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
УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ
підготовки бакалавра

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

Луцьк – 2023

Силабус навчальної дисципліни «Управління інформаційною безпекою» 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="7"></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 48 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: є</td><td>Лабораторні 60 год.</td></tr>
<tr><td>Самостійна робота 4 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

Управління інформаційною безпекою є одним із важливих розділів кібербезпеки та захисту інформації. Освітній компонент «Управління інформаційною безпекою» 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 знань із захисту інформації, 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, ризики інформаційної безпеки, бізнес-ризики, моніторинг загроз.

2. Пререквізити: Базові знання із хмарних технологій, програмування, організаційне забезпечення захисту інформації, прикладна криптологія, нормативно-правова база.

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 технічного захисту інформації, інженерного захисту інформації, криптографічного захисту 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 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки.
ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
ФК 4. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики безпеки.
ФК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
ФК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою та/або кібербезпекою.
ФК 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
ПРН 44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.
ПРН 45. Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
ПРН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних 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.

Структура освітнього компонента.

Назви змістових модулів і тем	Усього	Лек.	Лабор.	Сам. роб.	Конс.	Форма контролю/ Бали
Змістовий модуль 1. Основні поняття інформаційної безпеки.						
Тема 1. Нормативні документи інформаційної безпеки.	13	6	6	1		РЗ
Тема 2. Критерії оцінки інформаційної безпеки.	13	6	6		1	РЗ
Тема 3. Модель ПВПД для процесів СУІБ.	13	6	6		1	РЗ, РМГ
Тема 4. Сладові політики інформаційної безпеки. Визначення критичних бізнес процесів. Надання доступу до інформації. Контроль доступу. Парольний захист. Антивірусний захист.	13	6	6		1	РЗ
Тема 5. Захист мережі банку. Віддалений доступ до ресурсів мережі. Ідентифікація та автентифікація ресурсів СУІБ.	14	6	6	1	1	
Разом за модулем 1	66	30	30	2	4	**14**
Змістовий модуль 2. Криптографічні системи						
Тема 1. Криптографічний захист інформації.	9	2	6	1		РЗ
Тема 2. Криптосистема з відкритим ключем.	11	4	6		1	РЗ
Тема 3. Криптографічні хеш-функції.	11	4	6		1	РЗ
Тема 4. Цифровий підпис.	12	4	6	1	1	РЗ
Тема 5. Основи криптографії на еліптичних кривих.	11	4	6		1	РЗ
Разом за модулем 2	54	18	30	2	4	26
Види підсумкових робіт						Бал
Тестування						25
Модульна контрольна робота						10
ІНДЗ 1						15
ІНДЗ 2						10
Всього годин/Балів	120	48	60	4	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	Криптосистема Меркла-Хелмана.	1
2	Процес дешифрування, можливості та час.	1
3	Дослідити первісний корінь за модулем простого числа.	1
4	Опишіть алгоритм обміну ключами Діффі-Хелмана.	1
5		4

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 "Управління інформаційною безпекою", розміщеного на платформі дистанційного навчання Moodle, виконують всі домашні завдання. Прозвітуватися про виконання завдань можна, використовуючи дистанційний курс "Управління інформаційною безпекою", 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 "Управління інформаційною безпекою" 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 "Управління інформаційною безпекою" 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 ідея криптосистеми з відкритим ключем?

2. Хто є основоположниками криптографії з відкритим ключем?
3. Яка основна перевага асиметричних шифрів над симетричними?
4. Що таке одностороння функція?
5. На чому ґрунтується криптостійкість алгоритму шифрування даних RSA?
6. Як знайти модуль криптосистеми RSA?
7. Яким чином у алгоритмі RSA отримуються відкритий та закритий ключі?
8. На чому ґрунтується криптостійкість алгоритму шифрування даних Ель-Гамаля?
9. Яким чином у алгоритмі Ель-Гамаля отримуються відкритий та закритий ключі?
10. Опишіть алгоритм шифрування Ель-Гамаля.
11. Опишіть алгоритм обміну ключами Діффі-Хелмана.
12. Що таке первісний корінь за модулем простого числа?
13. Дайте визначення поняттю «хеш-функція».
14. Що таке дайджест повідомлення?
15. Які основні вимоги висуваються до криптографічної хеш-функції?
16. Що являє собою (електронний) цифровий підпис?107
17. Опишіть схему створення і перевірки ЦП.
18. Як здійснюється підпис RSA? Яка відмінність підпису RSA від шифру RSA?
19. Як здійснюється підпис Ель-Гамаля?
20. Які переваги мають криптосистеми на еліптичних кривих над звичайними
21. асиметричним алгоритмами?
22. Який загальний вигляд має крива, що використовується в криптографічних
23. системах, заснованих на еліптичних кривих?
24. Дайте визначення порядку групи точок еліптичної кривої.
25. Дайте визначення порядку точки еліптичної кривої.
26. Які основні операції виконуються над точками еліптичних кривих при їх
27. використанні в криптографічних системах?
28. Опишіть алгоритм Діффі-Хелмана на еліптичних кривих.
29. У чому полягає забезпечення конфіденційності, цілісності, доступності, інформаційних ресурсів?
30. У чому суть методу частотного криптоаналізу?
31. Поясніть відмінність між шифрами моноалфавітної та поліалфавітної підстановки (заміни).
32. У чому полягає основна слабкість шифрів простої моноалфавітної заміни.
33. Яка літера найчастіше зустрічається у текстах українською (англійською) мовою?
34. Які кроки потрібно виконати для визначення довжини ключа у шифрі Віженера методом Казіскі?
35. Як уточнити довжину ключа методом Фрідмана?
36. Що таке індекс збігу?
37. У чому полягає алгоритм одноразового блокноту?

38. Що являє собою операція XOR?
39. Які переваги і недоліки шифрування методом одноразового блокноту?
40. До яких шифрів належить стандарт шифрування даних DES?
41. Якою повинна бути довжина ключа у шифрі DES?
42. З яких кроків складається алгоритм шифрування DES?
43. Скільки разів виконується перетворення Фейстеля над блоком у DES?
44. Яка довжина блоку у алгоритмі IDEA?
45. Опишіть кроки шифрування за алгоритмом IDEA.
46. Яка довжина блоку в AES?
47. Як називають матрицю проміжного результату при шифруванні за допомогою алгоритму AES?
48. Опишіть операцію підстановки байтів у алгоритмі AES.
49. Опишіть операцію зсуву рядків у алгоритмі AES.
50. Опишіть операцію перемішування стовпців у алгоритмі AES.
51. Опишіть операцію додавання раундового ключа у алгоритмі AES.
52. Які особливості дешифрування за алгоритмом AES?
53. Від чого залежить кількість раундів шифрування за алгоритмом «Калина»?
54. Яка довжина ключа в алгоритмі «Калина»?
55. Як генерується допоміжний ключ в алгоритмі «Калина»?
56. Яким чином генеруються ключі з парними індексами в алгоритмі «Калина»?
57. Яким чином генеруються ключі з непарними індексами в алгоритмі «Калина»?
58. Скільки рядків має матриця стану в алгоритмі «Калина»?
59. Скільки таблиць замін використовується в криптографічному алгоритмі перетворення даних «Калина»?
60. Які особливості дешифрування за алгоритмом «Калина»? 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.