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

Cybersecurity Cisco

(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 «Cybersecurity Cisco» призначений для розширення компетентностей випускників спеціальності 123 - Комп'ютерна інженерія для набуття студентами базових знань засобів захисту інформації, забезпечення оволодіння студентами загальними та фаховими компетентностями і досягнення ними програмних результатів навчання; використання програмно-апаратних методів для побудови систем захисту.

2. Мета навчальної дисципліни: надання студентам необхідної теоретичної та практичної підготовки для того, щоб вміти: використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо безпечного здійснення професійної діяльності; аналізувати та виявляти загрози інформації, а також проводити реалізацію алгоритмів шифрування та дешифрування даних; аналізувати наслідки кібератак; знати різні категорії вразливостей програмного та апаратного забезпечення і систем безпеки; описати, які технології, продукти і процедури використовуються для захисту конфіденційності, забезпечення цілісності та високої доступності; пояснити, як професіонали кібербезпеки використовують технології, процеси та процедури для захисту всіх компонентів мережної інфраструктури; розробляти моделі загроз інформації та моделі порушників інформаційної безпеки.

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: найновіші досягнення в галузі захисту інформації; характеристики основних підсистем ідентифікації та аутентифікації; характеристики основних механізмів доступу; характеристики підсистем захисту основних класів операційних систем; основні принципи формування політики безпеки підприємства; основні канали витоку інформації та методи боротьби з ним; критерії захищеності автоматизованих систем; характеристики основних стандартних профілів захищеності автоматизованих систем; основні характеристики захищених протоколів передавання даних.

4.2. Вміти: здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних

систем; вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

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.

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.

СК6. Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп'ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності.

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.

РН6. Аналізувати проблематику, ідентифікувати та формулювати конкретні проблеми, що потребують вирішення, обирати ефективні методи їх вирішення.

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

РН8. Застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення складних задач комп'ютерної інженерії та дотичних проблем.

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 *Cybersecurity Cisco*												
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. Напрями забезпечення кібербезпеки												
Тема 1. Основні положення забезпечення кібербезпеки.	14	2	-	2	-	10	14	1	-	1	-	12
Тема 2. Технологічні аспекти забезпечення кібербезпеки інформаційних систем	14	2	-	2	-	10	14	0	-	-	-	14
Тема 3. Кібербезпека - загрози, вразливості та атаки	14	2	-	2	-	10	16	1	-	1	-	14
Тема 4. Захист домену кібербезпеки.	14	2	-	2	-	10	16	0	-	-	-	16
Разом за змістовим модулем 1	56	8	-	8	-	40	60	2	-	2	-	56
Змістовий модуль 2. Технологічні рішення щодо забезпечення конфіденційності, цілісності та доступності												
Тема 5. Мистецтво захисту таємниць.	19	2	-	2	-	15	20	1	-	1	-	18
Тема 6. Мистецтво забезпечення цілісності даних.	19	2	-	2	-	15	18	0	-	-	-	18
Тема 7. Концепція п'яти дев'яток.	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.	Комунікація у кібер-світі	2
2.	Вивчення аутентифікації, авторизації та обліку	2
3.	Налаштування транспортного режиму VPN	2
4.	Брандмауери на сервері та ACL на маршрутизаторі	2
5.	Вивчення шифрування файлів і даних	3
6.	Використання перевірок цілісності файлів та даних	3
7.	Резервування маршрутизаторів і комутаторів	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: середовище програмування Cisco Packet Tracer.

5.4. Зміст завдань для самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Дії у кіберпросторі та напрями забезпечення кібербезпеки України	10
2	Забезпечення цілісності баз даних	10
3	Впровадження заходів аварійного відновлення	10
4	Укріплення захисту серверів та мереж	15
5	Домени кібербезпеки.	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 усна та письмова відповідь студента при здачі іспиту.

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. Напрями забезпечення кібербезпеки

Т1. Основні положення забезпечення кібербезпеки (виконання та захист лабораторної роботи №1 на основі лекційного матеріалу та методичних вказівок до

лабораторної роботи – 5 балів).

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

Т3. Кібербезпека - загрози, вразливості та атаки (виконання та захист лабораторної роботи № 3 на основі лекційного матеріалу та методичних вказівок до лабораторної роботи – 5 балів).

Т4. Захист домену кібербезпеки (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. Технологічні рішення щодо забезпечення конфіденційності, цілісності та доступності

Т5. Мистецтво захисту таємниць (виконання та захист лабораторної роботи № 5 на основі лекційного матеріалу та методичних вказівок до лабораторної роботи – 10 балів).

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

Т7. Концепція п'яти дев'яток (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. Бурячок В. Л. Інформаційний та кіберпростори : проблеми безпеки,методи та засоби боротьби. Навчальний посібник / В. Л. Бурячок, С.В. Толюпа, В.В. Семко, Л.В. Бурячок, П.М. Складанний, Н.В. Лукова-Чуйко - К. : ДУТ- КНУ, 2016.-178 с.
4. Кавун С. В. Інформаційна безпека : навч. посіб. Ч.1 / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків : ХНЕУ, 2008. – 352с. – Бібліогр.: с. 338-349. – ISBN 978-966-676-281-1.

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. Даник Ю. Г. Основи кібернетичної безпеки: монографія / Ю. Г. Даник, Р. В. Грищук; за заг. ред. проф. Ю. Г. Даника. – Житомир: ЖНАЕУ, 2016. – 636 с.
3. Даник Ю. Г. Визначення сутності та змісту кібернетичної загрози / Ю.Г. Даник, В. І. Шестаков, С. В. Чернишук // Проблеми створення, випробування та експлуатації складних інформаційних систем: зб. наук.праць. – Житомир: ЖВІНАУ, 2012. – Спецвипуск 2. – С. 5-1
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 .