Чернівецький національний університет імені Юрія Федьковича

(повне найменування закладу вищої освіти)

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

(назва інституту/факультету)

Кафедра комп'ютерних систем та мереж

(назва кафедри)

СИЛАБУС

навчальної дисципліни

Кібербезпека

(вкажіть назву навчальної дисципліни (іноземною, якщо дисципліна викладається іноземною мовою))

вибіркова

(обов'язкова чи вибіркова)

Освітньо-професійна програма – *" Комп'ютерна інженерія "*

Спеціальність *123 – Комп'ютерна інженерія*

(шифр і назва спеціальності)

Галузь знань *12 – Інформаційні технології*

(шифр і назва галузі знань)

Рівень вищої освіти – *другий (магістерський)*

(вказати: перший (бакалаврський)/другий (магістерський)/третій (освітньо-науковий))

Інститут фізико-технічних і комп'ютерних наук

(назва факультету / інституту, на якому здійснюється підготовка фахівців за вказаною освітньо-професійною програмою)

Мова навчання – *українська*

(мова, на якій читається дисципліна)

Розробники: Іванущак Наталія Михайлівна, асистент кафедри КСМ, кандидат техн. наук,

(вказати авторів (викладач (ів)), їхні посади, наукові ступені, вчені звання)

Профайл викладача (-ів) https://csn.chnu.edu.ua,
https://csn.chnu.edu.ua/employees/ivanushhak-nataliya-myhajlivna/

Контактний тел. +(38) 0372 50 94 32 (кафедра КСМ) – Іванущак Н.М.

E-mail: n.ivanuschak@chnu.edu.ua

Сторінка курсу в мережній академії Cisco https://lms.netacad.com/course/view.php?id=998606

Консультації *on-line: середа з 17.00 до 18.00*

1. Анотація дисципліни

Курс «Кібербезпека» призначений для розширення компетентностей випускників спеціальності 123 - Комп'ютерна інженерія для набуття студентами базових знань з побудови комплексної системи захисту інформації, оволодіння студентами загальними та фаховими компетентностями із кібербезпеки.

2. Мета навчальної дисципліни: надання студентам систематизованих знань для побудови комплексної системи захисту інформації, отримання знань та умінь, які необхідні для успішного виявлення вразливостей у комп'ютерних системах і мережах та усунення проблем безпеки шляхом розробки та впровадження захисних заходів. Вивчення даної вибіркової дисципліни надає студентам ряд переваг, оскільки засвоєння дисципліни дозволить майбутнім фахівцям забезпечити необхідний рівень володіння інструментами дослідження і проектування комплексної системи захисту інформації, дасть можливість здійснювати опис принципів конфіденційності, цілісності та доступності відносно стану даних та заходів протидії загрозам в області кібербезпеки; прогнозувати, виявляти та оцінювати можливі загрози інформаційному просторі держави, суспільства, організації та дестабілізуючі чинники в роботі систем управління; дасть змогу описати тактику, методи та процедури, які використовуються кіберзлочинцями.

3. Пререквізити. Для коректного розуміння і засвоєння матеріалу даного курсу слухачі повинні попередньо пройти курси: криптографія та побудова систем безпеки, захист інформації в комп'ютерних системах, комп'ютерні мережі, комп'ютерний захист фінансової інформації. Доцільно також мати певні уявлення з архітектури комп'ютерів, основ баз даних, програмування.

4. Результати навчання

У результаті вивчення навчальної дисципліни студент повинен

4.1. Знати: перелік найбільш поширених загроз в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; заходи протидії цим загрозам; кроки для створення комплексної системи захисту інформації; кроки для проведення моніторингу та тестування створеної захищеної системи.

4.2. Вміти: критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; розв'язувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів у інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з

використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

4.3. Набути компетентностей:

ЗК - загальних

ЗК1. Здатність до адаптації та дій в новій ситуації.

ЗК2. Здатність до абстрактного мислення, аналізу і синтезу.

ЗК4. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК6. Здатність виявляти, ставити та вирішувати проблеми.

ЗК7. Здатність приймати обґрунтовані рішення.

СК – фахових (спеціальних)

СК1. Здатність до визначення технічних характеристик, конструктивних особливостей, застосування і експлуатації програмних, програмно-технічних засобів, комп'ютерних систем та мереж різного призначення.

СК2. Здатність розробляти алгоритмічне та програмне забезпечення, компоненти комп'ютерних систем та мереж, Інтернет додатків, кіберфізичних систем з використанням сучасних методів і мов програмування, а також засобів і систем автоматизації проектування.

СК3. Здатність проектувати комп'ютерні системи та мережі з урахуванням цілей, обмежень, технічних, економічних та правових аспектів.

СК4. Здатність будувати та досліджувати моделі комп'ютерних систем та мереж.

СК5. Здатність будувати архітектуру та створювати системне і прикладне програмне забезпечення комп'ютерних систем та мереж.

СК9. Здатність представляти результати власних досліджень та/або розробок у вигляді презентацій, науково-технічних звітів, статей і доповідей на науково-технічних конференціях.

СК10. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп'ютерних систем, мереж та їхніх компонентів.

ПРН - програмних результатів навчання

РН2. Знаходити необхідні дані, аналізувати та оцінювати їх.

РН3. Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.

РН4. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері комп'ютерної інженерії, необхідні для професійної діяльності, оригінального мислення та проведення досліджень, критичного осмислення проблем інформаційних технологій та на межі галузей знань.

РН7. Вирішувати задачі аналізу та синтезу комп'ютерних систем та мереж.

РН11. Приймати ефективні рішення з питань розроблення, впровадження та експлуатації комп'ютерних систем і мереж, аналізувати альтернативи, оцінювати ризики та імовірні наслідки рішень.

5. Опис навчальної дисципліни
5.1. Загальна інформація

Назва навчальної дисципліни *Кібербезпека*												
Форма навчання	**Рік підготовки**	**Семестр**	**Кількість**			**Кількість годин**						**Вид підсум-кового контролю**
			кредитів	**годин**	**змістових модулів**	**лекції**	**практичні**	**семінарські**	**лабораторні**	**самостійна робота**	**індивідуальні завдання**	
Денна	**1(5)**	**2(10)**	**4**	**120**	**2**	**15**	**-**	**-**	**15**	**90**	**-**	**Екзамен**
Заочна	**1(5)**	**2(10)**	**4**	**120**	**2**	**4**	**-**	**-**	**4**	**112**	**-**	**Екзамен**

Примітка. Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить: для денної форми навчання – 0,33 ((15+15)/90);
для заочної форми навчання – 0,07 ((4+4)/112).

5.2. 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
Змістовий модуль 1. Кібербезпека як основна складова побудови захищеної системи												
Тема 1. Кібербезпека – світ експертів і злочинців	14	2	-	2	-	10	14	1	-	1	-	12
Тема 2. Куб кібербезпеки	14	2	-	2	-	10	14	0	-	-	-	14
Тема 3. Види шкідливого програмного забезпечення	14	2	-	2	-	10	16	1	-	1	-	14
Тема 4. Захист систем та пристроїв	14	2	-	2	-	10	16	0	-	-	-	16
Разом за змістовим модулем 1	56	8	-	8	-	40	60	2	-	2	-	56
Змістовий модуль 2. Побудова комплексної системи захисту інформації												
Тема 5. Шифрування даних та стеганографія	19	2	-	2	-	15	20	1	-	1	-	18
Тема 6. Типи засобів контролю цілісності даних	19	2	-	2	-	15	18	0	-	-	-	18
Тема 7. Заходи покращення доступності та реагування на інциденти	26	3	-	3	-	20	22	1	-	1	-	20
Разом за змістовим модулем 2	64	7	-	7	-	50	60	2	-	2	-	56
Усього годин	120	15	-	15	-	90	120	4	-	4	-	112

5.3. Тематика лабораторних занять

№	Назва теми (завдання)	Кількість годин
1.	Встановлення віртуальної машини на персональний комп'ютер	2
2.	Вивчення аутентифікації, авторизації та обліку	2
3.	Виявлення загроз і вразливостей	2
4.	Використання стеганографії	2
5.	Злам паролів	3
6.	Віддалений доступ	3
7.	Захист Linux систем	3
	Разом	15

Примітка. Методичні рекомендації та завдання до лабораторних робіт доступні на інтернет-ресурсі Академії CISCO Cybersecurity Essentials : https://www.netacad.com/courses/cybersecurity/cybersecurity-essentials

Програмне забезпечення для виконання лабораторних робіт: віртуальна машина Oracle VirtualBox і доповнення Ubuntu_CyberEss.

5.4. Зміст завдань для самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Дії у кіберпросторі та напрями забезпечення кібербезпеки України.	10
2	Фахівці з кібербезпеки – хто вони?	10
3	Вплив Інтернету речей на кібербезпеку.	10
4	Вплив технології Big Data на кібербезпеку.	15
5	Кібер закони та відповідальність.	15
6	Розуміння етики роботи у кібербезпеці, цивільний захист та безпека праці.	15
7	Організаційний рівень безпеки та підготовки фахівців з кібербезпеки.	15
	Разом	90

6. Система контролю та оцінювання

Засобами оцінювання та демонстрування результатів навчання є

- контрольні роботи;
- стандартизовані тести;
- презентації результатів виконаних завдань та досліджень;
- завдання на лабораторному обладнанні.

Формами поточного контролю рівня знань є усна та письмова відповідь студента при захисті виконаних лабораторних робіт, кількість отриманих балів при виконанні тестового завдання, а також письмова відповідь при написанні модульних контрольних робіт. Формами підсумкового контролю рівня знань є виконання підсумкового тестування.

6.1. Критерії оцінювання результатів навчання з навчальної дисципліни

Критерієм успішного проходження здобувачем освіти підсумкового

оцінювання є досягнення ним мінімальних порогових рівнів оцінок за кожним запланованим результатом навчання навчальної дисципліни.

Шкала та критерії оцінювання: національна та ЄКТС (Європейська кредитна трансферно-накопичувальна система, ECTS)

Оцінка за шкалою ЄКТС	Критерії	Пояснення	Оцінка за 100-бальною шкалою	Оцінка за національною шкалою
A	Відмінний рівень компетентностей у межах обов'язкового матеріалу, з можливими незначними недоліками	відмінно	**90 – 100**	**відмінно**
B	Достатньо високий рівень компетентностей у межах обов'язкового матеріалу без суттєвих (грубих) помилок	дуже добре	**80-89**	**добре**
C	В цілому добрий рівень компетентностей із незначною кількістю помилок	добре	**70-79**	
D	Посередній рівень компетентностей із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності	задовільно	**60-69**	**задовільно**
E	Мінімально можливий допустимий рівень компетентностей	достатньо	**50-59**	
FX	Незадовільний рівень компетентностей, з можливістю повторного перескладання за умови належного самостійного доопрацювання	(незадовільно) з можливістю повторного складання	**35-49**	**незадовільно**
F	Дуже поганий рівень компетентностей, що вимагає повторного вивчення дисципліни	(незадовільно) з обов'язковим повторним курсом	**1-34**	

Розподіл балів, які отримують студенти

Поточне тестування та самостійна робота									Підсумковий тест (екзамен)	Сума балів
Змістовий модуль 1					Змістовий модуль 2				30	100
Т1	Т2	Т3	Т4	М1	Т5	Т6	Т7	М2		
5	5	5	5	10	10	10	10	10		

6.2. Перелік тем і розподіл максимально можливої кількості балів, які отримують студенти за виконання всіх видів навчальної діяльності

Змістовий модуль 1. Кібербезпека як основна складова побудови захищеної системи

Т1. Кібербезпека – світ експертів і злочинців (виконання та захист лабораторної роботи №1 на основі лекційного матеріалу та методичних вказівок до лабораторної роботи – 5 балів).

Т2. Куб кібербезпеки (виконання та захист лабораторної роботи № 2 на основі лекційного матеріалу та методичних вказівок до лабораторної роботи – 5 балів).

Т3. Види шкідливого програмного забезпечення (виконання та захист лабораторної роботи № 3 на основі лекційного матеріалу та методичних вказівок до лабораторної роботи – 5 балів).

Т4. Захист систем та пристроїв (виконання та захист лабораторної роботи № 4 на основі лекційного матеріалу та методичних вказівок до лабораторної роботи – 5 балів).

М1 – модульна контрольна робота №1 (10 балів)

Змістовий модуль 2. Побудова комплексної системи захисту інформації

Т5. Шифрування даних та стеганографія (виконання та захист лабораторної роботи № 5 на основі лекційного матеріалу та методичних вказівок до лабораторної роботи – 10 балів).

Т6. Типи засобів контролю цілісності даних (виконання та захист лабораторної роботи № 6 на основі лекційного матеріалу та методичних вказівок до лабораторної роботи – 10 балів).

Т7. Заходи покращення доступності та реагування на інциденти (виконання та захист лабораторної роботи № 7 на основі лекційного матеріалу та методичних вказівок до лабораторної роботи – 10 балів).

М2 – модульна контрольна робота №2 (10 балів).

Підсумковий контроль (**іспит**) – 30 балів: здійснюється виконання фінальної контрольної роботи на курсі Академії CISCO Cybersecurity Essentials. **Сумарна кількість балів** – 100.

6.3. Умови зарахування результатів неформальної освіти

Студент, згідно Положення ЧНУ «Про неформальну освіту» може отримати додаткові бали, або бути звільненим від окремих видів роботи з окремих тем, якщо у нього наявні сертифікати про неформальну освіту з проблем, які вивчаються на дисципліні «Комп'ютерні системи штучного інтелекту».

Також, як виконані види роботи з відповідних тем зараховуються студенту бали за наукові публікації у матеріалах науково-практичних конференцій та фахових чи апробаційних виданнях.

7. Рекомендована література

Фахова (основна)

1. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г.Даник, П.П. Воробієнко, В.М. Чернега. – О.: ОНАЗ ім. О.С. Попова, 2018. − 228 с. ISBN 978-617-582-064-3

2. Дудатьєв А. В. Захист комп'ютерних мереж. Теорія та практика. Навчальний посібник / Дудатьєв А. В., Войтович О. П., Каплун В. А.- Вінниця ВНТУ, 2010.-219 с.
3. Мережко О. О. Проблеми теорії міжнародного публічного та приватного права / О. О. Мережко. – 2010. – Режим доступу: www.twirpx.com/file/1827023.

Допоміжна

1. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Науково-дослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В.І. Вернадського. – К., 2019. – No6 (червень). – 71с.
2. Слободянюк А. В. Аналіз небезпеки кібервійни на сучасній світовій арені. / А. В. Слободянюк. – 2017. – Режим доступу: conferences. vntu.edu.ua/index.php/all-hum/all-hum-2017/paper/download/2332/1739.
3. Курбан О. В. Сучасні інформаційні війни у мережевому он-лайн просторі: навч. посіб. / О. В. Курбан. – Київ, 2016. – С.56–57.
4. Присяжнюк М. М. Особливості забезпечення кібербезпеки / М. М. Присяжнюк, Є. І. Цифра // Реєстрація, зберігання та обробка даних. – 2017. – Т. 19. – No 2. –С. 61 – 68.
5. Указ Президента України від 15 березня 2016 року No 96/2016 «Про рішення Ради національної безпеки і оборони України» від 27 січня 2016 року "Про Стратегію кібербезпеки України".
6. Закон України «Про основні засади забезпечення кібербезпеки України» // Відомості Верховної Ради України, 2017. – No 45. – Ст.403.
7. Закон України «Про оборону України» // Відомості Верховної Ради України. – 2017. – No 45. – Ст.403.

8. Інформаційні ресурси

1. https://csn.chnu.edu.ua/about-us/ok-rivni/
2. https://csn.chnu.edu.ua/spetsialnist-123-komp-yuterna-inzheneriya-opp-komp-yuterna-inzheneriya-magistratura-1-5-r/

3. Cisco -Україна. Режим доступу:: https://www.cisco.com
4. Annual Threat Reports. Режим доступу:: https://www.fireeye.com/current-threats/annual-threat-report.html
5. European union agency for cybersecurity. Режим доступу:: https://www.enisa.europa.eu
6. Cybersecurity Essentials. Інтернет-ресурс Академії CISCO, Режим доступу: https://www.netacad.com/courses/cybersecurity/cybersecurity-essentials .