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
КРИПТОАНАЛІЗ

підготовки бакалавра

спеціальності 125 Кібербезпека

освітньо-професійної програми Інформаційна безпека

Луцьк – 2022

Силабус навчальної дисципліни «Криптоаналіз» підготовки бакалавра, галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека, за освітньою програмою Інформаційні технології.

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 29 вересня 2022 р.

Завідувач кафедри:  Гришанович Т. О.

І. Опис освітнього компонента

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітньо-професійна програма, освітній рівень</th><th>Характеристика освітнього компонента</th></tr>
<tr><td rowspan="2">Денна форма навчання</td><td rowspan="6">12 Інформаційні технології

125 Кібербезпека

Інформаційна безпека</td><td>Нормативна</td></tr>
<tr><td>Рік навчання 4</td></tr>
<tr><td rowspan="2">Кількість годин/кредитів 120 / 4</td><td>Семестр 7-ий</td></tr>
<tr><td>Лекції 34 год.</td></tr>
<tr><td rowspan="2">ІНДЗ: є</td><td>Лабораторні 34 год.</td></tr>
<tr><td>Самостійна робота 44 год.</td></tr>
<tr><td colspan="2">Мова навчання: українська</td><td>Консультації 8 год.
Форма контролю: екзамен</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

Основи криптоаналізу є одним із важливих розділів сучасних комп'ютерних наук. Освітній компонент «Криптоаналіз» належить до переліку нормативних навчальних дисциплін програми підготовки бакалавра за спеціальністю 125 «Кібербезпека». Вивчається як окремий розділ криптології та спрямована на вивчення методів отримання вихідного значення зашифрованої інформації, не маючи доступу до секретної інформації (ключа), необхідної для цього. Дослідження самого процесу є надзвичайно цікавим, дешифрування та необхідні ресурси та знання, які потрібно використати, можливість оцінити сильні та слабкі сторони методів шифрування.

2. Пререквізити: Базові знання із організація та обробка електронної інформації, програмування.

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 розробляти і застосовувати криптографічні алгоритми та протоколи 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: Формування знання про роботу розглядаючи класичний та сучасний криптоаналіз; основні та додаткові методи криптоаналізу; класифікацію, характеристики, приклади та типи криптоатак; навчитися досліджувати алгоритми криптоаналізу, виконувати криптоаналіз класичних шифрів, оцінювати слабкі та сильні сторони шифрів, аналізувати процес дешифрування. Способи програмної реалізації; формування умінь і навичок програмно обробляти дані з використанням різних методів доступу до інформації.

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 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.

ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

ФК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібезбезпеки.

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.

Структура освітнього компонента.

Назви змістових модулів і тем	Усього	Лек.	Лабор.	Сам. роб.	Конс.	Форма контролю/ Бали
Змістовий модуль 1. Вступ до криптології						
Тема 1. ОСНОВНІ ПОНЯТТЯ КРИПТОЛОГІЇ 1.1. Основні терміни. 1.2. Вимоги до криптографічних систем. 1.3. Принципи побудови й схеми криптологічних систем. 1.4. Класифікація алгоритмів шифрування.	10	6	2	2		РЗ
Тема 2. ОСНОВИ КРИПТОЛОГІЇ, КРИПТОГРАФІЇ ТА	11	6	2	2	1	РЗ

КРИПТОГРАФІЧНОГО АНАЛІЗУ 2.1. Загальні відомості про захист інформації в інформаційно-телекомунікаційних системах. 2.2. Роль криптографічних протоколів у загальній задачі забезпечення інформаційної безпеки.						
Тема 3. Загальні відомості про класичну криптологію, криптографію та криптографічний аналіз. 3.1. Загальні відомості про криптологію. 3.2. Історія розвитку криптології.	9	4	2	2	1	РЗ, РМГ
Тема 4. ОСНОВИ ТЕОРІЇ ЗВ'ЯЗКУ 1. Основи теорії засекреченого зв'язку К. Шеннона. 2. Класифікація методів шифрування повідомлень. 3. Криптографічний аналіз. 4. Атака на зашифрований текст. 5. Атака на відомий вхідний текст. 6. Атака на обраний вхідний текст. 7. Атака на обраний зашифрований текст.	13	2	4	6	1	РЗ
Тема 5. ШИФРУВАННЯ ТА ІНФРАСТРУКТУРА ВІДКРИТИХ КЛЮЧІВ 1. Захист комунікацій. 2. Криптологія та криптоаналіз. 3 Криптографія – шифри. 4. Криптоаналіз – злом коду. 5.Використання ключів у	15	4	4	6	1	

шифруванні.						
Разом за модулем 1	60	22	14	18	4	**14**
Змістовий модуль 2.						
Тема 1. ЦІЛІСНІСТЬ І ДОСТОВІРНІСТЬ 1. Криптографічні хеш-функції. 2. Як працює криптографічний алгоритм хешування. 3. MD5 і SHA. 4. Код аутентифікації повідомлень на основі хешу.	10	2	2	6		РЗ
Тема 2. ШИФРУВАННЯ 1. Симетричне шифрування. 2. Симетричні алгоритми шифрування. 3. Алгоритми асиметричного шифрування. 4. Асиметричне шифрування - конфіденційність. 5. Асиметричне шифрування - аутентифікація. 6. 6 Асиметричне шифрування - цілісність.	11	2	2	6	1	РЗ
Тема 3. Алгоритм Діффі – Хеллмана.	13	2	4	6	1	РЗ
Тема 4. ВИКОРИСТАННЯ ЦИФРОВИХ ПІДПИСІВ 1. Цифрові підписи. 2. Цифрові підписи коду. 3.Цифрові підписи для цифрових сертифікатів.	13	2	4	6	1	РЗ
Тема 5. ЦЕНТРИ СЕРТИФІКАЦІЇ І СИСТЕМА ДОВІРИ НА ОСНОВІ PKI 1. Управління загальними ключами. 2. Система центрів PKI. 3. Система довіри на основі PKI. 4. Взаємодія різних постачальників PKI. 5. Реєстрація, аутентифікація та відкликання сертифікатів. 6. Застосування PKI. 7. Шифрування мережевих транзакцій.	13	4	8	4	1	РЗ

8. Шифрування і моніторинг безпеки. 9. Шифрування та інфраструктура відкритих ключів. 10. Шифрування та інфраструктура відкритих ключів.						
Разом за модулем 2	60	12	20	28	4	26
Види підсумкових робіт						Бал
Тестування						25
Модульна контрольна робота						10
ІНДЗ 1						15
ІНДЗ 2						10
Всього годин/Балів	120	34	34	44	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 практичних занять.

– Підготовка до практичних занять, виконання домашніх завдань.

– Перевірка здійснюється під час практичних занять.

– Систематизація вивченого матеріалу перед заліком. Перевірка здійснюється під час заліку.

– Вивчення тем, що не розглядаються в курсі лекцій. Перевірка здійснюється під час модульних контрольних заходіві оцінюється відповідною кількістю балів.

– Підготовка ІНДЗ. Перевірка здійснюється під час здачі індивідуального звдання.

№ з/п	Тема	Кількість годин
1	Розглянути звичайну перестановку, продемонструвати застосування на прикладі. (Метод Цезаря)	4
2	Розглянути звичайну рядково-стовпчикову табличну перестановку, продемонструвати застосування на прикладі. (Шенона Фано)	4
3	Розглянути рядково-стовпчикову табличну перестановку із застосуванням ключа стовпців, продемонструвати застосування на прикладі. (Таблиці Трісімуса)	4

4	Розглянути рядково-стовпчикову табличну перестановку із застосуванням ключа рядків, продемонструвати застосування на прикладі.	4
5	Розглянути рядково-стовпчикову табличну перестановку з двома ключами, продемонструвати застосування на прикладі.	4
6	Розглянути табличну перестановку з використанням трафарету, продемонструвати застосування на прикладі.	4
7	Створення та шифрування файлів.	8
8	Робота з документами, та методи шифрування в Україні в умовах війни.	4
9	Програма «Дія», методи шифрування інформації.	4
10	Розглянути шифр «Калина», метод використовується в Україні.	4
11	Всього	44

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 творчою, 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 практичні заняття курсу. Кожен студент повинен бути учасником дистанційного курсу “Криптоаналіз”, 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 “Криптоаналіз”, розміщеного на платформі

дистанційного навчання Moodle, виконують всі домашні завдання. Прозвітуватися про виконання завдань можна, використовуючи дистанційний курс “Криптоаналіз”, 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 “Криптоаналіз” 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 – 75 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 “Криптоаналіз” 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.

Екзамен з освітнього компонента “Криптоаналіз” передбачає усну відповідь на теоретичні питання. До білету входять 3 теоретичних питання та 2 практичні задачі. Кожне із завдань оцінюється 20 балами. Викладач залишає за собою право ставити уточнюючі питання під час відповіді студента. Студент залишається вільним у виборі програми створення презентації, за допомогою якої реалізує практичне завдання.

Питання до екзамену

Основи криптології. (теоретичні запитання)

1. Термінологія та історія створення криптології. Криптографічний аналіз.
2. Суть та характеристики криптології. Загальна структура криптосистеми.
3. Класифікація алгоритмів шифрування.
4. Роль криптографічних протоколів у загальній задачі забезпечення інформаційної безпеки.
5. Основи теорії засекреченого зв’язку К. Шеннона. Досконала криптографічна система.
6. Класифікація методів шифрування повідомлень.

Шифрування та інфраструктура відкритих ключів. (практичні задачі для групи студентів)

1. Криптографія – шифри. Метод Цезаря. Практична реалізація. Відеокоментар.
   Ключ : імена учасників команди. Гасло : «Все буде Україна», перший стовпчик пісні «Ой у лузі червона калина».
2. Криптографія – шифри. Багатоалфавітніх шифри. Метод Віженера. Практична реалізація. Відеокоментар.
   Ключ : прізвища учасників команди. Гасло : «Все буде Україна», другий стовпчик пісні «Ой у лузі червона калина».
3. Криптоаналіз – злом коду. Метод Шенона – Фано. Практична реалізація. Відеокоментар.
   Ключ : імена учасників команди. Гасло : «Все буде Україна» Державний гімн України.
4. Криптографія – шифри. Метод Трісімуса. Практична реалізація. Відеокоментар.
   Ключ : прізвища учасників команди. Гасло : «Все буде Україна», Рецепт Пасочки. (у приват).

5. Криптографія – шифри. Метод Трісімуса і його різновиди. Практична реалізація. Відеокоментар.
   Ключ : імена учасників команди. Гасло : «Все буде Україна», Т.Г. Шевченко «Отак подивишся здаля на москаля».
6. Криптоаналіз – злом коду. Подвоєння ключів. Метод Віженера, Метод Цезаря - порівняльна таблиця результатів шифрування інформації.
   Ключ : прізвища учасників команди. Гасло : «Все буде Україна», Леся Українка, вірш «Надія».

Зарубіжний досвід щодо розвитку систем протидії загрозам кібертероризму на державному рівні: національні структури, які забезпечують кібербезпеку у зарубіжних країнах, а також підготовка кібервійськ провідних держав світу, їх можливості та перспективи. (реалізація завдання у програмі CANVA)

1. США. Досвід для України.
2. КНР. Досвід для України.
3. Ізраїль. Досвід для України.
4. Естонія. Досвід для України.
5. Литва. Латвія. Досвід для України.
6. Нідерланди. Досвід для України.

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

VI. Рекомендована література та інтернет-ресурси.

Основна література

1. **Криптоаналіз** [Текст]: конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» галузь знань 12 Інформаційні технології спеціальності 125 Кібербезпека / уклад. О.К.Жигаревич – Луцьк : ВНУ ім. Лесі Українки, 2021. – 62 с.
2. **Криптоаналіз** [Текст]: методичні вказівки до лабораторних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» галузь знань 12 Інформаційні технології спеціальності 125 Кібербезпека / уклад. О.К.Жигаревич, Ю.С.Павленко – Луцьк : ВНУ ім. Лесі Українки, 2021. – 30 с.
3. **Криптоаналіз** [Текст]: методичні вказівки до виконання самостійної роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» галузь знань 12 Інформаційні технології спеціальності 125 Кібербезпека / уклад. О.К. Жигаревич – Луцьк : ВНУ ім. Лесі Українки, 2021. – 16 с.
4. Когут Ю.І. Кібербезпека та ризики цифрової трансформації компаній. Практичний посібник. Київ, 2021р.370с.
5. Кіберзахист Литви: https://kam.lt/en/cyber-security
6. Місія в Україні:https://therecord.media/cyber-command-sent-a-hunt-forward-team-to-help-lithuania-harden-its-systems/
7. Когут Ю.І. Кібервійни, кібертероризм, кіберзлочинність (концепції, стратегії, технології). Практичний посібник., Київ, 2022р.281с.
8. Когут Ю.І. Корпоративна безпека: практичний посібник/Ю.І.Когут. – Київ: Колсантингова компанія «СІДКОН», 2021. – 460 с.
9. Пасічник В.В., Пасічник О.В., Угрин Д.І. Веб-технології. [Текст] : підручник / Львів : «Магнолія2006», 2018. – 336 с.
10. Закон України «Про захист персональних даних» // Відомості Верховної Ради України, 2010, No 34, ст. 481. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/2297-17

11. Постанова Правління Національного банку України від 28.10.2010 No 474 «Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України». [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/v0474500-10 Інформаційні ресурси

Додаткова дітература та Інтернет-ресурси

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. Основы криптоанализа. [Електронний ресурс]. – Режим доступу до ресурсу: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema18
4. 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.