Чернівецький національний університет імені Юрія Федьковича

(повне найменування закладу вищої освіти)

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 технологій інтернету речей та кіберфізичних систем"*

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))

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.

1.1. 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.

1.2. Завдання навчальної дисципліни «Комп’ютерний захист фінансової інформації» - вивчення студентами основних теоретичних понять захисту інформації; уміння застосовувати їх для розв’язку завдань, що ставить перед ними виробництво; набуття студентами практичних навичок; вільне володіння основними методами захисту інформації; розуміння основних понять і сучасного стану даного предмету; здатність проектувати та аналізувати ефективність засобів захисту та управління безпекою в програмно-апаратних рішеннях системи захисту інформації; уміння створювати і застосовувати інформаційні комп’ютерні системи відповідно до сучасних концепцій інженерії даних і знань.

1.3. 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.

2. Результати навчання

У результаті вивчення навчальної дисципліни студент повинен

2.1. 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.

2.2. 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.

2.3. Набути компетентностей:

Z - загальних

Z3. Здатність застосовувати знання у практичних ситуаціях.

Z7. Вміння виявляти, ставити та вирішувати проблеми.

Z8. Здатність працювати в команді.

P - фахових

P2. Здатність використовувати сучасні методи і мови програмування для розроблення алгоритмічного та програмного забезпечення.

P3. Здатність створювати системне та прикладне програмне забезпечення комп'ютерних систем та мереж.

P5. Здатність використовувати засоби і системи автоматизації проектування до розроблення компонентів комп'ютерних систем та мереж, Інтернет додатків, кіберфізичних систем тощо.

P7. 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.

P8. Готовність брати участь у роботах з впровадження комп'ютерних систем та мереж, введення їх до експлуатації на об'єктах різного призначення.

P10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

P11. Здатність оформляти отримані робочі результати у вигляді презентацій, науково-технічних звітів.

P15. Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати та захищати прийняті рішення.

ПРН - програмовані результати навчання за загальними та загально-професійними фаховими компетентностями

N1. Знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж.

N2. Мати навички проведення експериментів, збирання даних та моделювання в комп'ютерних системах.

N3. Знати новітні технології в галузі комп'ютерної інженерії.

N6. Вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.
N7. Вміти розв'язувати задачі аналізу та синтезу засобів, характерних для спеціальності.

N8. Вміти системно мислити та застосовувати творчі здібності до формування нових ідей.
N9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності.
N10. Вміти розробляти програмне забезпечення для вбудованих і розподілених застосувань, мобільних і гібридних систем, розраховувати, експлуатувати, типове для спеціальності обладнання.
N13. Вміти ідентифікувати, класифікувати та описувати роботу комп'ютерних систем та їх компонентів.
N14. Вміти поєднувати теорію і практику, а також приймати рішення та виробляти стратегію діяльності для вирішення завдань спеціальності з урахуванням загальнолюдських цінностей, суспільних, державних та виробничих інтересів.
N15. Вміти виконувати експериментальні дослідження за професійною тематикою.
N16. Вміти оцінювати отримані результати та аргументовано захищати прийняті рішення.
N20. Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення.

3. Опис навчальної дисципліни
3.1. Загальна інформація

Назва навчальної дисципліни *ППВ1 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	**5**	**7**	**4**	**120**	**2**	**15**	**-**	**-**	**15**	**90**	**-**	**Залік**
Заочна	**5**	**7**	**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).

3.2. 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. Вступ. Основні поняття електронної комерції та банкінгу.	14	2	-	2	-	10	13	1	-	1	-	12
Тема 2. Гроші та платіжні системи	16	2	-	2	-	10	15	0	-	-	-	14
Тема 3. Електронна комерція типу B2B та системи обміну даними	16	2	-	2	-	10	15	1	-	1	-	14
Тема 4. Віддалені платежі за допомогою банківських карток.	14	2	-	2	-	10	17	0	-	-	-	16
Разом за змістовим модулем 1	60	8	-	8	-	40	60	2	-	2	-	56
Змістовий модуль 2. Комп'ютерний захист фінансової інформації												
Тема 5. Захищені протоколи.	18	2	-	2	-	15	18	1	-	1	-	18
Тема 6. Безпека мікропроцесорних карток.	26	2	-	2	-	15	20	0	-	-	-	18
Тема 7. Сучасні криптовалюти.	16	3	-	3	-	20	22	1	-	1	-	20
Разом за змістовим модулем 2	60	7	-	7	-	50	60	2	-	2	-	56
Усього годин	120	15	-	15	-	90	120	4	-	4	-	112

3.2.1. Теми семінарських або практичних, або <u>лабораторних</u> занять

№	Назва теми
1.	Вивчення системи захисту даних TrueCrypt
2.	Вивчення системи захисту даних Криптобанк
3.	Дослідження захисту інформації у спрощених EDI- системах
4.	Розробка системи "Банкоматик"
5.	Використання електронних гаманців у системах е-торгівлі
6.	Вивчення захисту повідомлень у спрощеному протоколі SET
7.	Розробка навчальної криптовалюти

3.2.2. Тематика індивідуальних завдань

В даному курсі виконання індивідуальних завдань не передбачено.*

* ІНДЗ – може бути рекомендовано в окремих випадках для студентів, які успішно освоїли основний навчальний матеріал, з метою поглибленого вивчення чи удосконалення матеріалів певного змістового модуля, або в цілому для навчальної дисципліни за рішенням кафедри чи викладача.

3.2.3. Самостійна робота

№ з/п	Назва теми
1	Створення спрощеної системи захисту протоколів iKP.
2	Розробка спрощеної версії механізмів захисту протоколу SET.
3	Розробка спрощеної версії системи мобільної торгівлі.
4	Розробка спрощеної версії системи електронних гаманців.
5	Емуляція роботи смарт-картки на основі флеш- накопичувача.Розробка спрощеної системи цифрової готівки.
6	Розробка спрощеної системи цифрової готівки.
7	Емуляція системи захисту смарт-картки.

3.3. 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.

Методи: проблемний виклад матеріалу, частково-пошукові та дослідницькі лабораторні практикуми, презентації, консультації і дискусії, робота в інтернет-класі: електронні лекції, лабораторні роботи, дистанційні консультації та ін., спрямовані на активізацію і стимулювання навчально-пізнавальної діяльності студентів.

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

Реалізація навчального процесу здійснюється під час лекційних, лабораторних занять, самостійної позааудиторної роботи з використанням сучасних інформаційних технологій навчання, консультацій з викладачами.

Для **формувань уміння та навичок** застосовуються такі **методи навчання**:

- вербальні/словесні *(лекція, пояснення, розповідь, бесіда, інструктаж);*
- наочні *(спостереження, ілюстрація, демонстрація);*
- практичні *(проведення експерименту, практики);*
- пояснювально-ілюстративний або інформаційно-рецептивний, який передбачає пред’явлення готової інформації викладачем та її засвоєння студентами*;*
- репродуктивний *(виконання лабораторних завдань за зразком);*
- метод проблемного викладу матеріалу на лекційних заняттях.

3.4. Технічне й програмне забезпечення/обладнання.

Комп’ютери в комп’ютерних класах 8 к. ЧНУ кафедри КСМ з наступною конфігурацією:

- Motherboard Asus Prime H310M-A R2.0
- CPU Intel Pentium Gold G5400 (BX80684G5400) s1151 BOX
- SSD Apacer AS350 Panther 240GB 2.5" SATAIII TLC (AP240GAS350-1)

- Memory HyperX DDR4-2400 8192MB PC4-19200 Fury Black (HX424C15FB2/8)
- Case GameMax ET-207 400 Вт
- Keyboard Defender Element HB-520 PS/2 Black (45520)
- Mouse 2E MF107 USB Black (2E-MF107UB
- Monitor 21.5" Philips.

Програмне забезпечення: ліцензійні пакети Windows 10, MS Office sotfware 79P-05726 OfficeProPlus 2019 UKR OLP NL Acdmc Non-specific No Level (Word, Excel, Power Point, Access); хмарний сервіс Google Colab, програмне забезпечення Cisco Packet Tracer.

4. Система контролю та оцінювання

4.1. Розподіл максимально можливої кількості балів, які отримують студенти за виконання всіх видів навчальної діяльності

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. Вступ. Основні поняття електронної комерції та банкінгу (виконання та захист лабораторної роботи №1 на основі лекційного матеріалу та матеріалів практичних занять – 5 балів).

Т2. Гроші та платіжні системи (виконання та захист лабораторної роботи № 2 на основі лекційного матеріалу та матеріалів практичних занять – 5 балів).

Т3. Електронна комерція типу B2B та системи обміну даними (виконання та захист лабораторної роботи № 3 на основі лекційного матеріалу та матеріалів практичних занять – 5 балів).

Т4. Віддалені платежі за допомогою банківських карток (виконання та захист лабораторної роботи № 4 на основі лекційного матеріалу та матеріалів практичних занять – 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 матеріалів практичних занять – 10 балів).

Т6. Безпека мікропроцесорних карток (виконання та захист лабораторної роботи № 6 на основі лекційного матеріалу та матеріалів практичних занять – 10 балів).

Т7. Сучасні криптовалюти (виконання та захист лабораторної роботи № 7 на основі лекційного матеріалу та матеріалів практичних занять – 10 балів).

М2 – модульна контрольна робота №2 (10 балів).

4.2. Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	**A**	відмінно	зараховано
80 – 89	**B**	добре	
70 – 79	**C**		
60 – 69	**D**	задовільно	
50 – 59	**E**		
35 – 49	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0 – 34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

4.3. Засоби оцінювання

Засобами оцінювання результатів навчання студента є: завдання для виконання лабораторних робіт, тести, а також модульні контрольні роботи.

4.4. 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.

Формами підсумкового контролю рівня знань є усна та письмова відповідь студента при здачі заліку або підсумкове тестування у системі Moodle.

4.5. Політика дисципліни

Визначається системою вимог викладача щодо рівня знань і засвоєння матеріалу студентом при вивченні дисципліни, та ґрунтується на засадах академічної доброчесності з урахуванням норм законодавства України щодо академічної доброчесності та Статуту, положень Університету, й інших нормативних документів, які регламентують організацію освітнього процесу при вивченні дисципліни.

Вимоги стосуються заохочень і нарахування додаткових балів за активну участь у дискусіях щодо аналізу і обговорення тематичного матеріалу на лекціях і лабораторних заняттях, ґрунтовної підготовки до занять, відсутності пропусків без поважних причин, виявлення поглиблених знань під час захисту звітів з лабораторного практикуму і модульного контролю.

5. Перелік питань до підсумкового модуль-контролю (заліку)

1. Дайте порівняльну характеристику традиційної та електронної комерції.
2. Проаналізуйте основні завдання захисту інформації в області електронної та мобільної комерції.
3. Проаналізуйте стандартні механізми класичних грошей та основних платіжних засобів.
4. Проаналізуйте основні типи дематеріалізованих грошей. Дайте коротку характеристику кожного типу та електронним гаманцям.
5. Охарактеризуйте транзакційні властивості дематеріалізованих грошей.
6. Дайте порівняльну характеристику сучасних електронних засобів платежу.
7. Проаналізуйте можливості технології захисту банківської інформації EDI та її компонентів.
8. Дайте порівняльну характеристику компонентів технології EDI.
9. Проаналізуйте структурування документів, форм та даних у системі EDI.
10. Проаналізуйте принципи забезпечення безпеки системи електронного обміну даними EDI.
11. Охарактеризуйте стандарт міжбанківської комунікації SWIFT.
12. Охарактеризуйте систему EDIFACT.
13. Протокол SSL та його основні переваги та недоліки.
14. Архітектура SET. Сервіси безпеки SET.
15. Класифікація та області використання мікропроцесорних карток.
16. Стандартизація карток. Атаки на смарт-картки. Безпека смарт-карток.
17. Поняття про криптовалюти.
18. Безпека криптовалют на прикладі BitCoin.
19. Процес майнінгу: отримання нових одиниць криптовалюти.
20. Структурування документів, форм та даних. Безпека систем електронного обміну даними.

6. Рекомендована література

6.1. Базова (основна)

1. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.:BHV, 2009. – 608 с.
2. 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.
3. Міщенко В.І., Слав'янська Н.Г., Коренєва О.Г. Банківські операції : підручник. 2-гевид., перероб. ідоп. К. : Знання, 2007. 796 с.
4. 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.
5. Страхарчук А.Я., Страхарчук В.П. Інформаційні системи і технології в банках : навч. посіб. К. : Знання, 2010. 515 с.

6.2. 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.

7. 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=3840
4. https://colab.research.google.com
5. www.scipy-lectures.org