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

Луцьк – 2024

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 затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

протокол № 4 від 21.11.2024 р.

Завідувач кафедри:  Гришанович Т. О.

І. Опис освітнього компонента

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітня програма</th><th>Характеристика освітнього компонента</th></tr>
<tr><td rowspan="2">Денна форма навчання</td><td rowspan="8">12 Інформаційні технології
125 Кібербезпека та захист інформації
бакалавр</td><td>Нормативна</td></tr>
<tr><td>Рік навчання 1</td></tr>
<tr><td rowspan="2">Кількість годин/кредитів 120/4</td><td>Семестр 2-ий.</td></tr>
<tr><td>Лекції 24 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: немає</td><td>Лабораторні 32 год.</td></tr>
<tr><td>Самостійна робота 56 год.</td></tr>
<tr><td>Консультації 8 год.</td></tr>
<tr><td>Форма контролю: залік</td></tr>
<tr><td colspan="2">Мова навчання: українська</td><td></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 https://ps.vnu.edu.ua/cgi-bin/timetable.cgi

ІІІ. 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.

4. 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. роб.	Конс.	Форма контролю/ Бали
Змістовий модуль 1. Основи організації захисту інформації						
Тема 1. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.		2	2			РЗ/К/ Звіт по лаб.р. 4 б.
Тема 2. Організаційна робота із захисту інформації в країнах НАТО та ЄС.		4	2			РЗ/К/ Звіт по лаб.р. 4 б.
Тема 3. Міжнародний стандарт з оцінювання безпеки інформаційних технологій (ISO/IEC 15408).		2	4			РЗ/К/ Звіт по лаб.р. 4 б.
Тема 4. Організаційна робота служби захисту інформації в автоматизованих системах.		2	4		2	РЗ/К/ Звіт по лаб.р. 4 б.
Тема 5. Технічні канали витоку інформації. Засоби технічної розвідки.		2	2		2	РЗ/К/ Звіт по лаб.р. 4 б.
Разом за модулем 1		12	14		4	**20**
Змістовий модуль 2. Організація захисту інформації в комп'ютерних системах						
Тема 1. Основні відомості про захист інформації в комп'ютерних системах.		2	2			РЗ/К/ Звіт по лаб.р. 4 б.
Тема 2. Загальні положення з організації якості реалізації заходів з ТЗІ.		2	4			РЗ/К/ Звіт по лаб.р. 4 б.
Тема 3. Організація та порядок контролю за функціонуванням системи ТЗІ в Україні.		2	4			РЗ/К/ Звіт по лаб.р. 4 б.
Тема 4. Основні засоби та механізми захисту інформації в комп'ютерних системах.		2	4			РЗ/К/ Звіт по лаб.р. 4 б.
Тема 5. Заходи з організації забезпечення захисту інформації на підприємствах.		4	4			РЗ/К/ Звіт по лаб.р. 4 б.
Разом за модулем 2		12	18		3	20
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 локалізаці	4
3	Підбір кадрів та робота з кадрами.	4
4	Захист інформації в мережі Інтернет.	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, загальноприйнятих 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); 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 "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 залік– 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 уміння синтезувати отриманні знання і застосовувати їх під час виконання практичних задач.

Питання до заліку

1.	Використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
2.	Побудова захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
3.	Задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом.
4.	Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
5.	Вирішувати задачі управління процедурами ідентифікації, аутентифікації, авторизації процесів і користувачів згідно кібербезпеки.
6.	Забезпечення функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
7.	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
8.	Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
9.	Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
10.	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки.

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.Довгопологo. 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. 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. *Holistic Info-Sec for Web Developers*. URL: https://holisticinfosecforwebdevelopers.com (date of access: 10.08.2024).

4. 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).