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
Сигнали та процеси в системах захисту інформації

підготовки бакалавра

спеціальності 125 Кібербезпека

освітньо-професійної програми Інформаційна безпека

Луцьк – 2022

Силабус навчальної дисципліни «Сигнали та процеси в системах захисту інформації**»** підготовки бакалавра, галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека, за освітньою програмою Інформаційні технології.

Розробник: Гаращенко 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 № 3 від 13 жовтня 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 2</td></tr>
<tr><td rowspan="2">Кількість годин/кредитів 135 / 4,5</td><td>Семестр 4-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 48 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: Гаращенко Володимир Вікторович
Науковий Вчене звання -
Посада старший викладач
Контактна інформація vg@socprime.com
Дні занять http://194.44.187.20/cgi-bin/timetable.cgi?n=700

ІІІ. Опис освітнього компонента

1. Анотація курсу

Основи захищених систем є одним із важливих розділів сучасних комп'ютерних наук. Освітній компонент «Сигнали та процеси в системах захисту інформації» належить до переліку нормативних навчальних дисциплін програми підготовки бакалавра за спеціальністю 125 «Кібербезпека», забезпечує професійний розвиток бакалавра та спрямована на формування у майбутніх фахівців базових знань, вмінь та навичок вивчення методів технологій безпечного захисту інформації в системах інформаційної та кібербезпеки; виконувати 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 організація та захисту 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: надання теоретичних знань та формування практичних навичок щодо дослідження безпечного програмування 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 5. Здатність до пошуку, оброблення та аналізу інформації.
ФК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
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 кібербезпеки.
ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

ПРН36. Виявляти небезпечні сигнали технічних засобів.
ПРН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.

Структура освітнього компонента.

Назви змістових модулів і тем	**Усього**	**Лек.**	**Лабор.**	**Сам. роб.**	**Конс.**	**Форма контролю/ Бали**
Змістовий модуль 1. Властивості інформації як об'єкта захисту.						
Тема 1. ВИДИ, ДЖЕРЕЛА ТА НОСІЇ ІНФОРМАЦІЇ, ЩО ПІДЛЯГАЄ ЗАХИСТУ 1. Поняття цінності та ціни інформації. 2. Складові ціни інформації. 3. Види, джерела та носії інформації, що підлягає захисту. Класифікація демаскуючих ознак об'єктів захисту. 4. Демаскуючі ознаки	12	2	2			РЗ

сигналів.						
Тема 2. НЕБЕЗПЕЧНІ СИГНАЛИ ТА ЇХ ДЖЕРЕЛА 1. Поняття небезпечного сигналу. 2. Види побічних небезпечних електромагнітних випромінювань. 3. Небезпечні сигнали, що утворюються в результаті 4. акустоелектичних перетворень. 5. Низько - та високочастотні випромінювання.	13	2	2	4	1	РЗ
Тема 3. ТЕХНІЧНА РОЗВІДКА 1. Поняття та принципи технічної розвідки. 2. Основні задачі та ограни технічної розвідки. 3. Види технічної розвідки. Поняття промислового шпигунства. 4. Законні та незаконні методи добування конфіденційної інформації про діяльність конкурентів. Контррозвідувальна діяльність. 5. Комплексний захист конфіденційної інформації, його види. 6. Пасивні та активні методи захисту конфіденційної інформації.	15	2	4	4	1	РЗ, РМГ
Тема 4. КОНЦЕПЦІЯ І МЕТОДИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ. 1. Комплексне застосування методів захисту. 2. Основні напрямки інженерно-технічного захисту інформації. 3. Методи фізичного захисту інформації.	15	2	4	4	1	РЗ
Тема 5. Класифікація засобів виявлення та локалізації заклад-	17	4	4	2	1	

них пристроїв. 1. Методи та засоби виявлення випромінювання закладних пристроїв. 2. Методи та засоби виявлення не випромінюючих закладних пристроїв.						
Разом за модулем 1	69	32	16	14	4	**14**
Змістовий модуль 2. Протидії спостереженню в оптичному діапазоні.						
Тема 1. МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ВІД СПОСТЕРЕЖЕННЯ ТА ПІДСЛУХОВУВАННЯ. 1. Енергетичне приховування акустичного сигналу. 2. Засоби звукоізоляції та звукопоглинання. 3. Класифікація засобів виявлення та локалізації закладних пристроїв.	12	2	2	8		РЗ
Тема 2. ЗАСОБИ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ ПОБІЧНІ ЕЛЕКТРОМАГНІТНІ ВИПРОМІНЮВАННЯ. 1. Придушення небезпечних сигналів акустоелектричних перетворювачів. 2. Екранування електромагнітних полів. 3. Запобігання витоку інформації по ланцюгам електроживлення.	15	2	4	8	1	РЗ
Тема 3. МЕТОДИ І ЗАСОБИ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В КАНАЛАХ ЗВ'ЯЗКУ 1. Структурне приховування мовної інформації в каналах зв'язку. 2. Засоби контролю телефонних ліній. 3. Перехват повідомлень в GSM каналах. 4. Будова та основні технічні характеристиками аналізаторів телефон-	15	2	4	8	1	РЗ

них ліній.						
Тема 4. СИСТЕМИ ТЕХНІЧНОЇ ОХОРОНИ ОБ'ЄКТІВ. 1. Класифікація засобів інженерного захисту об'єктів. 2. Системи охорони периметра та простору контрольованої території. 3. Класифікація ідентифікаційних карт, як засобів атрибутивних ідентифікаторів людей.	15	2	4	8	1	РЗ
Тема 5. МЕТОДИ І ЗАСОБИ ТЕХНІЧНОЇ ОХОРОНИ ОБ'ЄКТІВ. СИСТЕМИ СИГНАЛІЗАЦІЇ ТА ВІДЕО СПОСТЕРЕЖЕННЯ. 1. Системи телевізійного спостереження. 2. Засоби телевізійної охорони. 3. Основні характеристики відеокамер. 4. Засоби запису та реєстрації зображення. 5. Класифікація систем відеоспостереження.	13	4	4	4	1	РЗ
Разом за модулем 2	66	12	18	32	4	26
Види підсумкових робіт						Бал
Тестування						25
Модульна контрольна робота						10
ІНДЗ 1						15
ІНДЗ 2						10
Всього годин/Балів	135	34	34	48	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	Наведіть типи математичних моделей сигналів і поясніть їх призначення.	4
2	У чому полягає цифрова обробка сигналів?	4
3	Як вибрати частоту дискретизації безперервного в часі сигналу?	4
4	Дайте визначення частотного спектра сигналу.	4
5	Для яких цілей використовують цифрові фільтри?	4
6	Дайте визначення вейвлет-перетворення.	4
7	Чим відрізняється вейвлет-перетворення від дискретного перетворення Фур'є?	4
8	Поясніть принцип вимірювання дальності радаром (ближня і дальня локація).	4
9	Як визначити дальність до цілі, використовуючи дискретне перетворення Фур'є ?	4
10	Як визначити дальність до цілі, використовуючи вейвлет-перетворення?	12
11		48

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 “ Сигнали та процеси в системах захисту інформації”, 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 “Сигнали та процеси в системах захисту інформації”, розміщеного на платформі дистанційного навчання Moodle, виконують всі домашні завдання. Прозвітуватися про виконання завдань можна, використовуючи дистанційний курс “ Сигнали та процеси в системах 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 “Сигнали та процеси в системах захисту інформації ” 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 “Сигнали та процеси в системах захисту інформації ” 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 "Сигнали та процеси в системах захисту інформації" 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

1. Поняття і класифікація видів та методів несанкціонованого доступу.
2. Визначення і модель зловмисника.
3. Управління віддаленим доступом.
4. Класифікація способів захисту інформації в комп'ютерних системах.
5. Організація захисту інформації.
6. Фізичні методи захисту інформації.
7. Законодавчі методи захисту інформації.
8. Криптографічні методи захисту інформації.
9. Види та класифікація умисних загроз безпеки інформації.
10. Безпека використання технологій оптоволоконних кабельних систем.
11. Особливості комп'ютерних мереж, як каналів скачування інформації.
12. Криптографічний методом приховання інформації.

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. Jeremiah Grossman. XSS Attacks CROSS SITE SCRIPTING EXPLOITS AND DEFENSE. – USA.: Amazon DS, 2018 – 630 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. / Л.
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: www.owasp.org
6. Топ-10 OWASP-2017 Десять самых критичных угроз безопасности веб-приложений. [Електронний ресурс] – Режим доступу: https://owasp.org/www-pdf-archive/OWASP_Top_10- 2017-ru.pdf

1. Когут Ю.І. Кібербезпека та ризики цифрової трансформації компаній. Практичний посібник. Київ, 2021р.370с.
2. Кіберзахист Литви: https://kam.lt/en/cyber-security
3. Місія в Україні:https://therecord.media/cyber-command-sent-a-hunt-forward-team-to-help-lithuania-harden-its-systems/
4. Когут Ю.І. Кібервійни, кібертероризм, кіберзлочинність (концепції, стратегії, технології). Практичний посібник., Київ, 2022р.281с.
5. Когут Ю.І. Корпоративна безпека: практичний посібник/Ю.І.Когут. – Київ: Колсантингова компанія «СІДКОН», 2021. – 460 с.
6. Пасічник В.В., Пасічник О.В., Угрин Д.І. Веб-технології. [Текст] : підручник / Львів : «Магнолія2006», 2018. – 336 с.
7. 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
8. 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 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. 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.