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
Системи моніторингу загроз
підготовки бакалавра

спеціальності 125 Кібербезпека та захист інформації

освітньо-професійної програми Кібербезпека та захист інформації

Луцьк – 2023

Силабус навчальної дисципліни «Системи моніторингу загроз» підготовки бакалавра, галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека та захист інформації, за освітньою програмою Кібербезпека та захист інформації.

Розробник: Гаращенко В.В., 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 вересня 2023 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="7">12 Інформаційні технології

125 Кібербезпека та захист інформації

Інформаційна безпека</td><td>Нормативна</td></tr>
<tr><td>Рік навчання 2</td></tr>
<tr><td rowspan="2">Кількість годин/кредитів 120/4</td><td>Семестр 4-ий</td></tr>
<tr><td>Лекції 40 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: є</td><td>Лабораторні 54 год.</td></tr>
<tr><td>Самостійна робота 18 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 : 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

Системи моніторингу загроз є одним із важливих розділів сучасних систем захисту інформації. Освітній компонент «Системи моніторингу загроз» 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, розпізнавання шкідливого програмного забезпечення 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 хмарних технологій, програмування, організаційне забезпечення захисту інформації.

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 моніторингу загроз 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 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки.
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 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.
ПРН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

Структура освітнього компонента.

Назви змістових модулів і тем	**Усього**	**Лек.**	**Лабор.**	**Сам. роб.**	**Конс.**	**Форма контролю/ Бали**
Змістовий модуль 1. Основи моніторингу та особливості систем моніторингу						
Тема 1. Основні поняття: "моніторинг", "системи моніторингу", схема моніторингу. Складові системи моніторингу, рівні забезпечення моніторингу, структура АІС моніторингу.	9	4	4	1		РЗ
Тема 2. Сутність моніторингу в окремих сферах діяльності.Класифікація систем моніторингу.	11	4	4	2	1	РЗ
Тема 3. Функції, задачі та принципи моніторингу. Аналітика моніторингу організації. Інформаційно-технологія.	13	4	6	2	1	РЗ, РМГ

Тема 4. Побудова, функціонування, та оцінювання моніторингу.	13	4	6	2	1	РЗ
Тема 5. Спеціалізовані системи моніторингу.	15	6	6	2	1	
Разом за модулем 1	61	22	26	9	4	**14**
Змістовий модуль 2. Моніторинг ІТ та приклади систем моніторингу загроз						
Тема 1. Моніторинг інформаційних технологій. Приклади систем моніторингу.	7	2	4	1		РЗ
Тема 2. Класифікація загроз безпеки та види загроз інформаційній безпеці.	13	4	6	2	1	РЗ
Тема 3. Системи моніторингу та управління безпекою: SIEM- 15 системи.	13	4	6	2	1	РЗ
Тема 4. Модель загроз в розподілених мережах. Загрози інформаційної безпеки держави в соціальних мережах.	13	4	6	2	1	РЗ
Тема 5. Системи моніторингу у різних сферах.	13	4	6	2	1	РЗ
Разом за модулем 2	59	18	28	9	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 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	Захист від кібератак і внутрішніх загроз зі SPLUNK USER BEHAVIOR ANALYTICS.	2
2	Механізми підвищення ефективності процедури моніторингу безпеки в розподілених базах даних.	2
3	Нормативно-правове регулювання моніторингу в Україні. Архітектура та розвиток систем моніторингу інфраструктури ІТ.	2
4	Nagios – найвідоміший інструмент для моніторингу ІТ- інфраструктур, в тому числі робочих станцій кінцевого користувача, ІТ-сервісів і активних мережевих компонентів.	2
5	Hyperic (проект компанії VMware) – система моніторингу та адміністрування для віртуальних середовищ.	2
6	Системи моніторингу: HP Operations Manager, ManageEngine OpManager, SolarWinds, IBM Tivoli, WhatsUp Gold.	2
7	Zabbix – моніторинг серверів, мережевих пристроїв і додатків зі збором детальної статистики, що стосується продуктивності.	2
8	Базові інструменти роботи з журналами реєстрацій подій безпеки та лог файлами. Цифрова трансформація та кібербезпека.	2
9	Шкідливе програмне забезпечення. Поширення під час війни.	2
10		18

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 практичні 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 "Система моніторингу загроз", розміщеного на платформі дистанційного навчання Moodle, виконують всі домашні завдання. Прозвітуватися про виконання завдань можна, використовуючи дистанційний курс " Система моніторингу загроз ", 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 " Система моніторингу загроз " 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.

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.

синтезувати отриманні знання і застосовувати їх під час виконання практичних задач.

Питання до заліку

1. Основні питання: "моніторинг", "системи моніторингу".
2. Схема та об'єкти моніторингу.

3. Складові системи моніторингу.
4. Рівні забезпечення моніторингу.
5. Структура АІС моніторингу.
6. Сутність моніторингу в окремих сферах діяльності.
7. Класифікація систем моніторингу.
8. Функції моніторингу.
9. Задачі моніторингу.
10. Принципи організації моніторингу.
11. Інформаційно-аналітична технологія моніторингу.
12. Побудова та функціонування моніторингу.
18. Моніторинг загроз в умовах війни.
13. Система моніторингу загроз національній безпеці.
14. Система моніторингу загроз економічній безпеці.
15. Система моніторингу загроз соціальній безпеці.
16. Загрози інформаційної безпеки держави в соціальних мережах.
17. Модель загроз в розподілених мережах.
18. Системи моніторингу безпеки: SIEM-системи.
19. Види загроз інформаційній безпеці.
20. Класифікація загроз безпеки.
21. Спеціалізовані системи моніторингу: банківський моніторинг. 22. Спеціалізовані системи моніторингу: моніторинг науково технічного потенціалу.
23. Оцінювання моніторингу.
24. Моніторинг загроз перед початком війни в Україні.

25. Спеціалізовані системи моніторингу: система моніторингу, інвестиційної активності.
26.Моніторинг у сфері управління ІТ.
27. Вимоги до систем моніторингу ІТ.
28. Технологія проведення моніторингу ІТ
29. Засоби підтримки процесу моніторингу ІТ.
30. Інші системи моніторингу загроз.

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. 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.
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.