

**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**

Кібербезпека

(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

Кібербезпека

(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

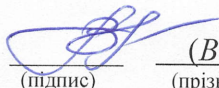
(П.І.Б. авторів, посада, науковий ступінь, вчене звання)

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.)

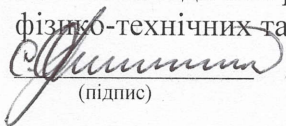
(підпис)

(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)

## 1. Мета навчальної дисципліни

**Мета:** 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 простору держави, суспільства, організації та дестабілізуючі чинники в роботі систем управління; дасть змогу описати тактику, методи та процедури, які використовуються кіберзлочинцями.

## 2. Результати навчання

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

**2.1. 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.

**2.2. 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.

### **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.
- 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.

### 3. Опис навчальної дисципліни

#### 3.1. Загальна інформація

Назва навчальної дисципліни <i>Кібербезпека</i>												
Форма навчання	Рік підготовки	Семестр	Кількість			Кількість годин						Вид підсумкового 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													
	усього	Денна форма					Заочна форма							
		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		
<b>Змістовий модуль 1. Кібербезпека як основна складова побудови захищеної системи</b>														
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		
<b>Змістовий модуль 2. Побудова комплексної системи захисту інформації</b>														
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
<b>Усього годин</b>	120	15	-	15	-	90	120	4	-	4	-	112

### 3.5. 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

### 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	Фахівці з кібербезпеки – хто вони? / результати використовуються при виконанні модульної контрольної роботи (МКР) № 1 (5 балів)	10
3	Вплив Інтернету речей на кібербезпеку / результати використовуються при виконанні лабораторної роботи № 1 (5 балів)	10
4	Вплив технології Big Data на кібербезпеку / результати використовуються при виконанні лабораторної роботи № 2 (5 балів)	10
5	Кібер закони та відповідальність / результати використовуються при виконанні МКР № 2 (5 балів)	15
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 «Кібербезпека» використовуються такі 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» та мережній академії «Cisco».

### **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
<b>Відмінно</b>	A (90-100)	відмінно
<b>Добре</b>	B (80-89)	дуже добре
	C (70-79)	добре
<b>Задовільно</b>	D (60-69)	задовільно
	E (50-59)	достатньо
<b>Незадовільно</b>	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					
T1	T2	T3	T4	M1	T5	T6	T7	M2	30	100
5	5	5	5	10	10	10	10	10		

T1, T2 ... T7 – теми змістових модулів; M1, M2 – модульні контрольні роботи



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

## 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](http://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. – Νοб (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](http://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. – Νο 2. –С. 61 – 68.
5. Указ Президента України від 15 березня 2016 року Νο 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. – Νο 45. – Ст.403.
7. Закон України «Про оборону України» // Відомості Верховної Ради України. – 2017. – Νο 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> .