Чернівецький національний університет імені Юрія Федьковича

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

Кафедра комп'ютерних систем та мереж

"ЗАТВЕРДЖУЮ"
Директор навчально-наукового інституту
фізико-технічних та комп'ютерних наук
_____ **Петро ШПАТАР**
"31" серпня 2026 року

РОБОЧА ПРОГРАМА
навчальної дисципліни

ВК14 Стандарти та політики кібербезпеки
(назва навчальної дисципліни)

вибіркова
(вказати: обов'язкова / вибіркова)

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

Спеціальність F7 Комп'ютерна інженерія
(вказати: код, назва)

Галузь знань F 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 2026 рік

Робоча програма навчальної дисципліни «Стандарти та політики кібербезпеки» складена відповідно до освітньо-професійної програми «Комп'ютерна інженерія».

Розробник: Іванущак Наталія Михайлівна, асистент кафедри КСМ, канд. техн. наук

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

Викладач (чі), що забезпечує читання даної навчальної дисципліни: Іванущак Наталія Михайлівна, асистент кафедри КСМ, канд. техн. наук

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

Затверджено на засіданні кафедри *комп'ютерних систем та мереж*

Протокол № 2 від "31" серпня 2026 року

Завідувач кафедри _____ **Георгій ВОРОБЕЦЬ**

(підпис)

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

Протокол № 1/2 від "31" серпня 2026 року

Голова методичної ради навчально-наукового інституту фізико-технічних та комп'ютерних наук

_____ **Іван КОЗЯРСЬКИЙ**

(підпис)

1. Мета навчальної дисципліни

Мета: формування у здобувачів вищої освіти знань і практичних навичок щодо застосування нормативно-правових вимог, міжнародних стандартів і рекомендацій у сфері кібербезпеки, розроблення та впровадження внутрішніх політик інформаційної безпеки, управління ризиками, оцінювання відповідності вимогам безпеки та організації контролю ефективності заходів кіберзахисту.

2. Результати навчання

Вивчення навчальної дисципліни сприяє формуванню у здобувачів вищої освіти таких компетентностей:

ЗК - загальних

ЗК1. Здатність до адаптації та дій в новій ситуації.
ЗК3. Здатність проводити дослідження на відповідному рівні.
ЗК4. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК5. Здатність генерувати нові ідеї (креативність).
ЗК6. Здатність виявляти, ставити та вирішувати проблеми.
ЗК7. Здатність приймати обґрунтовані рішення.

СК – фахових (спеціальних)

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.
СК7. Здатність досліджувати, розробляти та обирати технології створення великих і надвеликих систем.
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.
СК12. Здатність вирішувати завдання комп'ютерної інженерії з використанням апаратно-програмної обробки даних, засобів штучного інтелекту, хмарних технологій, Інтернету речей та комп'ютеризованих інформаційно-вимірювальних систем і комплексів.

РН - програмних результатів навчання

РН2. Знаходити необхідні дані, аналізувати та оцінювати їх.
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.

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.

Знати: нормативно-правові засади забезпечення кібербезпеки в Україні, основні законодавчі вимоги щодо захисту інформації та персональних даних; основні принципи цифрової етики та відповідального використання інформаційних технологій; принципи, функції та особливості застосування NIST Cybersecurity Framework і CIS Controls для організації кіберзахисту; призначення, структуру та основні етапи розроблення й упровадження внутрішніх політик і процедур інформаційної безпеки; основні поняття та методи управління ризиками кібербезпеки, ідентифікації загроз і оцінювання вразливостей; принципи оцінювання відповідності систем інформаційної безпеки нормативним вимогам, стандартам і внутрішнім політикам організації; основні методи проведення аудиту кібербезпеки, моніторингу дотримання політик і оцінювання ефективності заходів захисту; принципи організації реагування на інциденти кібербезпеки, документування порушень і впровадження коригувальних заходів.

Вміти: аналізувати нормативно-правові акти України та визначати вимоги, що стосуються забезпечення кібербезпеки й захисту персональних даних; застосовувати принципи цифрової етики під час роботи з інформацією та інформаційними системами; використовувати положення NIST Cybersecurity Framework і CIS Controls для визначення пріоритетів кіберзахисту та вибору відповідних заходів безпеки; розробляти проєкти внутрішніх політик і процедур інформаційної безпеки з урахуванням специфіки діяльності організації та чинних нормативних вимог; ідентифікувати загрози інформаційній безпеці, оцінювати ризики та обґрунтовувати вибір заходів щодо їх зменшення; оцінювати відповідність організаційних і технічних заходів захисту вимогам стандартів, нормативних документів і внутрішніх політик; аналізувати результати аудиту кібербезпеки, виявляти недоліки в організації захисту інформації та формулювати рекомендації щодо їх усунення; визначати основні етапи реагування на інциденти кібербезпеки та розробляти пропозиції щодо вдосконалення відповідних процедур; формувати рекомендації щодо підвищення рівня кібербезпеки

організації на основі аналізу ризиків, результатів аудиту та оцінювання ефективності впроваджених заходів захисту.

3. Опис навчальної дисципліни
3.1. Загальна інформація

Форма навчання	Рік підготовки	Семестр	Кількість		Кількість годин						Вид підсумкового контролю
			кредитів	всього годин	лекції	практичні	семінарські	лабораторні	самостійна робота	індивідуальні завдання	
Денна	1(5)	1(9)	4	90	14	-	-	16	60	-	Залік
Заочна	1(5)	1(9)	4	90	4	-	-	4	82	-	Залік

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. Нормативно-правові та міжнародні стандарти кібербезпеки												
Тема 1. Нормативно-правова база України в галузі кібербезпеки.	14	2	-	2	-	10	15	1	-	1	-	13
Тема 2. Цифрова етика та захист персональних даних.	15	2	-	3	-	10	14,5	0,5	-	0	-	13
Тема 3. Стандарти NIST Cybersecurity Framework та CIS Controls.	15	2	-	3	-	10	15,5	0,5	-	1	-	14
Разом за змістовим модулем 1	44	6	-	8	-	30	45	2	-	2	-	40
Змістовий модуль 2. Політики кібербезпеки та управління ризиками												
Тема 4. Розроблення внутрішніх політик підприємства.	11,5	2	-	2	-	7,5	12	0,5	-	1	-	10,5
Тема 5. Управління ризиками інформаційної безпеки	11,5	2	-	2	-	7,5	11	0,5	-	0	-	9,5

Тема 6. Оцінювання відповідності вимогам кібербезпеки (Compliance)	11,5	2	-	2	-	7,5	11	0,5	-	1	-	9,5
Тема 7. Аудит кібербезпеки, моніторинг дотримання політик і реагування на інциденти	11,5	2	-	2	-	7,5	11	0,5	-	0	-	10,5
Разом за змістовим модулем 2	46	8	-	8	-	30	45	2	-	2	-	40
Усього годин	90	14		16	-	56	90	4	-	4	-	80

3.3. Тематика лекційних занять з переліком питань

№	Назва теми з основними питаннями
1	**Нормативно-правова база України в галузі кібербезпеки**. Основні положення законодавства України у сфері кібербезпеки, захисту інформації та функціонування національної системи кібербезпеки. Повноваження державних органів, правові вимоги до суб’єктів кібербезпеки та відповідальність за порушення встановлених вимог.
2	**Цифрова етика та захист персональних даних**. Принципи цифрової етики, відповідального використання інформаційних технологій і дотримання прав людини в цифровому середовищі. Нормативні та організаційні засади захисту персональних даних, забезпечення конфіденційності інформації й запобігання її неправомірному використанню.
3	**Стандарти NIST Cybersecurity Framework та CIS Controls**. Структура, основні принципи та особливості застосування NIST Cybersecurity Framework і CIS Controls для організації системи кіберзахисту підприємства. Використання відповідних фреймворків для визначення пріоритетів захисту, вибору заходів безпеки та підвищення рівня кіберстійкості організації.
4	**Розроблення внутрішніх політик підприємства**. Призначення, структура та основні етапи розроблення внутрішніх політик і процедур кібербезпеки з урахуванням специфіки діяльності підприємства. Визначення правил доступу до інформаційних ресурсів, розподілу відповідальності працівників, вимог до захисту інформації та порядку контролю дотримання встановлених правил.
5	**Управління ризиками інформаційної безпеки**. Основні поняття, принципи та методи управління ризиками інформаційної безпеки, зокрема ідентифікація активів, загроз і вразливостей, аналіз і оцінювання ризиків. Вибір заходів оброблення ризиків, визначення пріоритетів кіберзахисту та оцінювання

	залишкового ризику.
6	**Оцінювання відповідності вимогам кібербезпеки (Compliance)**. Принципи оцінювання відповідності діяльності організації вимогам законодавства, міжнародних стандартів, галузевих нормативів і внутрішніх політик кібербезпеки. Методи перевірки виконання встановлених вимог, документування невідповідностей і розроблення коригувальних заходів для забезпечення належного рівня інформаційної безпеки.
7	**Аудит кібербезпеки, моніторинг дотримання політик і реагування на інциденти**. Мета, завдання та основні етапи аудиту кібербезпеки, методи перевірки ефективності організаційних і технічних заходів захисту та контролю виконання внутрішніх політик. Організація моніторингу подій безпеки, виявлення й класифікація інцидентів, документування результатів і реалізація заходів реагування та відновлення.

3.4. Тематика лабораторних занять

№	Назва теми (завдання)	Кількість годин
1.	Розгортання операційної системи для проведення аудиту кібербезпеки комп’ютерних мереж та систем	2
2.	Інструменти прихованого збору технічної інформації з комп’ютерної системи або мережі.	2
3.	Дослідження вразливостей системи або мережі за допомогою спеціалізованого сканера вразливостей – Nessus.	3
4.	Визначення вразливостей вебресурсів та вебдодатків. Сканер вразливостей – OWASP ZAP	3
5.	Пошук вразливостей та чутливої інформації у відкритих джерелах за допомогою засобу Maltego	3
6.	Навички збору технічної та чутливої інформації за допомогою ПЗ класу «сніфери»	3
	Разом	16

3.5. Самостійна робота студента

№	Назва теми/ кількість балів/ форма контролю	Кількість годин
1	Аналіз міжнародного досвіду правового регулювання кібербезпеки / результати використовуються при виконанні модульної контрольної роботи (МКР) № 1	8
2	Етичні аспекти використання штучного інтелекту та цифрових технологій / результати використовуються при виконанні модульної контрольної роботи (МКР) № 1	8
3	Порівняльний аналіз міжнародних стандартів і фреймворків кібербезпеки / результати використовуються при виконанні	8

	лабораторної роботи № 2	
4	Розроблення політики управління доступом до інформаційних ресурсів підприємства / результати використовуються при виконанні лабораторної роботи № 3	8
5	Методи оцінювання та оброблення ризиків інформаційної безпеки / результати використовуються при виконанні МКР № 2	8
6	Оцінювання відповідності підприємства вимогам стандартів кібербезпеки / результати використовуються при виконанні МКР № 2	8
7	Розроблення плану реагування на інциденти кібербезпеки / результати використовуються при виконанні МКР № 2	8
	Разом	56

4. Форми і методи навчання

Основними формами організації навчання є лекційні та лабораторні заняття, а також самостійна робота здобувачів вищої освіти. Самостійна робота спрямована на опрацювання матеріалів лекцій та літературних джерел.

У процесі вивчення дисципліни застосовуються такі методи навчання:

- Пояснювально-ілюстративний метод – виклад теоретичного матеріалу з використанням прикладів схем, діаграм, таблиць і мультимедійних презентацій для пояснення основних понять, принципів і методологій.
- Демонстраційний метод – показ прикладів розробки та реалізації комп’ютерних систем.
- Практичний метод – виконання лабораторних завдань, спрямованих на формування навичок роботи з апаратно-програмними засобами комп’ютерних систем.
- Проблемно-пошуковий метод – постановка практичних проблем і ситуацій, пов’язаних розробкою та застосуванням комп’ютерних систем.
- Аналіз практичних ситуацій – розгляд прикладів побудови комп’ютерних систем для вирішення прикладних завдань із застосуванням мікроконтролерів, мікрокомп’ютерів та комп’ютерних кластерів.
- Обговорення та навчальні дискусії – колективний аналіз проблемних питань, обговорення результатів виконання лабораторних робіт, порівняння можливих підходів до побудови комп’ютерних систем.
- Презентація результатів виконаних завдань – представлення та захист розроблених програмних моделей комп’ютерних систем, обґрунтування прийнятих рішень і формулювання висновків.

Застосовуються інноваційні освітні технології, зокрема, інформаційно-комунікаційні та студентоцентрованого навчання. Освітні технології передбачають використання мультимедійних матеріалів для лекційних занять, методичних вказівок для виконання лабораторних робіт, мов та середовищ

розробки комп’ютерних програм, комп'ютерної та телекомунікаційної техніки, відеоконференцій, системи електронного навчання Moodle з метою розвитку навичок аналізу, розробки та використання комп’ютерних систем штучного інтелекту.

5. Система контролю та оцінювання

Система контролю та оцінювання передбачає перевірку рівня засвоєння теоретичних знань, сформованості практичних умінь і здатності застосовувати цифрові інструменти для виконання навчальних завдань. Оцінювання здійснюється систематично протягом семестру з урахуванням своєчасності, самостійності, правильності та якості виконаних робіт.

Форми та методи контролю

***Поточний контроль*:** *усне опитування* студента на лекційних заняттях (фронтальне, індивідуальне); *письмовий контроль* (звіти із виконання лабораторних робіт); *практичний контроль* (захист лабораторних робіт); *тестовий/машинний контроль* (тести у системі Moodle).

Рубіжний контроль: письмові контрольні роботи у кінці змістових модулів №1 і №2.

Підсумковий контроль – залік.

6. Критерії оцінювання поточного та підсумкового контролю

Поточне оцінювання (аудиторна та самостійна робота)									**Підсумковий контроль (залік)**	**Сумарна кількість балів**
Змістовий модуль 1				**Змістовий модуль 2**						
Т1	Т2	Т3	М1	Т4	Т5	Т6	Т7	М2		
5	5	5	10	5	5	5	10	10	40	100

Т1, Т2 ... Т15 – теми змістових модулів; М1, М2, М3 – модульні контрольні роботи

Залежно від характеру відповіді здобувача освіти зазначена кількість балів може бути скоригована за наступними критеріями:

К-ть балів	**Критерії оцінки**
max	здобувач освіти дає вичерпну відповідь на поставлене запитання;
0,8 · max	здобувач освіти при відповіді на поставлене запитання припустився незначних неточностей, які не впливають на суть відповіді;
0,6 · max	здобувач освіти 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	здобувач освіти 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 здобувач освіти, 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 здобувач освіти 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.

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

Шкала оцінювання: національна та ЄКТС

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

7. Перелік питань для самоконтролю та підсумкового контролю навчальних досягнень здобувачів освіти

Змістовий модуль 1. Нормативно-правові та міжнародні стандарти кібербезпеки

1. Які основні нормативно-правові акти України регулюють сферу кібербезпеки та захисту інформації?
2. Які основні положення Закону України «Про основні засади забезпечення кібербезпеки України»?
3. Які міжнародні підходи до правового регулювання кібербезпеки застосовуються в Європейському Союзі?
4. Які основні принципи цифрової етики та відповідального використання інформаційних технологій?
5. Які етичні проблеми виникають під час використання штучного інтелекту?

6. Які основні вимоги законодавства щодо захисту персональних даних?
7. Які основні функції та структурні компоненти NIST Cybersecurity Framework?
8. Яке призначення CIS Critical Security Controls і як вони застосовуються для підвищення рівня кібербезпеки?
9. У чому полягають основні відмінності між NIST Cybersecurity Framework і CIS Controls?
10. Що таке політика кібербезпеки організації та яке її призначення?
11. Які основні етапи розроблення, затвердження та впровадження внутрішніх політик кібербезпеки?
12. Які основні вимоги висуваються до політики управління доступом до інформаційних ресурсів підприємства?
13. У чому полягає принцип найменших привілеїв (Least Privilege) і як він реалізується на практиці?
14. Які основні методи ідентифікації, автентифікації та авторизації користувачів?
15. Які основні етапи процесу управління ризиками інформаційної безпеки?
16. Як визначаються активи, загрози та вразливості інформаційної системи?
17. Які методи використовуються для оцінювання ймовірності реалізації загроз і можливих наслідків кіберінцидентів?

Змістовий модуль 2. Політики кібербезпеки та управління ризиками

1. Як здійснюється якісне та кількісне оцінювання ризиків інформаційної безпеки?
2. Які основні стратегії оброблення ризиків інформаційної безпеки?
3. Що таке залишковий ризик і за яких умов він може бути прийнятним для організації?
4. Що означає відповідність вимогам кібербезпеки (Compliance) та які її основні завдання?
5. Які етапи передбачає оцінювання відповідності діяльності підприємства вимогам законодавства, стандартів і внутрішніх політик?
6. Які методи та інструменти використовуються для перевірки відповідності вимогам кібербезпеки?
7. Як розробляється контрольний перелік (чекліст) для оцінювання відповідності організації вимогам вибраного стандарту?
8. Які типові невідповідності виявляються під час оцінювання системи управління інформаційною безпекою?
9. Що таке аудит кібербезпеки та які його основні цілі й завдання?
10. Які організаційні й технічні заходи контролю перевіряються під час аудиту кібербезпеки?
11. Які основні етапи проведення аудиту кібербезпеки та оформлення його результатів?
12. Що таке інцидент кібербезпеки та за якими критеріями здійснюється його класифікація?
13. Які основні етапи процесу реагування на інциденти кібербезпеки?
14. Які завдання виконуються під час виявлення, реєстрації, локалізації та усунення наслідків кіберінциденту?
15. Які функції та повноваження відповідальних осіб мають бути визначені в плані реагування на інциденти?

16. Які заходи забезпечують відновлення роботи інформаційних систем після кіберінциденту?
17. Як здійснюються моніторинг дотримання політик кібербезпеки та контроль ефективності впроваджених заходів?
18. Які показники можна використовувати для оцінювання ефективності системи управління кібербезпекою?
19. Як результати аудиту, оцінювання ризиків та аналізу інцидентів використовуються для вдосконалення системи кібербезпеки організації?
20. Які основні вимоги висуваються до документування результатів оцінювання відповідності, аудиту та реагування на інциденти?
21. Які рекомендації доцільно надати підприємству за результатами виявлення невідповідностей вимогам кібербезпеки?
22. Як забезпечити безперервне вдосконалення політик, процедур і заходів кібербезпеки з урахуванням змін загроз, технологій і нормативних вимог?

8. Зарахування результатів неформальної освіти

Відповідно до «Положення про взаємодію формальної та неформальної освіти, визнання результатів навчання (здобутих шляхом неформальної та/або інформальної освіти, в системі формальної освіти) у Чернівецькому національному університеті імені Юрія Федьковича (протокол №16 від 25 листопада 2024 року) (https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/poriadok-vyznannia-u-chernivetskomu-natsionalnomu-universyteti-imeni-yuriia-fedkovycha-rezultativ-navchannia-zdobutykh-shliakhom-neformalnoi-taabo-informalnoi-osvity/) у процесі вивчення дисципліни здобувачу освіти може бути зараховано до 25% балів, отриманих за результатами неформальної та/ або інформальної освіти, які відповідають тематиці дисципліни.

9. Рекомендована література

Фахова (основна)

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/go/2163-19.
2. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/go/2297-17.
3. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (.
4. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT). Київ : ДП «УкрНДНЦ», 2023.
5. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg : NIST, 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29.

6. 10. Center for Internet Security. CIS Critical Security Controls v8.1. URL: https://www.cisecurity.org/controls.
7. Вступ до кібербезпеки: Методичні рекомендації до виконання лабораторних робіт для студентів денної форми навчання галузі 12 Інформаційні технології. / уклад. Смірнов О.А., Буравченко К.О., Смірнова Т.В., Конопліцька-Слободенюк О.К., Смірнов С.А., Козлов Я.О. / М-во освіти і науки України, Центральноукр. нац. техн. ун-т; – Кропивницький: ЦНТУ – 2022. – 155 с.

Допоміжна

1. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12.
2. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20.
3. Державна служба спеціального зв'язку та захисту інформації України. Офіційний вебсайт. URL: https://cip.gov.ua/.
4. ДСТУ 8302:2015. Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. Київ : ДП «УкрНДНЦ», 2016.
5. Joint Task Force. Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53 Rev. 5. Gaithersburg : National Institute of Standards and Technology, 2020. DOI: https://doi.org/10.6028/NIST.SP.800-53r5.
6. National Institute of Standards and Technology. Cybersecurity Framework. URL: https://www.nist.gov/cyberframework.
7. Center for Internet Security. CIS Controls Navigator. URL: https://www.cisecurity.org/controls/cis-controls-navigator.

10. Інформаційні ресурси

1. Система електронного навчання Чернівецького національного університету імені Юрія Федьковича (Moodle). URL: https://moodle.chnu.edu.ua/
2. Освітні програми кафедри КСМ – URL: https://csn.chnu.edu.ua/about-us/ok-rivni/
3. ОПП «Комп'ютерна інженерія» (магістратура). URL: https://csn.chnu.edu.ua/spetsialnist-123-komp-yuterna-inzheneriya-opp-komp-yuterna-inzheneriya-magistratura-1-5-r/
4. 10. CERT-UA. Урядова команда реагування на комп'ютерні надзвичайні події України. URL: https://cert.gov.ua/.
5. OWASP. OWASP Top 10: The Ten Most Critical Web Application Security Risks. URL: https://owasp.org/www-project-top-ten/.
6. Center for Internet Security. CIS Critical Security Controls Navigator. URL: https://www.cisecurity.org/controls/cis-controls-navigator.
7. SANS Institute. Information Security Policy Templates. URL: https://www.sans.org/information-security-policy/.

11. Політика академічної доброчесності

Дотримання політики щодо академічної доброчесності учасниками освітнього процесу при вивченні освітнього компонента регламентовано чинними документами ЧНУ:

- «Етичний кодекс Чернівецького національного університету імені Юрія Федьковича» https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/etychnyi-kodeks-chernivetskoho-natsionalnoho-universytetu-imeni-yuriia-fedkovycha/
- «Положенням про виявлення та запобігання академічного плагіату у Чернівецькому національному університеті імені Юрія Федьковича» https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/polozhennia-pro-vyiavlennia-ta-zapobihannia-akademichnomu-plahiatu-u-chernivetskomu-natsionalnomu-universyteti-imeni-yuriia-fedkovycha/
- «Політика використання штучного інтелекту в Чернівецькому національному університеті імені Юрія Федьковича» https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/polityka-vykorystannia-shtuchnoho-intelektu-v-chernivetskomu-natsionalnomu-universyteti-imeni-yuriia-fedkovycha/

Використання здобувачами освіти інструментів штучного інтелекту (ШІ) під час виконання навчальних завдань:

- допускається за умови дотримання принципів академічної доброчесності (здобувач освіти несе відповідальність за зміст, достовірність і результати поданої роботи, а у разі використання ШІ зобов'язаний зазначити факт і спосіб його застосування);
- не допускається використання ШІ як заміни самостійного виконання завдань або з метою порушення вимог академічної доброчесності;
- додаткові обмеження чи вимоги щодо використання ШІ можуть визначатися викладачем в освітньому процесі для конкретних видів навчальної діяльності відповідно до особливостей дисципліни.