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

СИЛАБУС
нормативного освітнього компонента
ПРИКЛАДНА КРИПТОЛОГІЯ
підготовки бакалавра

спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Кібербезпека та захист інформації

Луцьк – 2023

Силабус навчальної дисципліни «Прикладна криптологія» підготовки бакалавра, галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека, за освітньою-професійною програмою Кібербезпека та захист інформації.

Розробник: Жигаревич О.К., старший викладач

Погоджено
Гарант освітньо-професійної програми:  Глинчук Л.Я.

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

протокол № 2 від 28.09.2023 р.

Завідувач кафедри:  Гришанович Т. О.

І. Опис освітнього компонента

<table>
<tr><th>Найменування показників</th><th>12 Інформаційні технології
125 Кібербезпека та захист інформації
бакалавр</th><th>Характеристика освітнього компонента</th></tr>
<tr><td rowspan="2">Денна форма навчання</td><td rowspan="8"></td><td>Нормативна</td></tr>
<tr><td>Рік навчання 3</td></tr>
<tr><td rowspan="2">Кількість годин/кредитів 120/4</td><td>Семестр 5-ий</td></tr>
<tr><td>Лекції 32 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: є</td><td>Лабораторні 44 год.</td></tr>
<tr><td>Самостійна робота 36 год.</td></tr>
<tr><td>Консультації 8 год.</td></tr>
<tr><td colspan="2">Мова навчання: українська</td><td>Форма контролю: іспит</td></tr>
</table>

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

Прикладна криптологія є одним із важливих розділів сучасних систем криптології. Освітній компонент «Прикладна криптологія» належить до переліку нормативних навчальних дисциплін програми підготовки бакалавра за спеціальністю 125 «Кібербезпека та захист інформації», забезпечує професійний розвиток бакалавра та спрямована на формування у майбутніх фахівців базових знань, розпізнавання методів шифрування інформації; 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 для передачі через мережу.

2. Пререквізити: Базові знання із хмарних технологій, програмування, організаційне забезпечення захисту інформації.

Постреквізити: Знання та вміння, отримані в результаті вивчення дисципліни, можуть бути використані для написання курсової роботи з навчальних дисциплін циклу професійної підготовки, а також у професійному розвитку та роботі з використання криптографічних алгоритмів та протоколів для захисту інформації; реалізовувати системи захисту інформації в інформаційних і комунікаційних системах; застосовувати методи і засоби запобігти звичайному перехопленню даних.

3. Мета і завдання освітнього компонента: надання теоретичних знань та формування практичних навичок щодо організації захисту інформації з метою розв'язування прикладних задач та створення програмного забезпечення систем інформаційної безпеки.

4. Результати навчання.

1. Загальні компетентності:

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.
ЗК 2. Знання та розуміння предметної області та розуміння професії.
ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.
ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки.
ФК 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).
адженої системи управління інформаційною безпекою та/або кібербезпекою.
ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.
ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН 22. Вирішувати задачі управління процедурами ідентифікації, аутентифікації, авторизації процесів і користувачів в інформаційно- телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
ПРН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

Структура освітнього компонента.

Назви змістових модулів і тем	Усього	Лек.	Лабор.	Сам. роб.	Конс.	Форма контролю/ Бали
Змістовий модуль 1. Основні поняття та визначення криптоаналізу.						
Тема 1. Основні поняття криптології.	12	4	4	4		РЗ
Тема 2. Класичні алгоритми шифрування інформації. Шифр Цезаря. Шифр Частоколу.	13	2	4	6	1	РЗ
Тема 3. Класичні алгоритми шифрування інформації. Шифр	15	4	4	6	1	РЗ, РМГ

Плейфера. Криптосистема Хілла.						
Тема 4. Класичні алгоритми шифрування інформації. Шифр Віженера.	15	2	4	8	1	РЗ
Тема 5. Основи криптоаналізу класичних шифрів. Частотний криптоаналіз. Метод касіски та метод Фрідмана.	17	4	4	4	1	
Разом за модулем 1	72	16	20	28	4	**14**
Змістовий модуль 2. Симетричні та асиметричні криптографічні системи						
Тема 1. Потокові симетричні шифри. Шифр Вермана. RS4.	10	4	4	2		РЗ
Тема 2.Потокові симетричні шифри. Генерація псевдовипадкових послідовностей.	10	2	4	2	1	РЗ
Тема 3. Блокові симетричні шифри. Алгоритм DES, IDEA.	11	2	6	2	1	РЗ
Тема 4. Блокові симетричні шифри. Удосконалений стандарт шифрування AES.	9	4	4		1	РЗ
Тема 5. Блокові симетричні шифри. Національний стандарт шифрування ДСТУ 7624-2014. Режим роботи блокових симетричних шифрів.	13	4	6	2	1	РЗ
Разом за модулем 2	53	16	24	8	4	26
Види підсумкових робіт						Бал
Тестування						25
Модульна контрольна робота						10
ІНДЗ 1						15
ІНДЗ 2						10
Всього годин/Балів	120	32	44	36	8	100

Методи контролю*: ДС – дискусія, ДБ – дебати, Т – тести, ТР – тренінг, РЗ/К – розв’язування задач/кейсів, ІНДЗ/ІРС – індивідуальне завдання/індивідуальна робота здобувача освіти, РМГ – робота в малих групах, МКР/КР – модульна контрольна робота/ контрольна робота, Р – реферат, а також аналітична записка, аналітичне есе, аналіз твору тощо.

2. Завдання для самостійного опрацювання.
   Самостійна робота здобувачів включає в себе:

- Опрацювання лекційного матеріалу.
- Перевірка здійснюється під час лабораторних занять.
- Підготовка до лабораторних занять, виконання домашніх завдань.

– Систематизація вивченого матеріалу перед екзаменом. Перевірка здійснюється під час екзамену.
– Вивчення тем, що не розглядаються в курсі лекцій. Перевірка здійснюється під час модульних контрольних заходів і оцінюється відповідною кількістю балів.
– Підготовка ІНДЗ. Перевірка здійснюється під час здачі індивідуального звдання.

№ з/п	Тема	Кількість годин
1	Алгоритм шифрування Ель-Гамаля.	4
2	Процес дешифрування, можливості та час.	4
3	Дослідити первісний корінь за модулем простого числа.	4
4	Опишіть алгоритм обміну ключами Діффі-Хелмана.	4
5	Основні вимоги до криптографічної хеш-функції.	4
6	Електронний цифровий підпис.	4
7	Опишіть схему створення і перевірки ЦП.	4
8	Основні характеристики підпису RSA? Яка відмінність підпису RSA від шифру RSA?	2
9	Підпис Ель-Гамаля.	4
10	Переваги криптосистеми на еліптичних кривих.	2
11		36

IV. Політика оцінювання

Політика викладача щодо студента

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку ВНУ імені Лесі Українки, загально-прийнятих моральних принципів, правил поведінки та корпоративної культури; підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності. Атмосфера на заняттях повинна бути творчо-професійною, відкритою до конструктивної критики. Недопустимі запізнення на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття; списування. Очікується, що всі студенти відвідають усі лекції і лабораторні заняття курсу. Кожен здобувач освітньої програми повинен бути учасником дистанційного курсу, розміщеного на платформі дистанційного навчання Moodle. Завдання для практичного виконання (лабораторні роботи, ІНДЗ, самостійні роботи), завдання підсумкового контролю (тести, контрольні роботи, що передбачають розробку програм) здаються із використанням засобів дистанційного курсу.

Політика щодо академічної доброчесності

Під час навчання учасники освітнього процесу зобов’язані дотримуватися академічної доброчесності: етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової діяльності.

Дотримання академічної доброчесності здобувачами передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю (для осіб з особливим освітніми потребами ця вимога застосовується з урахуванням їх індивідуальних потреб і можливостей); посилання на джерела інформації у разі використання ідей,

тверджень, відомостей; дотримання норм законодавства про авторське право; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

Під час оцінювання результатів навчання студенти не користуються забороненими засобами (мобільний телефон, планшет, конспект, навчальна література, інші джерела інформації, в тому числі Інтернет-ресурси), самостійно виконують запропоновані завдання. При виконанні лабораторних робіт з курсу здобувачі мають право використовувати власні ноутбуки, якщо вони підтримують необхідне програмне забезпечення.

Політика щодо дедлайнів та перескладання

Якщо здобувач вищої освіти був відсутній на заняттях з будь-якої причини, він/вона вивчають теоретичний матеріал самостійно використовуючи навчальні посібники, конспекти лекцій, матеріали дистанційного курсу "Прикладна криптологія", розміщеного на платформі дистанційного навчання Moodle, виконують всі домашні завдання. Прозвітуватися про виконання завдань можна, використовуючи дистанційний курс "Прикладна криптологія", або під час консультацій, одночасно при цьому з'ясувати незрозумілі моменти, задати запитання викладачу. Існує можливість використання форуму дистанційного курсу. Перескладання контрольних робіт та тестувань заборонено. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку.

V. Підсумковий контроль

Підсумковою формою контролю освітнього компонента "Прикладна криптологія" є екзамен. Оцінювання навчальних досягнень здійснюється за 100 бальною шкалою. Оцінка включає в себе поточний контроль (оцінюється робота на парах, вчасне і якісне виконання домашніх завдань) та підсумковий контроль (самостійне виконання індивідуальних завдань, контрольні роботи, перевірка теоретичної підготовки у формі тестування, ІНДЗ). Максимальна кількість балів, яку може отримати здобувач під час поточного оцінювання за семестр – 60 балів. Максимальна кількість балів, яку може отримати здобувач за підсумковий контроль за семестр складає 100 балів.

Передбачається виконання індивідуальних завдань. Варіант ІНДЗ включає себе набір задач, що охоплюють одну або кілька близьких тем. Або одне завдання, розв'язання якого вимагає самостійного опрацювання невеликих тем.

Відповідно до пункту 3.3 Положення про визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті у Волинському національному університеті імені Лесі Українки з дисципліни "Прикладна криптологія" визнання таких результатів навчання не проводиться.

Якщо за результатами семестру накопичено не менше 75 балів і студент погоджується із цим результатом, то оцінка за семестр може виставлятися без складання екзамену. В іншому випадку студент складає екзамен; максимальна кількість балів, яку можна отримати на екзамені– 100 балів. Вони замінюють бали модульного семестрового контролю, поточний семестровий контроль при цьому не зберігається.

На екзамен виносяться основні питання, типові та комплексні задачі, ситуації, завдання, що потребують творчої відповіді та уміння синтезувати отриманні знання і застосовувати їх під час виконання практичних задач.

Питання до екзамену
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?
26. У чому полягає алгоритм одноразового блокноту?
27. Що являє собою операція XOR?
28. Які переваги і недоліки шифрування методом одноразового блокноту?
29. До яких шифрів належить стандарт шифрування даних DES?
30. Якою повинна бути довжина ключа у шифрі DES?
31. З яких кроків складається алгоритм шифрування DES?
32. Скільки разів виконується перетворення Фейстеля над блоком у DES?
33. Яка довжина блоку у алгоритмі IDEA?
34. Опишіть кроки шифрування за алгоритмом IDEA.
35. Яка довжина блоку в AES?
36. Як називають матрицю проміжного результату при шифруванні за допомогою алгоритму AES?
37. Опишіть операцію підстановки байтів у алгоритмі AES.
38. Опишіть операцію зсуву рядків у алгоритмі AES.
39. Опишіть операцію перемішування стовпців у алгоритмі AES.
40. Опишіть операцію додавання раундового ключа у алгоритмі AES.
41. Які особливості дешифрування за алгоритмом AES?
42. Від чого залежить кількість раундів шифрування за алгоритмом «Калина»?
43. Яка довжина ключа в алгоритмі «Калина»?

44. Як генерується допоміжний ключ в алгоритмі «Калина»?
45. Яким чином генеруються ключі з парними індексами в алгоритмі «Калина»?
46. Яким чином генеруються ключі з непарними індексами в алгоритмі «Калина»?
47. Скільки рядків має матриця стану в алгоритмі «Калина»?
48. Скільки таблиць замін використовується в криптографічному алгоритмі перетворення даних «Калина»?
49. Які особливості дешифрування за алгоритмом «Калина»?
50. Назвіть основні режими роботи блокових симетричних алгоритмів шифрування.

VI. Шкала оцінювання

Шкала оцінювання знань здобувачів освіти з освітніх компонентів, де формою контролю є екзамен

Оцінка в балах	Лінгвістична оцінка	Оцінка за шкалою ECTS	
		оцінка	пояснення
90–100	Відмінно	A	відмінне виконання
82–89	Дуже добре	B	вище середнього рівня
75–81	Добре	C	загалом хороша робота
67–74	Задовільно	D	непогано
60–66	Достатньо	E	виконання відповідає мінімальним критеріям
1–59	Незадовільно	Fx	Необхідне перескладання

VII. Рекомендована література та інтернет-ресурси.

Основна література

1. Бобало Ю. Я. Інформаційна безпека: навч. посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник та ін.; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук доц. І. ВГорбатого. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.
2. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч.посібник / Г. Л. Козіна. – Запоріжжя : НУ «Запорізька політехніка», 2020. – 192 с.
3. Урядовий портал. Постанова Кабінету Міністрів України від 29 березня 2006 р. №373.
4. 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.
5. Holistic Info-Sec for Web Developers. [Electronic resource]. – Access mode: https://holisticinfosecforwebdevelopers.com/
6. OWASP Web Security Testing Guide. [Electronic resource]. – Access mode : https://owasp.org/www-project-web-security-testing-guide/
7. Open Web Application Security Project [Електронний ресурс]. Режим доступу:
    a. www.owasp.org
8. Когут Ю.І. Кібербезпека та ризики цифрової трансформації компаній. Практичний посібник. Київ, 2021р.370с.
9. Місія в Україні:https://therecord.media/cyber-command-sent-a-hunt-forward-team-to-help-lithuania-harden-its-systems/
10. Когут Ю.І. Кібервійни, кібертероризм, кіберзлочинність (концепції, стратегії, технології). Практичний посібник., Київ, 2022р.281с.
11. Когут Ю.І. Корпоративна безпека: практичний посібник/Ю.І.Когут. – Київ: Колсантингова компанія «СІДКОН», 2021. – 460 с.

12. Додаткова дітература та Інтернет-ресурси

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