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

Комп'ютерний захист фінансової інформації

(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))

Навчально-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 Moodle https://moodle.chnu.edu.ua/course/view.php?id=1561

Консультації *on-line: середа з 17.00 до 18.00*

1. Анотація дисципліни

Курс «Комп'ютерний захист фінансової інформації» призначений для розширення компетентностей випускників спеціальності 123 - Комп'ютерна інженерія для набуття студентами базових знань засобів захисту інформації, специфічних для комерційно-банківського сектору; навчання методам боротьби з несанкціонованим доступом до інформації з обмеженим доступом, у тому числі комерційного характеру; використання програмно-апаратних методів для побудови систем захисту.

2. Мета навчальної дисципліни: надання студентам систематизованих знань з інформаційної безпеки електронного бізнесу: мети, завдань, принципів організації комплексних систем електронної комерції та банківського бізнесу; забезпечення вмінням боротьби з загрозами інформації у банківських системах. Матеріал курсу допоможе при аналізі інформаційних джерел, підготовці курсових і дипломних робіт, статей, доповідей на науково-практичних конференціях. Окрім цього, засвоєння дисципліни дозволить майбутнім фахівцям забезпечити необхідний рівень володіння інструментами дослідження і проектування комплексної системи захисту інформації, в тому числі комерційного характеру.

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, програмування. Доцільно також мати певні уявлення з архітектури комп'ютерів, основ баз даних, основ конструювання обчислювальної техніки. Результати навчання за цим курсом потрібні при вивченні дисципліни «Кібербезпека Cisco» та виконанні дипломного проекту.

4. Результати навчання

У результаті вивчення навчальної дисципліни студент повинен

4.1. Знати: найновіші досягнення в галузі інформаційної безпеки банківського бізнесу, характеристики основних підсистем ідентифікації та аутентифікації, характеристики основних механізмів доступу, пов'язаних з особливостями банківської сфери, характеристики підсистем захисту основних захищених протоколів, у тому числі спеціалізованих, основні поняття безпеки мікропроцесорних карток, основні канали витоку інформації та методи боротьби з ними, основні поняття безпеки систем електронної комерції та платіжних систем.

4.2. Вміти: використовувати програмні, організаційно-адміністративні та технічні засоби захисту банківської та комерційної інформації; орієнтуватися в законодавчо-нормативній базі в галузі захисту інформації; правильно налагоджувати підсистеми захисту сучасних операційних систем; використовувати спеціалізовані підсистеми захисту протоколів передавання даних, в т.ч. спеціалізованих; правильно визначати та застосовувати критерії захищеності автоматизованих систем обробки банківської інформації.

4.3. Набути компетентностей:

ЗК - загальних

ЗК3. Здатність проводити дослідження на відповідному рівні.

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.

СК7. Здатність досліджувати, розробляти та обирати технології створення великих і надвеликих систем.

СК8. Здатність забезпечувати якість продуктів і сервісів інформаційних технологій на протязі їх життєвого циклу.

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.

РН9. Розробляти програмне забезпечення для вбудованих і розподілених застосувань, мобільних і гібридних систем.

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 *Комп'ютерний захист фінансової інформації*												
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)**	**1(9)**	**4**	**120**	**2**	**15**	**-**	**-**	**15**	**90**	**-**	**Залік**
Заочна	**1(5)**	**1(9)**	**4**	**120**	**2**	**4**	**-**	**-**	**4**	**112**	**-**	**Залік**

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. Традиційна та електронна комерція												
Тема 1. Види та засоби захисту електронної комерції.	14	2	-	2	-	10	14	1	-	1	-	12
Тема 2. Види платіжних систем та транзакцій в електронному бізнесі.	14	2	-	2	-	10	14	0	-	-	-	14
Тема 3. Технологія Eectronic Data Interchange (EDI).	14	2	-	2	-	10	16	1	-	1	-	14
Тема 4. Структура системи розрахунку за допомогою цифрової готівки.	14	2	-	2	-	10	16	0	-	-	-	16
Разом за змістовим модулем 1	56	8	-	8	-	40	60	2	-	2	-	56
Змістовий модуль 2. Комп'ютерний захист фінансової інформації												
Тема 5. Захищені протоколи.	19	2	-	2	-	15	20	1	-	1	-	18
Тема 6. Стандартизація та структура платіжних карток.	19	2	-	2	-	15	18	0	-	-	-	18
Тема 7. Сучасні криптовалюти.	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	Кількість годин
1.	Механізми захисту інформації у спрощених EDI-системах	2
2.	Емуляція роботи банкомату	2
3.	Використання електронних гаманців у системах електронної торгівлі	2
4.	Механізми захисту повідомлень в протоколі SET	2
5.	Розробка навчальної криптовалюти	3
6.	Генерування користувачів та транзакцій	3
7.	Майнінг	3
	Разом	15

Примітка. Методичні рекомендації та завдання до лабораторних робіт доступні на інтернет-ресурсах: https://moodle.chnu.edu.ua/course/view.php?id=1561

Програмне забезпечення для виконання лабораторних робіт: мова програмування Python.

5.4. Зміст завдань для самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Створення спрощеної системи захисту протоколів iKP.	10
2	Розробка спрощеної версії механізмів захисту протоколу SET.	10
3	Розробка спрощеної версії системи мобільної торгівлі.	10
4	Розробка спрощеної версії системи електронних гаманців.	15
5	Емуляція роботи смарт-картки на основі флеш- накопичувача.	15
6	Розробка спрощеної системи цифрової готівки.	15
7	Емуляція системи захисту смарт-картки.	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 заліку або виконання підсумкового тестування в системі Moodle.

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

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

Розподіл балів, які отримують студенти

Поточне тестування та самостійна робота									Підсумковий тест (залік)	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		

Змістовий модуль 1. Традиційна та електронна комерція

Т1. Види та засоби захисту електронної комерції (виконання та захист лабораторної роботи №1 на основі лекційного матеріалу та методичних вказівок до лабораторної роботи – 5 балів).

Т2. Види платіжних систем та транзакцій в електронному бізнесі (виконання та захист лабораторної роботи № 2 на основі лекційного матеріалу та методичних вказівок до лабораторної роботи – 5 балів).

Т3. Технологія Eectronic Data Interchange (EDI) (виконання та захист лабораторної роботи № 3 на основі лекційного матеріалу та методичних вказівок до лабораторної роботи – 5 балів).

Т4. Структура системи розрахунку за допомогою цифрової готівки (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. Комп'ютерний захист фінансової інформації

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

Т6. Стандартизація та структура платіжних карток (виконання та захист лабораторної роботи № 6 на основі лекційного матеріалу та методичних вказівок до лабораторної роботи – 10 балів).

Т7. Сучасні криптовалюти (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 (**залік**) – 30 балів: підсумкове тестування студентів у системі Moodle. **Сумарна кількість балів** – 100.

7. Рекомендована література

Фахова (основна)

1. Комп'ютерний захист фінансової інформації: конспект лекцій / уклад.: Н.М. Іванущак. Чернівці: ЧНУ, 2022. 98 с.
2. Комп'ютерний захист фінансової інформації: методичні вказівки до лабораторних робіт / уклад.: Н.М. Іванущак. Чернівці: ЧНУ, 2022. 50 с.
3. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.:ВНV, 2009. – 608 с.
4. Електронний банкінг : (організаційно-правове забезпечення) / [Новацький А. М. та ін. ; зазаг. ред. А. М. Новацького] ; Нац. ун-т держ. податк. служби України, Наук.-дослід. центрз пробл. оподаткування, Наук.-дослід. центр прав. інф-ки при Акад. прав. наук України. — Ірпінь : Нац. ун-т ДПС України, 2008. — 294 с.
5. Міщенко В.І., Слав'янська Н.Г., Коренєва О.Г. Банківські операції : підручник. 2-гевид., перероб. ідоп. К. : Знання, 2020. 796 с.
6. Методи аналізу та моделювання безпеки розподілених інформаційних систем / [В. В.Литвинов та ін.] ; за заг. ред. С. М. Шкарлета ; М-во освіти і науки України, Черніг. нац.технол. ун-т. — Чернігів : Черніг. нац. технол. ун-т, 2017. — 204 с. : іл., табл.
7. Страхарчук А.Я., Страхарчук В.П. Інформаційні системи і технології в банках : навч. посіб. К. : Знання, 2010. 515 с.

Допоміжна

1. Закон України «Про захист інформації в автоматизованих системах».
2. Закон України «Про інформацію».
3. Закон України «Про державну таємницю».
4. Kwak, Kyung Sup, Sana Ullah, and Niamat Ullah. "An Overview of IEEE 802.15.6 Standard." 2010 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2010) (November 2010). doi:10.1109/isabel.2010.5702867.

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. https://moodle.chnu.edu.ua/course/view.php?id=1561