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 – 2023

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:  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 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: є</td><td>Лабораторні 30 год.</td></tr>
<tr><td>Самостійна робота 58 год.</td></tr>
<tr><td>Консультації 8 год.</td></tr>
<tr><td colspan="2">Мова навчання: українська</td><td>Форма контролю: залік</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

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; обирати методи зберігання та ефективні алгоритми обробки для відповідних структур даних для створення захищених програм.

2. Пререквізити: Базові знання із хмарних технологій, 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 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 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.
ЗК 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки.
ФК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
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 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) 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,	12	2	2	8		РЗ

телекомунікаційних та інформаційно-телекомунікаційних системах.						
Тема 2. Організаційна робота із захисту інформації в країнах НАТО та ЄС.	13	2	2	8	1	РЗ
Тема 3. Вивчення міжнародного стандарту з оцінювання безпеки інформаційних технологій (ISO/IEC 15408).	15	2	4	8	1	РЗ, РМГ
Тема 4. Вивчення організаційної роботи служби захисту інформації в автоматизованих системах.	15	2	4	8	1	РЗ
Тема 5. Технічні канали витоку інформації. Засоби технічної розвідки.	17	4	4	4	1	
Разом за модулем 1	72	12	16	36	4	**14**
Змістовий модуль 2. Організація захисту інформації в комп'ютерних системах						
Тема 1. Основні відомості прозахист інформації в комп'ютерних системах.	8	2	2	4		РЗ
Тема 2. Основи криптографічного захисту інформації.	11	2	4	4	1	РЗ
Тема 3. Організація та порядок контролю за функціонуванням системи ТЗІ в Україні.	11	2	4	4	1	РЗ
Тема 4. Загальні положення з організації якості реалізації заходів з ТЗІ.	9	2	2	4	1	РЗ
Тема 5. Основні засоби та механізми захисту інформації в комп'ютерних системах.	13	4	2	6	1	РЗ
Разом за модулем 2	53	12	14	22	4	26
Види підсумкових робіт						Бал
Тестування						25
Модульна контрольна робота						10
ІНДЗ 1						15
ІНДЗ 2						10
Всього годин/Балів	120	24	30	58	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 лабораторних занять, виконання домашніх завдань.

– Перевірка здійснюється під час лабораторних 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 заходів і оцінюється відповідною кількістю балів.

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

№ з/п	Тема	Кількість годин
1	Захист компонентів операційних систем.	4
2	Безпека комп'ютерних мереж.	4
3	Сучасні технології захисту комп'ютерних мереж.	4
4	Захист інформації в мережі Internet.	4
5	Криптографічні засоби захисту інформації в комп'ютерних системах.	4
6	Принципи генерації розподілу та збереження ключів.	4
7	Криптографія в сучасних комп'ютерних технологіях.	4
8	Сертифікація засобів захисту інформації.	6
9	Порядок експлуатації управління та супроводження систем захисту інформації в захищених комп'ютерних системах.	8
10	Оцінка захищеності обчислювальної техніки.	8
11		58

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); 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 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 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. Урядовий портал. Постанова Кабінету Міністрів України від 29 березня 2006 р. №373.
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. [Electronic resource]. – Access mode: https://holisticinfosecforwebdevelopers.com/
4. OWASP Web Security Testing Guide. [Electronic resource]. – Access mode : https://owasp.org/www-project-web-security-testing-guide/
5. Open Web Application Security Project [Електронний ресурс]. Режим доступу:
   a. www.owasp.org
6. Когут Ю.І. Кібербезпека та ризики цифрової трансформації компаній. Практичний посібник. Київ, 2021р.370с.
7. Кіберзахист Литви: https://kam.lt/en/cyber-security
8. Місія в Україні:https://therecord.media/cyber-command-sent-a-hunt-forward-team-to-help-lithuania-harden-its-systems/
9. Когут Ю.І. Кібервійни, кібертероризм, кіберзлочинність (концепції, стратегії, технології). Практичний посібник., Київ, 2022р.281с.
10. Когут Ю.І. Корпоративна безпека: практичний посібник/Ю.І.Когут. – Київ: Колсан-тингова компанія «СІДКОН», 2021. – 460 с.

Додаткова дітература та Інтернет-ресурси

1. Офіційний сайт Google, на якому розміщена документація по роботі 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. 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.