [10, 11]. Цей програмний продукт широко використовують інструктори та слухачі мережевих академій *Cisco* в усьому світі. Основне призначення *CPT* – допомогти вивчити принципи побудови мереж, а також розвинути практичні навички роботи виключно з мережевим обладнанням *Cisco*.

Ця програма має інтуїтивно зрозумілий графічний інтерфейс (рис. 1) та не пострибує значних системних ресурсів для своєї роботи. Уже після її встановлення без додаткових

налаштувань можна створювати базові мережеві топології простим переміщенням пристроїв та ліній зв'язку між ними на робочу ділянку програми. Інструмент ідеально підходить для тих, хто робить перші кроки у вивченні принципів роботи мереж.

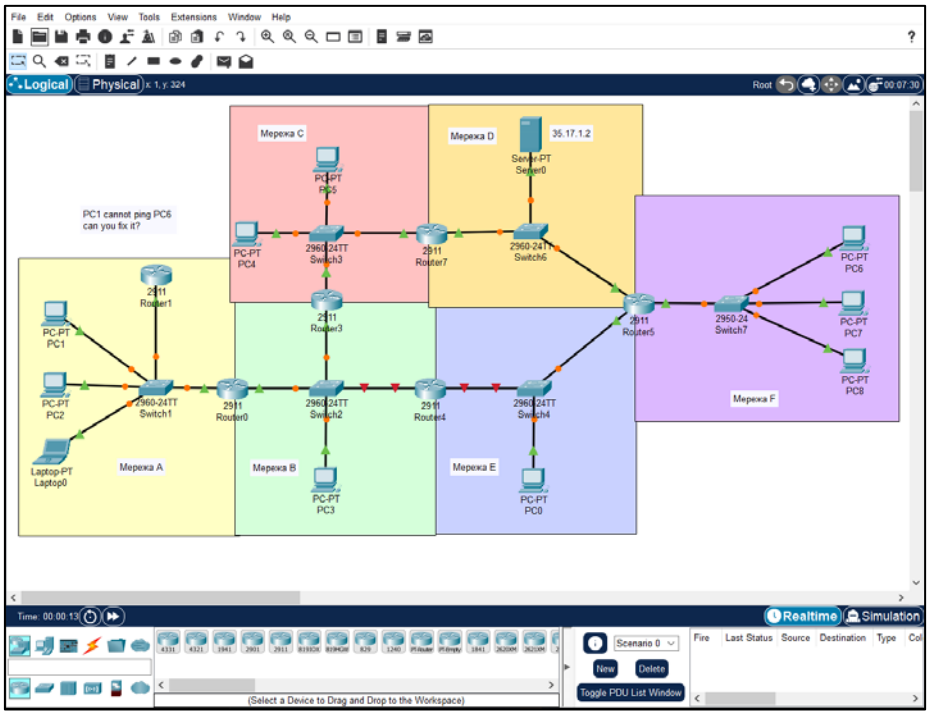

Рис. 1. Інтерфейс Cisco Packet Tracer

Основними можливостями *CPT* є такі [10–12]:

симуляція мережевих (маршрутизаторів, комутаторів, серверів, екранів тощо) та кінцевих (ПЕОМ, *IP*-телефонів, елементів *IoT* тощо) пристроїв. Проте в мережевих пристроях підтримується лише емуляція командного інтерфейсу (*CLI*) *Cisco* і не використовуються реальні образи обладнання. Це означає, що деякі команди та функції можуть бути недоступними або працюватимуть обмежено порівняно з реальними пристроями. Що стосується кінцевого обладнання, то тут здійснюється емуляція виключно ключових функцій, таких як: командний рядок, веббраузер, налаштування *Wi-Fi* під'єднання тощо без прив'язки до конкретної ОС;

конфігурація різних мережевих протоколів та служб (*OSPF, EIGRP, ACL, DHCP, DNS, FTP* тощо);

візуалізація трафіку та моніторинг пакетів.

CPT включає кілька функцій, що можуть бути використані для вивчення основ кібербезпеки, зокрема виключно для кіберзахисту [12]. Наприклад, програма дозволяє:

налаштовувати контроль доступу за допомогою *ACL* (*Access Control List*), що допомагає практикуватися у створенні правил для управління доступом до ресурсів;

моделювати мережеві прості загрози й відпрацьовувати механізми захисту від них, зокрема блокування портів пристроїв у разі несанкціонованого доступу, встановлення фільтрів тощо;

конфігурувати мережеві брандмауери та *VPN*, що імітує реальні сценарії захисту даних;

вивчати принципи роботи таких протоколів безпеки, як: *IPsec, SSL* та *HTTPS,* – які широко використовуються для захисту інформації в разі її передавання мережею.

Основними перевагами використання *CPT є:*

доступність та зручність для моделювання мереж без необхідності в дорогому апаратному забезпеченні. Це надає можливість навчатися в будь-який час і з будь-якого місця, використовуючи звичайний комп'ютер;

інтерактивність: ті, хто навчаються, можуть налаштовувати мережеві компоненти, створювати свої власні топології та експериментувати з конфігураціями без ризику для реальної мережі;

підтримка багатьох протоколів і технологій, що дає можливість отримати повне уявлення про структуру та функціонування мережі.

Разом із тим для *CPT* притаманні обмеження, які мають частковий влив на можливість його використання для відпрацювання питань кібербезпеки, зокрема:

обмежена підтримка складних протоколів. *CPT* не підтримує повного спектра протоколів, що використовуються в реальних мережах, таких як більш складні функції безпеки *Cisco ASA;*

відсутність реальної взаємодії з кіберзагрозами. Хоча ПЗ дозволяє імітувати деякі загрози, реальні атаки часто набагато складніші й потребують використання спеціалізованих платформ;

обмежений у можливостях розширення, тобто *CPT* працює виключно з обладнанням компанії *Cisco* та не підтримує додавання зовнішніх образів устаткування інших вендорів, наприклад *Mikrotik, Juniper* тощо.

Наступним представником програмних засобів моделювання мереж є *GNS*3, його вважають більш професійним, ніж *CPT* [13].

*GNS*3 (*Graphical Network Simulator*) – графічний емулятор комп'ютерних мереж [13, 14]. Його повноцінну роботу забезпечують такі компоненти:

Dynamips – ядро програми, яке дозволяє емулювати образи таких мережевих ОС, як *CiscoIOS, Mikrotik* тощо;

Dynagen – утиліта (текстовий інтерфейс) для *Dynamip,* що дозволяє швидко створювати віртуальні мережі та керувати ними за допомогою конфігураційного файлу типу *INI*;

PEM емулятор брандмауера *CiscoPIX* на основі *Qemu* [15].

*GNS*3 має власний графічний інтерфейс (рис. 2), де необхідні пристрої можна переносити в робочу ділянку та з'єднувати між собою. Цей підхід інтуїтивно зрозумілий. Проте для недосвідченого користувача може виникнути проблема, пов'язана з налаштуванням та першим запуском програми. Передусім це пояснюється тим, що *GNS*3 емулює роботу апаратної частини пристрою, тому для його використання, на відміну від *CPT*, необхідно мати реальний образ ОС цього пристрою, який слід додати до бібліотеки програми, а вже тільки після цих маніпуляцій можливо його використовувати для під'єднання до мережі, що моделюється.

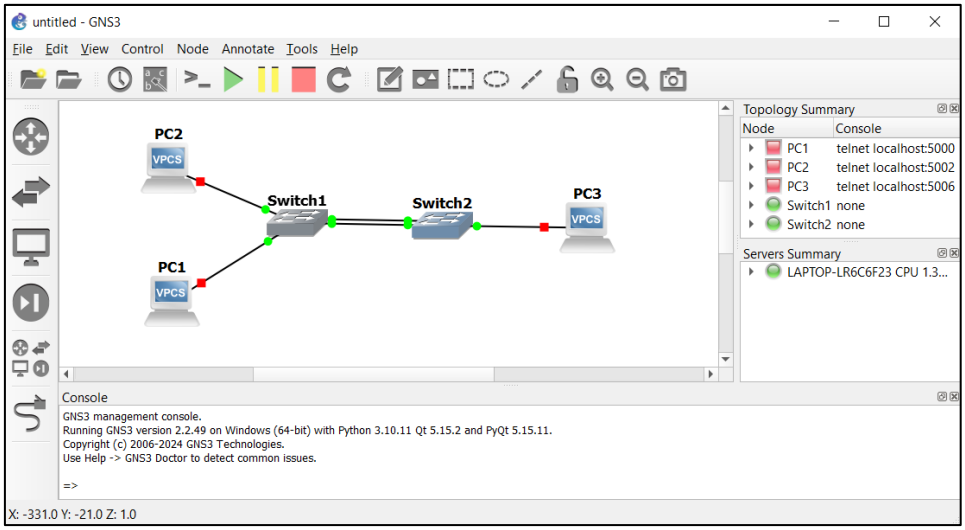

Рис. 2. Інтерфейс GNS3

Що ж стосується кінцевих пристроїв, то тут вже є два варіанти. Перший – використовувати наявний у бібліотеці віртуальний ПЕОМ, функціональні можливості якого значно обмежені. У разі другого варіанта за кінцевий пристрій можливо використати повноцінний віртуальний комп'ютер з *Windows* або *Linux,* чи з будь-якою іншою ОС, оскілки *GNS*3 підтримує технології віртуалізації та інтегровану роботу з такими програмними засобами віртуалізації, як *VirtualBox* або *VMWare.*

Отже, основними можливостями програми *GNS*3 є [14, 16]:

емуляція мережевих пристроїв (маршрутизаторів, комутаторів, серверів) за рахунок їх реальних образів ОС, що дозволяє створювати реалістичні мережеві архітектури;

інтеграція з програмою аналізу мережевого трафіку *Wireshark* для його реального моніторингу та аналізу даних;

підтримка декількох протоколів для налаштування *VPN*, *ACL*, *NAT*, протоколів маршрутизації (*OSPF*, *BGP*);

гнучкість у налаштуванні топологій: використання реальних образів ОС пристроїв, які імітують справжню роботу кінцевих пристроїв;

можливість під'єднання створеної в програмі віртуальної мережі до реальної мережі або Інтернету, що дає змогу максимально реалістично відтворювати складні топології та взаємодію різних мереж.

Зазначені можливості значно підвищують спроможності *GNS*3 порівняно з *CPT* у вивченні питань кібербезпеки.

Для кіберзахисту *GNS*3 дозволяє створювати топології, що включають брандмауери, *VPN*, маршрутизацію з безпечним доступом та сегментацію мережі. Це дає змогу відпрацювати дії з нейтралізації різних типів атак, таких як: відмова в обслуговуванні (*DoS* / *DDoS*), атаки на маршрутизацію (наприклад, *BGP hijacking*), а також спроби обходу брандмауерів. GNS3 також підтримує тестування мережевих інфраструктур на стійкість до атак, що сприяє підготовці до реальних ситуацій. Крім того, завдяки інтеграції з інструментами для аналізу трафіку, зокрема *Wireshark, GNS*3 дозволяє вивчати

структуру мережевого трафіку, аналізувати пакети та виявляти аномалії. Це є критично важливим у навчанні виявлення вторгнень (*Intrusion Detection System, IDS*) та розумінні мережевих атак на рівні даних.

Завдяки використанню в *GNS*3 реальних ОС, наприклад *Kali Linux,* є можливість практикуватися в проведенні тестувань на проникнення або окремих його елементів, таких як: сканування мережі, перехоплення трафіку, виявлення вразливостей тощо.

Отже, перевагами *GNS3* є таке:

використання реальних образів ОС, що робить симуляції максимально наближеними до реальних умов;

підтримка мультивендорних середовищ не тільки пристроїв *Cisco*, але й інших постачальників (наприклад, *Juniper*), що робить *GNS*3 універсальним інструментом;

гнучкість у налаштуванні мережевих топологій: платформа дозволяє створювати складні архітектури, які можуть включати віртуальні машини, брандмауери, *VPN* та інші компоненти;

інтеграція з аналітичними інструментами, можливість підключення до *Wireshark,* що забезпечує аналіз трафіку й тестування безпеки мережевих сегментів.

Попри свої численні переваги, *GNS*3 також має певні обмеження:

високі вимоги до апаратного забезпечення, оскільки може вимагати значних ресурсів комп'ютера, особливо під час емуляції великих топологій із багатьма пристроями.

складність у використанні для початківців, ПЗ має порівняно складний інтерфейс і вимагає певних технічних знань для ефективного налаштування;

обмеження віртуалізації деяких типів пристроїв, зокрема комутаторів серії *Catalyst,* оскільки на них використовується велика кількість специфічних інтегральних мікросхем, які складно емулювати. Це, у свою чергу, дещо обмежує можливість тестування певних конфігурацій;

потреба в образах ОС, тому що для роботи з реальними ОС маршрутизаторів і комутаторів потрібні власні образи, які можуть бути недоступними через ліцензійні обмеження.

Останнім програмним засобом, що розглядяться в рамках цієї статті, є *EVE-NG.*

Emulated Virtual Environment – Next Generation (EVE-NG) – це емульоване віртуальне середовище для професіоналів у сфері мереж, безпеки та *DevOps*, орієнтоване на корпоративних користувачів [17]. *EVE-NG* доступне у двох версіях: *Community* (безкоштовна) та *Professional* (платна). Професійна версія надає більше функцій: додаткові інструменти для спільної роботи та покращене управління топологією. У цілому обидві версії працюють як вебдодаток, а це, в свою чергу, вимагає наявності окремого сервера. Клієнтська частина *EVE-NG* має вебінтерфейс (рис. 3), що дозволяє користувачам працювати через браузер [18].

За своїми функціональними можливостями *EVE-NG* дуже подібний до *GNS*3. Він також підтримує великий вибір мережевого обладнання від різних вендорів. Як і в *GNS*3, є можливість на кінцевих пристроях емулювати реальні ОС. Але ключова відмінність – це клієнт-серверна архітектура *EVE-NG,* завдяки якій спрощується доступ до віртуальних

лабораторій із будь-якого пристрою без необхідності встановлення додаткового ПЗ на клієнтському комп'ютері. Крім того, ця архітектура підтримує мультикористувацький режим, який дозволяє декільком користувачам одночасно працювати в одному середовищі. Це особливо корисно для навчальних закладів, курсів та тренінгів. Проте налаштування сервера та додавання образів як мережевих, так і кінцевих пристроїв є складним процесом, потребує додаткового ПЗ та вимагає від користувача більш глибоких знань управління ОС [19].

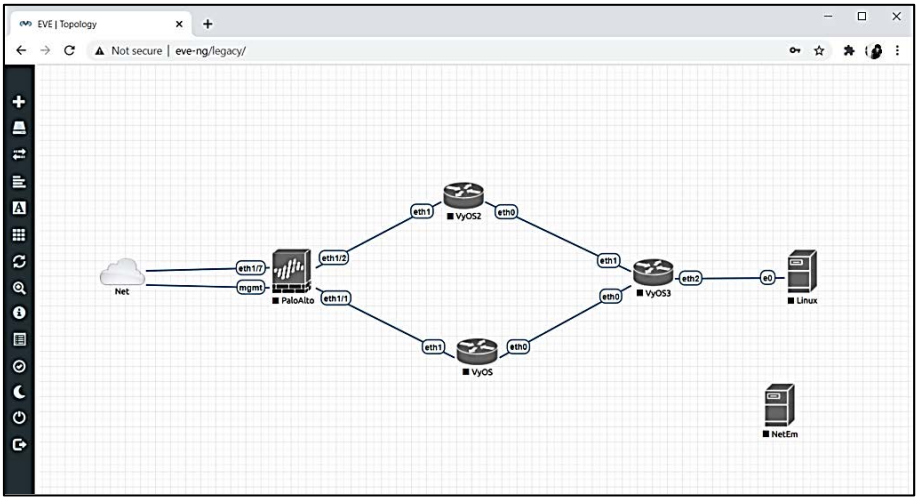

Рис. 3. Інтерфейс EVE-NG

У цілому перевагами використання цієї програми є такі:

реалістичність і повний контроль над середовищем, можливість налаштовувати різні пристрої, платформи та протоколи, створюючи лабораторії, максимально наближені до реальних корпоративних мереж;

доступність великого вибору образів, *EVE-NG* підтримує багато різноманітних пристроїв і мережевих ОС, що надає студентам можливість отримати досвід роботи з різними виробниками мережевого обладнання;

інтеграція з аналітичними інструментами, зокрема можливість використовувати *Wireshark, Splunk, Snort*, що надає тим, хто навчається, глибоке розуміння принципів виявлення та аналізу кіберзагроз.

Крім того, EVE-NG має й певні недоліки:

високі вимоги до апаратного забезпечення, оскільки його сервер потребує значної витрати ресурсів, особливо для великих і складних топологій;

складність для новачків, бо інтерфейс і конфігурації можуть бути незрозумілими для початківців, навчання на *EVE-NG* потребує базових знань у галузі мереж та мережевих технологій;

ліцензійні обмеження, оскільки деякі образи мережевих ОС потребують комерційних ліцензій, що може бути проблемою для навчальних закладів із малим бюджетом.

Узагальнений порівняльний аналіз розглянутих у статті програмних засобів моделювання мереж наведено в табл. 1.

Таблиця 1

Узагальнена порівняльна характеристика програмних засобів моделювання мереж

Характеристика	*CPT*	*GNS3*	*EVE-NG*
Інтерфейс користувача	Зручний	Зручний	Зручний
Можливість використання обладнання різних вендорів	Немає	Є	Є
Використання реальних образів ОС	Ні	Так	Так
Складність додавання нових образів пристроїв	_	Частково	Складно
Потреба в ресурсах ПЕОМ	Низька	Середня	Висока для сервера
Можливість аналізувати трафік	Часткова	Є	Є
Можливість моделювання сценаріїв кіберзахисту	Часткова	Є	Є
Можливість моделювання сценаріїв кібервпливу	Немає	Є	Є

Висновки. *Cisco Packet Tracer, GNS*3 та *EVE-NG* – це три популярні програмні продукти для емуляції та симуляції роботи мереж, які, з урахуванням їх функціональних особливостей можуть бути використані не тільки для формування навичок роботи з комп'ютерною мережею, а й для здобуття практичних навичок із кібербезпеки. Кожен із них має унікальні особливості, які визначають його ефективність у вивченні питань кібербезпеки.

Cisco Packet Tracer доцільно використовувати для навчання та здобуття базових навичок із кібербезпеки. Його перевагами є простий інтерфейс і зручні функції, що дають змогу початківцям вивчити мережеві протоколи, основи маршрутизації та безпекові політики. Однак *CPT* має певні обмеження у відтворенні складних мережевих топологій та кіберзагроз, що знижує його ефективність для глибокого вивчення питань кібербезпеки.

У свою чергу, *GNS*3 є потужнішим інструментом, що забезпечує підтримку реальних образів мережевих пристроїв й емуляцію різних ОС. Це дозволяє створювати більш реалістичні топології, досліджувати роботу складних мережевих протоколів і відпрацьовувати захист від кібератак у віртуальному середовищі. Крім того, він забезпечує гнучкість налаштувань і може бути використаний для навчання мережевій безпеці на середньому та вищому рівнях. Проте його продуктивність дещо знижується у великих топологіях, а конфігурація вимагає значних ресурсів і технічних знань.

EVE-NG є найбільш потужним інструментом для симуляції складних мережевих середовищ і тренувань із кібербезпеки, що потребують умов, максимально наближених до реальних. Завдяки підтримці мультивендорних мережевих образів, можливості багатокористувацької роботи та інтеграції з аналітичними інструментами (*Wireshark* і *Snort), EVE-NG* дозволяє створювати складні лабораторії для відпрацювання виявлення загроз, аналізу трафіку та реагування на інциденти. Цей інструмент є ідеальним для навчальних програм і тренінгів із кібербезпеки на вищому рівні, однак він вимагає значних обчислювальних ресурсів та базових знань у мережевих технологіях.

Отже, *Cisco Packet Tracer, GNS3* та *EVE-NG* доповнюють один одного в процесі отримання практичних навичок із кібербезпеки на різних рівнях навчання. Використання всіх трьох інструментів у навчальних програмах дозволить формувати комплексні знання та практичні навички, необхідні для ефективного захисту критичної інформаційної інфраструктури від кібератак.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Грищук Р. В. Кіберполігон як навчальне середовище з метою підготовки персоналу для боротьби з кіберзлочинністю // Кібербезпека в Україні: правові та організаційні питання : матеріали Всеукр. наук.-практ. конф. Одеса : Одеський держ. ун-т внутр. справ, 2017. С. 152–153.
2. Даник Ю. Г., Грищук Р. В. Основи кібернетичної безпеки : монографія / За заг. ред. проф. Ю. Г. Даника. Житомир : ЖНАЕУ, 2016. 636 с.
3. Даник Ю. Г. Особливості створення кіберполігонів для дослідження комплексних кібердій та підготовки фахівців з кібербезпеки // Сучасні інформаційні технології у сфері безпеки та оборони. 2019. № 1 (34). С. 95–102. https://doi.org/10.33099/2311-7249/2019-34-1-95-102
4. Ciuperca E., Stanciu A., Cîrnu C. Postmodern Education and Technological Development. Cyber Range as a Tool for Developing Cyber Security Skills // INTED 2021 Proceedings. P. 8241–8246. https://doi.org/10.21125/inted.2021.1675
5. Muhammad Mudassar Yamin, Basel Katt, Vasileios Gkioulos. Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture // Computers & Security. January 2020. Vol. 88. P. 101636. https://doi.org/10.1016/j.cose.2019.101636
6. Грищук Р. В., Охрімчук В. В. Напрямки підвищення захищеності комп'ютерних систем та мереж від кібератак // Актуальні питання забезпечення кібербезпеки та захисту інформації : тези доп. учасників ІІ Міжнар. наук.-практ. конф. Київ : Вид-во Європейського ун-ту, 2016. С. 60–61.
7. Liu J. A Primer for Real-Time Simulation of Large-Scale Networks // 41st Annual Simulation Symposium. 2008. P. 85–94. https://doi.org/10.1109/anss-41.2008.18
8. Тугай М. Ю., Чорна А. В. Аналіз вільного програмного забезпечення для роботи з комп'ютерними мережами // Сучасний рух науки : тези доп. ІІІ Міжнар. наук.-практ. інтернет-конф. 2018. С. 1354–1359.
9. Емулятори, симулятори чи реальний пристрій – порівнюємо можливості та умови для тестування. URL: https://dou.ua/forums/topic/44451/ (дата звернення: 07.11.2024).
10. Офіційний сайт Мережевої академії Cisco. URL: https://www.netacad.com/ (дата звернення: 01.11.2024).
11. What is Cisco Packet Tracer. URL: https://www.geeksforgeeks.org/what-is-cisco-packet-tracer/ (last accessed: 08.10.2024).
12. Брашовецький В. Є., Семенова О. О. Можливості програми імітаційного моделювання Cisco Packet Tracer версії 7.3.1. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/41213/17378.pdf?sequence=3&isAllowed=y (дата звернення: 06.10.2024).

13. Колесник В. В., Вакалюк Т. А. Огляд програмних емуляторів та симуляторів для побудови працездатних моделей мережі. URL: https://conf.ztu.edu.ua/wp-content/uploads/2021/01/7.pdf (дата звернення: 08.11.2024).
14. Офіційний сайт *GNS*3. URL: https://www.gns3.com/ (дата звернення: 08.11.2024).
15. Абрамов В. О. Застосування комбінованих моделей комп'ютерних мереж в навчальному процесі // Кібербезпека: освіта, наука, техніка. 2019. № 4 (4). С. 24–31. https://doi.org/10.28925/2663-4023.2019.4.2431
16. Галата Л. П., Корнієнко Б. Я. Дослідження системи захисту інформації корпоративної мережі на основі *GNS*3 // Наукоємні технології. 2020. № 2 (46). С. 172–179. https://doi.org/10.18372/2310-5461.46.14807
17. Офіційний сайт EVE-NG. URL: https://www.eve-ng.net/ (дата звернення: 08.09.2024).
18. EVE-NG CE Community Edition Cookbook. URL: https://www.eve-ng.net/wp-content/uploads/2024/05/EVE-CE-BOOK-6.2-2024.pdf (last accessed: 08.09.2024).
19. Matkurbanov D., Rakhimjanov K. Analysis of Network Emulation and Simulation Software // Sciences of Europe. 2021. № 79. P. 38–46. https://doi.org/10.24412/3162-2364-2021-79-1-38-46

Стаття надійшла до редакції 12.11.2024.

REFERENCES

1. Hryshchuk, R. V. (2017). Kiberpolihon yak navchalne seredovyshche z metoiu pidhotovky personalu dlia borotby z kiberzlochynnistiu [Cyberrange as a Training Environment for Personnel to Combat Cybercrime]. In *Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia : materialy Vseukr. nauk.-prakt. konf. [Cybersecurity in Ukraine: Legal and Organisational Issues: Materials of the All-Ukrainian Scientific and Practical Conference]*. (pp. 152–153). Odesa [in Ukrainian].
2. Danyk, Yu. H., & Hryshchu, R. V. (2016). *Osnovy kibernetychnoi bezpeky: monohrafiia [Basics of cybernetic security: monograph]*. Zhytomyr [in Ukrainian].
3. Danyk, Yu. H. (2019). Osoblyvosti stvorennia kiberpolihoniv dlia doslidzhennia kompleksnykh kiberdii ta pidhotovky fakhivtsiv z kiberbezpeky [Peculiarities of Creating Cyberranges for the Study of Complex Cyber Actions and Training of Cybersecurity Specialists]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony [Modern Information Technologies in the Field of Security and Defence]*, *1* (34), 95–102. https://doi.org/10.33099/2311-7249/2019-34-1-95-102 [in Ukrainian].
4. Ciuperca, E., Stanciu, A., & Cîrnu, C. (2021). Postmodern Education and Technological Development. Cyber Range as a Tool for Developing Cyber Security Skills. *INTED 2021 Proceedings*, 8241–8246. https://doi.org/10.21125/inted.2021.1675
5. Muhammad Mudassar Yamin, Basel Katt, & Vasileios Gkioulos. (2020). Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture. *Computers & Security, 88*, 101636. https://doi.org/10.1016/j.cose.2019.101636
6. Hryshchuk, R. V., & Okhrimchuk, V. V. (2016). Napriamky pidvyshchennia zakhyshchenosti komp'iuternykh system ta merezh vid kiberatak [Directions of Increasing the Security of

Computer Systems and Networks from Cyberattacks]. In *Aktualni pytannia zabezpechennia kiberbezpeky ta zakhystu informatsii: tezy dop. uchasnykiv II Mizhnar. nauk.-prakt. konf. [Actual Issues of Cybersecurity and Information Protection: Abstracts of the Participants of the II International Scientific and Practical Conference]*. (pp. 60–61. Kyiv [in Ukrainian].
7. Liu, J. (2008). A Primer for Real-Time Simulation of Large-Scale Networks. In *41st Annual Simulation Symposium*. (pp. 85–94). https://doi.org/10.1109/anss-41.2008.18
8. Tuhai, M. Yu., & Chorna, A. V. (2018). Analiz vilnoho prohramnoho zabezpechennia dlia roboty z komp'iuternymy merezhamy [Analysis of Free Software for Working with Computer Networks]. In *Suchasnyi rukh nauky : tezy dop. III Mizhnar. nauk.-prakt. internet-konf. [Modern Scientific Movement: Abstracts of the 3rd International Scientific-Practical Internet Conference]*. (pp. 1354–1359). [in Ukrainian].
9. *Emuliatory, symuliatory chy realnyi prystrii – porivniuiemo mozhlyvosti ta umovy dlia testuvannia [Emulators, Simulators or a Real Device – Comparing Possibilities and Conditions for Testing]*. (n. d.). Retrieved from https://dou.ua/forums/topic/44451/ [in Ukrainian].
10. *Official website of the Cisco Network Academy*. (n. d.). Retrieved from https://www.netacad.com/ [in Ukrainian].
11. *What is Cisco Packet Tracer*. (n. d.). Retrieved from https://www.geeksforgeeks.org/what-is-cisco-packet-tracer/
12. Brashovetskyi, V. Ye., & Semenova, O. O. (n. d.). *Mozhlyvosti prohramy imitatsiinoho modeliuvannia Cisco Packet Tracer versii 7.3.1 [Features of Cisco Packet Tracer simulation software version 7.3.1]*. Retrieved from https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/41213/17378.pdf?sequence=3&isAllowed=y [in Ukrainian].
13. Kolesnyk, V. V., & Vakaliuk, T. A. (n. d.). *Ohliad prohramnykh emuliatoriv ta symuliatoriv dlia pobudovy pratsezdatnykh modelei merezhi [An Overview of Software Emulators and Simulators for Building Working Network Models]*. Retrieved from https://conf.ztu.edu.ua/wp-content/uploads/2021/01/7.pdf [in Ukrainian].
14. *Official website of the GNS3*. (n. d.). Retrieved from https://www.gns3.com/
15. Abramov, V. O. (2019). Zastosuvannia kombinovanykh modelei komp'iuternykh merezh v navchalnomu protsesi [Use of Combined Models of Computer Networks in the Educational Process]. *Kiberbezpeka: osvita, nauka, tekhnika [Cyber Security: Education, Science, Technology]*, *4* (4), 24–31. https://doi.org/10.28925/2663-4023.2019.4.2431 [in Ukrainian].
16. Halata, L. P., & Korniienko, B. Ya. (2020). Doslidzhennia systemy zakhystu informatsii korporatyvnoi merezhi na osnovi GNS3 [Research of the Corporate Network Information Security System Based on GNS3]. *Naukoiemni tekhnolohii [Science-Intensive Technologies]*, *2* (46), 172–179. https://doi.org/10.18372/2310-5461.46.14807 [in Ukrainian].
17. *Official website of the EVE-NG*. (n. d.). Retrieved from https://www.eve-ng.net/
18. EVE-NG CE Community Edition Cookbook. (n. d.). Retrieved from https://www.eve-ng.net/wp-content/uploads/2024/05/EVE-CE-BOOK-6.2-2024.pdf
19. Matkurbanov, D., & Rakhimjanov, K. (2021). Analysis of Network Emulation and Simulation Software. *Sciences of Europe, 79,* 38–46. https://doi.org/10.24412/3162-2364-2021-79-1-38-46

ISSN 2076-1546

V. V. Okhrimchuk, I. A. Okhrimchuk

ANALYSIS OF NETWORK MODELLING TOOLS FOR THE POSSIBILITY OF THEIR USE FOR PRACTICAL TRAINING OF CYBERSECURITY SPECIALISTS

Despite the existing information security systems, the key aspect of effective cyber defense remains the level of training of personnel responsible for cyber security. Today, the training of a cybersecurity specialist should be based on a comprehensive study of modern information technologies, mechanisms and patterns of cyberattacks, ways to counter them, and include both theoretical and practical components. It has been established that the most common practice in the leading educational and scientific institutions of the world and Ukraine in terms of practical training of cybersecurity specialists is the creation and deployment of complex software and hardware complexes - cyber training grounds, but this requires significant resources. Therefore, software tools for emulating and simulating computer networks are becoming an alternative to obtaining initial practical skills in cybersecurity.

The article analyses three of the most popular free tools for simulating and emulating computer networks - Cisco Packet Tracer, GNS3 and EVE-NG - with regard to the possibility of their use for practical training of cybersecurity specialists. The analysis found that Cisco Packet Tracer, which is aimed at novice users, provides simulation of network devices exclusively from Cisco, allows you to configure basic protocols and practice the basics of cyber defence. GNS3 is slightly more advanced than Cisco Packet Tracer in terms of functionality, emulates real operating system images and supports many network device vendors, making it useful for complex training tasks. In addition, GNS3 provides the ability to recreate cyberattack scenarios, and the integrated Wireshark network analyser allows you to monitor traffic and analyse the course of a cyberattack on the system. In turn, EVE-NG is a powerful network emulation platform that is very close to GNS3 in terms of functionality. It also provides extensive hardware support and enables the deployment of complex network topologies. However, the main feature of EVE-NG is its client-server architecture, which enables multi-user operation.

Thus, Cisco Packet Tracer, GNS3, and EVE-NG complement each other in the process of acquiring practical cybersecurity skills at different levels of education. The use of all three tools in training programmers will help to develop the comprehensive knowledge and practical skills necessary to effectively protect critical information infrastructure from cyberattacks.

***Keywords**: cybersecurity; cyberdefence; cyberattack; emulator; simulator; virtualization; Cisco; GNS; EVE-NG.*