

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
ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ
підготовки бакалавра

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

Силабус навчальної дисципліни «Організаційне забезпечення захисту інформації»
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:

Чернящук Н.Л.

**Силабус освітнього компонента
комп'ютерних наук та кібербезпеки**

затверджено на засіданні кафедри

протокол № 4 від 21.11.2024 р.

Завідувач

кафедри:



Гришанович Т. О.

I. Опис освітнього компонента

Найменування показників	Галузь знань, спеціальність, освітня програма	Характеристика освітнього компонента
Денна форма навчання	12 Інформаційні технології 125 Кібербезпека та захист інформації бакалавр	Нормативна
Кількість годин/кредитів 120/4		Рік навчання 1
		Семестр 2-ий.
ІНДЗ: немає		Лекції 24 год.
		Лабораторні 32 год.
		Самостійна робота 56 год.
		Консультації 8 год.
Форма контролю: залік		
Мова навчання: українська		

II. Інформація про викладача

ППП : Жигаревич Оксана Костянтинівна
Науковий Вчене звання -
Посада старший викладач
Контактна інформація zhyharevych.oksana@vnu.edu.ua
Дні занять <https://ps.vnu.edu.ua/cgi-bin/timetable.cgi>

III. Опис освітнього компонента

1. Анотація курсу

Організаційне забезпечення захисту інформації є одним із важливих розділів сучасних систем захисту інформації. Освітній компонент «Організаційне забезпечення захисту інформації» 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 шкідливого програмного забезпечення в системах інформаційної та кібербезпеки; аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування та вразливостей; обрання методів зберігання та ефективної обробки захищеної інформації.

2. 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.

3. Результати навчання.

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК 7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

СК 4. Здатність забезпечувати захист інформації інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК 5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)

СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

РН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

РН 3. Застосовувати принципи неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.

РН 4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН 5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН 11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

РН 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

РН 17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

РН 20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.

РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

Структура освітнього компонента.

Назви змістових модулів і тем	Усього	Лек.	Лабор.	Сам.		Форма
-------------------------------	--------	------	--------	------	--	-------

				роб.	Конс.	контролю/ Бали
Змістовий модуль 1. Зміст організаційного забезпечення захисту інформації						
Тема 1. Поняття та завдання організаційного забезпечення захисту інформації.	6	2	2	2		РЗ/К/ Звіт по лаб.р. 2 б.
Тема 2. Визначення інформаційних ресурсів, що підлягають захисту.	10	2	4	4		РЗ/К/ Звіт по лаб.р. 4 б.
Тема 3. Виявлення загроз безпеки інформаційним ресурсам та реагування на них.	11	2	4	4	1	РЗ/К/ Звіт по лаб.р. 4 б.
Тема 4. Організація забезпечення технічного захисту інформації.	9	2	2	4	1	РЗ/К/ Звіт по лаб.р. 4 б.
Тема 5. Організаційна робота із захисту інформації в країнах НАТО та ЄС.	8	2	2	4		РЗ/К/ Звіт по лаб.р. 2 б.
Разом за модулем 1	44	10	14	18	2	16
Змістовий модуль 2. Заходи з організації захисту бізнес-процесів						
Тема 1. Заходи з організації забезпечення захисту інформації в організаціях.	8	2	2	4		РЗ/К/ Звіт по лаб.р. 2 б.
Тема 2. Політика інформаційної безпеки.	10	2	2	6		РЗ/К/ Звіт по лаб.р. 4 б.
Тема 3. Підбір персоналу. Робота з персоналом.	10	2	2	6		РЗ/К/ Звіт по лаб.р. 2 б.
Тема 4. Організаційний захист інформації в комп'ютерних системах.	13	2	4	6	1	РЗ/К/ Звіт по лаб.р. 4 б.
Тема 5. Забезпечення захисту інформації при здійсненні міжнародного науково-технічного та економічного співробітництва.	11	2	2	6	1	РЗ/К/ Звіт по лаб.р. 4 б.
Разом за модулем 2	52	10	12	28	2	16
Змістовий модуль 3. Методологія наукових досліджень в галузі кібербезпеки						
Тема 1. Організація наукових дослідження в галузі кібербезпеки та захисту інформації.	10	2	2	4	2	РЗ/К/ Звіт по лаб.р. 2 б.

Тема 2. Підготовка та представлення наукових робіт в галузі кібербезпеки та захисту інформації.	14	2	4	6	2	РЗ/К/ Звіт по лаб.р. 6 б.
Разом за модулем 3	24	4	6	10	4	8
Види підсумкових робіт						Бал
Тестування						30
Контрольна робота 1						15
Контрольна робота 2						15
Всього годин/Балів		24	32	56	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. 12 год

Перевірка здійснюється під час лабораторних занять.

Підготовка до лабораторних занять, виконання домашніх завдань. 16 год

Перевірка здійснюється під час лабораторних занять.

Систематизація вивченого матеріалу перед контрольними заходами, тестуванням. 8 год

Перевірка здійснюється під час контрольних заходів, тестування.

Вивчення тем, що не розглядаються в курсі лекцій. 20 год

Перевірка здійснюється під час контрольних заходів і оцінюється відповідною кількістю балів.

№ з/п	Тема	Кількість годин
1	Аналіз і оцінка загроз інформаційної безпеки об'єкта щодо його організаційного забезпечення	4
2	Оцінка збитків внаслідок протиправного розкриття інформації обмеженого доступу і заходи щодо його локалізації	4
3	Основні міжнародні стандарти (наприклад, ISO/IEC 27001) та їхнє застосування в організаціях	4
4	Дослідження механізмів впливу на персонал, які використовують зловмисники, та способи підвищення обізнаності працівників	4
5	Забезпечення захисту інформації при здійсненні міжнародного науково-технічного та економічного співробітництва	4
		20

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 лабораторні заняття курсу. Кожен студент 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); посилення 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 “Організаційне забезпечення захисту інформації”, розміщеного на платформі дистанційного навчання Moodle, виконують всі домашні завдання. Прозвітуватися про виконання завдань можна, використовуючи дистанційний курс “Організаційне забезпечення захисту інформації”, 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 “Організаційне забезпечення захисту інформації” є залік. 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 “Організаційне забезпечення захисту інформації” визнання таких результатів навчання не проводиться.

Якщо за результатами семестру накопичено не менше 60 балів і студент погоджується із цим результатом, то оцінка за семестр може виставлятися без складання заліку. В іншому випадку студент складає залік; максимальна кількість балів, яку можна отримати на заліку – 100 балів. Вони замінюють бали модульного семестрового контролю, поточний семестровий контроль при цьому не зберігається.

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

Питання до заліку

1. Що таке організаційне забезпечення захисту інформації? Які основні завдання включає організаційне забезпечення захисту інформації?
2. Чим відрізняється організаційне забезпечення від технічного та правового захисту інформації?
3. Що таке інформаційні ресурси? Наведіть приклади.
4. Які критерії використовуються для визначення інформаційних ресурсів, що підлягають захисту?
5. Як класифікуються інформаційні ресурси залежно від рівня їхньої важливості?
6. Які основні види загроз існують для інформаційних ресурсів?
7. У чому полягає процес аналізу ризиків для інформаційних ресурсів?
8. Які методи реагування на загрози ви знаєте?
9. Які основні етапи організації технічного захисту інформації?
10. Які системи моніторингу використовуються для технічного захисту інформації?
11. Які принципи захисту інформації застосовуються в країнах НАТО?
12. Як реалізується співробітництво країн ЄС у сфері інформаційної безпеки?
13. Які є приклади стандартів або регламентів захисту інформації в країнах НАТО чи ЄС?
14. Які основні етапи розробки заходів із захисту інформації в організації?
15. Що таке аудит інформаційної безпеки, і як він впливає на організацію?
16. Як впроваджуються адміністративні заходи для захисту інформації?
17. Що таке політика інформаційної безпеки?
18. Які основні елементи повинні входити до політики інформаційної безпеки організації?
19. Яким чином забезпечується дотримання політики інформаційної безпеки?
20. Як здійснюється підбір персоналу для забезпечення інформаційної безпеки?
21. Які заходи спрямовані на підвищення обізнаності працівників щодо захисту інформації?
22. Що таке внутрішні загрози від персоналу, і як їх можна мінімізувати?
23. Які організаційні заходи застосовуються для захисту інформації в комп'ютерних системах?
24. Що таке розподіл доступу до ресурсів у комп'ютерних системах, і чому це важливо?
25. Як здійснюється моніторинг і управління доступом у комп'ютерних системах?
26. Які ризики виникають під час міжнародного обміну інформацією?

27. Як забезпечується конфіденційність і цілісність інформації в міжнародних проектах?
28. Що таке транснаціональні угоди про захист інформації, і як вони впливають на співробітництво?
29. Які напрямки досліджень є актуальними в галузі кібербезпеки?
30. Які інструменти використовуються для наукових досліджень у галузі кібербезпеки?
31. Які етапи підготовки наукової роботи з кібербезпеки є найважливішими?
32. Як правильно структурувати наукову роботу в галузі кібербезпеки?
33. Які особливості презентації результатів досліджень у сфері захисту інформації?
34. Як здійснюється ідентифікація та оцінка загроз інформаційної безпеки в організаційному середовищі?
35. Які основні етапи оцінки збитків від протиправного розкриття інформації та як здійснюється локалізація наслідків?
36. Які ключові вимоги стандарту ISO/IEC 27001, і як вони впроваджуються в організаціях?
37. Які методи соціальної інженерії використовуються зловмисниками, і як можна підвищити обізнаність працівників щодо цих загроз?
38. Які заходи забезпечення захисту інформації застосовуються під час міжнародного співробітництва?

VI. Шкала оцінювання

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

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. Кібервійна як різновид інформаційних війн. Захист кіберпростору України / Я. Дмитрук, Т. Гришанович, Л. Глинчук, О. Жигаревич. *Cybersecurity: Education, Science, Technique*. 2022. Т. 16, № 4. С. 28–36. DOI: <https://doi.org/10.28925/2663-4023.2022.16.2836>.

2. Когут Ю.І. Кібербезпека та ризики цифрової трансформації компаній. Практичний посібник. Київ: Консалтингова компанія «СІДКОН», 2021р. 370с.
3. Когут Ю.І. Кібервійни, кібертероризм, кіберзлочинність (концепції, стратегії, технології). Практичний посібник., Київ: Колсантингова компанія «СІДКОН»2022р. 281 с.
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.
5. Когут Ю.І. Корпоративна безпека: практичний посібник/Ю.І.Когут. Київ: Колсантингова компанія «СІДКОН», 2021. 460 с.
6. Смірнов С., Резніченко В. Організаційне забезпечення захисту інформації. Методичні рекомендації до виконання практичних робіт для студентів денної та заочної форми навчання за спеціальністю 125 «Кібербезпека». Кропивницький : Центральноукраїнський національний технічний університет, 2022 р. 88 с.

Додаткова література та Інтернет-ресурси

1. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник/ Київ: ООО "Д.В.К.", 2004. 758 с.
2. Калякін С. В., Онищенко Ю. М., Носов В. В. Кібербезпека міської інфраструктури. *Право і безпека*, 2023. №1(88). С. 190-202.
3. 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.
4. Holistic Info-Sec for Web Developers. *Holistic Info-Sec for Web Developers*. URL: <https://holisticinfosecforwebdevelopers.com> (date of access: 10.08.2024).
5. OWASP Web Security Testing Guide | OWASP Foundation. *OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation*. URL: <https://owasp.org/www-project-web-security-testing-guide/> (date of access: 12.08.2024).