

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет інформаційних технологій і математики
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС
Вибіркового освітнього компонента
ОРГАНІЗАЦІЯ ТА ОБРОБКА ЕЛЕКТРОННОЇ ІНФОРМАЦІЇ
Підготовки першого (бакалаврського) рівня вищої освіти

Луцьк – 2026

Силабус вибіркового освітнього компонента “Організація та обробка електронної інформації”. Підготовки першого (бакалаврського) рівня вищої освіти

Розробник:

Жигаревич О.К., старший викладач кафедри комп’ютерних наук та кібербезпеки

Погоджено

Гарант освітньо-професійної програми:

Н.Л.



Чернящук

Силабус освітнього компонента затверджено на засіданні кафедри комп’ютерних наук та кібербезпеки

протокол № 6 від 15.01.2026 р.

Завідувач кафедри:



Гришанович Т. О.

I Опис освітнього компонента

Найменування показників	Характеристика освітнього компонента
	Вибірковий
Денна форма навчання	Рік підготовки 2
150/5 кредитів	Семестр 3
	Лекції 10 год.
	Лабораторні 20 год.
	Самостійна робота 110 год.
ІНДЗ: є	Консультації 10 год.
	Форма контролю: залік

II. Інформація про викладача

ППП : Жигаревич Оксана Костянтинівна
Науковий Вчене звання -
Посада старший викладач
Контактна інформація zhyharevych.oksana@vnu.edu.ua
Дні занять [http:згідно розкладу](http://zгідно розкладу)

III. Опис освітнього компонента

1. Анотація курсу.

“Організація та обробка електронної інформації” забезпечує професійний розвиток бакалавра та спрямована на формування у майбутніх фахівців базових знань, вмінь та навичок вивчення методів технологій безпечного захисту інформації в системах інформаційної та кібербезпеки; виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування та вразливостей; обирати методи зберігання та ефективні алгоритми обробки для відповідних структур даних для створення захищених програм.

Обсяг матеріалу становить необхідний мінімум при підготовці слухачів першого (бакалаврського) рівня вищої освіти.

2. Мета навчальної дисципліни: надання теоретичних знань та формування практичних навичок щодо дослідження безпечного програмування з метою розв’язування прикладних задач та створення програмного забезпечення систем інформаційної безпеки.

Завдання:

- знання основних процесів, фаз та ітерацій життєвого циклу програмного забезпечення;
- знання фундаментальних концепцій, парадигм і основних принципів функціонування мовних, інструментальних і обчислювальних засобів інженерії програмного забезпечення, прийомів застосування інформаційних технологій обробки, зберігання та передачі даних;
- знання методів та засобів створення мобільних додатків, крос- та мультиплатформного програмування, зокрема, для кібер-фізичних та енергетичних систем;
- знання основних принципів застосування мови Kotlin;
- вміння організувати, налаштувати та програмувати у комп’ютерних мережах;
- вміння аналізувати, вибирати, застосовувати засоби забезпечення інформаційної безпеки, зокрема в енергетиці.
- вміння застосовувати засоби мови програмування, опису інформаційних ресурсів, специфікацій під час проектування та створення

інформаційних систем;

- вміння програмно реалізувати алгоритми розв'язування задач;
- вміння проектувати компоненти програмного забезпечення;
- вміння виконувати аналіз коректності програм.

3. Soft skills

- Інформаційна грамотність — уміння критично оцінювати електронні дані, визначати їх достовірність, актуальність і релевантність для поставлених завдань.
- Організованість і тайм-менеджмент — здатність ефективно структурувати електронну інформацію, керувати файлами та даними, дотримуватися термінів виконання завдань.
- Аналітичне мислення — уміння аналізувати великі обсяги електронної інформації, виявляти закономірності, узагальнювати та формувати обґрунтовані висновки.
- Увага до деталей — здатність працювати з даними без помилок, коректно обробляти, формувати та перевіряти електронну інформацію.
- Комунікаційні навички — уміння чітко й зрозуміло представляти результати обробки електронної інформації в усній та письмовій формах, у тому числі в цифровому середовищі.

4. Структура освітнього компонента

Назви змістових модулів і тем	Кількість годин					Форма контролю / бали
	Усього	у тому числі				
		Лек.	Лаб.	Сам. роб.	Конс.	
Змістовий модуль 1. Обробка електронної інформації.						
Тема 1: Види, джерела, та носії інформації, що підлягають захисту.	13	2	2	8	1	Звіт по лаб. роботі /5
Тема 2. Небезпечні сигнали та їх джерела.	13	2	2	8	1	Звіт по лаб. роботі /5
Тема 3. Поняття та принципи технічної розвідки.	13	2	2	8	1	Звіт по лаб. роботі /5
Тема 4. Комплексне застосування методів захисту.	15	2	4	8	1	Звіт по лаб. роботі /10
Тема 5. Енергетичне приховування акустичного сигналу.	19		4	14	1	Звіт по лаб. роботі /10
Тема 6. Структурне приховування мовної інформації в каналах зв'язку.	15	2	4	8	1	Звіт по лаб. роботі /10
Тема 7. Класифікація засобів інженерного захисту об'єктів.	20		2	16	2	Звіт по лаб. роботі /5
Тест	11			10	1	Тестовий контроль знань / 16
Контрольна робота (розв'язування задач).	11			10	1	Контрольна робота (розв'язування задач)/18
ІНДЗ	20			20		Робота в групах/30
Всього годин/Балів	150	10	20	110	10	150 / 100 балів

Завдання для самостійного опрацювання

№ з/п	Тема	Кількість годин
1	Підготовка до лабораторних робіт	30

2	Підготовка до контрольних робіт	18
3	Опрацювання лекційного матеріалу	12
4	Виконання ІНДЗ	18
5	Зведення даних на Kotlin.	4
6	Завантаження файлів на Kotlin	4
7	Скасування виконання async-корутини.	4
8	Канали на мові програмування Kotlin.	4
9	Патерн producer-consumer.	4
10	Відмінність між Dispatchers.Default і Dispatchers.IO.	4
11	CoroutineScope застосування.	8
	Разом	110

IV. Політика оцінювання

Політика щодо академічної доброчесності. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно, а результати раніше зданих робіт анулюються і виконуються повторно у порядку визначеному викладачем. При цьому викладач залишає за собою право змінити завдання.

Комунікаційна політика. Здобувачі вищої освіти повинні мати активовану університетську пошту. Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту, можливе інше (додаткове) джерело комунікації, визначене викладачем для більш оперативного зв'язку зі студентами.

Політика щодо перескладання. Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний).

Політика щодо оскарження оцінювання. Політика щодо оскарження оцінки. Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку згідно «Положення про порядок і процедури вирішення конфліктних ситуацій у Волинському національному університеті імені Лесі Українки»

Політика щодо відвідування занять. Для здобувачів вищої освіти денної форми відвідування занять є обов'язковим. Поважними причинами для неявки на заняття є хвороба, академічна мобільність, які необхідно підтверджувати відповідними документами. Про відсутність на занятті та причини відсутності здобувач вищої освіти має повідомити викладача або особисто, або через старосту.

За об'єктивних причин навчання може проводитися у дистанційній формі за погодженням з керівником курсу та деканом факультету. Декан факультету видає розпорядження про дистанційне навчання на основі заяви здобувача. Під час дистанційного навчання лабораторні роботи виконуються відповідно до розкладу занять. На початку заняття викладач повідомляє варіант завдання, який здобувач повинен виконати. Звіт про виконання лабораторної роботи необхідно завантажити в Moodle до завершення заняття. Вимоги до звітів наведені в описах лабораторних робіт у системі Moodle. Після закінчення заняття можливість задачі буде припинено. Роботи, подані несвоєчасно, не підлягають оцінюванню.

Навчання може здійснюватися за індивідуальним графіком відповідно до Положення про організацію освітнього процесу здобувачів освіти за індивідуальним графіком навчання у Волинському національному університеті імені Лесі Українки. Для

цього здобувач подає заяву на ім'я декана, який, враховуючи успішність та підстави, погоджує або відхиляє подану заяву. У разі погодження здобувач освіти погоджує із викладачем план роботи, форми та терміни контролю. Індивідуальний графік затверджується на один семестр, а під час академічної мобільності – не більше ніж на рік.

Усі умови навчання в дистанційній формі та за індивідуальним графіком також подані у дистанційному курсі цього освітнього компоненту системи Moodle.

Бонуси. Після завершення вивчення курсу та перед початком екзаменаційної сесії здобувачам вищої освіти можуть бути нараховані додаткові бали за наукову діяльність. Такі бали надаються за участь у наукових конференціях, підготовку публікацій, здобути результати в олімпіадах чи конкурсах студентських наукових робіт та інші досягнення у предметній галузі освітнього компонента. Порядок і систему нарахування бонусних балів визначає та затверджує науково-методична комісія факультету.

Визнання результатів навчання, отриманих у формальній, неформальній освіті. Під час вивчення освітнього компонента можливе визнання результатів навчання отриманих у формальній, неформальній та/або інформальній освіті. Порядок визнання результатів навчання для здобувачів вищої освіти, набутих у: формальній освіті (академічна мобільність студентів на території України чи поза її межами, для студентів, які переводяться, поновлюються з інших ЗВО (вітчизняних чи іноземних); неформальній та/або інформальній освіті здійснюється згідно «ПОЛОЖЕННЯ про визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті у Волинському національному університеті імені Лесі Українки».

Підсумковий контроль

Форма контролю – семестровий залік. Оцінювання здійснюється за 100-бальною шкалою. Оцінка включає в себе оцінювання всіх видів запланованої навчальної роботи протягом семестру: нараховується за якісне виконання лабораторних, контрольних, тестових контрольних робіт та виконання індивідуального завдання. Максимальна кількість балів, яку може отримати здобувач під час поточного оцінювання за семестр – 100 балів. Залік виставляється за результатами поточної роботи за умови, що здобувач освіти виконав ті види навчальної роботи, які визначено силабусом освітнього компонента.

У випадку, якщо здобувач освіти не відвідував окремі аудиторні заняття (з поважних причин), на консультаціях він має право відпрацювати пропущені заняття та добрати ту кількість балів, яку було визначено на пропущені теми. У дату складання заліку викладач записує у відомість суму поточних балів, які здобувач освіти набрав під час поточної роботи.

У випадку, якщо здобувач освіти протягом поточної роботи набрав менше як 60 балів, він складає залік під час ліквідації академічної заборгованості. У цьому випадку бали, набрані під час поточного оцінювання анулюються. Максимальна кількість балів на залік під час ліквідації академічної заборгованості, становить 100. На заліку, під час ліквідації академічної заборгованості, здобувач отримує комплексне завдання, яке охоплює всі теми і всі форми контролю, які пропонувалися при вивченні освітнього компонента.

Питання, які виносяться на залік під час ліквідації академічної заборгованості.

1. Поняття і класифікація видів та методів несанкціонованого доступу.
2. Визначення і модель зловмисника.
3. Управління віддаленим доступом.
4. Класифікація способів захисту інформації в комп'ютерних системах.
5. Організація захисту інформації.
6. Фізичні методи захисту інформації.
7. Законодавчі методи захисту інформації.

8. Криптографічні методи захисту інформації.
9. Види та класифікація умисних загроз безпеки інформації.
10. Безпека використання технологій оптоволоконних кабельних систем.
11. Особливості комп'ютерних мереж, як каналів скачування інформації.
12. Криптографічний методом приховання інформації.

V. Шкала оцінювання

Оцінка в балах за всі види навчальної діяльності	Оцінка
90 – 100	Відмінно
82 – 89	Дуже добре
75 - 81	Добре
67 -74	Задовільно
60 - 66	Достатньо
1 – 59	Незадовільно

VI. Рекомендована література та інтернет-ресурси

Основна

1. Jeremiah Grossman. XSS Attacks CROSS SITE SCRIPTING EXPLOITS AND DEFENSE. – USA.: Amazon DS, 2018 – 630 с.
2. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с. 8. Створення та обробка баз даних: навч. посібник для студ. техн. спец. вищ. навч. закл. / Л.
3. Holistic Info-Sec for Web Developers. [Electronic resource]. – Access mode: <https://holisticinfosecforwebdevelopers.com/>
4. OWASP Web Security Testing Guide. [Electronic resource]. – Access mode : <https://owasp.org/www-project-web-security-testing-guide/>
5. Open Web Application Security Project [Електронний ресурс]. Режим доступу: www.owasp.org

Додаткова

1. Когут Ю.І. Кібербезпека та ризики цифрової трансформації компаній. Практичний посібник. Київ, 2021р.370с.
2. Кіберзахист Литви: <https://kam.lt/en/cyber-security>
3. Місія в Україні: <https://therecord.media/cyber-command-sent-a-hunt-forward-team-to-help-lithuania-harden-its-systems/>
4. Когут Ю.І. Кібервійни, кібертероризм, кіберзлочинність (концепції, стратегії, технології). Практичний посібник., Київ, 2022р.281с.
5. Когут Ю.І. Корпоративна безпека: практичний посібник/Ю.І.Когут. – Київ: Колсантингова компанія «СІДКОН», 2021. – 460 с.