МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет ветеринарної медицини та біотехнологій імені С.З. Ґжицького
Факультет механіки, енергетики та інформаційних технологій
Кафедра Інформаційних технологій

ЗАТВЕРДЖЕНО
Гарант освітньо-професійної програми «Комп'ютерні науки» першого (бакалаврського) рівня вищої освіти
к.т.н., доцент В.В. Пташник

СИЛАБУС
НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ТЕХНОЛОГІЇ І СТАНДАРТИ ЗАХИСТУ ДАНИХ»

освітньо-професійна програма « Комп’ютерні науки »
спеціальність 122 « Комп’ютерні науки »

ВИКЛАДАЧ **СТАНЬКО ВОЛОДИМИР ЮРІЙОВИЧ**
E-mail: VStanko@lnup.edu.ua

Доцент кафедри інформаційних технологій Львівського національного університету ветеринарної медицини та біотехнологій ім. С.З. Гжицького, кандидат економічних наук. Викладач з понад 23-річним досвідом, автор та співавтор понад 40 наукових статей та понад 35 навчально-методичних розробок.

Читає курс: *Інформаційна безпека, Інформаційні та комунікаційні технології, Технології і стандарти захисту даних.*

Сфера наукових інтересів: *діджиталізація технічних процесів та впровадження інформаційних технологій у виробничо-організаційну діяльність підприємств і організацій.*

ЛЬВІВ 2025

Рівень вищої освіти – перший (бакалаврський)
Кількість кредитів – 4 (іспит)
Рік підготовки, семестр – 4 рік, 8 семестр
Компонент освітньої програми: вибірковий
Мова викладання: українська

Опис дисципліни

У сучасному інформаційному суспільстві дані стали стратегічним ресурсом, що визначає рівень розвитку держави, бізнесу та науки. Інформація перетворилася на товар, який генерує додану вартість, а її захист – на ключовий елемент національної безпеки. Незаконне втручання, викрадення або маніпуляція даними становлять серйозну загрозу для державних структур, приватних компаній і громадянського суспільства.

Міждисциплінарні зв'язки: вивчення дисципліни «Технології і стандарти захисту даних» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів: «Інформаційні технології», «Комп'ютерні мережі», «Операційні системи та системне програмування», «Інформаційна безпека».

Вимоги до знань та умінь визначаються галузевими стандартами вищої освіти України.

Предметом вивчення освітньої компоненти «Технології і стандарти захисту даних» є теоретичні, методичні та практичні аспекти передбачені освітньо-кваліфікаційною характеристикою, технологічними умовами, нормами законодавства та правилами суспільства.

Метою вивчення освітньої компоненти «Технології і стандарти захисту даних» є формування у студентів системного розуміння принципів, технологій і стандартів захисту даних, а також розвиток практичних навичок виявлення вразливостей інформаційних систем, побудови політик безпеки, застосування сучасних засобів шифрування, автентифікації та контролю доступу.

Основними завданнями освітньої компоненти «Технології і стандарти захисту даних» є набуття здобувачами вищої освіти теоретичних знань щодо оцінювання та забезпечення захисту інформації в інформаційних системах. Вивчення сучасних технологій захисту даних, включаючи апаратні та програмні засоби. Опанування міжнародних стандартів у сфері інформаційної безпеки (ISO/IEC 27001, NIST, GDPR, PCI DSS). Аналіз вразливостей інформаційних систем та методів їх усунення. Використання засобів шифрування та криптографічного захисту інформації. Застосування політик контролю доступу та автентифікації.

Ось структурований план занять для курсу «Технології і стандарти захисту даних» у форматі таблиці з темами, очікуваними результатами навчання та відповідними завданнями:

Години аудиторних занять (лек./ лаб.)	Тема заняття	Результати навчання	Завдання
2/2	Вступ до технологій і стандартів захисту даних	Розуміти роль захисту даних у сучасному цифровому середовищі	Ознайомлення з термінами, аналіз прикладів порушень безпеки
2/2	Законодавча та нормативна база	Знати основні міжнародні та національні стандарти (GDPR, ISO/IEC 27001)	Порівняльний аналіз вимог GDPR та українського законодавства
2/2	Класифікація загроз та вразливостей	Вміти класифікувати загрози та оцінювати ризики	Побудова моделі загроз для заданої ІС
2/2	Основи криптографії	Розуміти принципи симетричного та асиметричного шифрування	Практика: шифрування/ дешифрування тексту (AES, RSA)
2/2	Аутентифікація та контроль доступу	Вміти застосовувати механізми автентифікації та авторизації	Налаштувати ACL, RBAC, MFA у симульованій системі
2/2	Захист мережевих комунікацій	Знати принципи захисту даних у мережі	Конфігурація VPN, аналіз HTTPS-трафіку
2/2	Захист даних у хмарних середовищах	Розуміти особливості безпеки в хмарі	Аналіз політик безпеки CSP, Zero Trust
2/2	Стандарти безпеки: ISO, NIST, PCI DSS	Вміти застосовувати стандарти до реальних кейсів	Розробка політики безпеки згідно ISO/IEC 27001
2/2	Аналіз вразливостей та тестування	Вміти виявляти та усувати вразливості	Використання OWASP ZAP або аналогів для сканування
2/2	Політики безпеки та управління ризиками	Вміти формувати політики та оцінювати ризики	Розробка політики безпеки для навчальної ІС
2/2	Практичне моделювання систем захисту	Вміти інтегрувати знання для побудови комплексної системи	Командна розробка моделі захисту для кейс-сценарію
2/2	Підсумкове заняття	Презентація власних рішень, аргументувати вибір технологій	Захист проєкту, обговорення, рецензування робіт

Навчальний контент

Літературні джерела

1. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.1994 // Відомості Верховної Ради України, 1994, № 31. – Ст. 286, із змінами 2005 р.

2. Закон України “Про інформацію” // Відомості Верховної Ради, 1992, № 48. – Ст. 650 – 651.
3. Баранов, О. А. Інформаційна безпека: навч. посіб. / О. А. Баранов. – Київ: КНТ, 2020. – 312 с.
4. Єфіменко В. В. Технології захисту інформації: навч. посіб. / В. В. Єфіменко. – Київ: НАУ, 2021. – 198 с.
5. Загребельний А. В. Захист інформації в комп’ютерних системах: навч. посіб. / А. В. Загребельний, І. В. Козлов. – Львів: ЛНУ ім. І. Франка, 2019. – 280 с.
6. Коженевський С.Р. Термінологічний довідник з питань захисту інформації / С.Р. Коженевський, Г.В. Кузнецов, В.О. Хорошко, Д.В. Чирков. – К.: ДУІКТ, 2007. – 382 с.
7. Нестеров А. В. Криптографія та захист інформації: навч. посіб. / А. В. Нестеров. – Харків: Фоліо, 2021. – 256 с.
8. Хомич В. С. Основи інформаційної безпеки: навч. посіб. / В. С. Хомич. – Житомир: ЖДУ ім. І. Франка, 2020. – 224 с.

Допоміжна

9. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.
10. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Проведення робіт.
11. Русин Б.П. Біометрична аутентифікація та криптографічний захист / Б.П. Русин, Я.Ю. Варецький. – Львів: «Коло», 2007. – 287 с.
12. Термінологічний довідник з питань технічного захисту інформації / Коженевський С.Р., Кузнецов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.
13. General Data Protection Regulation (GDPR). Regulation (EU) 2016/679 of the European Parliament and of the Council. – Brussels: European Union, 2016. – [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
14. PCI Security Standards Council. Payment Card Industry Data Security Standard: Requirements and Security Assessment Procedures. – Version 4.0. – Wakefield, MA: PCI SSC, 2022. – 139 p.
15. Ross Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020.
16. William Stallings. "Cryptography and Network Security: Principles and Practice." Pearson, 2016. (784 p.) – https://www.pearson.com/us/highereducation/program/Stallings-Cryptography-and-Network-Security-Principles-and-Practice-7th-Edition/PGM335896.html
17. Ross Anderson. "Security Engineering: A Guide to Building Dependable Distributed Systems." Wiley, 2020. (1024 p.) – https://www.wiley.com/enus/Security+Engineering%3A+A+Guide+to+Building+Dependable+Distributed+Systems%2C+3rd+Edition-p-9781119642787

18. Brian Krebs. "Krebs on Security" – Online blog focusing on cybersecurity. – https://krebsonsecurity.com/

Інформаційні ресурси

19. Coursera: Cybersecurity Specialization – Various courses from leading universities. – https://www.coursera.org/specializations/intro-cyber-security
20. http://dstszi.gov.ua.
21. ISO/IEC 27001:2013 – Information Security Management Systems – Requirements. https://www.iso.org/standard/54534.html
22. ISO/IEC 27001:2022. Information technology – Security techniques – Information security management systems – Requirements. – Geneva: International Organization for Standardization, 2022. – 33 p.
23. National Cyber Security Centre (NCSC) – Various publications and recommendations. – https://www.ncsc.gov.uk/
24. NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. – Gaithersburg, MD: National Institute of Standards and Technology, 2020. – 487 p. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
25. OWASP Foundation. OWASP Top Ten Web Application Security Risks – 2023. – [Електронний ресурс]. – Режим доступу: https://owasp.org/www-project-top-ten/
26. Virtual Hacking Labs – Practical labs for ethical hacking and penetration testing. – https://www.virtualhackinglabs.com/
27. www.rootshell.com.
28. www.securityfocus.com.
29. www.sysinternals.com.

КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Успішність студента оцінюється шляхом проведення поточного контролю та захистом виконаних проектів.

Максимальна кількість балів з дисципліни «Технології і стандарти захист даних», яку може отримати студент протягом семестру за всі види роботи, становить 100, при цьому 50 балів за результатами поточного оцінювання, та 50 – за результатами захисту виконаних робіт.

Результати поточного контролю оцінюються за чотирибальною («2», «3», «4», «5») шкалою. В кінці семестру обчислюється середнє арифметичне значення (САЗ) усіх отриманих студентом оцінок з наступним переведенням його у 50-ти бальну шкалу за формулою:

$$\mathbf{ПК = 10 \cdot САЗ}$$

Критерії поточного оцінювання знань студентів

Оцінка	Критерії оцінювання
5 («відмінно»)	У повному обсязі володіє навчальним матеріалом, вільно, самостійно та аргументовано його викладає, глибоко і всебічно розкриває зміст, використовуючи обов'язкову та додаткову літературу. Правильно вирішив 90% тестових завдань.
4 («добре»)	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає, в основному розкриває зміст завдань, використовуючи обов'язкову літературу. При викладанні окремих питань не вистачає достатньої глибини та аргументації, допускаються несуттєві неточності й незначні помилки. Правильно вирішив більшість тестових завдань.
3 («задовільно»)	У цілому володіє навчальним матеріалом, викладає його основний зміст, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи окремі суттєві неточності та помилки. Правильно вирішив близько половини тестових завдань.
2 («незадовільно»)	Не в повному обсязі володіє навчальним матеріалом. Викладає матеріал фрагментарно та поверхово, без аргументації й обґрунтування, недостатньо розкриває зміст теоретичних і практичних завдань, допускає суттєві неточності. Правильно вирішив меншість тестових завдань.

Переведення підсумкових рейтингових оцінок з дисципліни, виражених у балах за 100-бальною шкалою, у оцінки за національною шкалою та шкалою ECTS

Таблиця 1 – **Шкала оцінювання: національна та ECTS**

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, диференційованого заліку, курсового проєкту (роботи), практики	для заліку
90–100	**A**	відмінно	зараховано
82–89	**B**	добре	
74–81	**C**		
64–73	**D**	задовільно	
60–63	**E**		
35–59	**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

До Силабусу також готуються матеріали навчально-методичного комплексу:

1) Навчальний контент (розширений план лекцій)
2) Тематика та зміст лабораторних робіт
3) Питання на іспит
4) Електронне навчання у системі MOODLE.