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
МАТЕМАТИЧНІ ОСНОВИ КРИПТОГРАФІЇ
Підготовки першого (бакалаврського) рівня вищої освіти

Луцьк – 2026

Силабус вибіркового освітнього компонента “Математичні основи криптографії”. Підготовки першого (бакалаврського) рівня вищої освіти

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

Погоджено
Гарант освітньо-професійної програми:  Чернящук Н.Л.

Силабус освітнього компонента затверджено на засіданні кафедри комп’ютерних наук та кібербезпеки
протокол № 6 від 15.01.2025 р.

Завідувач кафедри:  Гришанович Т. О.

І Опис освітнього компонента

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

ІІ. Інформація про викладача

ПІП : Жигаревич Оксана Костянтинівна
Науковий Вчене звання -
Посада старший викладач
Контактна інформація zhyharevych.oksana@vnu.edu.ua
Дні занять http://194.44.187.20/cgi-bin/timetable.cgi?n=700

ІІІ. Опис освітнього компонента

1. Анотація курсу. "Математичні основи криптографії", є пріоритетним напрямком розвитку галузі захисту інформації у мережі. Важливо вміти використовувати сучасні інструменти для захисту особистих даних, для популяризації власних наукових напрацювань, для безпеки об'єктів критичної інфраструктури .
Обсяг матеріалу становить необхідний мінімум при підготовці слухачів першого (бакалаврського) рівня вищої освіти.

2. Мета навчальної дисципліни: надати здобувачам компетентностей і навичок, необхідних для використання у подальшому професійному житті, для здійснення наукової діяльності, для представлення результатів своїх досліджень, для ефективного здійснення науково-практичної діяльності у державних органах влади, також у приватному секторі.
Здобувачі отримають необхідні знання та навички щодо застосування сучасних новітніх технологій, пошуку оновленої наукової інформації у галузі обробки електронної інформації; презентації результатів власної наукової діяльності; якісного візуального оформлення чисельних та схематичних результатів досліджень; популяризації обраного наукового напряму досліджень за допомогою сучасних технологій.

3. Soft skills

- **Аналітичне та логічне мислення** — здатність оперувати абстрактними математичними поняттями, аналізувати криптографічні алгоритми та доводити їх властивості.
- **Критичне мислення** — уміння оцінювати надійність криптографічних методів, коректність математичних моделей та обґрунтованість припущень.
- **Уважність до формальних деталей** — здатність працювати з математичними формулами, доведеннями та алгоритмічними описами без помилок.
- **Здатність до розв'язання складних проблем** — уміння формалізувати задачі криптографії та знаходити адекватні математичні методи їх розв'язання.
- **Самоорганізація та наполегливість** — здатність працювати з теоретично складним матеріалом, систематично опановувати нові поняття й методи.

- **Комунікаційні навички** — уміння чітко та аргументовано пояснювати математичні ідеї та принципи криптографічних протоколів у письмовій і усній формах.
- **Відповідальність та академічна доброчесність** — усвідомлення важливості коректного використання математичних методів і дотримання етичних норм у сфері інформаційної безпеки.

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. Основні поняття та визначення криптоаналізу.						
Тема 1: Основні поняття криптології.	13	2	2	8	1	Звіт по лаб. роботі /5
Тема 2. Класичні алгоритми шифрування інформації. Шифр Цезаря. Шифр Частоколу. Шифр Віженера.	13	2	2	8	1	Звіт по лаб. роботі /5
Тема 3. Основи криптоаналізу класичних шифрів. Частотний криптоаналіз. Метод Касіски та метод Фрідмана.	13	2	2	8	1	Звіт по лаб. роботі /5
Тема 4. Потокові симетричні шифри. Шифр Вермана. RS4.	15	2	4	8	1	Звіт по лаб. роботі /10
Тема. 5. Потокові симетричні шифри. Генерація псевдовипадкових послідовностей.	19		4	14	1	Звіт по лаб. роботі /10
Тема. 6. Блокові симетричні шифри. Алгоритм DES, IDEA.	15	2	4	8	1	Звіт по лаб. роботі /10
Тема. 7. Блокові симетричні шифри. Національний стандарт шифрування ДСТУ 7624-2014. Режим роботи блокових симетричних шифрів.	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	Маршрутизатори MikroTik RB4011iGS+5HACQ2HND-IN	4
6	Апаратний міжмережевий екран Cisco ASA5506-X Міні IP WiFi камера для прихованого відеонагляду	4
7	Блокові симетричні шифри.	4
8	Удосконалений стандарт шифрування AES.	4

9	Режим роботи блокових симетричних шифрів.	4
10	Детектор прихованих камер та жучків CC-308+ Raspberry Pi 4 Model B 8GB	4
11	Шифр Плейфера. Криптосистема Хілла.	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 здачі 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, здобуті 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 анульовуються. 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 компонета.

Питання, які виносяться на залік під час ліквідації академічної заборгованості.
1. У чому полягає забезпечення конфіденційності, цілісності, доступності інформаційних ресурсів? 2. Дайте визначення поняттям: криптологія, криптографія та криптоаналіз. 3. Що таке криптографічний алгоритм та шифр? 4. Що таке криптографічний ключ? 5. Розкрийте поняття зашифрування та дешифрування даних. 6. Дайте визначення відкритого та закритого тексту. 7. Назвіть складові криптографічної системи. 8. У чому полягає криптостійкісьть криптографічної системи? 9. Що таке атака на криптографічну систему? 10. Дайте коротку класифікацію шифрів. 11. Опишіть алгоритм шифрування Цезаря.

12. До якого виду шифрів заміни (підстановки) відносять шифр Цезаря?
13. Опишіть алгоритм шифру частоколу.
14. Опишіть алгоритм шифру Плейфера.
15. Опишіть алгоритм шифрування криптосистемою Хілла.
16. Що являє собою ключ в криптосистемі Хілла?
17. Що є ключем у шифрі Віженера?
18. Опишіть алгоритм шифрування Віженера.
19. У чому суть методу частотного криптоаналізу?
20. Поясніть відмінність між шифрами моноалфавітної та поліалфавітної підстановки (заміни).
21. У чому полягає основна слабкість шифрів простої моноалфавітної заміни.
22. Яка літера найчастіше зустрічається у текстах українською (англійською) мовою?
23. Які кроки потрібно виконати для визначення довжини ключа у шифрі Віженера методом Казіскі?
24. Як уточнити довжину ключа методом Фрідмана?
25. Що таке індекс збігу?

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 література

1. Урядовий портал. Постанова Кабінету Міністрів України від 29 березня 2006 р. №373.
2. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, 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.
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:

6. www.owasp.org
7. Когут Ю.І. Кібербезпека та ризики цифрової трансформації компаній. Практичний посібник. Київ, 2021р.370с.
8. Місія в Україні:https://therecord.media/cyber-command-sent-a-hunt-forward-team-to-help-lithuania-harden-its-systems/
9. Когут Ю.І. Кібервійни, кібертероризм, кіберзлочинність (концепції, стратегії, технології). Практичний посібник., Київ, 2022р.281с.
10. Когут Ю.І. Корпоративна безпека: практичний посібник/Ю.І.Когут. – Київ: Колсантингова компанія «СІДКОН», 2021. – 460 с.

Додаткова дітература

1. Офіційний сайт Google, на якому розміщена документація по работі із Google App Engine. [Електронний ресурс]. – Режим доступу: https://cloud.google.com/products/app-engine
2. Офіційний сайт Microsoft, на якому розміщена документація по роботі із платформою Microsoft Azure. [Електронний ресурс].
3. Когут Ю.І. Кібервійна та безпека об’єктів критичної інфраструктури [практичний посібник] / Ю.І. Когут; за редакцією доктора тех., наук, проф. А.С.Довгопологo. – Київ: Консалтингова компанія «СІДКОН»; ВД Дакор, 2021. – 332 с.