УДК 004.4
DOI: 10.25140/2411-5363-2020-2(20)-229-236

Євген Риндич, Тарас Петренко, Леся Черниш, Сергій Семендяй, Георгій Біленький

НАВЧАЛЬНИЙ СТЕНД ДЛЯ ВИВЧЕННЯ ДИСЦИПЛІН ІЗ ЗАБЕЗПЕЧЕННЯ МЕРЕЖЕВОГО ЗАХИСТУ ІНФОРМАЦІЇ

Актуальність теми дослідження. *На сьогодні набули значного поширення комп'ютерні мережі, без яких уже не можливо уявити функціонування будь-якої комп'ютерної системи. Поширення та доступність призвели до необхідності розмежувати доступ до компонентів таких систем та впроваджувати до навчання технічних спеціальностей таких дисциплін, як «Організація комп'ютерних мереж», «Системи захисту обчислювальних мереж» та інші.*

Постановка проблеми. *У галузі вивчення дисциплін пов'язаних із сучасними комп'ютерними мережами та їх безпекою значне місце посідають практичні навички налаштування програмного та апаратного забезпечення. Одним з найефективніших методів є навчання з використанням півнатурних та натурних моделей комп'ютерних мереж.*

Аналіз останніх досліджень і публікацій. *Розглянуто останні публікації у відкритому доступі, включаючи дані навчальних центрів компаній Cisco та Mikrotik.*

Виділення недосліджених частин загальної проблеми. *Розробка та обґрунтування використання півнатурних моделей сучасних комп'ютерних мереж у навчальному процесі спеціалізованих дисциплін вищих учбових закладів.*

Постановка завдання. *Запропонувати базову півнатурну модель комп'ютерної мережі для стенду вивчення дисциплін із забезпечення мережевого захисту інформації.*

Виклад основного матеріалу. *У статті наведено аналіз, вимоги та півнвтурна модель стенду комп'ютерної мережі для вивчення дисциплін з забезпечення мережевого захисту інформації.*

Висновки відповідно до статті. *Запропоновано півнатурну модель стенду комп'ютерної мережі для вивчення дисциплін з забезпечення мережевого захисту інформації з використанням мережевого обладнання Mikrotik.*

Ключові слова: *комп'ютерна мережа; інформаційні технології; кібербезпека; комутація; MikroTikЯ; шифрування; моделювання.*

Рис.: 2. Табл.: 1. Бібл.: 7.

Актуальність теми дослідження. Сучасний етап розвитку комп'ютерних систем та мереж призвів до значного збільшення та ускладнення елементів сучасних систем. Вивчення мережевих систем вимагає як теоретичних, так і практичних навичок. Створення стенду для демонстрації основних етапів побудови мережі, її налаштуванні та обмеженнях, знайомство з мережевим обладнанням та його конфігурацією є одним з кращих способів показати та навчити студентів роботі з апаратним та програмним забезпеченням. Особливим напрямком практичного використання мереж є створення безпечного підключення до зовнішніх мереж та ознайомлення з базовими поняттями маршрутизації та організації безпечної взаємодії головного офісу(HQ) підприємства та його віддалених підрозділів(BO). Також можлива практика в пошуку вразливостей та дослідженню способів проникнення в систему через знайдені вразливості для їх усунення. Стенд дасть можливість як адмініструвати та набирати практичні навички, так і дасть базу для подальших досліджень структур мережі, локальної та глобальної.

Постановка проблеми. У галузі вивчення дисциплін пов'язаних із сучасними комп'ютерними мережами та їх безпекою значне місце посідають практичні навички налаштування програмного та апаратного забезпечення. Одним з найефективніших методів є навчання з використанням півнатурних та натурних моделей комп'ютерних мереж. Також, працюючи з мережевим обладнанням, необхідно розуміти, що кожен елемент мережі необхідно налаштовувати як самостійну структуру, зі своїми правилами, обмеженнями та дозволами, тому для цієї задачі мережеве обладнання MikroTik підходить найкраще.

Конфігурації та налаштування для MikroTik можна заносити як на фізичні пристрої, так і тестувати за допомогою додаткового ПО, це дозволяє відпрацювати праце спроможність того чи іншого елемента мережі перед його інтеграцією в реальну систему.

Аналіз останніх досліджень і публікацій. При побудові захищеної мережі не має завдання дати користувачам можливість впливати на захищеність та внутрішні конфігурації системи, студентам для розуміння понять комутації, маршрутизації, побудови локальних виділених мереж або обслуговуванні мережевого обладнання необхідно знайомитися з купою документації без можливості самостійно конфігурувати пристрої мережі,

налаштовувати точки доступу, основні сервера, маршрути, протоколи захисту та обмежень. Всі ці можливості студенти пізнають або на віртуальних машинах, або на власних роутерах. Стенд з можливістю відкату налаштувань та з тестовим простором може дати студентам реальну можливість попрактикуватися у різних напрямках адміністрування мережі, як від фізичного рівня та побудови захищених маршрутів на локальному рівні, так і додавання обмежень в зовнішній мережі на доступ, сканування або вторгнення.

У досліджених роботах є багато прикладів побудови мережі, налаштуванні обладнання, однак основною проблемою для студентів є те, що просто ознайомлюючись з такими статтями він не здобуде практичних навичок адміністрування.

Наприклад в [1], показані принципи налаштування способів тунельного з'єднання між віддаленими мережами, однак у студента, який ознайомиться з цією статтею і одразу перейде до налаштування мережеве обладнання, може виникнути безліч питань щодо налаштування, конфігурацій та самого процесу побудови.

Використання стенду в навчальних цілях також може допомогти в побудові гуртків по налаштуванню і контролю мережі, що може включити в себе Wi-Fi точки доступу, дослідження HotSpot [2] та інші мережеві технології, які можуть допомогти студентам в опануванні перерахованих віще понять.

Виділення недосліджених частин загальної проблеми. Розробка та обґрунтування використання півнатурних моделей сучасних комп'ютерних мереж у навчальному процесі спеціалізованих дисциплін вищих учбових закладів не береться до уваги при складанні подібних статей, бо всі вони направленні на окремі елементи, проблеми, завдання, і не ставлять перед собою завдання в навчанні окремих осіб повному спектру необхідних налаштувань. Стенд півнатурних моделей сучасних комп'ютерних мереж допоможе у вирішенні цих проблем.

Мета статті. Метою статті є розробка та обґрунтування використання півнатурних моделей сучасних комп'ютерних мереж у навчальному процесі спеціалізованих дисциплін вищих учбових закладів

Виклад основного матеріалу дослідження. Будь-яка система − це набір елементів і зв'язків між ними. Для системи, яка реалізується, такими елементами можуть виступати, наприклад:

1) Основний маршрутизатор - електронний пристрій, що використовується для поєднання двох або більше мереж і керує процесом маршрутизації, тобто на підставі інформації про топологію мережі та певних правил приймає рішення про пересилання пакетів мережевого рівня (рівень 3 моделі OSI) між різними сегментами мережі.

2) Wi-Fi точка – бездротова базова станція, призначена для забезпечення бездротового доступу до вже існуючої мережі (бездротовий або провідний) або створення абсолютно нової бездротової мережі. Бездротовий зв'язок здійснюється за допомогою технології Wi-Fi. Проводячи аналогію, точку доступу можна умовно порівняти з вишкою стільникового оператора, з одним застереженням, що у точки доступу менший радіус дії і зв'язок між підключеними до неї пристроями здійснюється за технологією Wi-Fi. Радіус дії стандартної точки доступу - приблизно 200-250 метрів, за умови, що на цій відстані не буде ніяких перешкод (наприклад, металоконструкцій, перекриттів із бетону та інших споруд погано пропускають радіо хвилю) [3].

3) Мережевий комутатор — пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента.

4) Користувачі – ПК або ноутбуки які будуть приєднуватися до мережі студентами для виконання лабораторних робіт та доступу до мережі Інтернет, проведення тестів на доступність та можливість втручання в процес маршрутизації інших студентів.

Архітектура системи.

Будь-яка система обробки й передачі даних повинна забезпечувати масштабованість, високу швидкість роботи і надійність. Проєктуванням стенду та системи загалом необхідно з урахуванням кількості потенційних студентів, їх потреб та потреб курівництва.

При розробці та реалізації циклу лабораторних робіт з мережевих технологій запропоновано використовувати маршрутизатори MikroTik RB2011UiAS-2HnD-IN як основних маршрутизаторах на відокремлених ділянках. Також в стенді використовується MikroTik RB750 який моделює роботу «Глобальну мережі» з зовнішніми IP адресами для емуляції мережі Інтернет[4].

Для стенду було обрано мережеве обладнання MikroTik через його відносно невелику вартість, різноманітність функцій та зручне налаштування з використанням операційної системи RouterOS.

Дане ПО має великий функціонал. Завдяки ньому можна налаштувати правила маршрутизації, різні інтерфейси та обмеження для доступу, що дозволить студентам отримати практичний досвід для майбутньої роботи в сфері мережевого обладнання та налаштування захищених систем класу АС-2 та АС-3. Слід зазначити, що операційна система розроблена на базі Linux, що дозволяє знизити рівень особливих знань для початку налаштування.

Вбудовані функції безпеки дозволяють за допомогою ознайомити здобувачів з процесами створення тунелів, автентифікації, перевірки цілісності та шифруванню IP-пакетів.

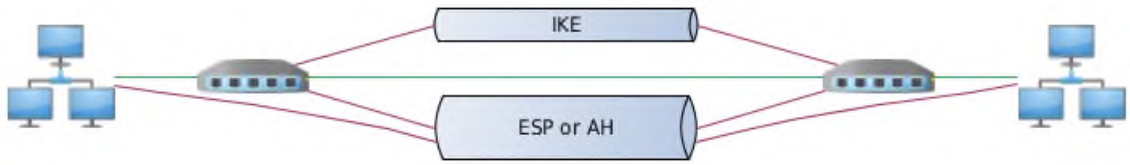

Рис. 1. Схема створення тунелів між віддаленими вузлами

Основні можливості, які можна використати при використанні стенду:

- базові функції комутації;
- базові функції та протоколи маршрутизації, їх безпека;
- створення та дослідження віртуальних мереже(VLAN);
- вивчення технології Network Address Translation (NAT);
- створення та дослідження тунелів з шифруванням та без шифрування (PPTP, PPPoE, SSTP, OpenVPN, L2TP/IPSec);
- дослідження протоколу SNMP;
- дослідження та порівняння алгоритмів шифрування даних;
- дослідження та порівняння базових протоколів автентифікації

У таблиці наведено адресацію мереж, а на рис. 2 – схема стенду з вказаними IP адресами та обладнанням.

Таблиця

IP адреси стенда

№	Призначення	Адреса мережі	Шлюз	Маска мережі
1	Головний офіс	192.168.1.0	192.168.1.254	255.255.255.0
2	Віддалений підрозділ	192.168.100.0	192.168.100.254	255.255.255.0
3	Зовнішня мережа. Провайдер головного офісу	65.65.65.0	65.65.65.254	255.255.255.0
4	Зовнішня мережа. Провайдер віддаленого підрозділу	75.75.75.0	75.75.75.254	255.255.255.0

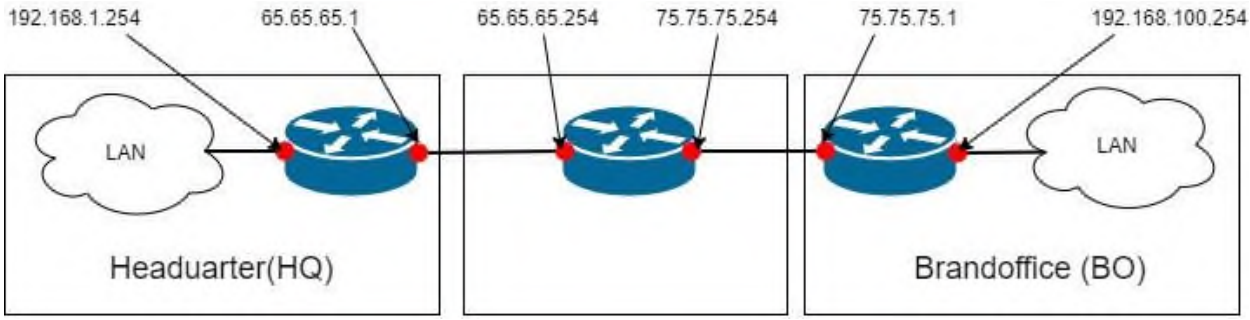

Рис. 2. Схема з'єднання та адресації

В ході розробки та тестування було також виявлено, що для більш поглибленого вивчення деяких дисциплін необхідно додати додаткове обладнання. Так для вивчення захисту зовнішнього периметру доцільно розширити запропоновану схему апаратним брандмауером та зовнішнім аналізатором трафіку та, зважаючи на відтворення критичної інфраструктури, додати джерела безперебійного живлення з можливістю відстеження стану та доступу за допомогою мережевих протоколів.

Первинне налаштування.

Беручи до уваги постійне збільшення загроз та способи захисту постійне оновлення налаштувань має лягти на плечі керівникам стенду та системи, та студентам які будуть користуватися мережею, для їх же безпеки та отриманні професійних навичок [4].

Базові налаштування MikroTik можна проводити в групах студентами під наглядом кураторів для перевірки. Наступні конфігурації є базовими, однак необхідними для стабільної та безпечної роботи мережі. Подальші конфігурації можуть бути виконані в ході виконання лабораторних робіт та розроблені викладачами. Ідеї з налаштування та способів покращення безпеки мережі, її гнучкості та адаптивності повинно проводитися постійно, бо технології захисту постійно оновлюються, а зловмисники постійно знаходять вразливості в системі.

Налаштування полягає у виконанні таких кроків [5]:

1. Необхідно запустити програму Winbox і перейдіть на вкладку Neighbors.
2. У списку відобразиться роутер. Для з'єднання необхідно натиснути лівою кнопкою миші на його MAC адресу.
3. Натисніть кнопку Connect.

Login за замовчуванням admin, пароль порожній.

Для першого порту ether1 необхідно записати коментар "WAN". Для налаштування порту необхідно:

1. Відкрити меню Interfaces.
2. Вибрати перший інтерфейс ether1.
3. Натиснути жовту кнопку Comment.
4. У вікні ввести коментар "WAN".
5. Натиснути кнопку OK.

Для другого порту ether2 необхідно записати коментар "LAN". Для налаштування порту необхідно:

1. Вибрати інтерфейс ether2.
2. Натиснути жовту кнопку Comment.
3. У вікні ввести коментар "LAN".
4. Натиснути кнопку OK.

Якщо інтернет провайдер видає мережеві налаштування автоматично, то необхідно налаштувати WAN порт роутера MikroTik на отримання налаштувань по DHCP, для цього необхідно:

1. Відкрити меню IP.
2. Вибрати DHCP Client.

3. У вікні натиснути кнопку Add (плюсик).
4. У новому вікні в списку Interface: треба вибрати WAN інтерфейс ether1.
5. Натиснути кнопку OK для збереження налаштувань.

Для налаштування статичного IP адреси і маски підмережі WAN порту MikroTik необхідно:

1. Відкрити меню IP.
2. Вибрати Addresses.
3. У вікні натиснути кнопку Add (плюсик).
4. У новому вікні в полі Address: прописати статичний IP адреса/маску підмережі.
5. У списку Interface: вибирати WAN інтерфейс ether1.
6. Для збереження налаштувань необхідно натиснути кнопку OK.

Для налаштування адреси інтернет шлюза MikroTik необхідно:

1. Відкрити меню IP.
2. Вибрати Routes.
3. У вікні натиснути кнопку Add (плюсик).
4. У новому вікні в полі Gateway: прописати IP адресу шлюза.
5. Необхідно натиснути кнопку OK для збереження налаштувань.

Для додавання адреси DNS серверів MikroTik необхідно:

1. Відкрити меню IP.
2. Вибрати DNS.
3. У вікні натиснути кнопку Settings.
4. У новому вікні в полі Servers: прописати IP адресу пріоритетного DNS сервера.
5. Необхідно натиснути кнопку «вниз» (чорний трикутник), щоб додати ще одне поле для введення.
6. У новому полі прописати IP адресу альтернативного DNS сервера.
7. Поставити галочку Allow Remote Requests.
8. Натиснути кнопку OK для збереження налаштувань.

Для створення об'єднання bridge-local (міст) необхідно:

1. Відкрити меню Bridge.
2. Натиснути кнопку Add (плюсик).
3. У поле Name прописати ім'я об'єднання bridge-local.
4. Натиснути кнопку OK.

Для додавання в об'єднання провідних Ethetnet портів 2-5 необхідно:

1. Перейти на вкладку Ports.
2. Натиснути кнопку Add (плюсик).
3. У списку Interface вибрати ethernet порт ether2.
4. У списку Bridge вибрати ім'я об'єднання bridge-local.
5. Натиснути кнопку OK.
6. Повторити процедуру для портів ether3, ether4, ether5.

Для додавання Wi-Fi інтерфейсу необхідно.

1. Перейти на вкладку Ports.
2. Натиснути кнопку Add (плюсик).
3. У списку Interface вибрати бездротовий інтерфейс wlan1.
4. У списку Bridge вибрати ім'я об'єднання bridge-local.
5. Натиснути кнопку OK.

Для налаштувати IP адресу локальної мережі MikroTik необхідно:

1. Відкрити меню IP.
2. Вибрати Addresses.
3. Натиснути кнопку Add (плюсик).
4. У полі Address ввести адресу і маску локальної мережі, наприклад 192.168.88.1/24.

5. У списку Interface вибрати bridge-local.
6. Натиснути кнопку OK.

Налаштування NAT виконується такими командами:

- ip firewall nat add chain = srcnat out-interface = ether1 action = masquerade

Protect router - команди для захисту роутера:

- ip firewall filter add action=accept chain=input disabled=no protocol=icmp
- ip firewall filter add action=accept chain=input connection-state=established disabled=no in-interface=ether1
- ip firewall filter add action=accept chain=input connection-state=related disabled=no in-interface=ether1
- ip firewall filter add action=drop chain=input disabled=no in-interface=ether1

Protect LAN - захист внутрішньої мережі:

- ip firewall filter add action=jump chain=forward disabled=no in-interface=ether1 jump-target=customer
- ip firewall filter add action=accept chain=customer connection-state=established disabled=no
- ip firewall filter add action=accept chain=customer connection-state=related disabled=no
- ip firewall filter add action=drop chain=customer disabled=no.

Для призначення типів інтерфейсів для захисту внутрішньої мережі (external - зовнішній, internal - внутрішній LAN) необхідно ввести команди:

- ip upnp interfaces add disabled = no interface = ether1 type = external
- ip upnp interfaces add disabled = no interface = ether2 type = internal
- ip upnp interfaces add disabled = no interface = ether3 type = internal
- ip upnp interfaces add disabled = no interface = ether4 type = internal
- ip upnp interfaces add disabled = no interface = ether5 type = internal
- ip upnp interfaces add disabled = no interface = bridge-local type = internal

Щоб змінити пароль доступу до роутера MikroTik, необхідно виконати наступні дії:

1. Відкрити меню System;
2. Вибрати Users;
3. Виконати подвійний клік кнопкою миші на користувача admin;
4. Натиснути кнопку Password ...;
5. У поле New Password ввести новий пароль;
6. У поле Confirm Password підтвердити новий пароль;
7. У вікні Change Password натиснути кнопку OK;
8. У вікні User натиснути кнопку OK.

Зловмисників часто цікавить розділ Scripts, через який вони можуть отримати доступ до обладнання та Інтернет каналу у своїх цілях. Що б перевірити, що все в порядку, необхідно перевірити розділ System - Scripts.

Перевіряти необхідно вкладку Scripts на відсутність будь-яких незрозумілих записів, за замовчуванням він чистий.

Висновки відповідно до статті. Як було показано в цій статті, на сучасному етапі розвитку обчислювальної техніки й загального наукового прогресу цілком реально створювати масштабні, швидкодіючі, системи з мінімальною вартістю для обслуговування потреб студентів у доступі до мережі Інтернет. Практичні навички здобуті у ході проектування, налаштування, виконання лабораторних робіт та самостійного дослідження допоможуть студентам краще зрозуміти можливості мережевого обладнання, способи його конфігурації, захисту та експлуатації. Також такий стенд дасть можливість здобувати практичні навички у сфері кібербезпеки для студентів, які в звичайних умовах не мали б можливості це зробити. Проєктування, встановлення та налаштування подібної системи було проведено на практиці та показало стабільну роботу як у режимі звичайної роботи

мережевого обладнання, так і як навчальний стенд для практики студентів. Таким чином, можна зробити висновок, що розроблена система може використовуватися як самостійна система для окремого забезпечення Інтернетом студентів, так і як складова частина навчального процесу студентів спеціальності кібербезпека.

Використання мережевого обладнання MikroTik для побудови стенду півнатурних моделей сучасних комп'ютерних мереж у навчальному процесі спеціалізованих дисциплін вищих учбових закладів зумовлене тим, що ці прилади мають багато можливостей. Мережеве обладнання MikroTik виступає як комплексне рішення для керування мережею, трафіком, користувачами та іншими елементами системи.

Стенд також можна доповнювати окремими елементами типу **FortiGate,** як мережевий екран нового покоління[6; 7], так і іншими елементами, які мають малий профіль роботи, але як елемент комплексної системи показує себе невід'ємною частиною

Список використаних джерел

1. Кузьмицкий А. Объединяем офисы с помощью Mikroti. URL: http://mikrotik.axiom-pro.ru/articles/mtoffice.php.

2. Простая Точка Доступа на Mikrotik. URL: http://mikrotik.axiom-pro.ru/articles/mikrotikap.php.

3. MikroTik Routers and Wireless – Products: RB2011UiAS-2HnD-IN. URL: https://mikrotik.com/product/RB2011UiAS-2HnD-IN.

4. Литвинов В. В., Казимир В. В., Риндич Є. В. Сучасний стан захисту інформації в IP-телефонії. *Математичні машини і системи*. 2009. № 2. С. 76–84.

5. Настройка роутера MikroTik. URL: https://www.technotrade.com.ua/Articles/ mikrotik_router_setup.php.

6. Риндич Є. В., Коняшин В. В., Зайцев С. В., Усов Я. Ю. Особливості створення мережевої системи виявлення вторгнень у комп'ютерні системи. *Математичні машини і системи*. 2018. № 3. URL: https://cyberleninka.ru/article/n/osoblivosti-stvorennya-merezhevoyi-sistemi-viyavlennya-vtorgnen-u-kompyuterni-sistemi/viewer.

7. Глобальні мережі : метод. вказ. до виконання лаб. робіт з дисципліни – Новітні архітектури та засоби побудови глобальних та корпоративних мереж для студ. спец. 8.05010201 – Комп'ютерні системи та мережі, 8.05010202 – Системне програмування, 8.05010203 – Спеціалізовані комп'ютерні системи / уклад.: Є. В. Риндич. Чернігів : ЧНТУ, 2013. 16 с.

References

1. Kuzmitsky, A. (n.d.). We unite offices with the help of Mikrotik. Retrieved from http://mikrotik.axiom-pro.ru/articles/mtoffice.php.

2. Prostaia Tochka Dostupa na Mikrotik [Simple Access Point on Mikrotik]. Retrieved from http://mikrotik.axiom-pro.ru/articles/ mikrotikap.php.

3. MikroTik Routers and Wireless – Products: RB2011UiAS-2HnD-IN. Retrieved from https://mikrotik.com/product/RB2011UiAS-2HnD-IN.

4. Litvinov, V. V., Kazimir, V. V., Rindich, E. V. (2009). Suchasnyi stan zakhystu informatsii v IP-telefonii [The current state of information security in IP-telephony]. *Matematychni mashyny i systemy – Mathematical Machines and Systems,* 2, 76–84.

5. Nastroika routera MikroTik [Configuring the MikroTik router]. Retrieved from https://www.technotrade.com.ua/Articles/ mikrotik_router_setup.php.

6. Ryndych, Ye. V., Koniashyn, V. V., Zaitsev, S. V., Usov, Ya. Yu. (2018). Osoblyvosti stvorennia merezhevoi systemy vyiavlennia vtorhnen u kompiuterni systemy [Peculiarities of creating a network system for detecting intrusions into computer systems]. *Matematychni mashyny i systemy – Mathematical Machines and Systems,* 3. Retrieved from https://cyberleninka.ru/article/n/osoblivosti-stvorennya-merezhevoyi-sistemi-viyavlennya-vtorgnen-u-kompyuterni-sistemi/viewer.

7. Ryndych, Ye. V. (2013). *Hlobalni merezhi : metod. vkaz. do vykonannia lab. robit z dystsypliny – Novitni arkhitektu-ry ta zasoby pobudovy hlobalnykh ta korporatyvnykh merezh dlia stud. spets. 8.05010201 – Kompiuterni systemy ta merezhi, 8.05010202 – Systemne prohramuvannia, 8.05010203 – Spetsiali-zovani kompiuterni systemy [Global networks: a method. decree. to perform lab. work on the discipline – The latest architectures and tools for building global and corporate networks for students. special 8.05010201 – Computer systems and networks, 8.05010202 – System programming, 8.05010203 – Specialized computer systems]*. Chernihiv: ChNTU [in Ukrainian].

UDC 004.4

Yevhen Ryndych, Taras Petrenko, Lesia Chernysh, Sergiy Semendyay, Heorhiy Bilenky

TRAINING STAND FOR THE STUDY OF DISCIPLINES TO ENSURE NETWORK INFORMATION PROTECTION

Relevance of the research topic. *Today, computer networks have become widespread, without which it is no longer possible to imagine the functioning of any computer system. Widespread and accessible led to the need to differentiate access to the components of such systems and to introduce into the training of technical specialties such disciplines as "Organization of computer networks", "Computer network protection systems" and others.*

Formulation of the problem. *In the field of studying disciplines related to modern computer networks and their security, a significant place is occupied by practical skills of setting up software and hardware. One of the most effective methods is training using semi-natural and full-scale models of computer networks.*

Analysis of recent research and publications. *Recent open source publications are reviewed, including data from Cisco and Mikrotik training centers.*

Selection of unexplored parts of the general problem. *Development and substantiation of the use of semi-natural models of modern computer networks in the educational process of specialized disciplines of higher educational institutions.*

Setting objectives. *To offer a basic semi-natural model of a computer network for a stand for studying disciplines on providing network information protection.*

Presenting main material. *The article presents the analysis, requirements and half-scale model of a computer network stand for studying disciplines for network information protection.*

Conclusions in accordance with the article. *A full-scale model of a computer network stand is proposed for studying disciplines on providing network information protection using Mikrotik network equipment.*

Keywords*: computer network, information technologies, cybersecurity, switching, MikroTik, encryption, modeling.*
Fig .: 2. References: 7.

Риндич Євген Володимирович – кандидат технічних наук, доцент, доцент кафедри інформаційних та комп'ютерних систем, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Yevhen Ryndych – PhD in Technical Science, Associate Professor, Associate Professor of Information and Computer Department, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: yevhen.ryndych@stu.cn.ua
ORCID: http://orcid.org/0000-0002-2723-4144
ResearcherID: F-6080-2014
SCOPUS Author ID: 57188702150

Петренко Тарас Анатолійович – кандидат технічних наук, доцент кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Petrenko Taras – PhD in Technical Science, Associate Professor of Department of Cybersecurity and Mathematical Simulation, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: mail_taras@ukr.net
ORCID: https://orcid.org/0000-0001-5571-3815
ResearcherID: G-5801-2014
SCOPUS Author ID: 57193026484

Черниш Леся Григорівна – кандидат технічних наук, доцент, доцент кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Chernysh Lesia – PhD in Technical science, Associate Professor, Associate Professor of Department of Cybersecurity and Mathematical Simulation, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: lg4@ukr.net
ORCID: http://orcid.org/0000-0001-7446-1684

Семендяй Сергій Матвійович – завідувач лабораторії кібербезпеки, аспирант, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Semendiai Serhii – Head of the cybersecurity laboratory, PhD Student, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: sovnarcom@ukr.net
ORCID: http://orcid.org/0000-0002-7751-5956

Біленький Георгій Сергійович – магістр кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Bilenkyi Heorhiy – Master of the Department of Cybersecurity and Mathematical Modeling, Chernihiv National Technological University (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: damian2000@bigmir.net
ORCID: https://orcid.org/0000-0001-6056-0526

Риндич Є., Петренко Т., Черниш Л., Семендяй С., Біленький Г. Навчальний стенд для вивчення дисциплін із забезпечення мережевого захисту інформації. *Технічні науки та технології.* 2020. № 2 (20). С. 229-236.