СИЛАБУС
Кафедра кібербезпеки та математичного моделювання

Назва курсу	Технології безпеки бездротових і мобільних мереж
Мова викладання	Українська
Викладач (-і)	М.Є. Шелест професор кафедри кібербезпеки та математичного моделювання, доктор технічних наук, професор
Профайл викладача (-ів)	0000-0001-7110-4876
Контакти викладача	mishel3141@gmail.com

1. Анотація курсу - в даному курсі розглядаються засоби та методи забезпечення безпеки бездротових мереж, вивчаються комерційні бездротові протоколи. Тематика курсу – сучасні інформаційні технології.

2. Мета та цілі курсу - формування науково-професійного світогляду магістра спеціальності Кібербезпека в області безпеки інформаційних і комунікаційних систем, уміння вирішувати задачі адміністрування бездротових і мобільних мереж та систем, застосовувати нормативно-правові, організаційні та технічні процедури при роботі безпроводових і мобільних технологій.

Під час вивчення дисципліни здобувач вищої освіти (ЗВО) має набути або розширити наступні загальні (КЗ) та фахові (КФ) компетентності, передбачені освітньою програмою спеціальності 125 - Кібербезпека:

КЗ1. Здатність застосовувати знання у практичних ситуаціях.

КЗ2. Знання та розуміння предметної області та розуміння професії.

КЗ4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КФ3. Здатність до проектування, впровадження, супроводження інформаційних мереж і ресурсів, інфраструктури установи, архітектури використання інформаційних технологій (хмарних), а також бізнес/операційних процесів з метою якісного функціонування інформаційно-комунікаційних систем (комутативних або без комутативних), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації.

КФ5. Здатність розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, а також систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації.

3. Результати навчання –

Під час вивчення дисципліни ЗВО має досягти або вдосконалити наступні програмні результати навчання (ПРН), передбачені освітньою програмою:

ПРН2. планувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

ПРН3. використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

ПРН4. аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

ПРН7. проектувати, впроваджувати, та супроводжувати інформаційно-комунікаційні системи, а також забезпечувати захист інформаційних ресурсів мереж (мережева безпека) та всієї інфраструктури установи на базі сучасних моделей, методів і засобів передачі даних в комутативних або без комутативних каналах зв’язку, хмарного простору, протоколів обміну даними, мережного устаткування, тощо ;

ПРН8. проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту додатків (веб - додатків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації;

ПРН10. розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно - апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації.

Після курсу здобувач вищої освіти отримає наступні навички:

1. розробляти бездротові інфраструктури;
2. вибирати бездротову конфігурацію;
3. створювати політики безпеки;
4. встановлювати рейтинги дозволів;
5. проводити аудит службової мережі;
6. з’єднувати поточну мережу з іншими провідними та безпроводовими мережами;
7. забезпечувати доступність та масштабованість бездротової мережі;
8. захищати мобільні пристрої та канали зв’язку від кібератак.

4. Обсяг курсу. Зазначте загальну кількість кредитів, кількість занять та годин самостійної роботи

Вид заняття	**Загальна к-сть годин**
лекції	20
лабораторні заняття	20
самостійна робота, РГР	110

5. Пререквізити – для вивчення даної дисципліни бажаним є прослуховування курсу «Комп'ютерні мережі».

6. Система оцінювання та вимоги

Загальна система оцінювання курсу	З дисципліни ЗВО може набрати до 60% підсумкової оцінки за виконання всіх видів робіт, що виконуються протягом семестру і до 40% підсумкової оцінки – на заліку.
Вимоги до РГР	Відповідність умовам завдання – до 4 балів; експериментальне підтвердження – до 2 балів; обґрунтованість рішень – до 3 балів; посилання на першоджерела – до 2 балів; відповідність оформлення вимогам – до 2 балів; своєчасність здачі – до 2 балів. Захист РГР: самостійність виконання (відповіді на запитання) – до 5 балів.
Умови допуску до підсумкового контролю	У випадку, якщо ЗВО протягом семестру не виконав в повному обсязі передбачених робочою програмою всіх видів навчальної роботи, має невідпрацьовані лабораторні роботи або не набрав мінімально необхідну кількість балів (20), він не допускається до складання екзамену під час сесії, але має право ліквідувати академічну заборгованість у порядку, передбаченому «Положенням про поточне та підсумкове оцінювання знань ЗВО ЧНТУ».

7. Політики курсу - Виконання та особистий захист усіх лабораторних робіт, зазначених у робочій навчальній програмі з дисципліни, є обов'язковим. Поточний контроль проводиться шляхом спілкування із ЗВО під час лекцій та консультацій та опитувань ЗВО під час захисту лабораторних робіт.

8. Рекомендована література

1. Соколов, В. Ю. Безпека безпроводових і мобільних мереж : Лабораторний практикум / В. Ю. Соколов, М. Тадж-Діні / ред. перекл. О. П. Райтер. — К. : ДУТ, 2018. — 122 с.

2. Sokolov, V. Wireless and Mobile Security : Laboratory Workshop / V. Sokolov, M. Taj Dini, V. Buryachok. — K. : SUT, 2017. — 124 p.

3. Wireless Geographic Logging Engine database https://wigle.net/graph-large.html.

4. Astapenya V. M., Sokolov V. Yu. "Modified accelerating lens as a means of increasing the throughput, range and noise immunity of IEEE 802.11 systems," ICATT'2015 Proceedings of the X Anniversary International Conference on Antenna Theory and Techniques, Kharkiv, Apr. 2015, pp. 267–269.

5. “CC2500 Low-Cost Low-Power 2.4 GHz RF Transceiver,” Texas Instruments, 2016, 97 p.

6. “Pololu Wixel User’s Guide,” Pololu Corporation, 2015, 67 p.

7. V. Buryachok, G. Gulak, V. Sokolov. “Miniaturization of Wireless Monitoring Systems 2.4–2.5 GHz Band,” Proceedings of the II International Scientific-Technical Conference on Actual Problems of Science and Technology, Kiev, Dec. 2015, p. 41.

8. “nRF24L01 Single Chip 2.4GHz Transceiver Product Specification,” Nordic Semiconductor ASA, Version 2.0, July 2007, 74 p.

9. Graham, E., Steinbart, P.J. Wireless Security. 2006.

10. Cisco. Dictionary attack on Cisco LEAP vulnerability, Revision 2.1, 19 July 2004.

11. CSI. CSI/FBI Computer Crime and Security Survey. 2004.

12. Hopper, D. I.(2002). Secret Service agents probe wireless networks in Washington.

13. IEEE 802.11-2007, New York, NY, USA. 2007.

14. IEEE 802.11i-2004, New York, NY, USA. 2004.

15. Bellardo, J., Savage, S. 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In: Proceedings of the 12th USENIX Security Symposium, Berkeley, CA, USA, USENIX Association, 2003.

16. Aime, M.D., Calandriello, G., Lioy, A.: Dependability in wireless networks: Can we rely on WiFi IEEE Security and Privacy 5, p. 23–29, 2004.

17. Devine, C., d’Otreppe, T., Beck, M.: Aircrack-ng. 2009. http://www.aircrack-ng.org.

18. Smith, J.: Denial of service: Prevention, modelling and detection. 2007.

19. Glass, S., Muthukkumarasamy, V.: A study of the TKIP cryptographic DoS attack. In: ICON 2007: Proceedings of the 15th IEEE International Conference on Networks, New York, NY, USA, IEEE, p. 59–65. 2007.

20. Tews, E., Beck, M.: Practical attacks against WEP and WPA. In: WiSec ’09: Proceedings of the second ACM conference on Wireless network security, New York, NY, USA, ACM, p. 79–86. 2009.