ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет програмування та комп'ютерних і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем і мереж

ЗАТВЕРДЖУЮ
Декан ФПКТС
_____ Савенко О.С.
«___» _____ 2021 р.

СИЛАБУС
Навчальна дисципліна: "Безпека безпроводових і мобільних технологій"

Освітньо-професійна програма: «Кібербезпека»

Рівень вищої освіти: перший (бакалаврський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Орленко Вікторія Сергіївна
Профайл викладач(ів)	http://ksm.khnu.km.ua/sklad-kafedry/
E-mail викладача(ів)	orlenkovs@khmnu.edu.ua
Контактний телефон	Наявний в ІСУ
Сторінка дисципліни в ІСУ	https://msn.khnu.km.ua/course/view.php?id=6775
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us04web.zoom.us/j/8577265687 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2021-2022, семестр V (осінньо-зимовий)
Розклад	
Консультації	

Характеристика дисципліни

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття					Залік	Іспит
Д	3	5	5	150	68	34	34	-	-	82	-	-	-	+

Анотація дисципліни

Дисципліна формує у студентів знання про безпеку інтернет-речей, забезпечення конфіденційності для користувачів безпроводових та мобільних технологій на етапі їх проектування, загрози конфіденційності в безпроводових та мобільних технологіях, безпеку та конфіденційність у підтримці хмарних технологій.

Дисципліна викладається для студентів денної форми навчання спеціальності «Кібербезпека». При викладанні дисципліни використовуються наступні форми (методи) навчання: пояснювально-ілюстративні, практичні, продуктивні, контекстні, моделювання, застосування інформаційно-комп'ютерних технологій (автоматизована система проектування Cisco Packet Tracer, інструменти та утиліти ОС Kali Linux).

Пререквізити: електроніка і схемотехніка систем захисту.

Кореквізити: комплексні системи захисту інформації: проектування, впровадження, супровід.

Мета і завдання дисципліни

Метою викладання навчальної дисципліни «Безпека безпроводових і мобільних технологій» є формування у майбутніх спеціалістів умінь та компетенцій для оцінювання та забезпечення необхідного рівня захищеності інформації в безпроводових та мобільних мережах; розвиток у студентів фахового стилю мислення; надання глибоких та міцних знань з питань безпеки та захисту сучасних безпроводових та мобільних технологій; сучасного програмно-апаратного забезпечення безпроводових та мобільних технологій тощо.

Предметом дисципліни є міжнародні практики щодо здійснення щодо здійснення професійної діяльності з питань захисту та безпеки мобільних технологій та безпроводових мереж; методи та засоби оцінювання та забезпечення необхідного рівня захищеності інформації.

Завданням дисципліни є забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до Стандарту вищої освіти та освітньо-професійної програми підготовки бакалаврів зі спеціальності «Кібербезпека»:

***компетентності*:**

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах;

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки;

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

результати навчання:

РН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.

РН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень.

РН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

РН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

РН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

Студент, який успішно завершив вивчення дисципліни, повинен: *застосовувати* сучасні методи і моделі інформаційної безпеки та/або кібербезпеки, теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем, в тому числі безпроводових та мобільних систем; *вирішувати* завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та *давати* оцінку результативності якості прийнятих рішень; *використовувати* сучасне програмно-апаратне забезпечення інформаційно-телекомунікаційних систем, зокрема безпроводових та мобільних систем; *реалізовувати* заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; *аналізувати* проекти безпроводових та мобільних систем, базуючись на стандартизованих технологіях та протоколах передачі даних, *виявляти* та *оцінювати* можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам безпроводових та мобільних систем згідно з встановленою політикою інформаційної та/або кібербезпеки.

Тематичний і календарний план вивчення дисципліни

№ тижня	**Тема лекції***	**Тема лабораторної роботи (ЛР) ****	**Самостійна роботи**		
			Зміст	**Год.**	**Література**
1	**Загрози та атаки на безпроводові мережі.** Класифікація атак на безпроводові мережі та їх характеристики. Моделі та критерії загроз у безпроводових мережах. Методи оцінки загроз у безпроводових мережах	**ЛР1.** Розгортання робочого середовища для проведення аудиту безпеки безпроводових мереж	Опрацювання теоретичного матеріалу. Підготовка до виконання ЛР1.	5	[1] с. 13-25 [6] с. 9-21 [7] с. 15-29 [8] с. 346-356, с. 390-407
2	**Захист безпроводових мереж.** Технології побудови безпроводових мереж. Шляхи захисту безпроводових мереж	-	Опрацювання теоретичного матеріалу. Підготовка до захисту ЛР1.	5	[1] с. 25-58 [8] с. 346-356, с. 390-407 [12] с. 29-44
3	**Загрози та вразливості мобільних пристроїв.** Загальні положення. Класифікація загроз та вразливостей мобільних пристроїв	**ЛР2.** Сканування мережевих протоколів	Опрацювання теоретичного матеріалу. Підготовка до виконання ЛР2.	5	[2] с. 1-9 [6] с. 9-31 [7] с. 15-47 [15]

4	**Управління мобільними пристроями.** Управління з метою забезпечення захисту. Життєвий цикл рішень з безпеки мобільних пристроїв	-	Опрацювання теоретичного матеріалу. Підготовка до захисту ЛР2.	5	[2] с. 9-17 [11] с. 18-38 [16] с. 10-12, 25-27
5	**Загрози та вразливості мобільних телекомунікаційних систем.** Загрози та вразливості стандартів 3G. Загрози та вразливості стандартів 4G. Загрози та вразливості стандартів 5G	**ЛР3.** Збирання технічної та чуттєвої інформації в безпроводових мережах	Опрацювання теоретичного матеріалу. Підготовка до виконання ЛР3.	5	[2] с. 17-24 [6] с. 21-31, с. 48-54 [7] с. 29-61 [11] с. 38-68
6	**Загрози та вразливості Wi-Fi-мереж.** Класифікація загроз та вразливостей Wi-Fi-мереж. Методи захисту Wi-Fi-мереж	-	Опрацювання теоретичного матеріалу. Підготовка до захисту ЛР3.	5	[2] с. 24-41 [8] с. 396-407
7	**Загрози та вразливості мобільних додатків.** Класифікація загроз та вразливостей мобільних додатків. Аналіз захищеності мобільних додатків	**ЛР4.** Дослідження вразливостей безпроводових мереж	Опрацювання теоретичного матеріалу. Підготовка до виконання ЛР4.	5	[2] с. 41-48 [6] с. 48-62 [7] с. 47-61 [11] с. 160-212
8	**Вступ до Інтернету речей.** Загальні принципи побудови та архітектура IoT. Класифікація систем IoT	-	Опрацювання теоретичного матеріалу. Підготовка до захисту ЛР4.	5	[9] с. 5-43 [10] с. 208-233

9	**Засоби ідентифікації в IoT**. Класифікація засобів автоматичної ідентифікації. MAC-адреса. Радіочастотна ідентифікація (RFID). Система позиціонування в режимі реального часу RTLS. Оптичні ідентифікатори	**ЛР5.** Дослідження технологій злому безпроводових мереж	Опрацювання теоретичного матеріалу. Підготовка до виконання ЛР5.	5	[6] с. 54-62 [7] с. 61-75 [9] с. 44-63
10	**Технології передачі даних в IoT (частина 1).** Стандарт IEEE 802.15.4. Bluetooth (IEEE 802.15.1). ZigBee. Wi-Fi та IEEE 802.11	-	Опрацювання теоретичного матеріалу. Підготовка до захисту ЛР5.	5	[4] с. 60-76 [9] с. 120-156
11	**Технології передачі даних в IoT (частина 2).** Технологія LPWAN. Технологія PLC	**ЛР6.** Дослідження способів здійснення атак на відмову	Опрацювання теоретичного матеріалу. Підготовка до виконання ЛР6.	5	[5] с. 107-259 [7] с. 61-75, с. 87-97
12	**Огляд основних протоколів IoT.** Протоколи обміну даними	-	Опрацювання теоретичного матеріалу. Підготовка до захисту ЛР6.	5	[4] с. 60-76 [9] с. 64-156
13	**Забезпечення безпеки в IoT (частина 1).** Проблема безпеки IoT. Проблеми конфіденційності в IoT	**ЛР7.** Програмування пристроїв Інтернету речей засобами Cisco Packet Tracer	Опрацювання теоретичного матеріалу. Підготовка до виконання ЛР7.	5	[3] с. 5-30 [5] с. 385-427 [7] с. 87-97
14	**Забезпечення безпеки в IoT (частина 2).** Анатомія кібератак на IoT-пристрої. Фізична і апаратна безпека. Криптографія, як складова безпеки в IoT. Блокчейн і криптовалюта в Інтернеті речей	-	Опрацювання теоретичного матеріалу. Підготовка до захисту ЛР7.	5	[5] с. 385-427

15	**Топологія хмарних обчислень.** Модель хмарних сервісів. Види хмар та хмарна архітектура. Хмарна архітектура OpenStack. Обмеження хмарних архітектур	**ЛР8.** Захист хмарних сервісів Інтернету речей	Опрацювання теоретичного матеріалу. Підготовка до виконання ЛР8.	5	[3] с. 5-36 [13] с. 170-207 [14] с. 33-41
16	**Топологія туманних обчислень.** Туманні обчислення Архітектура OpenFog RA. Amazon Greengrass і лямбда-функції. Туманні топології	-	Опрацювання теоретичного матеріалу. Підготовка до захисту ЛР8.	5	[5] с. 312-340
17	Технології Big Data. Поняття Big Data, їх характеристики та сфери застосування. Категорії даних (грані даних) та процес data science. Технології та тенденції роботи з Big Data	**Контрольна робота**	Опрацювання теоретичного матеріалу. Підготовка до контрольної роботи за пройденим матеріалом.	2	[3] с. 31-36 [5] с. 341-384

*** лекції проводяться по 2 години щотижня;**
**** лабораторні проводяться по 4 години раз в два тижні.**

ПОЛІТИКА ДИСЦИПЛІНИ

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції, лабораторні роботи згідно з розкладом, не запізнюватися на заняття, вчасно виконувати та здавати лабораторні роботи. Термін виконання лабораторної роботи вважається своєчасним, якщо студент здав/захистив її на поточному або наступному за ним занятті. За несвоєчасний захист лабораторної роботи з набраної студентом суми балів вираховується один бал. Пропущене з поважної причини лабораторне заняття студент повинен відпрацювати у встановлений викладачем термін.

Набуті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок перезарахування результатів навчання та визначення академічної різниці у ХНУ https://www.khnu.km.ua/root/files/01/10/03/006.pdf.

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів за ваговими коефіцієнтами

	Аудиторна робота	**Контрольні заходи**	**Підсумковий контрольний захід**
Вид заняття	Лабораторні роботи	Контрольна робота	Семестровий контроль (іспит)
Тема	1,3,4	2	1-4
Ваговий коефіцієнт	0,45	0,15	0,4

Оцінювання лабораторних робіт. Оцінка, яка виставляється за лабораторне заняття, складається з таких елементів: усне опитування студентів перед допуском до виконання лабораторної роботи; знання теоретичного матеріалу з теми; якість оформлення звіту; вільне володіння студентом спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні рішення; своєчасний захист лабораторної роботи.

Термін захисту звіту з лабораторної роботи вважається своєчасним, якщо студент захистив її в день виконання або на наступному після виконання роботи занятті. Пропущене лабораторне заняття студент зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Оцінку за лабораторне заняття викладач оголошує одразу після захисту звіту з лабораторної роботи і проставляє в електронний журнал дисципліни.

Оцінювання контрольних робіт. Контрольна робота складається з теоретичного питання за відповідною темою. Оцінювання здійснюється за чотирибальною шкалою.

Оцінку «відмінно» отримує студент який дав повну письмову відповідь на теоретичне питання.

Оцінку «добре» отримує студент, який дав правильну відповідь на теоретичне питання, але у відповіді присутні дві-три несуттєві помилки.

Оцінку «задовільно» отримує студент, який дав часткову відповідь на теоретичне питання.

Оцінку «незадовільно» отримує студент, який не дав відповіді на теоретичне питання.

Оцінку за контрольну роботу викладач проставляє в електронний журнал дисципліни не пізніше ніж через десять днів після проведення контрольного заходу.

Семестровий контроль (іспит). Підсумковий контрольний захід з дисципліни проводиться в формі іспиту. Екзаменаційний білет складається з двох теоретичних питань. Під час іспиту за наданими відповідями і рішеннями (розв'язками) виконується оцінювання рівня засвоєння студентом матеріалу дисципліни.

Оцінка за підсумковий контрольний захід проставляється викладачем в електронний журнал дисципліни в день здачі іспиту і враховується в автоматизованому режимі при визначенні підсумкової семестрової оцінки студента з дисципліни за інституційною шкалою і шкалою ЄКТС

Засвоєння студентом матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями.

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	**Узагальнений критерій**
Відмінно	Студент глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає, логічний виклад відповіді державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки.
Добре	Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві–три несуттєві помилки.
Задовільно	Студент виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, допускає неточності і суттєві помилки у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно	Студент виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка "незадовільно" виставляється студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни.

Якщо студент отримав негативну оцінку за певним видом робіт, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

Студент, який не набрав позитивний середньозважений бал за поточну роботу або не виконав індивідуальний план з дисципліни повністю, вважається невстигаючим.

У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані терміни без поважних причин, то під час відпрацювання заборгованості при позитивній відповіді йому виставляється оцінка «задовільно».

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Інституційна інтервальна шкала балів**	**Інституційна оцінка, критерії оцінювання**	
A	4,75–5,00	5	***Відмінно*** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74	4	***Добре*** – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4	***Добре*** – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3	***Задовільно*** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3	***Задовільно*** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	2	***Незадовільно*** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2	***Незадовільно*** – необхідна серйозна подальша робота і повторне вивчення дисципліни

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ ЗДОБУТИХ СТУДЕНТАМИ РЕЗУЛЬТАТІВ НАВЧАННЯ

1. Мережі Wi-Fi. Стандарти IEEE 802.11.
2. Фізичний рівень: методи модуляції.
3. Специфікації і топологія мереж IEEE 802.11.
4. Канальний рівень: формат і типи кадрів. Структура заголовків і призначення.
5. Доступ: централізований і децентралізований режими.
6. Загрози інформаційної безпеки мереж стандарту IEEE 802.11.
7. Класифікація загроз інформаційній безпеці бездротових мереж стандарту IEEE 802.11.
8. Класифікація бездротових мереж стандарту IEEE 802.11 по набору застосовуваних засобів захисту.
9. Порушники як джерела загроз інформаційній безпеці бездротових мереж стандарту IEEE 802.11.
10. Атаки на бездротові мережі стандарту IEEE 802.11
11. Відкрита аутентифікація і аутентифікація з загальним ключем. Шифрування. та аутентифікація в безпровідних мережах.
12. Механізм шифрування WEP. Специфікація WPA.
13. Стандарт IEEE 802.11i. Технології цілісності і конфіденційності переданих даних.
14. Архітектура мережі GSM. Основні принципи організації мережі GSM. Протоколи GSM. Сигнальні протоколи третього рівня Частотний план в стандарті GSM. Структура кадрів в стандарті GSM
15. Безпека в мережах GSM. Загальна схема криптографічного захисту GSM мереж. Можливі атаки. Безпека в GPRS
16. Безпека мобільної станції
17. Мережі на основі CDMA. архітектура мережі. Канали трафіку та управління.
18. Кодування в прямому каналі. Кодування в зворотному каналі. М'яка передача виклику і управління потужністю в CDMA.
19. Реалізація безпеки передачі інформації в стандарті стільникового зв'язку CDMA 2000 1xRTT. Безпека в CDMA мережах
20. Аутентіфікація. Безпека передачі голосових даних, інформації та службових повідомлень. Анонімность. 6.5 3G CDMA 2000
21. Технічні характеристики мереж стандарту 802.15. Фізичний і канальний уровени стандарту 802.15.1.
22. Топологія, стек протоколів і профілі Bluetooth.
23. Типи пристроїв, види з'єднань і взаємодія піко мереж Bluetooth.
24. Структура пакетів. Режими і обмін даними. Пошук і стикування пристроїв Bluetooth.
25. Безпека Bluetooth. Функції безпеки Bluetooth. Методи спарювання пристроїв. режими безпеки (Security Mode).
26. Стандарт Bluetooth Low Energy (BLE) з малими енергозатрарами.
27. Структура стека протоколів BLE. Види атак на Bluetooth. Bluetooth Piconet Security Checklist.
28. Комунікаційна архітектура сенсорних мереж. Сенсори і сенсорні мережі. Типи і архітектура. протоколи кластерно архітектури та і маршрутизації.
29. Показники QoS якості сенсорних мереж: тривалість життєвого циклу, верхове покриття, залишкова енергія, швидкість передачі, затримка і втрати пакетів.
30. Технологія ZigBee. Стандарт IEEE 802.15.4. Стек протоколів, мережі та профілі ZigBee.
31. Специфікації фізичного рівня і сервісів субрівнями MAC.
32. Формат кадрів. Алгоритм доступу до середовища передачі і взаємодії мережевих елементів.
33. Безпека в мережах ZigBee. Уразливості ZigBee Можливі атаки.
34. Загальна схема криптографічного захисту ZigBee мереж.
35. Ключі шифрування в ZigBee.
36. Аналіз існуючих загроз і атак на безпроводові технології.

37. Дерево атак на безпроводові мережі та їх характеристики.
38. Моделі та критерії загроз у безпроводових технологіях.
39. Методи оцінки загроз у безпроводових мережах
40. Шляхи захисту безпроводових мереж.
41. Загрози і вразливості мобільних пристроїв.
42. Управління мобільними пристроями.
43. Життєвий цикл рішень з безпеки мобільних пристроїв.
44. Загрози і вразливості мобільних телекомунікаційних систем
45. Загрози і вразливості Wi-Fi – мереж
46. Загрози і вразливості мобільних додатків
47. Проблема безпеки IoT.
48. Проблеми конфіденційності в IoT.
49. Анатомія кібератак на IoT-пристрої.
50. Фізична і апаратна безпека IoT. Криптографія.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни «Безпека безпроводових і мобільних технологій» повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі MOODLE.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

№	Назва	Режим доступу
1.	Методи забезпечення гарантоздатності і функціональної безпеки безпроводової інфраструктури на основі апаратного розділення абонентів: Монографія./ В.Л. Бурячок, В.Ю. Соколов. – Київ : КУБГ, 2019. - 164 с.	http://elibrary.kubg.edu.ua/id/eprint/28225/1/V_Buriachok_V_Sokolov_WMS.pdf
2.	Безопасность мобильных устройств, систем и приложений [Електронний ресурс]/ В.А. Артамонов. – IT-Защита: Мобильные устройства, 2019.	http://itzashita.ru/mobilnyie-ustroystva/bezopasnost-mobilnyih-ustroystv-sistem-i-prilozheniy-chast-1.html
3.	Програмування пристроїв Інтернету речей: лабораторний практикум: навч. посіб. [Електронний ресурс]/ уклад.: Л.М. Олещенко, Я.В. Хіцко. – Київ : КПІ ім. Ігоря Сікорського, 2019.	https://ela.kpi.ua/bitstream/123456789/28080/1/Prohramuvannia_prystroiv_Internetu_rechei.pdf
4.	Комп'ютерні мережі та Інтернет. Навчальний посібник/ В.М. Франчук. – К.: НПУ імені М.П. Драгоманова, 2015 р. – 141 с.	https://vfranchuk.fi.npu.edu.ua/images/files/statty/63.pdf
5.	Архитектура интернета вещей/ Л. Перри. – ДМК Пресс, 2018. – 456 с.	https://drive.google.com/file/d/1fCZeEwPjslfZNW_M8IKko9sbRi01GAB1/view?usp=sharing
6.	Інформаційна безпека держави: методичні вказівки до виконання лабораторних робіт/ уклад. О.А. Смірнов, О.К. Конопліцька-Слободенюк, В.Д. Хох, С.А. Смірнов/ – Кропивницький: ЦНТУ – 2017. – 90 с.	http://dspace.kntu.kr.ua/jspui/bitstream/123456789/8231/1/Inform_bezpeka_derjavu.PDF
7.	Безпека безпроводових і мобільних мереж: Навчальний посібник / В. Ю. Соколов, В. Л. Бурячок, М. М. Таджділні / ред. перекл. О. П. Райтер. — 2 вид., доп. - К. : КУБГ, 2019. - 130 с.	http://elibrary.kubg.edu.ua/id/eprint/27294/1/V_Sokolov_V_Buriachok_M_Taj_Dini_WMS_2.pdf
8.	Інформаційна безпека: навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та інші; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.	https://drive.google.com/file/d/1Zqzz0pxqtm8KfmDnUvqYRWDYi0o6qsR_/view?usp=sharing
9.	Интернет вещей: учеб. пособ. /А. В. Росляков, С. В. Ваняшин, А. Ю. Гребешков. – Самара. 2015. – 136 с.	https://iotas.ru/files/documents/wg/учебник%20ИВ%20Росляков.pdf
10.	Интернет вещей: новая технологическая революция/ М. Кранц. – ООО «Издательство «Эксмо», 2018. – 298 с.	https://drive.google.com/file/d/1w249WDHY5HhBEd9ejywJGekKUGF_29uj/view?usp=sharing
11.	Mobile Policy Handbook [Електронний ресурс] – 2019.	https://www.gsma.com/latinamerica/wp-content/uploads/2019/03/GSMA_Mobile-Policy-Handbook_2019_ENG.pdf
12.	Мережі бездротового широкосмугового доступу. Навчальний посібник/ В.Г. Сайко, В.Я. Казіміренко, Ю.М. Літвінов. – К.: ДУТ, 2015. – 196 с.	http://www.dut.edu.ua/uploads/l_881_80314158.pdf
13.	Хмарні та Грід-технології: навчальний посібник/ В.Я. Юрчишин. – К.: КПІ ім. Сікорського, 2019. – 264 с.	https://ela.kpi.ua/bitstream/123456789/29960/1/Khmarni_ta_grid-tekhnolohii_Konspekt_lektsii1.pdf
14.	Грід-системи та технології хмарних обчислень: методичний посібник [Електронний ресурс]/ В.І. Пецко, О.В. Міца. –	https://dspace.uzhnu.edu.ua/jspui/handle/lib/10187

	Ужгород: УНУ, 2016..	
15.	Аналіз загроз персональним даним в мобільному пристрої під час використання різноманітних додатків/ О.В. Сєвєрінов, В.М. Федорченко, В.І. Перепадя. – Системи озброєння та військова техніка. – 2016. – №4 (48). – С. 42-45.	http://212.111.199.244/bitstream/123456789/16442/1/soivt_2016_4_11.pdf
16.	Продукти ESET для бізнесу [Електронний ресурс]	https://infotel.ua/files/eset/Catalog_ESET_for__business_ukr.pdf

Додаткова

17.	The Internet of Things: making the most of the Second Digital Revolution [Електронний ресурс]. – UK Government Chief Scientific Adviser, 2014.	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf
18.	Network Security Assessment. Third edition/ Ch. McNab. – O'Reilly Media, Inc., 2017. – 546 p.	http://dl.hellodigi.ir/dl.hellodigi.ir/dl/book/Network%20Security%20Assessment%20Know%20Your%20Network%2C%203rd%20Edition.pdf
19.	Internet-of-Things (IoT) Systems Architectures, Algorithms, Methodologies/ D. Serpanos, M. Wolf. - Springer International Publishing AG, 2018. – 96 p.	https://drive.google.com/file/d/1Trt9oxdPIJznnPie5dPYqTiMGn1PC9TQ/view?usp=sharing
20.	Architecture Modeling and Analysis of Security in Android Systems/ B. Schmerl et al. – Software Architecture. – 2016. – P. 274-290.	http://acme.able.cs.cmu.edu/pubs/uploads/pdf/andorid-modeling-security-submitted.pdf
21.	IoT Automation Solutions [Електронний ресурс]. – Nexcom, 2016.	http://ebook.nexcom.com/Catalog/2016_IoT_Automation_Solution/2016_IoT_Automation_Solutions_opf_files/pdfs/2016_IoT_Automation_Solutions.pdf
22.	Internet of things (IoT) : technologies, applications, challenges and solutions/ B.K. Tripathy, J. Anuradha. – CRC Press, 2018. – 334 p.	https://drive.google.com/file/d/1_A--I4Pp6NNtJYrQoVzoaWz28gulvP5w/view?usp=sharing
23.	Internet of Things (IoT) in 5G Mobile Technologies/ C.X. Mavromoustakis, G. Mastorakis, J. M. Batalla. – Springer International Publishing Switzerland, 2016. – 499 p.	https://drive.google.com/file/d/1aM0JK9Tdsb0S1NMx41SoKThDdoxcAWdi/view?usp=sharing
24.	Комплексна безпека інформаційних мережевих систем. Навчальний посібник/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. – Львів, «Магнолія 2006», 2016. – 256 с.	http://elartu.tntu.edu.ua/handle/123456789/18299
25.	Развитие «Интернета вещей», дополненной реальности и коммуникационных технологий [Електронний ресурс]/ О.С. Смирнов, К.С. Голохваст, О. В. Тумялис. – ДВФУ. – 2019.	https://arxiv.org/ftp/arxiv/papers/1902/1902.08008.pdf
26.	Концепция интернет вещей/ М.Ю. Щербинина, Н.А. Стефанова. – Креативная экономика. - 2016. - т. 10, № 11. - С. 1323–1336.	https://www.researchgate.net/publication/311863315_Koncepcia_internet_vesej
27.	Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення/ Бурячок В. Л. та ін. /Наукові записки Українського науково-дослідного інституту зв'язку. - 2016. – №3. – С. 48-61.	http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Nzundiz_2016_3_8

28.	Уязвимости корпоративных информационных систем [Електронний ресурс]. – Positive Technologies, 2017.	https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Corp-Vulnerabilities-2017-rus.pdf
29.	Комп'ютерні мережі. Книга 1/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів, «Магнолія 2006», 2013. – 256 с.	http://elartu.tntu.edu.ua/bitstream/123456789/16930/5/Mykytyshyn_A_G_Mytnyk_M_M_Kompjuterni_merezhi_Knyga_1.pdf
30.	Комп'ютерні мережі. Книга 2/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів, «Магнолія 2006», 2014. – 312 с.	http://elartu.tntu.edu.ua/bitstream/123456789/16931/5/Mykytyshyn_A_G_Mytnyk_M_M_Kompjuterni_merezhi_Knyga_2.pdf

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання (розміщені усі необхідні матеріали з дисципліни, в тому числі завдання для поточного та семестрового контролю знань). Доступ до ресурсу: https://msn.khnu.km.ua.
2. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.

Розробник _____ (Підпис) к.т.н., доцент (Вчений ступінь, звання) В.С. Орленко (Ініціали, прізвище викладача(ів)

Погоджено

Гарант освітньої програми _____ (Підпис) к.т.н., доцент (Вчений ступінь, звання) В.М. Чешун (Ініціали, прізвище

Зав. кафедри кібербезпеки та комп'ютерних систем і мереж _____ (Підпис) к.т.н., доцент (Вчений ступінь, звання) Ю.П. Кльоц (Ініціали, прізвище