ЗАТВЕРДЖЕНО

Вченою радою факультету інформаційно комп'ютерних технологій

30 серпня 2021 р.,

протокол № 7

Голова Вченої ради

Надія ЛОБАНЧИКОВА

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Побудова захищених мережних інфраструктур на базі обладнання MikroTik»

для здобувачів вищої освіти освітнього ступеня «магістр»
спеціальності 125 «Кібербезпека»
освітньо-професійна програма «Кібербезпека»
факультет інформаційно комп'ютерних технологій
кафедра комп'ютерної інженерії та кібербезпеки

Схвалено на засіданні кафедри біомедичної інженерії та телекомунікацій
26 серпня 2021 р.,
протокол № 10

Завідувач кафедри
Тетяна НІКІТЧУК

Розробник: старший викладач кафедри біомедичної інженерії та телекомунікацій МОРОЗОВ Дмитро

Житомир
2021 – 2022 н.р.

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітній ступінь	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів 5	Галузь знань: 12 «Інформаційні технології»	за вибором	
Модулів – 5	Спеціальність: 125 «Кібербезпека»	Рік підготовки:	
Змістових модулів – 5		1	__
		Семестр	
Загальна кількість годин - 150		2	__
		Лекції	
Тижневих годин для денної форми навчання: аудиторних 4 самостійної роботи – 2	Освітній ступень: «магістр»	32 год.	__ год.
		Практичні	
		__ год.	__ год.
		Лабораторні	
		32 год.	__ год.
		Самостійна робота	
		86 год.	__ год.
		Вид контролю: Залік	

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання – _47_ % аудиторних занять, _53_ % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою дисципліни «Побудова захищених мережних інфраструктур на базі обладнання MikroTik» є вивчення теоретичних та практичних основ проектування, розробки і побудови захищених мережних інфраструктур на сучасному мережевому обладнанні від компанії MikroTik, вивчення основних прийомів роботи з операційною системою RouterOS і роботі з додатковими пакетами та утилітами, маршрутизації, бріджингу, налаштуванню файєрволів і керуванню трафіком. Особлива увала приділяється створенню, налаштуванню і роботі з віртуальними локальними мережами, питанням безпеки мережі і пошуку несправностей в роботі мережевої інфраструктури.

Завданнями вивчення дисципліни «Побудова захищених мережних інфраструктур на базі обладнання MikroTik» є розвиток у майбутнього фахівця уміння проектувати, обслуговувати і усувати несправності в роботі захищених мереж, засвоєння практичних навичок роботи з мережевим обладнанням MikroTik, налаштуваню, пошуку і виправленню несправностей, виконання заходів безпеки при розробці, розгортанні і експлуатації захищених мережевих інфраструктур на базі обладнання MikroTik

Зміст навчальної дисципліни направлений на формування наступних **компетентностей**:

- Здатність до використання сучасного мережевого обладнання, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки для побудови захищених мережевих інфраструктур.
- Здатність забезпечувати захист інформації, що обробляється в мережах на базу обладнання MikroTik з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
- Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації в мережах на базу обладнання MikroTik.

Отримані знання з навчальної дисципліни стануть складовими наступних **програмних результатів** навчання:

- Проектувати, налаштовувати і обслуговувати мережі на базі обладнання MikroTik.
- Вирішувати задачі захисту потоків даних в мережі побудованій на базі обладнання MikroTik.
- Працювати з обладнанням Mikrotik та операційною системою RouterOS
- Захищати ресурси мережі з MikroTik RouterOS

- Налаштовувати захист мережі за допомогою засобів MikroTik RouterOS;
- Протидіяти різним атакам на мережну інфраструктуру;
- Проектувати і налаштовувати VPN із шифруванням, у тому числі IPSec;
- Налаштувати на мережевому обладнанні MikroTik Firewall, DNS, DHCP, QOS, обмеження швидкості, пріоритизацію специфічних типів трафіку (SIP, Web, RDP, Video та ін.)
- Проводити базові та розширені налаштування бездротових мереж на базі обладнання на MikroTik
- Проводити діагностику та усунення неправильних налаштувань маршрутизації та безпеки у бездротових мережах. Wi-Fi.
- Виконувати діагностику та усунення неправильних налаштувань маршрутизації Wi-Fi.

3. Програма навчальної дисципліни

Змістовий модуль 1. «Основи роботи з обладнанням MikroTik»

1. Введення в RouterOS. Що таке RouterOS та RouterBoard. Історія компанії MikroTik. Обладнання RouterBOARD фіксовані та інтегровані рішення. Розшифровка назви обладнання. Аксесуари та програма MFM. Семірівнева модель взаємодії відкритих систем ISO OSI та IP-протокол. Мережа Ethernet: історія появи, топологія, колізії, протокол CSMA/CD. Перешкодостійкість, вітчизняні проблеми із трифазними мережами та заземленням. Коаксіальний кабель і вита пара, хаби і комутатори. Адресація в мережах Ethernet, MAC-адреси. Адресація в мережі Інтернет, підмережі, розрахунок підмереж. Виділені блоки IP-адрес. IP-протоколи, IP-адреси та порти. Процес встановлення TCP-з'єднання. Підключення до маршрутизатора, Winbox, MAC-Winbox, SSH, Telnet, послідовний порт, інтерфейс командного рядка (CLI). WebFig та QiuckSet. Початкова конфігурація, встановлення IP-адрес, шлюзу за замовчуванням, DHCP-клієнт та NAT. Функціональність RouterOS, встановлення та видалення пакетів, апгрейд RouterOS та RouterBOOT. Ім'я маршрутизатора, керування користувачами та сервісами. Резервне копіювання та відновлення конфігурації. Скидання маршрутизатора у початкові налаштування. Опції кнопки Reset. Установка RouterOS за допомогою NetInstall. Ліцензування RouterOS.

2. ARP і DHCP. Протокол ARP, режими ARP, ARP-таблиця. DHCP-клієнт. DHCP-сервер, налаштування, керування виділенням адрес та мережевих

параметрів..

3. Bridging. Що таке бридж, створення, додавання портів, налаштування бриджу. Відмінності установок у різних версіях RouterOS. Архітектура маршрутизатора, вбудований комутатор. Особливості додавання до бриджу бездротових інтерфейсів.

Змістовий модуль 2. «Маршрутизація на обладнанні MikroTik»

4. Статична маршрутизація. Вибір маршруту. Точні маршрути. Дистанція. Маршрути рівної вартості (ECMP) та балансування трафіку між каналами. Check Gateway. Recursive next-hop та використання scope/target-scope. Автоматичне перемикання на резервний канал. Policy Based Routing (PBR). Traffic flow diagram. IP firewall mangle. Routing mark та route policy. Per Connection Classifier. Приклад балансування вихідного трафіку для трьох провайдерів. Переключення на резевого провайдера для трьох провайдерів. Адресація в мережах "Point-to-Point". Налаштування адресації в мережах "Point-to-Point".

5. **VPN.** Типи тунелів. Основні властивості тунелів, тунелі з шифруванням та без, способи шифрування. З'єднання майданчиків за допомогою тунелів ls (IPIP, EoIP, PPTP, SSTP, L2TP, PPPoE).VLAN в RouterOS. QinQ та його використання. Керований комутатор у RouterBoard, основні можливості. Налаштування VLAN на керованому комутаторі RouterBoard.

6. OSPF. Протокол OSPF та його місце у сімействі протоколів динамічної маршрутизації. Як працює OSPF (Hello protocol, Database distribution та типи LSA). Структура OSPF мережі (Areas, типи маршрутизаторів). Відносини суміжності у OSPF, типи суміжності, вибори DR та BDR. Методи застосування зовнішніх маршрутів (type1 і type2). Вартість інтерфейсу та тип інтерфейсу ((broadcast, NBMA, PtP, PtMP) Алгоритм SPT. OSPF та multicast трафік (проблеми в NBMA мережах). Типи area (Stub, NSSA, агрегування маршрутів). Використання Virtual Link. Фільтрування маршрутів.

Змістовий модуль 3. «Керування трафіком на обладнанні MikroTik»

7. Міжмережевий екран (Firewall). Принципи роботи Firewall. Connection tracking та стан з'єднання. Ланцюжки (chains). Дії над пакетами. Захист сервісів, що працюють на роутері. Захист клієнтів. Address List та робота з ним. Основи L7 фільтрації. Source NAT, masquerade and src-nat action Destination NAT, dst-nat and redirect actions. FastTrack.

8. QoS. Принципи керування трафіком, ідея "ковзного вікна" в TCP-протоколі. Прості черги (simple queue) Target, Destinations, Max-limit та limit-at, Bursting. Справедливий розподіл смуги пропускання. Принцип роботи Per Connection Queue (PCQ), pcq-rate та pcq-limit.

Змістовий модуль 4. «Бездротові мережі побудовані на обладнанні MikroTik»

9. Огляд бездротового обладнання Mikrotik. Огляд програмної частини реалізації бездротового зв'язку в RouterOS. Які бувають антени, характеристики антен. Процес перетворення цифрового сигналу на радіосигнал – принципи та обмеження. Стандарти 802.11a/b/g/n/ac/ah. Частоти, смуги, канали, швидкості передачі, вибір антени, потужність передавача та чутливість приймача. Адміністративні обмеження використання радіочастотного ресурсу. Розрахунок енергетики радіолінку. Wireless утиліти. Scan, Frequency usage, Spectral Scan/History, Snooper, Align, Sniffer. Вирішення проблем. Аналіз інформації у Registration table. Ack-Timeout/Distance. CCQ. 4. TX/RX Signal Strength. Frames and HW-frames. Data-rates.

10. Розширені налаштування Wi-Fi. HW-retries, HW-protection, Adaptive-noise-immunity. WMM. Регіональні налаштування та DFS. Управління потужністю передавача. Віртуальні точки доступу. Протоколи 802.11ah. Модуляції, швидкості, об'єднання каналів. Поєднання кадрів, захисний інтервал. Управління потужністю передавача у стандартах 802.11ah. MIMO та Chain settings. Налагодження бездротового лінка.

11. Безпека у бездротових мережах. Керування доступом до бездротової мережі. Access-List та Connect-List. Authentication, Encryption, Management Frame Protection. Протоколи EAP та авторизація на RADIUS-сервері. Робота бездротового клієнта в домені Windows. WDS та MESH. Динамічний та статичний WDS. RSTP Bridge. Wireless MESH, HWMP+. Wireless Bridging. WDS bridging. AP/Station-WDS. Типи pseudobridge. MPLS/VPLS тунелі. Протокол Nstreme. Конфігурація Nstreme. Налаштування Nstreme Dual. Протокол Nv2. Принцип роботи та основні можливості протоколу Nv2. Конфігурація Nv2. Налаштування Nv2.

12. CAPsMAN. Централізоване керування точками доступу - принцип роботи, основні можливості. Налаштування CAPsMAN-сервера та клієнтів. Особливості налаштування точок стандарту 802.11n/ac на прикладі дводіапазонної точки Mikrotik wAP ac.

Змістовий модуль 5 «Захист мереж побудованих на обладнанні MikroTik»

13. Безпека в RouterOS. Атаки, механізми та сервіси. Найпоширеніші небезпеки. Розгортання системи безпеки RouterOS. Порядок обробки потоку пакетів, ланцюжка міжмережевого екрану. Брандмауер із відстеженням стану. Таблиця RAW. Усунення наслідків SYN-флуду за допомогою таблиці RAW. Конфігурація RouterOS за промовчанням. Найкращі практики для управління доступом. Виявлення атаки на критично важливі служби інфраструктури. Низькорівневе фільтрування bridge. Розширені параметри у фільтрі брандмауера. ICMP-фільтрація. Атаки на рівні OSI. Атаки MNDP та їх запобігання. DHCP: підроблені сервери, атаки на виснаження пулу та їх запобігання. Атаки TCP SYN та їх запобігання. UDP-атаки та їх запобігання. ICMP Smurf-атаки та їх запобігання. Атаки на FTP, telnet та SSH методом перебору та їх запобігання. Виявлення та запобігання скануванню портів.

14. Криптографія. Введення в криптографію та термінологію. Методи шифрування. Алгоритми - симетричні та асиметричні. Інфраструктура відкритих ключів (PKI). Сертифікати. Самопідписані сертифікати. Безкоштовні чинні сертифікати. Використання сертифікатів у RouterOS.

15. Захист маршрутизатора. ICMP-Knocking, port-knocking. Безпечні з'єднання (HTTPS, SSH, WinBox). Стандартні порти для служб

16. Захищені тунелі. Вступ до Ipsec. Варіанти реалізації IPSec. Базове та розширене налаштування IPSec. Ipsec із сертифікатами. L2TP + Ipsec. SSTP із сертифікатами.

4. Структура (тематичний план) навчальної дисципліни

Кредитні модулі	Змістовні модулі	Кількість годин			
		Всього	Лекції	Лабораторні	Самостійна робота
1	2	3	4	5	6
№1	**Змістовий модуль 1. «Основи роботи з обладнанням MikroTik»**				
	1. Введення в RouterOS.	10	2	4	4
	2. ARP і DHCP.	6	2		4
	3. Bridging.	6	2		4
	Разом змістовний модуль 1	22	6	4	12

№2	**Змістовий модуль 2. «Маршрутизація на обладнанні MikroTik»**				
	4. Статична маршрутизація.	8	2		6
	5. VPN.	10	2	4	4
	6. OSPF.	10	2	4	4
	Разом змістовний модуль 2	28	6	8	14
№3	**Змістовий модуль 3. «Керування трафіком на обладнанні MikroTik»**				
	7. Міжмережевий екран (Firewall).	8	2		6
	8. QoS.	12	2	4	8
	Разом змістовний модуль 3	20	8	8	24
№4	**Змістовий модуль 4. «Бездротові мережі побудовані на обладнанні MikroTik»**				
	9. Огляд бездротового обладнання Mikrotik.	6	2		4
	10. Розширені налаштування Wi-Fi	14	2	4	8
	11. Безпека у бездротових мережах.	6	2		4
	12. CAPsMAN	14	2	4	8
	Разом змістовний модуль 4	40	8	8	24
№5	**Змістовий модуль 5 «Захист мереж побудованих на обладнанні MikroTik»**				
	13. Безпека в RouterOS.	12	2	4	6
	14. Криптографія.	4	2		2
	15. Захист маршрутизатора.	4	2		2
	16. Захищені тунелі.	10	2	4	4
	Разом змістовний модуль 5	40	8	8	14
	ВСЬОГО	150	32	32	86

5. Теми лабораторних робіт

№ з/п	Назва теми	Кількість годин
1	Знайомство з RouterOS	4
2	Налаштування маршрутизації в мережі, побудованій на обладнанні MikroTik	4
3	Налаштування Firewall в мережі, побудованій на обладнанні MikroTik	4
4	Налагодження бездротової мережі на роутері MikroTik hAP AC2.	4
5	Налагодження бездротової SOHO мережі на обладнанні MikroTik	4
6	Налагодження то дослідження роумінгу в бездротовій мережі побудованій за технологією CAPsMAN від MikroTik	4
7	Побудова захищеної мережевої інфраструктури на базі обладнання MikroTik	4
8	Пошук і виправлення помилок в налаштуванні мережі побудованої на обладнанні MikroTik	4
	Разом	32

6. Завдання для самостійної роботи

№	Назва теми	Кількість годин
1	Утиліти: E-mail, Netwatch, Ping, Traceroute, Profiler (завантаження CPU)	2
2	Інструменти моніторингу: Interface traffic monitor, Torch, Graphs, SNMP, The Dude.	2
3	Робота з техпідтримкою Mikrotik support@mikrotik.com supout.rif, autosupout.rif створення та перегляд.	2
4	Логування у RouterOS, детальні логи.	2
5	Правила найменування елементів та коментарі.	2
6	Мережева діаграма.	2
	Разом	**12**

7. Методи контролю

Освітній процес побудований на сполученні лекційних і лабораторних занять з самостійною роботою студенів. Лекційні заняття призначені для теоретичного осмислення й узагальнення складних розділів курсу, що висвітлюється в основному на проблемному рівні. Лабораторні заняття призначені для отримання практичних навичок роботи з мережевим обладнанням від MikroTik.

8. Схема нарахування балів

Модулі та їх елементи	Форма контролю	Максимальна кількість балів
Змістовий модуль 1. «Основи роботи з обладнанням MikroTik»		
Лекції 1-3 по темам 1-3	Модульна контрольна робота №1	10
Лабораторна робота №1	Виконання і захист ЛР	5
Разом за змістовий модуль 1		15
Змістовий модуль 2. «Маршрутизація на обладнанні MikroTik»		
Лекції 4-6 по темам 4-6	Модульна контрольна робота №2	10
Лабораторна робота №2	Виконання і захист ЛР	5
Лабораторна робота №3	Виконання і захист ЛР	5
Разом за змістовий модуль 2		20
Змістовий модуль 3. «Керування трафіком на обладнанні MikroTik»		

Лекції 7-8 по темам 7-8	Модульна контрольна робота №3	10
Лабораторна робота №4	Виконання і захист ЛР	5
Разом за змістовий модуль 3		15
Змістовий модуль 4. «Бездротові мережі побудовані на обладнанні MikroTik»		
Лекції 9-12 по темам 9-12	Модульна контрольна робота №4	10
Лабораторна робота №5	Виконання і захист ЛР	5
Лабораторна робота №6	Виконання і захист ЛР	5
Разом за змістовий модуль 4		20
Змістовий модуль 5 «Захист мереж побудованих на обладнанні MikroTik»		
Лекції 13-16 по темам 13-16	Модульна контрольна робота №5	10
Лабораторна робота №7	Виконання і захист ЛР	10
Лабораторна робота №8	Виконання і захист ЛР	10
Разом за змістовий модуль 5		30
Екзамен		100
Оцінка по дисципліні		**100**

9. Рекомендована література

Основна література

1. Stephen Discher. RouterOS by Example, 2nd Edition: B&W, 2016 - 440 pages.
2. Tyler Hart. Networking with MikroTik: MTCNA Study Guide, 2017 -360 pages.
3. Tyler Hart. MikroTik Security guide, 2017 – 127 pages.

Допоміжна література

4. Stephen R. W. Discher. RouterOS by Example: Understanding MikroTik RouterOS Through Real Life Examples, 2011 – 360 pages

12. Інформаційні ресурси в Інтернеті

1. https://mikrotik.com/
2. https://help.mikrotik.com/docs/
3. https://help.gowifi.co.nz/support/solutions/articles/48001077268-beginners-guide-to-configuring-a-mikrotik-router-from-start-to-finish
4. https://www.watchguard.com/help/docs/help-center/en-US/Content/Integration-Guides/General/Mikrotik%20VPN_firebox.html
5. https://mum.mikrotik.com/presentations/MN17/presentation_4575_1497945824.pdf