

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**

ОК29. Захист інформації в комп'ютерних системах

(назва навчальної дисципліни)

обов'язкова

(вказати: обов'язкова / вибіркова)

Освітньо-професійна програма Комп'ютерна інженерія,

Програмування мобільних і вбудованих комп'ютерних систем та

засобів Інтернету речей

Спеціальність 123 Комп'ютерна інженерія

(вказати: код, назва)

Галузь знань 12 Інформаційні технології

(вказати: шифр, назва)

Рівень вищої освіти перший (бакалаврський)

(вказати: перший бакалаврський/другий магістерський)

Навчально-науковий інститут 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

ОК29 Захист інформації в комп'ютерних системах

(назва навчальної дисципліни)

складена відповідно до освітньо-професійної програми

Комп'ютерна інженерія, Програмування мобільних і вбудованих

комп'ютерних систем та засобів Інтернету речей, 123 Комп'ютерна інженерія,

(назва освітньо-професійної програми, код та назва спеціальності)

12 Інформаційні технології, 30 червня 2022 р.

(галузь знань: шифр та назва; дата останнього затвердження)

Розробники: Іванущак Наталія Михайлівна, асистент кафедри КСМ,

канд. техн. наук, доцент

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

Затверджено на засіданні кафедри комп'ютерних систем та мереж

Протокол № 1 від “29” серпня 2022 року

Завідувач кафедри



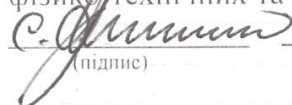
(Воробець Г.І.)

(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.)

(прізвище та ініціали)

1. Мета навчальної дисципліни

Мета: надання студентам систематизованих знань з основ захисту інформації: мети, завдань, принципів організації комплексних систем захисту інформації на основі нормативних документів; забезпечення вмінням боротьби з загрозами інформації в комп'ютерних мережах; теоретичними і практичними знаннями засобів захисту інформації від витоку технічними каналами; методами боротьби з несанкціонованим доступом до інформації з обмеженим доступом; використанням програмно-апаратних методів для побудови систем захисту.

2. Результати навчання

У результаті вивчення навчальної дисципліни студент 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: будувати політику безпеки в комп'ютерних мережах на основі аналізу загроз та оцінки ризиків; використовувати програмні, організаційно-адміністративні та технічні засоби захисту інформації; орієнтуватися в законодавчо-нормативній базі в галузі захисту інформації; правильно налагоджувати підсистеми захисту сучасних операційних систем; правильно визначати та застосовувати критерії захищеності автоматизованих систем.

2.3. Набути компетентностей:

ЗК – загальних

- ЗК1. Здатність до абстрактного мислення, аналізу і синтезу.
- ЗК3. Здатність застосовувати знання у практичних ситуаціях.
- ЗК7. Вміння виявляти, ставити та вирішувати проблеми.
- ЗК8. Здатність працювати в команді.

ФК – фахових (спеціальних)

- ФК5. Здатність використовувати засоби і системи автоматизації проектування до розроблення компонентів комп'ютерних систем та мереж, Інтернет додатків, кіберфізичних систем тощо.
- ФК7. 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.

ФК10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного 8 устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

ФК11. Здатність оформляти отримані робочі результати у вигляді презентацій, науково-технічних звітів.

ФК14. Здатність проектувати системи та їхні компоненти з урахуванням усіх аспектів їх життєвого циклу та поставленої задачі, включаючи створення, налаштування, експлуатацію, технічне обслуговування та утилізацію.

ФК15. Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати та захищати прийняті рішення.

ФК16. Здатність застосовувати технології комп'ютерних систем і мереж, дискретної обробки інформації та числових методів для реалізації інформаційно-вимірювальних систем і систем передачі даних.

ПРН – програмних результатів навчання

ПРН7. Вміти розв'язувати задачі аналізу та синтезу засобів, характерних для спеціальності.

ПРН8. Вміти системно мислити та застосовувати творчі здібності до формування нових ідей.

ПРН13. Вміти ідентифікувати, класифікувати та описувати роботу комп'ютерних систем та їх компонентів.

3. Опис навчальної дисципліни

3.1. Загальна інформація

Назва навчальної дисципліни <i>OK29 Захист інформації в комп'ютерних системах</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	4	7	4	120	2	24	-	-	24	72	-	Залік
Заочна	4	7	4	120	2	6	-	-	6	108	-	Залік

Примітка. Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить: для денної форми навчання – 0,66 $((24+24)/72)$;
для заочної форми навчання – 0,11 $((6+6)/108)$.

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. Політика безпеки підприємства												
Тема 1. Основні поняття та визначення захисту інформації.	15	3	-	3	-	9	15	1	-	1	-	13
Тема 2. Формальний та неформальний підхід опису загроз комп'ютерної системи.	15	3	-	3	-	9	15	0	-	1	-	13
Тема 3. Шкідливі програми та кіберзлочини. Політика безпеки.	15	3	-	3	-	9	15	1	-	0	-	14
Тема 4. Стандартизовані критерії оцінки захищеності інформації від НСД.	15	3	-	3	-	9	15	1	-	1	-	14
Разом за змістовим модулем 1	60	12	-	12	-	36	60	3	-	3	-	54
Змістовий модуль 2. Захист інформації в сучасних операційних системах												
Тема 5. Контроль цілісності даних і аутентифікація повідомлень.	15	3	-	3	-	9	15	1	-	1	-	13
Тема 6. Протоколи аутентифікації.	15	3	-	3	-	9	15	0	-	1	-	13
Тема 7. Механізми та протоколи керування криптографічними ключами.	15	3	-	3	-	9	15	1	-	1	-	14
Тема 8. Стеганографія. Основні принципи захисту інформації при підключенні до мережі Інтернет.	15	3	-	3	-	9	15	1	-	0	-	14
Разом за змістовим модулем 2	60	12	-	12	-	36	60	3	-	3	-	54
Усього годин	120	24	-	24	-	72	120	6	-	6	-	108

3.3. Тематика лабораторних занять

№	Назва теми	Кількість годин
1.	Механізми захисту операційної системи Windows (керування обліковими записами).	3
2.	Захист реєстру операційної системи Windows	3
3.	Модель безпеки операційної системи Windows	3
4.	Налаштування політики безпеки операційної системи Windows	3
5.	Вивчення можливостей захисту шифрованої файлової системи (EFS) Windows	3
6.	Дослідження можливостей брандмауєра Windows	3
7.	Реалізація дискреційної моделі політики безпеки	3
8.	Реалізація мандатної моделі політики безпеки	3
	Разом	24

Примітка. Методичні рекомендації та завдання до лабораторних робіт доступні на інтернет-ресурсі: <https://moodle.chnu.edu.ua/course/view.php?id=1357>

3.4. Самостійна робота студента

№ з/п	Назва теми	Кількість годин
1	Огляд підсистеми захисту операційної системи Linux Tails	9
2	Огляд підсистеми захисту операційної системи OpenBSD	9
3	Криптографічні засоби захисту операційної системи Linux Ubuntu	9
4	Огляд властивостей підсистеми захисту AppArmor	9
5	Засоби захисту операційної системи Android	9
6	Засоби захисту операційної системи iOS	9
7	Аутентифікація користувачів на основі токенів безпеки	9
8	Моделювання підсистеми керування доступом та аудиту	9
	Разом	72

4. Форми і методи навчання

Форми навчання – це проблемні й оглядові лекції, лабораторні заняття, заняття із застосуванням комп'ютерної та телекомунікаційної техніки, інтерактивні заняття з навчанням одних студентів іншими, інтегровані заняття, проблемні заняття, відеолекції, відеозаняття і відеоконференції засобами Google Meet, Zoom, заняття з використанням системи електронного навчання Moodle.

Підходи до навчання: використовуються студентоцентрований, проблемно-орієнтований, діяльнісний, комунікативний, професійно-орієнтований, міждисциплінарний підходи.

Для викладання матеріалів з навчальної дисципліни «Комп'ютерні системи» 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, де 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

Оцінка за національною шкалою (залік)	Оцінка за шкалою ЄКТС	
	Оцінка (бали)	Пояснення за розширеною шкалою
Зараховано	A (90-100)	Зараховано
	B (80-89)	
	C (70-79)	
	D (60-69)	
	E (50-59)	
Не зараховано	FX (35-49)	Не зараховано з можливістю повторного складання
	F (1-34)	Не зараховано з обов'язковим повторним вивченням дисципліни

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.

Поточне тестування та самостійна робота										Підсумковий тест (залік)	Сума балів
Змістовий модуль 1					Змістовий модуль 2						
T1	T2	T3	T4	M1	T5	T6	T7	T8	M2	40	100
5	5	5	5	10	5	5	5	5	10		

Формами підсумкового контролю рівня знань є виконання підсумкового тестування на курсі <https://moodle.chnu.edu.ua/course/view.php?id=1357>.

8. Рекомендована література

Фахова (основна)

1. Захист інформації в комп'ютерних системах : конспект лекцій / укл.: Іванущак Н.М. Чернівці : Чернівецький національний університет ім. Ю. Федьковича, 2022. – 82 с.
2. Захист інформації в комп'ютерних системах: методичні вказівки до лабораторних робіт / укл.: Іванущак Н.М. Чернівці : Чернівецький національний університет ім. Ю. Федьковича, 2022. – 52 с.
3. Остапов С.Е., Євсєєв С.П., Король О.Г. Кібербезпека: сучасні технології захисту. Львів: Новий світ-2000, 2020. - 678 с.
4. Остапов С.Е., Євсєєв С.П., Король О.Г. Технології захисту інформації. Чернівці: «Родовід», 2014. – 428 с.
5. Євсєєв С.П., Король О.Г., Шматко О.В. Кібербезпека: криптографія з PYTHON. Львів: Новий світ-2000, 2021. – 120 с.

Допоміжна

1. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. – К.: Видавничий дім «Кондор», 2019. – 272 с.
2. Андреев В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є Основи кібербезпеки / За ред. проф. В.О. Хорошка. вид., доп. і перероб. – К.: Вид. ДУІКТ, 2009. – 292 с.
3. Беззубов Д.О. Суспільна безпека (організаційно-правові засади забезпечення): монографія / Д.О. Беззубов. – Київ : «МП Леся», 2013. – 425 с.
4. Данільян О.Г. Національна безпека України: структура та напрямки реалізації : [навч. посібник] / О.Г. Данільян, О.П. Дзьобань, М.І. Панов. – Х. : Фоліо, 2002. – 285 с.
5. Жарков Я.М. Кібербезпека особистості, суспільства, держави : підручник / Я.М. Жарков, М.Т. Дзюба, І.В. Замаруєва та ін. — К. : Видавничо-поліграфічний центр Київський університет», 2008. – 256 с.
6. Кормич Б.А. Кібербезпека: організаційно-правові основи : Навч. посібн. / Б.А. Кормич. – К. : Кондор, 2008. – 382 с.

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-programuvannya-mobilnyh-i-vbudovanyh-komp-yuternyh-system-ta-zasobiv-internetu-rechej-bakalavrat-4-r/>
3. <https://moodle.chnu.edu.ua/course/view.php?id=1357>