

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ**

**ІНСТИТУТ З ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ ПІДРОЗДІЛІВ
НАЦІОНАЛЬНОЇ ПОЛІЦІЇ**

Факультет №2

Кафедра інформаційного та аналітичного забезпечення
діяльності правоохоронних органів

СИЛАБУС

ОК 24 ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

освітньо-професійна
програма
рівень вищої освіти
галузь знань
шифр і назва спеціальності
вид дисципліни
мова викладання

«Правоохоронні інформаційні системи»

перший (бакалаврський)
12 «Інформаційні технології»
126 «Інформаційні системи та технології»
обов'язкова
українська

Інформація про викладача

к. тех. н., доцент

Головатий Андрій Ігорович

andrii.i.holovatyi@lpnu.ua

Рильніков Михайло Олександрович

itv@lvduvs.edu.ua

Львів 2024

Розробник (викладач)

доцент кафедри інформаційного та
аналітичного забезпечення діяльності
правоохоронних органів к. тех. н., доц.

_____ Андрій ГОЛОВАТИЙ

Розглянуто та затверджено на засіданні кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів факультету №2 ШФПНП (протокол № 24 від 15.08.2024)

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ: силабус з навчальної дисципліни / Головатий А.І. Львів: Львівський державний університет внутрішніх справ, 2024. 10 с.

ХАРАКТЕРИСТИКА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Семестр навчання	7, 8-й
Обсяг	7 кредитів ЕКТС (210 год.)
Анотація	Предметом вивчення навчальної дисципліни є прикладні аспекти забезпечення кібернетичної безпеки інформаційно-комунікаційних систем (ІКС). Завданнями вивчення дисципліни є: <ul style="list-style-type: none"> – ознайомлення із різними видами атак на ІКС і способами захисту від них; – формування навичок аналізу можливих кіберзагроз, вразливостей, впровадження та експлуатація сервісів і засобів безпеки ІКС.
Мета вивчення дисципліни	Формування знань і вмінь забезпечувати кібернетичну безпеку в ІКС

ПРОГРАМНІ КОМПЕТЕНТНОСТІ ТА РЕЗУЛЬТАТИ НАВЧАННЯ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми в області інформаційних систем та технологій, або в процесі навчання, що характеризуються комплексністю та невизначеністю умов, які потребують застосування теорій та методів інформаційних технологій.
Загальні компетентності	КЗ 2. Здатність застосовувати знання у практичних ситуаціях. КЗ 3. Здатність до розуміння предметної області та професійної діяльності. КЗ 5. Здатність вчитися і оволодівати сучасними знаннями. КЗ 6. Здатність до пошуку, оброблення та узагальнення інформації з різних джерел. КЗ 8. Здатність оцінювати та забезпечувати якість виконуваних робіт
Спеціальні (фахові, предметні) компетентності	КС 2. Здатність застосовувати стандарти в області інформаційних систем та технологій при розробці функціональних профілів, побудові та інтеграції систем, продуктів, сервісів і елементів інфраструктури організації. КС 6. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків. КС 16. Здатність використовувати інструментальні засоби оцінки наявних вразливостей та враховувати їх під час проектування створення та налаштування спеціалізованих (правоохоронних) інформаційних систем і комунікаційного обладнання.

	КС 17. Здатність застосовувати існуючі інформаційно-телекомунікаційні системи спеціального призначення для вирішення завдань правоохоронної діяльності, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем, оцінювати їх ефективність
№ Програмних результатів за ОПШ	Програмні результати навчання з навчальної дисципліни
ПР 3.	Використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня із застосуванням об'єктно-орієнтованого програмування для розв'язання задач проектування і використання інформаційних систем та технологій.
ПР 12.	Здійснювати оцінку стану захищеності інформаційно-телекомунікаційної системи та використовувати можливості апаратного забезпечення, операційних систем, мережевого програмного забезпечення для усунення потенційних вразливостей.

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви тем	Кількість годин									
	денна форма					заочна форма				
	Усього	у тому числі				Усього	у тому числі			
		лек.	лаб.	сем.	сам. роб		лек.	лаб.	сем.	сам. роб
7 семестр										
Тема №1. Основні відомості про кібербезпеку	18	6	4		10	24	2	2		20
Тема №2. Криптографічний захист інформації	88	24	26		20	66	2	4		60
Разом годин за 7 семестр	90	30	30		30	90	4	6		80
Підсумковий контроль	залік									
8 семестр										
Тема №3. Тестування на вразливість до атак	74	18	24		40	66	2	4		60
Тема №4. Сервіси та механізми захисту ІКС	30	12	6		20	54	2	2		50
Разом годин за 8 семестр	120	30	30		60	120	4	6		110
Усього годин	210	60	60		90	210	8	12		190
Підсумковий контроль	екзамен									

ОРГАНІЗАЦІЯ НАВЧАННЯ І КОНТРОЛЮ

<p>Проведення занять та консультацій</p>	<p>Усі здобувачі вищої освіти незалежно від форми навчання зобов'язані відвідувати аудиторні заняття і проходити всі форми поточного та підсумкового контролю, передбачені індивідуальним навчальним планом здобувача та освітньо-професійною програмою ЛьвДУВС.</p> <p>Аудиторні заняття проводяться за розкладом відповідної групи у вказаних аудиторіях. Пропуски занять відпрацьовуються.</p> <p>Консультавання проводиться за розкладом консультацій викладача, розміщеним на інформаційному стенді (сайті) кафедри за адресою: м. Львів, вул. Замартинівська 9, (або через e-mail викладача).</p>
<p>Відпрацювання пропущених занять</p>	<p>Відповідно до Положення про організацію освітнього процесу у ЛьвДУВС порядок відпрацювання пропущених навчальних занять та незадовільних оцінок визначається (деканатом факультету) / кафедрою та доводиться до відома здобувачів вищої освіти.</p> <p>Відпрацювання відбуваються відповідно до графіку затвердженого на кафедрі, або у формі відеоконференцій із застосуванням засобів дистанційного навчання ZOOM.</p>
<p>Допуск до підсумкового контролю</p>	<p>Підсумковий контроль проводиться після проведення всіх видів занять, передбачених робочою навчальною програмою відповідної навчальної дисципліни. Оцінювання здійснюється за результатами накопичених балів із аудиторної та самостійної робіт (розділ 4 Положення Про організацію освітнього процесу у ЛьвДУВС https://www.lvduvs.edu.ua/uk/karta-dokumentiv/category/157-oop.html?download=6615:polozhennia-pro-orhanizatsiiu-osvitnoho-protsesu-u-lvivskomu-derzhavnomu-universyteti-vnutrishnikh-spravm)</p>
<p>Система оцінювання</p>	<p>Оцінювання рівня досягнення програмних результатів навчання проводиться шляхом поточного та підсумкового оцінювання.</p> <p>Поточне оцінювання застосовується для вивчення рівня досягнення програмних результатів навчання на</p>

практичних та лабораторних заняттях, за розв'язування прикладних задач з їх обговоренням, розв'язування індивідуальних контрольних завдань.

Оцінювання знань та умінь на лабораторних заняттях здійснюється за чотирибальною шкалою за такими критеріями:

Оцінка «**відмінно**» виставляється, якщо здобувач активно працює протягом усього практичного заняття, дає повні відповіді на запитання викладача у відповідності з планом практичного чи лабораторного заняття і показує при цьому глибоке оволодіння лекційним матеріалом, знання відповідної літератури, здатний аналізувати явища й факти, робити самостійні узагальнення й висновки, знає передбачені програмою основні методи розв'язання завдання і вміє їх застосовувати з необхідним обґрунтуванням, допускаючи не більше однієї арифметичної помилки або описки.

Оцінка «**добре**» виставляється за умови дотримання таких вимог: здобувач активно працює протягом практичного чи лабораторного заняття, питання висвітлені повно, викладення матеріалу логічне, обґрунтоване фактами, здобувач вміє виконувати навчальні завдання, частково аргументує математичні міркування. Але у відповідях допущені неточності, деякі незначні помилки або допущені 1-2 арифметичні і 1-2 логічні помилки при розв'язанні задач.

Оцінка «**задовільно**» виставляється в тому разі, коли здобувач у цілому оволодів суттю питань з даної теми, виявляє знання лекційного матеріалу, розв'язує завдання обов'язкового рівня за відомими алгоритмами з частковим поясненням. Але на занятті поводить себе пасивно, відповідає лише за викликом викладача, дає неповні відповіді на запитання, припускається грубих помилок при висвітленні теоретичного матеріалу або 3-4 логічних помилок при розв'язанні задач.

Оцінка «**незадовільно**» виставляється в разі, коли здобувач виявив неспроможність висвітлити питання чи питання висвітлені неправильно, виявлене невміння розв'язувати навчальні задачі.

Оцінювання рівня засвоєння матеріалу за результатами проведення тестового завдання здійснюється за чотирибальною шкалою за такими критеріями:

Оцінка «**Відмінно**» – виставляється, якщо здобувач

вищої освіти дав правильну відповідь на 90–100% завдань.

Оцінка «Добре»– виставляється, якщо здобувач вищої освіти дав правильну відповідь на 71–89% завдань.

Оцінка «Задовільно» – виставляється, якщо здобувач вищої освіти дав правильну відповідь на 50–70% завдань.

Оцінка «Незадовільно» – виставляється, якщо здобувач вищої освіти дав правильну відповідь на 0–49% завдань.

Оцінювання знань та умінь за підсумками написання контрольних робіт за індивідуальними завданнями, здійснюється за чотирибальною шкалою за такими критеріями:

Відповідь здобувача оцінюється «Відмінно», якщо дано розгорнуті, вичерпні відповіді на контрольні питання; здобувач вміє користуватися методами наукового аналізу явищ, процесів і характеризувати їх риси та форми виявлення, повністю і правильно виконав завдання, володіє здатністю здійснювати порівняльний аналіз та самостійно робити логічні висновки й узагальнення.

Із загального обсягу здобувач правильно виконує 90-100 % завдань.

Відповідь здобувача оцінюється «Добре», якщо не дано відповідь на 1-2 контрольних питання, або відповіді недостатньо вичерпні; здобувач вміє користуватися методами наукового аналізу економічних та соціальних явищ, процесів, хід виконання завдання є правильним, але допущені незначні помилки, володіє здатністю самостійно робити логічні висновки.

Із загального обсягу здобувач правильно виконує 71-90 % завдань.

Відповідь здобувача оцінюється «Задовільно», якщо не до кінця виконано завдання, відповідь мало обґрунтована, неповна.

Із загального обсягу здобувач правильно виконав 51-70 % завдань.

Відповідь здобувача оцінюється «Незадовільно», якщо не дано відповідь на понад 55% контрольних питання, або відповіді недостатньо вичерпні; завдання не виконане, допущені грубі помилки і здобувач не може їх виправити, відповідь не обґрунтована.

	<p>Із загального обсягу здобувач правильно виконав менше 50 % завдань</p> <p>Самостійна робота оцінюється окремо. Загальна кількість балів (максимум 20) за самостійну роботу визначається як сума отриманих балів за виконання таких видів робіт:</p> <ul style="list-style-type: none"> - підготовка реферату - до 4 балів; - підготовка презентацій (не менше 20 слайдів) – до 4 балів. <p>Виконання інших завдань, запропонованих здобувачем вищої освіти та узгоджених з науково-педагогічним працівником – до 5 балів.</p> <p>Види самостійної роботи обираються здобувачем вищої освіти на власний розсуд та можуть поєднуватися.</p> <p>Тематика завдань для самостійної роботи визначається у плані проведення практичних занять, а також може бути запропонована та погоджена здобувачем освіти чи науково-педагогічним працівником додатково.</p> <p>Підсумковий контроль у формі заліку проводиться після проведення всіх видів занять, передбачених робочою навчальною програмою відповідної навчальної дисципліни. Оцінювання здійснюється за результатами накопичених балів із аудиторної (максимум 80 балів) та самостійної робіт (максимум 20 балів).</p> <p>Підсумковий контроль у формі екзамену проводиться після проведення всіх видів навчальних занять, передбачених робочою навчальною програмою відповідної освітньої компоненти згідно з розкладом. Оцінювання здійснюється за результатами накопичення балів поточного контролю (аудиторної – до 40 балів та самостійної робіт – до 10 балів) та підсумкового контролю (екзамену – до 50 балів).</p> <p>Алгоритми розрахунку результатів навчання наведені у Положенні про організацію освітнього процесу у Львівському державному університеті внутрішніх справ (https://www.lvduvs.edu.ua/uk/karta-dokumentiv/category/157-oop.html?download=6615:polozhennia-pro-orhanizatsiiu-osvitnoho-protsesu-u-lvivskomu-derzhavnomu-universyteti-vnutrishnikh-spravm)</p>
Визнання результатів	Здобувачі вищої освіти, мають право звернутися в порядку, визначеному Положенням про порядок

<p>навчання, отриманих у неформальній освіті</p>	<p>визнання у Львівському державному університеті внутрішніх справ результатів навчання, отриманих у неформальній освіті, щодо визнання таких результатів. Критерії оцінки знань здобувачів вищої освіти, отриманих у неформальній освіті, визначаються згідно із Положенням про порядок визнання у Львівському державному університеті внутрішніх справ результатів навчання, отриманих у неформальній освіті, та Положенням про організацію освітнього процесу у Львівському державному університеті внутрішніх справ, виходячи з того, чи здобувач ініціює визнання результатів такого навчання з навчальної дисципліни загалом, окремого розділу, теми навчальної дисципліни.</p> <p>Здобувач вищої освіти може звернутися за консультацією щодо форм неформальної освіти, результати яких можуть бути визнані за цією навчальною дисципліною до науково-педагогічного працівника, який проводить аудиторні заняття в навчальній групі або до завідувача кафедри.</p>
<p>Шкала та критерії оцінювання за шкалою ECTS</p>	<p>Відображена у Таблиці 1 Положення про організацію освітнього процесу у Львівському державному університеті внутрішніх справ (https://www.lvduvs.edu.ua/uk/karta-dokumentiv/category/157-oop.html?download=6615:polozhennia-pro-orhanizatsiiu-osvitnoho-protsesu-u-lvivskomu-derzhavnomu-universyteti-vnutrishnikh-spravm)</p>

ЛІТЕРАТУРА ТА ІНФОРМАЦІЙНІ ДЖЕРЕЛА

Основна література

1. The NIST Cybersecurity Framework (CSF) 2.0. URL: <https://doi.org/10.6028/NIST.CSWP.29>
2. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗІ КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с.
3. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський. Київ : КПІ ім. Ігоря Сікорського, 2018.

4. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури : підручник / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. К.: КУБГ, 2019. 218 с.

Методичне забезпечення

1. Ron Ross (NIST), Mark Winstead (MITRE), Michael McEvelley (MITRE). NIST SP 800-160 Vol. 1 Rev. 1. Engineering Trustworthy Secure Systems. URL: <https://doi.org/10.6028/NIST.SP.800-160v1r1>
2. Allen L., Cardwell K. Advanced Penetration Testing for Highly-Secured Environments. Second edition. Packt Publishing, 2016.
3. NIST Special Publication 800-53 Revision 5. Security and Privacy Controls for Information Systems and Organizations. URL: <https://doi.org/10.6028/NIST.SP.800-53r5>.

ІНФОРМАЦІЙНІ РЕСУРСИ

1. NIST Computer Security Resource Center | CSRC. URL: <https://csrc.nist.gov/>
2. Cybersecurity Framework | NIST. URL: <https://www.nist.gov/cyberframework>
3. MITRE ATT&CK. URL: <https://attack.mitre.org/>
4. OWASP Top Ten | OWASP Foundation. URL: <https://owasp.org/www-project-top-ten/>
5. Hack The Box. URL: <https://app.hackthebox.com/>
6. The fast, easy, and affordable way to train your hacking skills. URL: <https://www.root-me.org/>
7. TryHackMe. URL: <https://tryhackme.com/hackactivities?tab=practice>