Чернівецький національний університет імені Юрія Федьковича
(повне найменування закладу вищої освіти)

Навчально-науковий інститут фізико-технічних та комп'ютерних наук
(назва навчально-наукового інституту / факультету)

Кафедра комп'ютерних систем та мереж

"**ЗАТВЕРДЖУЮ**"
Директор навчально-наукового інституту
фізико-технічних та комп'ютерних наук
_____ О. В. Ангельський
"___" _____ 2022 року

РОБОЧА ПРОГРАМА
навчальної дисципліни

Cybersecurity Cisco
(назва навчальної дисципліни)

вибіркова
(вказати: обов'язкова / вибіркова)

Освітньо-професійна програма Комп'ютерна інженерія
(назва програми)

Спеціальність 123 Комп'ютерна інженерія
(вказати: код, назва)

Галузь знань 12 Інформаційні технології
(вказати: шифр, назва)

Рівень вищої освіти другий (магістерський)
(вказати: перший бакалаврський/другий магістерський)

фізико-технічних та комп'ютерних наук
(назва факультету/ навчально-наукового інституту,
на якому здійснюється підготовка фахівців за вказаною освітньо-професійною програмою)

Мова навчання українська

Чернівці 2022 рік

Робоча програма навчальної дисципліни
Cybersecurity Cisco
(назва навчальної дисципліни)
складена відповідно до освітньо-професійної програми
Комп'ютерна інженерія, 123 Комп'ютерна інженерія,
(назва освітньо-професійної програми, код та назва спеціальності)
12 Інформаційні технології, 15 квітня 2021 р.
(галузь знань: шифр та назва; дата останнього затвердження)

Розробники: Іванущак Наталія Михайлівна, асистент кафедри КСМ,
канд. техн. наук, асистент
(П.І.Б. авторів, посада, науковий ступінь, вчене звання)

Погоджено з гарантом ОП і затверджено на засіданні кафедри
комп'ютерних систем та мереж

Протокол № 1 від "29" серпня 2022 року

Завідувач кафедри _____ *(Воробець Г.І.)*
(підпис) (прізвище та ініціали)

Схвалено методичною радою навчально-наукового інституту
фізико-технічних та комп'ютерних наук

Протокол № 1 від "31" серпня 2022 року

Голова методичної ради навчально-наукового інституту
фізико-технічних та комп'ютерних наук
_____ (Струк Я. М.)
(підпис) (прізвище та ініціали)

© Чернівецький національний університет , 2022 рік
© Чернівецький національний університет , 2023 рік

1. Мета навчальної дисципліни

Мета: 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.

Вивчення даної вибіркової дисципліни надає студентам ряд переваг, оскільки засвоєння дисципліни дозволить майбутнім фахівцям пояснити, як професіонали кібербезпеки використовують технології, процеси та процедури для захисту всіх компонентів мережної інфраструктури; розробляти моделі загроз інформації та моделі порушників інформаційної безпеки.

2. Результати навчання

У результаті вивчення навчальної дисципліни студент отримує компетентності, у результаті чого повинен

2.1. 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.

2.2. 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.

2.3. 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.

3. Опис навчальної дисципліни
3.1. 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).

3.2. Структура змісту 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

3.5. 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

3.7. Самостійна робота студента (ІНДЗ – індивідуальне навчально-дослідне завдання)

№	Назва теми/ кількість балів/ форма контролю	Кількість годин
1	Дії у кіберпросторі та напрями забезпечення кібербезпеки України / результати використовуються при виконанні модульної контрольної роботи (МКР) № 1 (5 балів)	10
2	Забезпечення цілісності баз даних / результати використовуються при виконанні модульної контрольної роботи (МКР) № 1 (5 балів)	10
3	Впровадження заходів аварійного відновлення / результати використовуються при виконанні лабораторної роботи № 1 (5 балів)	10
4	Укріплення захисту серверів та мереж / результати використовуються при виконанні лабораторної роботи № 2 (5 балів)	10
5	Домени кібербезпеки / результати використовуються при	15

	виконанні МКР № 2 (5 балів)	
6	Розуміння етики роботи у кібербезпеці, цивільний захист та безпека праці / результати використовуються при виконанні МКР № 2 (5 балів)	15
7	Організаційний рівень безпеки та підготовки фахівців з кібербезпеки / результати використовуються при виконанні МКР № 2 (5 балів)	20
	Разом	90

4. Методи навчання

Для викладання матеріалів з навчальної дисципліни «Cybersecurity Cisco» використовуються наступні методи навчання.

4.1. Словесні методи навчання. Навчальна лекція

За допомогою даного методу забезпечується усне викладення матеріалу великими ємністю й складністю логічних побудов, доказів і узагальнень. В ході лекції використовуються прийоми усного викладення інформації, підтримання уваги протягом тривалого часу, активізації мислення студентів, прийоми забезпечення логічного запам'ятовування, переконання, аргументації, доказів, класифікації, систематизації і узагальнення. В залежності від специфіки лекційного матеріалу іноді використовується лекція-діалог.

4.2. Індуктивний метод навчання

Даний метод навчання використовується в рамках лекційних занять, коли матеріал носить, здебільшого, фактичний характер. В рамках лабораторних занять метод застосовується при виконанні технічних задач, коли студенти використовують раніше здобуті теоретичні знання при роботі з конкретними пристроями (комп'ютерами) та програмними продуктами.

4.3. Репродуктивний метод навчання

Даний метод навчання використовується в рамках лекційних і лабораторних занять, а також під час самостійної роботи студентів. Метод передбачає роботу студентів за визначеним алгоритмом. Згідно з методом для виконання завдань студентам надаються методичні вказівки, правила і навчальні приклади.

4.4. Проблемно-пошукові методи навчання

Проблемно-пошукові методи застосовуються в ході проблемного навчання, а саме в процесі виконання лабораторних робіт та індивідуальних науково-дослідних завдань. Слід зауважити, що під проблемною ситуацією треба вважати невідповідність між тим, що вивчається і вже вивченим. При використанні проблемно-пошукових методів навчання викладач використовує такі прийоми: створює проблемну ситуацію (ставить питання, пропонує задачу, експериментальне завдання), організує колективне обговорення можливих підходів до рішення проблемної ситуації, стимулює висування гіпотез, тощо.

Студенти роблять припущення про шляхи вирішення проблемної ситуації, узагальнюють раніше набуті знання, виявляють причини явищ, пояснюють їхнє походження, вибирають найбільш раціональний варіант вирішення проблемної ситуації. Викладач обов'язково керує цим процесом на всіх етапах, а також за допомогою запитань-підказок. Також даний метод використовується при опрацюванні матеріалів в системі дистанційної освіти «Moodle».

4.5. Наочний метод навчання

Наочний метод достатньо важливий для студентів, оскільки забезпечує візуальне подання навчального матеріалу, зокрема, з використанням інформаційно-комунікаційних технологій. При викладанні дисципліни наочний метод навчання поєднується зі словесними методами для представлення інформації у вигляді таблиць, рисунків, схем та діаграм.

5. Критерії оцінювання результатів навчання з навчальної дисципліни

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

Оцінка за національною шкалою	**Оцінка за шкалою ЄКТС**	
	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

6. Засоби оцінювання

Засобами оцінювання та демонстрування результатів навчання є

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

7. Форми поточного та підсумкового контролю

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.

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		

Т1, Т2 ... Т7 – теми змістових модулів; М1, М2 – модульні контрольні роботи

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

8. 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.

9. 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 .