

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Львівський національний університет природокористування
Факультет механіки, енергетики та інформаційних технологій
Кафедра Інформаційних технологій



ЗАТВЕРДЖЕНО

Гарант освітньо-професійної програми «Автоматизація та комп'ютерно-інтегровані технології» першого (бакалаврського) рівня вищої освіти:

к.т.н., доцент  О.В. Лиса

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ІНФОРМАЦІЙНА БЕЗПЕКА»

освітньо-професійна програма «Автоматизація та комп'ютерно-інтегровані технології»

спеціальність 151 «Автоматизація та комп'ютерно-інтегровані технології»
перший (бакалаврський) рівень вищої освіти

ВИКЛАДАЧ



СТАНЬКО ВОЛОДИМИР ЮРІЙОВИЧ

E-mail: VStanko@ukr.net

Телефон +380679724391

Доцент кафедри інформаційних технологій Львівського національного університету природокористування, кандидат економічних наук. Викладач з понад 20-річним досвідом, автор та співавтор понад 38 наукових статей та понад 33 навчально-методичних розробок.

Читає курс: *Інформаційна безпека, Інформаційні технології.*

Сфера наукових інтересів: *використання інформаційних технологій в організації навчального процесу.*

ЛЬВІВ 2021

Галузь знань: 15 «Автоматизація та приладобудування»

Спеціальність: 151 «Автоматизація та комп'ютерно-інтегровані технології»

Освітньо-професійна програма «Автоматизація та комп'ютерно-інтегровані технології»

Рівень вищої освіти – перший (бакалаврський)

Кількість кредитів – 4 (іспит)

Рік підготовки, семестр – 4 рік, 7 семестр

Компонент освітньої програми: вибірковий

Мова викладання: українська

Опис дисципліни

Інформаційна складова життя суспільства, активно впливає на стан політичної, економічної, оборонної й інших складових національної безпеки України.

Сьогодні, як ніколи, відбувається безперервна боротьба за контроль над інформаційними потоками. Виграє той, хто не лише вміє їх формувати та регулювати у своїх власних інтересах, але й здатний забезпечити цілісність свого інформаційного ресурсу.

Основою сучасного суспільства є інформаційні технології та інформація, яка в таких умовах стає товаром й основним продуктом виробництва та створення додаткової вартості.

Зворотнім боком цієї “медалі” є тотальні незаконні зазіхання на чужу інформацію, що, в свою чергу, вимагає її захисту. Особливу небезпеку складають спроби викрадення інформації, що є власністю держави та містить державну або іншу таємницю.

Міждисциплінарні зв'язки: вивчення дисципліни «Інформаційна безпека» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів: «Вища математика», «Фізика», «Інформаційні технології».

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

Предметом вивчення освітньої компоненти «Інформаційна безпека» є теоретичні, методичні та практичні аспекти передбачені освітньо-кваліфікаційною характеристикою, технологічними умовами, нормами законодавства та правилами суспільства.

Метою вивчення освітньої компоненти «Інформаційна безпека» це – захистити інтереси суб'єктів інформаційних відносин. Інтереси ці різноманітні, але всі вони концентруються навколо трьох основних аспектів:

- доступність;
- цілісність;
- конфіденційність.

Основними завданнями освітньої компоненти «Інформаційна безпека» є набуття здобувачами вищої освіти теоретичних знань щодо оцінювання та забезпечення захисту інформації в інформаційних системах, принципів безпечного проектування ІС а ІТ методології безпечного програмування, погроз

і атак, безпеки комп'ютерних мереж, володіння навчально-методичними основами і стандартами в області ІТ, уміння їх застосовувати при розробці функціональних профілів ІТ, при побудові та інтеграції систем, продуктів і сервісів ІТ.

Години аудиторних занять (лек./ лаб.)	Тема	Результати навчання	Завдання
2/4	Тема 1. Концептуальні засади забезпечення інформаційної безпеки України.	Знати: Нормативно-правові основи захисту інформації в Україні. Концепцію національної інформаційної безпеки України. Основні поняття, терміни та визначення технічного захисту інформації.	Питання, індивідуальні заняття
2/4	Тема 2. Технічні канали витоку інформації. Способи несанкціонованого зняття інформації	Поняття технічного захисту інформації у системі інформаційної безпеки. Сутність та завдання технічного захисту інформації.	
2/4	Тема 3. Методи та засоби блокування технічних каналів витоку інформації	Види та класифікація технічних каналів витоку інформації. Основні поняття щодо захисту інформації в автоматизованих системах.	
2/4	Тема 4. Основи безпеки даних комп'ютерних системах	Вміти: Працювати з нормативно-правовими актами. Застосовувати заходи щодо попередження несанкціонованого доступу до інформації. Використовувати методи пасивного та активного захисту інформації. Визначати загрози безпеки даних та їх особливості. Розрізняти і класифікувати канали проникнення та принципи побудови систем захисту.	
2/4	Тема 5. Ідентифікація і аутентифікація користувачів	Знати: Поняття про ідентифікацію користувача та її особливості. Основні принципи та методи аутентифікації.	
2/4	Тема 6. Основи криптографії та захисту даних	Основні принципи захисту даних від несанкціонованого доступу.	

2/4	Тема 7. Стандарти із захисту інформації	<p>Моделі управління доступом. Криптографічні методи захисту інформації. Світові стандарти із захисту даних в комп'ютерних системах. Державний стандарт України із захисту інформації</p> <p>Вміти:</p> <p>Проводити ідентифікацію та аутентифікацію користувачів. Захищати дані від несанкціонованого доступу. Використовувати технічні засоби захисту даних від їх витоку. Застосовувати засоби захисту даних від комп'ютерних вірусів та шкідливих програм. Супроводжувати та підтримувати криптосистеми та алгоритми шифрування інформації. Здійснювати адміністрування ключами та цифровими підписами.</p>	
-----	---	---	--

Навчальний контент

Формування програмних компетентностей

Індекс в матриці ОПП	Програмні компоненти
ЗК01	Здатність застосовувати знання у практичних ситуаціях
ЗК04	Навички використання інформаційних і комунікаційних технологій
ЗК05	Здатність до пошуку, опрацювання та аналізу інформації з різних джерел
ЗК06	Навички здійснення безпечної діяльності
ПРН03	Вміти застосовувати сучасні інформаційні технології та мати навички розробляти алгоритми та комп'ютерні програми з використанням мов високого рівня та технологій об'єктно-орієнтованого програмування, створювати бази даних та використовувати інтернет-ресурси
ПРН14	Вміти використовувати у виробничій і соціальній діяльності фундаментальні поняття і категорії державотворення для обґрунтування власних світоглядних позицій та політичних переконань з урахуванням процесів соціально-політичної історії України, правових засад та етичних норм

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. 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.
4. Постанова Кабінету міністрів України “Про затвердження Концепції технічного захисту інформації в Україні” № 1126 від 08.11.1997 р.

Допоміжна

5. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.
6. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Проведення робіт.
7. Русин Б.П. Біометрична аутентифікація та криптографічний захист / Б.П. Русин, Я.Ю. Варецький. – Львів: «Коло», 2007. – 287 с.
8. 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. Інформаційні ресурси

9. <http://dstszi.gov.ua>.
10. 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>
2. 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>
11. ISO/IEC 27001:2013. "Information technology — Security techniques — Information security management systems — Requirements." - <https://www.iso.org/standard/54534.html>
12. NIST Special Publication 800-53. "Security and Privacy Controls for Federal Information Systems and Organizations." - <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>
13. "National Cyber Security Centre (NCSC)" - Various publications and recommendations. - <https://www.ncsc.gov.uk/>
14. Brian Krebs. "Krebs on Security" - Online blog focusing on cybersecurity. - <https://krebsonsecurity.com/>
15. Virtual Hacking Labs - Practical labs for ethical hacking and penetration testing. - <https://www.virtualhackinglabs.com/>

16.Coursera: "Cybersecurity Specialization" - Various courses from leading universities. - <https://www.coursera.org/specializations/intro-cyber-security>

17.www.rootshell.com.

18.www.securityfocus.com.

19.www.sysinternals.com.

Політика оцінювання

Політика щодо дедлайнів та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (75% від можливої максимальної кількості балів за вид діяльності балів). Перескладання модулів відбувається за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Списування під час контрольних робіт заборонені (в т.ч. із використанням мобільних девайсів). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки практичних завдань під час заняття.

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання. За об'єктивних причин (наприклад, хвороба, працевлаштування, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із ведучим викладачем курсу.

Оцінювання

Остаточна оцінка за курс розраховується наступним чином: поточний контроль оцінюється в 50 балів, та складається із сімох тем. Теми від першої до шостої оцінюються по 7 балів, сьома тема оцінюється 8 балів, підсумковий контроль 50 балів ($6 \times 7 + 1 \times 8 + 50 = 100$).

Поточне тестування та самостійна робота (разом 50 балів)							Підсумковий контроль	Сума
T1	T2	T3	T4	T5	T6	T7	іспит	
7	7	7	7	7	7	8	50	100

T1, T2 ... T7 – теми

До Силабусу також готуються матеріали навчально-методичного комплексу:

- 1) Навчальний контент (розширений план лекцій);
- 2) Тематика та зміст практичних робіт;
- 3) Завдання для підсумкової роботи, питання на іспит;
- 4) Електронне навчання у віртуальному навчальному середовищі ЛНУП