СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «КОМП'ЮТЕРНИЙ ЗАХИСТ ФІНАНСОВОЇ ІНФОРМАЦІЇ»

Компонента освітньої програми – ***вибіркова*** (*3 кредити*)

Освітньо-професійна програма	Комп'ютерна інженерія
Спеціальність	F7 Комп'ютерна інженерія
Галузь знань	F Інформаційні технології
Рівень вищої освіти	другий (магістерський)
Мова навчання	українська
Профайл викладача	Іванущак Наталія Михайлівна, асистент, кандидат технічних наук 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	*Очні консультації*: за попередньою домовленістю. *Онлайн-консультації*: згідно погодженого графіку

АНОТАЦІЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Дисципліна «Комп'ютерний захист фінансової інформації» спрямована на формування у здобувачів вищої освіти системи знань і практичних навичок щодо забезпечення конфіденційності, цілісності та доступності фінансової інформації під час її зберігання, оброблення й передавання в інформаційно-комунікаційних системах. У межах дисципліни розглядаються принципи функціонування електронної комерції та платіжних систем, технології електронного обміну даними EDI у системах B2B, особливості електронних платіжних систем на основі цифрових грошей, засоби ідентифікації та автентифікації користувачів із застосуванням платіжних карт і електронних ключів. Особлива увага приділяється технологіям захищеного передавання фінансових даних із використанням протоколу TLS, методам захисту електронних платежів, виявленню та попередженню шахрайських операцій, а також комплексному забезпеченню безпеки фінансових транзакцій. Вивчення дисципліни сприяє набуттю компетентностей щодо аналізу загроз фінансовим інформаційним системам, вибору й застосування засобів криптографічного захисту, автентифікації та контролю безпеки електронних платежів.

Метою навчальної дисципліни є формування у здобувачів вищої освіти

теоретичних знань і практичних умінь щодо застосування сучасних методів, технологій та засобів комп'ютерного захисту фінансової інформації в системах електронної комерції, електронного документообігу та платіжної інфраструктури, а також набуття здатності забезпечувати безпеку фінансових транзакцій, протидіяти шахрайству й мінімізувати ризики несанкціонованого доступу до фінансових даних.

Завдання вивчення навчальної дисципліни

Основними завданнями вивчення дисципліни є:

1. **Вивчення принципів функціонування електронної комерції та основних моделей взаємодії її учасників**, зокрема особливостей організації електронних платіжних систем.
2. **Ознайомлення з технологією EDI** та принципами захищеного електронного обміну фінансовими й комерційними даними в системах B2B.
3. **Дослідження особливостей електронних платіжних систем на основі цифрових грошей**, їхньої архітектури, механізмів проведення платежів і засобів забезпечення безпеки фінансових операцій.
4. **Вивчення засобів ідентифікації та автентифікації користувачів платіжних систем**, принципів застосування платіжних карт, електронних ключів та інших засобів підтвердження правомірності доступу.
5. **Засвоєння принципів захищеного передавання фінансової інформації з використанням протоколу TLS**, механізмів криптографічного захисту, цифрових сертифікатів і встановлення захищених з'єднань.
6. **Вивчення методів захисту електронних платежів від несанкціонованого доступу**, перехоплення даних, підміни платіжних реквізитів та інших видів кіберзагроз.
7. **Ознайомлення з методами виявлення та протидії фінансовому шахрайству**, зокрема несанкціонованим транзакціям, викраденню платіжних даних і зловживанню обліковими даними користувачів.
8. **Формування вмінь аналізувати безпеку фінансових транзакцій на різних етапах їх здійснення**: від ідентифікації платника й ініціювання платежу до підтвердження, оброблення та завершення операції.
9. **Набуття практичних навичок вибору й застосування засобів комплексного захисту фінансової інформації**, оцінювання ризиків і розроблення рекомендацій щодо підвищення рівня безпеки електронних платіжних систем.
10. **Формування розуміння принципів комплексного забезпечення безпеки фінансових операцій з урахуванням вимог до конфіденційності**, цілісності, доступності, автентичності та невідмовності фінансових транзакцій.

НАВЧАЛЬНИЙ КОНТЕНТ ОСВІТНЬОЇ КОМПОНЕНТИ

МОДУЛЬ 1. ЗАХИЩЕНА ПЕРЕДАЧА ФІНАНСОВОЇ ІНФОРМАЦІЇ	
Тема 1	Електронна комерція. Види електронної комерції. Платіжні системи
Тема 2	Технологія Eectronic Data Intercange (EDI) в системах B2B
Тема 3	Електронні платіжні системи на основі цифрових грошей
МОДУЛЬ 2. БЕЗПЕКА ПЛАТІЖНИХ КАРТ	

Тема 4	Ідентифікаційні платіжні карти та електронні ключі
Тема 5	Захищена передача фінансової інформації за допомогою TLS
Тема 6	Захист електронних платежів та протидія шахрайству
Тема 7	Комплексний захист фінансової транзакції

ФОРМИ, МЕТОДИ ТА ОСВІТНІ ТЕХНОЛОГІЇ 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 пояснювально-ілюстративний, демонстраційний, практичний і проблемно-пошуковий методи навчання, аналіз практичних ситуацій, обговорення, дискусії та презентація результатів виконаних завдань.

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.

ФОРМИ Й МЕТОДИ КОНТРОЛЮ ТА ОЦІНЮВАННЯ

***Поточний контроль*:** *усне опитування* студента на лекційних заняттях (фронтальне, індивідуальне); *письмовий контроль* (звіти із виконання лабораторних робіт); *практичний контроль* (захист лабораторних робіт).

Рубіжний контроль: тестовий контроль у кінці змістових модулів №1 і №2.

Підсумковий контроль – залік.

КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Оцінювання програмних результатів навчання здобувачів освіти здійснюється за шкалою європейської кредитно-трансферної системи (ECTS). Критерієм успішного оцінювання є досягнення здобувачем вищої освіти мінімальних порогових рівнів (балів) за кожним запланованим результатом навчання.

ПОЛІТИКА ЩОДО 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.

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Система електронного навчання Чернівецького національного університету імені Юрія Федьковича (Moodle). URL: https://moodle.chnu.edu.ua/
2. Національний банк України. Офіційний вебсайт. URL: https://bank.gov.ua/.
3. National Institute of Standards and Technology. Computer Security Resource Center. URL: https://csrc.nist.gov/.
4. European Union Agency for Cybersecurity. Офіційний вебсайт. URL: https://www.enisa.europa.eu/.
5. United Nations Economic Commission for Europe. UN/CEFACT. URL: https://unece.org/trade/uncefact.
6. Open Worldwide Application Security Project. Офіційний вебсайт. URL: https://owasp.org/.
7. International Organization for Standardization. Офіційний вебсайт. URL: https://www.iso.org/

Покликання на робочу програму навчальної дисципліни

https://csn.chnu.edu.ua/spetsialnist-123-komp-yuterna-inzheneriya-opp-komp-yuterna-inzheneriya-magistratura-1-5-r/sylabusy-vybirkovyh-dystsyplin/