Чернівецький національний університет імені Юрія Федьковича

Навчально-науковий інститут фізико-технічних та комп'ютерних наук

Кафедра радіотехніки та інформаційної безпеки

СИЛАБУС
навчальної дисципліни

Безпека кіберпростору

вибіркова

Освітньо-професійна програма _____
(назва програми)

Спеціальність _____
(вказати: код, назва)

Галузь знань _____
(вказати: шифр, назва)

Рівень вищої освіти **перший (бакалаврський)**

Дисципліна пропонується як загальноуніверситетська вибіркова
(назва факультету/інституту, на якому здійснюється підготовка фахівців за вказаною освітньо-професійною програмою)

Мова навчання **українська**

Розробники: к. ф.-м. н., доц. Кушнір М.Я., к. т. н., ас. Косован Г.В., к. т. н., ас. Круліковський О.В., к. т. н., доц. Ластівка Г.І., к. ф.-м. н., доц. Рождественська М. Г., к. т. н., доц. Шпатар П.М.
(автори , їхні посади, наукові ступені, вчені звання)

Профайл викладачів http://radiotech.cv.ua/teacher/
Контактний тел. **(**0372) 581271
E-mail: m.rozhdestvenska@chnu.edu.ua
Сторінка курсу в Moodle https://moodle.chnu.edu.ua/course/view.php?id=1937
Консультації графік складатиметься після узгодження розкладу занять

1. Анотація дисципліни (призначення навчальної дисципліни).

Курс «Безпека кіберпростору» пропонується як дисципліна вільного вибору для студентів, які прагнуть отримати базові знання з питань захисту інформації та методів протидії найбільш розповсюдженим кібератакам, практичні навички застосування технологічних і організаційних рішень, спрямованих на забезпечення інформаційної та кібернетичної безпеки.

Обсяг дисципліни – 90 год. (3 кредити).

Кількість аудиторних годин становить:

лекційних – 15;

лабораторних/практичних – 15.

Самостійна робота студента – 60 год.

Форма підсумкового контролю – залік.

2. Мета навчальної дисципліни: формування знань, умінь і навичок у студентів щодо основних понять, принципів і засобів забезпечення кібербезпеки складних інформаційних систем у кіберпросторі.

Вивчення даної вибіркової дисципліни дозволить студентам поглибити знання в галузі інформаційних технологій, сконцентруватись на аспектах безпечного користування сучасними інформаційно-телекомунікаційними системами та звернути увагу на необхідність комплексного підходу в питаннях захисту даних від дій зловмисників.

3. Завдання дисципліни:

- надати студентам теоретичні знання у галузі інформаційної безпеки;
- вивчити основні принципи забезпечення безпеки кіберпростору;
- надати студентам базові знання щодо процесу створення безпечних інформаційних систем та процесів підтвердження їх відповідності;
- студенти повинні набути практичних навичок застосування сучасних технологій забезпечення інформаційної безпеки.

4. Пререквізити.

Одночасно з вивченням даної дисципліни студентам рекомендується пройти курс «Вступ до кібербезпеки» мережної академії Cisco, після успішного завершення якого буде наданий відповідний сертифікат.

5. Результати навчання

В результаті вивчення даної дисципліни студенти повинні

знати:

- суть основних понять інформаційної безпеки об’єктів у кіберпросторі;
- варіанти реалізації, призначення та характеристики технологічних рішень, спрямованих на забезпечення інформаційної безпеки;
- базові поняття щодо криптографічного захисту інформації у кіберпросторі;
- типові рекомендації і вимоги, сформовані у вітчизняних нормативних документах в галузі захисту інформації та міжнародних стандартах з інформаційної безпеки щодо побудови та експлуатації захищених систем; особливості перевірки і підтвердження забезпечення достатнього рівня захисту;

вміти:

- використовувати на практиці отримані знання;
- вирішувати організаційні та технічні проблеми, що виникають в процесі діяльності, пов’язаної з безпекою кіберпростору;
- використовувати методи та засоби забезпечення кібербезпеки прикладного програмного забезпечення, віддалених інформаційних серверів, кінцевих користувачів;
- використовувати методи та засоби підтримки готовності систем та їх захисту від методів соціальної інженерії;
- використовувати офіційні та неофіційні ресурси, на яких публікуються виявлені вразливості та атаки.

3. Опис навчальної дисципліни
3.1. Загальна інформація

Назва навчальної дисципліни ___Безпека кіберпростору____												
Форма навчання	**Рік підго-товки**	**Семестр**	**Кількість**			**Кількість годин**						**Вид підсумк. конт-ролю**
			Кре-дитів	**Годин**	**Змі-стових моду-лів**	**Лек-ції**	**Прак-тичні**	**Семі-нар-ські**	**Лаб о-рат о-рні**	**Само-стій-на робо-та**	**Індиві-дуальні завдан-ня**	
Денна	2-3	3-7	3	90	3	15	-	-	15	45	15	залік
Заочна	2-3	3-7	3	90	3	4	-	-	4	67	15	залік

3.2. Дидактична карта навчальної дисципліни

Назви змістових модулів і тем	**Кількість годин**											
	денна форма						**заочна форма**					
	усього	**у тому числі**					**усього**	**у тому числі**				
		л	**п**	**лаб**	**інд**	**с.р.**		**л**	**п**	**лаб**	**інд**	**с.р.**
1	2	3	4	5	6	7	8	9	10	11	12	13
Теми лекційних занять	**Змістовий модуль 1.**											
Тема 1.1. Загальні поняття про інформацію, інформаційний і кіберпростори	4	2				2	11	1				10
Тема 1.2. Комплексний підхід – базовий метод забезпечення надійного захисту інформації в кіберпросторі	12	2		2		8	11	1				10
Тема 1.3. Основи забезпечення мережної безпеки інформаційно-телекомунікаційних систем	35	4		11		20	32	1		4		27
Разом за ЗМ1	51	8		13		30	54	3		4		47
Теми лекційних занять	**Змістовий модуль 2.**											
Тема 2.1. Системи технічного захисту інформації	8	3				5	5,5	0,5				5
Тема 2.2. Базові поняття про криптографічний захист інформації	8	2		2		4	5,5	0,5				5
Тема 2.3. Соціальна інженерія та методи протидії її шкідливим проявам.	8	2				6	10					10
Разом за ЗМ 2	24	7		2		15	21	1				20
Опрацювання матеріалів курсу «Вступ до кібербезпеки» мережної академії Cisco	15				15		15				15	
Усього годин	90	15		15	15	45	90	4		4	15	67

3.2.1. Теми лабораторних занять

№	Назва теми
1	Кібернетичний простір та доступ до системи WWW за допомогою web-браузера.
2	Фізична основа кіберпростору – Інтернет. Мережні утиліти та їх використання для моніторингу та діагностики мереж
3	Комп'ютерні віруси та інше шкідливе програмне забезпечення. Боротьба з malware
4	Механізми безпеки сучасних операційних систем
5	Контроль доступу користувачів до інформаційно-телекомунікаційної системи. Парольна аутентифікація
6	Криптографічні методи забезпечення конфіденційності та цілісності інформації

3.2.2. Тематика індивідуальних завдань*

№	Назва теми
1	Вивчення курсу «Вступ до кібербезпеки» мережної академії Cisco

* ІНДЗ – в цілому для навчальної дисципліни

3.2.3. Самостійна робота

№	Назва теми
1	Структура та стислий опис сучасних кібератак. Загальні поняття про організацію захисту від їх деструктивного впливу
2	Безпека Інтернету речей як складова кібербезпеки. Тенденції розвитку та перспективи захисту IoT-пристроїв у світі
3	Україна в умовах сучасних кіберзагроз: концептуальний підхід до формування систем інформаційної і кібербезпеки та захисту інформації
4	Криптосистеми та загрози їх безпеки
5	Сертифікація фахівців у галузі інформаційної безпеки

4. Система контролю та оцінювання

Види та форми контролю

Даною дисципліною передбачені наступні форми поточного контролю: усні та письмові (тестування, виконання і захист лабораторних/практичних робіт) відповіді студента.

Кількість балів за роботу з теоретичним матеріалом, виконання самостійної та лабораторних/практичних робіт залежить від дотримання таких вимог:

- своєчасність виконання навчальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності.

Форма підсумкового контролю - залік.

Засоби оцінювання

Засоби оцінювання та демонстрування результатів навчання даної дисципліни наступні:

- модульні контрольні роботи з використанням стандартизованих тестів;
- презентації результатів виконаних завдань;
- завдання на лабораторному обладнанні, реальних об'єктах;
- індивідуальні завдання в рамках курсу «Вступ до кібербезпеки».

Критерії оцінювання результатів навчання з навчальної дисципліни

Критерієм успішного проходження студентом оцінювання є досягнення ним мінімальних порогових рівнів оцінок за кожним запланованим результатом навчання даної дисципліни.

В залежності від характеру відповіді студента зазначена кількість балів може бути скоригована за наступними критеріями:

К-ть балів	Критерії оцінки
max	студент дає вичерпну відповідь на поставлене запитання;
0,8 · max	студент при відповіді на поставлене запитання припустився незначних неточностей, які не впливають на суть відповіді;
0,6 · max	студент при відповіді на поставлене запитання припустився помилок, які виправляє за допомогою викладача; в середньому може дати правильні відповіді на 50% питань теми;
0,4 · max	студент при відповіді на поставлене запитання припустився суттєвих помилок, які все ж таки виправляє за допомогою викладача; дає правильні відповіді на 30% питань теми;
0,2 · max	отримує студент, який за допомогою викладача фрагментарно відповідає на запитання, проте не в повній мірі володіє мінімальним рівнем знань з даного питання;
0	якщо характер відповідей дає підставу стверджувати, що студент неправильно зрозумів суть питання чи не знав правильної відповіді, а тому відповідав, припускаючись грубих помилок.

Примітка: за max прийнято максимальну оцінку для даного виду діяльності. Заокруглення проводиться до одиниць балу**.**

Критерії оцінювання виконання лабораторної роботи

К-ть балів	Критерії оцінки
1	Студент виконав лабораторну роботу
2	Студент провів всі розрахунки, акуратно оформив звіт з лабораторної роботи і здав звіт викладачу
3	Студент захистив роботу
Максимальна оцінка за лабораторну роботу 1+1+2=4 бали	

Згідно шкали ECTS загальна кількість балів, яку студент може отримати у процесі вивчення дисципліни, становить 100 балів, з яких 60 балів студент набирає при поточних видах контролю і 40 балів – у процесі підсумкового виду контролю (залік).

Оцінка за навчальну дисципліну виводиться відповідно до шкали оцінювання, затвердженої Міністерством освіти і науки України:

Шкала оцінювання

Оцінка за національною шкалою	Оцінка за шкалою ECTS	
	Оцінка (бали)	Пояснення за розширеною шкалою
Відмінно	A (90-100)	відмінно
Добре	B (80-89)	дуже добре
	C (70-79)	добре
Задовільно	D (60-69)	задовільно
	E (50-59)	достатньо
Незадовільно	FX (35-49)	(незадовільно) з можливістю повторного складання
	F (1-34)	(незадовільно) з обов'язковим повторним курсом

Мінімальна кількість балів для отримання заліку – 50. Якщо студент набирає 50 балів при поточному контролі, він може отримати залік з оцінкою, що у системі ECTS відповідає рівню E. Для отримання заліку вищого рівня студент складає залік.

Розподіл балів, які отримують студенти

Поточне оцінювання (*аудиторна та самостійна робота*)													Кіль-кість балів (залік)	Сумарна к-ть балів
Змістовий модуль 1			Змістовий модуль 2			Лабораторний практикум						Інд. завд.		
Т1.1	Т1.2	Т1.3	Т2.1	Т2.2	Т2.3	№1	№2	№3	№4	№5	№6			
4	4	8	4	4	2	4	4	4	4	4	4	10	40	100

Т1.1, Т1.2 ... Т2.3 – теми змістових модулів.

Таким чином згідно шкали ECTS і розподілу балів за різні види діяльності загальна кількість балів, яку студент може отримати у процесі вивчення дисципліни:

Змістовий модуль 1 + Змістовий модуль 2 + Лабораторний практикум + +Індивідуальне завдання = 16 + 10 + 24 + 10 = 60 балів

Підсумковий модуль (залік) – **40 балів.**

Всього за курс – **100 балів.**

5. Рекомендована література

5.1. Базова (основна)

1. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с. http://elibrary.kubg.edu.ua/id/eprint/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf

2. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа]; за заг. ред. д-ра техн. наук, професора В.Б. Толубка.— К.: ДУТ, 2015.— 288 с. http://www.dut.edu.ua/uploads/l_1209_69915296.pdf

3. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури. Постанова КМУ від 19.06.2019; №518. https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

4. НД ТЗІ 1.1-003-99, «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу», - 30с. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102106&cat_id=46556&ctime=1344502446343

5. Яремчук Ю. Є. Комплексні системи захисту інформації. Навчальний посібник / Ю. Є. Яремчук, П.В. Павловський, В.С. Катаєв, В. В. Сінюгін. Режим доступу: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/index.html

6. Кобозева А.А., Мачалін І.О., Хорошко В.О., Аналіз захищеності інформаційних систем. Підручник. – К.: вид. ДУІКТ, 2010. - 316 с.

7. Закон України “Про доступ до публічної інформації ”від 13.01.2011 № 2939-VI// Відомості Верховної Ради України. – 2011. – № 16. – с. 93. https://zakon.rada.gov.ua/laws/show/2939-17#Text

8. Закон України “Про інформацію”// Відомості Верховної Ради, 1992, № 48, с.650 – 651. Електронний ресурс. Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text

5.2. Допоміжна

1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В.Л. Бурячок, Г.М. Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.

2. Гулак Г.М., Гринь А.К., Мельник С.В. Методологія захисту інформації: навчально-методичний посібник. – К.: Видавництво НА СБ України, 2015. – 251 с.

3. Кузнецов М. В. Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов. – СПб.: БХВ-Петербург, 2007. – 368 с. Режим доступу: http://library.khpg.org/files/docs/1392898102.pdf

4. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. /В.Л. Бурячок, С.В. Толюпа, А.О. Аносов, В.А. Козачок, Н.В. Лукова-Чуйко/ – К.:ДУТ, 2015. – 345 с. http://www.dut.edu.ua/uploads/l_1242_54311567.pdf

5. Богуш В.М., Довидьков О.А., Кривуца В.Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. – К.: ДУІКТ, 2010. – 454 с.

6. Захист баз даних — запорука безпеки корпоративної мережі. Електронний ресурс. Режим доступу: https://eset.ua/ua/blog/view/14/-

7. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT). https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf

8. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT)

9. ДСТУ ISO 19011:2012 Настанови щодо здійснення аудитів систем управління (ISO 19011:2011, IDT).

10. ISO/IEC TR 27019:2013 Information technology – Security techniques – Information security management guide lines based on ISO/IEC 27002 for process control systems specific to the energy utility industry (Інформаційні технології. Методи захисту. Настанова щодо менеджменту інформаційної безпеки на основі ISO/IEC 27002 для систем керування процесами в індустрії енергетичних сервісних програм).

11. ДСТУ IEC/TS 62351-1:2014 Керування енергетичними системами та пов'язаний з ним інформаційний обмін. Безпека даних та комунікацій. Частина 1. Безпека зв'язку мережі та системи. Загальні положення (IEC/TS 62351-1:2007, IDT).

6. Інформаційні ресурси

1. Офіційний сайт КІБЕРПОЛІЦІЇ УКРАЇНИ: [Електронний ресурс]. – Режим доступу: https://cyberpolice.gov.ua/

2. Верховна Рада України. Законодавство України: [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/

3. Computer Emergency Response Team of Ukraine: [Електронний ресурс]. – Режим доступу: https://cert.gov.ua/

4. Державна служба спеціального зв'язку та захисту інформації: [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/index

5. Сетевая академия Cisco: [Електронний ресурс]. – Режим доступу: https://www.netacad.com/ru

6. Базові правила безпеки в цифровому середовищі: [Електронний ресурс]. – Режим доступу: https://cybereducation.org/mc/index.php/usr/login/login?lang=uk