СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ІНЦИДЕНТАМИ В СИСТЕМАХ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ»

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="2">Рижаков Микола Миколайович,
доктор філософії,
старший викладач Технічних систем кіберзахисту</td><td colspan="2">Контактна інформація лектора (e-mail), сторінка курсу в GWE</td><td colspan="2">e-mail: m.ryzhakov@duikt.edu.ua
сторінка курсу в Classroom:
https://classroom.google.com/c/ODU5NDI5OTk5MjEw?cjc=wtfryvay
код доступу – wtfryvay</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="2">12 Інформаційні технології</td><td colspan="2">Рівень вищої освіти</td><td colspan="2">Магістр</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="2">F5 Кібербезпека та захист інформації</td><td colspan="2">Семестр</td><td colspan="2">1</td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="2">Кібербезпека</td><td colspan="2">Тип дисципліни</td><td colspan="2">Цикл вибіркових компонент ОНП</td></tr>
<tr><td rowspan="2">Обсяг:</td><td>Кредитів ECTS</td><td>Годин</td><td colspan="6">За видами занять:</td></tr>
<tr><td>5</td><td>150</td><td>Лекцій
24</td><td>Семінарських занять
-</td><td>Практичних занять
18</td><td>Лабораторних занять
12</td><td colspan="2">Самостійна підготовка
96</td></tr>
<tr><td colspan="9">АНОТАЦІЯ КУРСУ</td></tr>
<tr><td colspan="9">Взаємозв’язок у структурно-логічній схемі</td></tr>
<tr><td colspan="3">Освітні компоненти, які передують вивченню</td><td colspan="6">Методи та засоби технічного захисту інформації; комплексні системи захисту інформації; управління інформаційною безпекою; основи кібербезпеки.</td></tr>
<tr><td colspan="3">Освітні компоненти для яких є базовою</td><td colspan="6">Переддипломна практика; кваліфікаційна робота магістра; проєктування процесів захисту інформації та реагування на інциденти</td></tr>
<tr><td>Мета курсу:</td><td colspan="8">формування здатності магістрів планувати, організовувати, здійснювати та оцінювати процес управління інформаційними інцидентами в системах технічного захисту інформації з урахуванням ризиків, нормативних вимог, доказової бази, комунікацій та відновлення функціонування об'єкта захисту.</td></tr>
<tr><td colspan="9">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="4">Soft-skills / Загальні компетентності (ЗК)</td><td colspan="5">Hard-skills / Спеціальні компетентності (СК)</td></tr>
<tr><td colspan="4">ЗК-1. Здатність до системного аналізу складних проблем у сфері кібербезпеки та захисту інформації.
ЗК-2. Здатність приймати обґрунтовані рішення в умовах неповної визначеності.
ЗК-3. Здатність працювати в команді, організовувати професійну комунікацію та ескалацію.
ЗК-4. Здатність дотримуватися норм академічної доброчесності, права та професійної етики.</td><td colspan="5">СК-1. Здатність виявляти, класифікувати та оцінювати інформаційні інциденти в системах ТЗІ.
СК-2. Здатність розробляти політики, плани реагування, playbook-и та процедури ескалації.
СК-3. Здатність організовувати локалізацію, усунення причин інциденту та відновлення систем.
СК-4. Здатність аналізувати журнали подій, телеметрію, технічні канали витоку та цифрові докази.
СК-5. Здатність готувати технічну, управлінську та нормативну звітність за результатами інциденту.
СК-6. Здатність удосконалювати систему ТЗІ на основі уроків інцидентів і метрик ефективності.</td></tr>
<tr><td colspan="9">Програмні результати навчання (ПРН)</td></tr>
<tr><td colspan="9">ПРН-1. Ідентифікувати події безпеки та визначати, чи мають вони ознаки інформаційного інциденту.
ПРН-2. Розробляти класифікатор інцидентів, матрицю критичності та порядок ескалації для систем ТЗІ.
ПРН-3. Застосовувати методи тріажу, аналізу журналів, фіксації доказів і документування перебігу реагування.
ПРН-4. Планувати локалізацію, усунення причин, відновлення та перевірку захищеності після інциденту.</td></tr>
</table>

ПРН-5. Готувати технічні звіти, управлінські резюме та рекомендації щодо запобігання повторенню інцидентів.
ПРН-6. Аргументовано презентувати рішення щодо реагування, враховуючи правові, етичні та організаційні обмеження.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Тема 1: «Основи управління інформаційними інцидентами в системах ТЗІ». **Знати**: поняття інформаційного інциденту, життєвий цикл реагування, класифікацію та нормативну базу. **Вміти**: будувати базовий класифікатор інцидентів та визначати ролі реагування. **Формування компетентностей:** ЗК-1-ЗК-4, СК-1-СК-6. **Результати навчання:** ПРН-1-ПРН-6. **Рекомендовані джерела:** 1-10.			
Інформаційний інцидент у системах ТЗІ.	Лекція 1 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Розроблення класифікатора інформаційних інцидентів для об'єкта ТЗІ.	Практичне заняття 1 2 год	4 бали	Практичне завдання, короткий звіт, захист результатів.
Нормативно-методична база.	Лекція 2 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Побудова матриці ролей, відповідальності та ескалації під час реагування.	Практичне заняття 2 2 год	4 бали	Практичне завдання, короткий звіт, захист результатів.
Організація процесу реагування.	Лекція 3 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Налаштування журналювання та збір подій для виявлення інформаційних інцидентів.	Лабораторна робота 1 2 год	2 бали	Лабораторне моделювання, робота з журналами подій, оформлення звіту.
Аналіз тестового набору журналів подій: пошук ознак компрометації та витоку інформації.	Лабораторна робота 2 2 год	2 бали	Лабораторне моделювання, робота з журналами подій, оформлення звіту.
Тема 1: «Основи управління інформаційними інцидентами в системах ТЗІ».	Самостійна робота 1 24 год	3 балів	Самостійна підготовка за джерелами, оформлення матеріалів до захисту.
Тема 2: «Підготовка, моніторинг і первинна аналітика». **Знати:** склад плану реагування, джерела телеметрії, методи виявлення та тріажу. **Вміти**: описувати джерела даних, оцінювати критичність події та обґрунтовувати ескалацію. **Формування компетентностей:** ЗК-1-ЗК-4, СК-1-СК-6. **Результати навчання:** ПРН-1-ПРН-6. **Рекомендовані джерела:** 5-18.			
Підготовка до реагування.	Лекція 4 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.

Опис джерел телеметрії та журналювання для виявлення інцидентів.	Практичне заняття 3 2 год	4 бали	Практичне завдання, короткий звіт, захист результатів.
Моніторинг і виявлення інцидентів.	Лекція 5 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Первинний аналіз події безпеки: тріаж, пріоритет, межі інциденту.	Практичне заняття 4 2 год	4 бали	Практичне завдання, короткий звіт, захист результатів.
Тріаж, класифікація та пріоритизація.	Лекція 6 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Побудова правил виявлення та матриці критичності у навчальному SIEM-сценарії.	Лабораторна робота 3 2 год	4 бали	Лабораторне моделювання, робота з журналами подій, оформлення звіту.
Тема 2: «Фрагмент плану реагування: ролі, ескалація, канали комунікації, контрольні списки».	Самостійна робота 2 24 год	3 балів	Самостійна підготовка за джерелами, оформлення матеріалів до захисту.
Тема 3: «Операційне реагування на інциденти». **Знати:** методи локалізації інцидентів доступу, витоку інформації та порушення роботи систем. **Вміти**: формувати playbook-и реагування та документувати дії команди. **Формування компетентностей:** ЗК-1-ЗК-4, СК-1-СК-6. **Результати навчання:** ПРН-1-ПРН-6. **Рекомендовані джерела:** 5-18.			
Реагування на несанкціонований доступ.	Лекція 7 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Playbook реагування на несанкціонований доступ або компрометацію облікового запису.	Практичне заняття 5 2 год	4 бали	Практичне завдання, короткий звіт, захист результатів.
Інциденти витоку інформації технічними каналами.	Лекція 8 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Playbook реагування на витік інформації технічними каналами.	Практичне заняття 6 2 год	4 бали	Практичне завдання, короткий звіт, захист результатів.
Локалізація, усунення та відновлення.	Лекція 9 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
План локалізації, усунення та відновлення після інциденту.	Практичне заняття 7 2 год	4 бали	Практичне завдання, короткий звіт, захист результатів.
Моделювання інциденту несанкціонованого доступу та виконання дій локалізації	Лабораторна робота 4 2 год	2 год 2 бали	Лабораторне моделювання, робота з журналами подій, оформлення звіту
Моделювання інциденту витоку інформації технічним каналом та фіксація доказів	Лабораторна робота 5	2 год 2 бали	Лабораторне моделювання, робота з журналами подій, оформлення звіту

	2 год		
Тема 3: «Аналіз методів виявлення інцидентів у системах ТЗІ та карта джерел телеметрії».	Самостійна робота 3 24 год	3 балів	Самостійна підготовка за джерелами, оформлення матеріалів до захисту.
Тема 4: «Відновлення, звітність і вдосконалення системи ТЗІ». **Знати:** порядок відновлення, chain of custody, post-incident review, метрики ефективності. **Вміти**: готувати звіт, аналізувати першопричини та пропонувати коригувальні заходи. **Формування компетентностей:** : ЗК-1-ЗК-4, СК-1-СК-6. **Результати навчання:** ПРН-1-ПРН-6. **Рекомендовані джерела:** 5-18.			
Докази, журналювання та звітність	Лекція 10 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Підготовка технічного звіту та управлінського резюме за результатами інциденту.	Практичне заняття 8 2 год	4 бали	Практичне завдання, короткий звіт, захист результатів.
Аналіз причин та вдосконалення системи ТЗІ	Лекція 11 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Комплексна tabletop-вправа з управління інформаційним інцидентом.	Практичне заняття 9 2 год	4 бали	Практичне завдання, короткий звіт, захист результатів.
Комплексна програма управління інцидентами	Лекція 12 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Захист індивідуальної моделі процесу управління інцидентами для об'єкта ТЗІ.	Лабораторна робота 6 2 год	2 год 2 бали	Лабораторне моделювання, робота з журналами подій, оформлення звіту.
Тема 4: «Індивідуальний звіт за кейсом інциденту: причини, вплив, реагування, уроки.».	Самостійна робота 3 24 год	3 балів	Самостійна підготовка за джерелами, оформлення матеріалів до захисту.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Комп'ютерний клас або персональні комп'ютери здобувачів, мультимедійний проєктор, мережа Інтернет.
Віртуальне навчальне середовище Google Workspace / Google Classroom.
Тестові набори журналів подій, шаблони incident response plan, playbook, звіту та post-incident review.
Навчальні або демонстраційні засоби моніторингу та реагування: Wazuh, Elastic Stack, Zeek, Suricata, журнали Windows/Linux, DLP/SIEM-подібні події.
Нормативні документи з кібербезпеки, захисту інформації та технічного захисту інформації.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. ISO/IEC 27035-1:2023. Information technology - Information security incident management - Part 1: Principles and process. https://www.iso.org/standard/78973.html
2. ISO/IEC 27035-2:2023. Information technology - Information security incident management - Part 2: Guidelines to plan and prepare for incident response. https://www.iso.org/standard/78974.html
3. ISO/IEC 27035-3:2020. Information technology - Information security incident management - Part 3: Guidelines for ICT incident response operations. https://www.iso.org/standard/74033.html
4. NIST SP 800-61 Rev. 3. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. 2025. https://doi.org/10.6028/NIST.SP.800-61r3

5. NIST CSWP 29. The NIST Cybersecurity Framework (CSF) 2.0. 2024. https://doi.org/10.6028/NIST.CSWP.29
6. Закон України «Про основні засади забезпечення кібербезпеки України». https://zakon.rada.gov.ua/
7. Закон України «Про захист інформації в інформаційно-комунікаційних системах». https://zakon.rada.gov.ua/
8. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
9. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
10. FIRST. CSIRT Services Framework. https://www.first.org/standards/frameworks/csirts/
11. ENISA. Good Practice Guide for Incident Management. https://www.enisa.europa.eu/
12. MITRE ATT&CK. Enterprise Matrix and Knowledge Base. https://attack.mitre.org/
13. Wazuh Documentation. Security monitoring and incident response. https://documentation.wazuh.com/
14. Elastic Security Documentation. Detection and response workflows. https://www.elastic.co/guide/
15. The DFIR Report. Incident reports and threat actor tradecraft examples. https://thedfirreport.com/
16. CERT-UA. Повідомлення та рекомендації щодо кіберінцидентів. https://cert.gov.ua/.

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі, аналіз реалістичних кейсів та аргументований захист прийнятих рішень.
- Середовище в аудиторії є відкритим до конструктивної критики, професійної дискусії та коректного обговорення помилок реагування.
- Освоєння дисципліни передбачає відвідування лекцій, практичних і лабораторних занять, а також системну самостійну роботу.
- Усі завдання мають бути виконані у встановлений термін. У разі поважної причини відсутності здобувач погоджує з викладачем порядок відпрацювання.
- Під час виконання завдань потрібно посилатися на використані джерела, не розголошувати чутливі дані та дотримуватися правил академічної доброчесності.

КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є набрання здобувачем 60 балів у сукупності за всіма темами дисципліни.

Форми контролю	**Види навчальної роботи**	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	• Виконання практичних робіт	36 балів
	• Виконання лабораторних робіт	12 балів
	• Самостійна робота	12 балів
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Залік***	Метою *заліку* є контроль сформованості практичних навичок та професійних компетентностей.	40 балів

Додаткова оцінка

Види навчальної роботи	**Оцінювання**
Участь у наукових конференціях, підготовка наукових публікацій за тематикою освітньої компоненти:	
- тези доповіді на фаховій конференції;	2 бали
- стаття у фаховому виданні України;	6 балів
- стаття в іноземному рецензованому виданні.	10 балів

Максимальна кількість додаткових балів, які можуть бути зараховані здобувачу освіти – 10 балів.

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

БАЛИ	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка /** *запис в заліковій відомості*
90-100	Здобувач демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає силабусу дисципліни, правильно й обґрунтовано приймає рішення в різних нестандартних ситуаціях управління інформаційними інцидентами. Вміє реалізувати теоретичні положення дисципліни у практичних завданнях: класифікує інциденти, визначає критичність, формує порядок ескалації, обирає	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, визначених силабусом дисципліни. Власні пропозиції здобувача щодо оцінювання	Відмінно / Зараховано (A)

	заходи локалізації, відновлення та післяінцидентного вдосконалення системи ТЗІ. Знає сучасні підходи ISO/IEC 27035, NIST SP 800-61 Rev. 3, NIST CSF 2.0, принципи роботи SOC/CSIRT, вимоги до журналювання, доказів і звітності. Під час практичних і лабораторних робіт самостійно розв'язує поставлені завдання, активно бере участь у дискусіях, аргументує власну позицію та здатний захищати прийняті рішення.Зменшення 100-бальної оцінки може бути пов'язане з неповним розкриттям окремих питань, які виходять за межі основного обсягу курсу, або з невпевненістю у тлумаченні складних практичних ситуацій.	інцидентів, удосконалення процесів реагування та підвищення ефективності системи ТЗІ демонструють здатність використовувати знання, отримані під час вивчення цієї та суміжних дисциплін.	
82-89	Здобувач демонструє гарні знання, добре володіє матеріалом, що відповідає силабусу дисципліни, робить на його основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення під час вирішення практичних задач управління інцидентами, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи виявлення, тріажу, локалізації, документування й аналізу причин інцидентів. Під час виконання практичних і лабораторних завдань дає вичерпні пояснення щодо прийнятих рішень, однак окремі висновки можуть потребувати уточнення або додаткового обґрунтування.	**Достатній** Забезпечує здобувачу самостійне вирішення основних практичних задач в умовах, коли вихідні дані змінюються порівняно з прикладами, що розглядались під час вивчення дисципліни. Здатний адаптувати типові playbook-и та процедури реагування до конкретного об'єкта ТЗІ.	Добре / Зараховано (B)
75-81	Здобувач загалом добре володіє матеріалом, знає основні положення курсу, робить на їх основі аналіз можливих ситуацій та вміє застосовувати їх під час вирішення типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні етапи виконаних завдань, визначити категорію інциденту, запропонувати порядок реагування, підготувати базовий звіт і дати правильні відповіді у разі зміни вихідних параметрів. Помилки у відповідях, рішеннях або висновках не є системними. Знає характеристики основних процесів, що мають визначальне значення для управління інформаційними інцидентами в системах ТЗІ.	**Достатній** Конкретний рівень за вивченим матеріалом силабусу дисципліни. Додаткові питання щодо використання теоретичних положень у нестандартних практичних ситуаціях можуть викликати утруднення, однак основні задачі курсу виконуються.	Добре / Зараховано (C)
67-74	Здобувач засвоїв основний теоретичний матеріал, передбачений силабусом дисципліни, та розуміє постановку стандартних практичних завдань. Має пропозиції щодо напрямів їх вирішення, розуміє основні положення, що є визначальними в курсі, може виконувати подібні завдання до тих, що розглядалися з викладачем.Під час аналізу інцидентів, заповнення шаблонів звітності, побудови матриці критичності або опису процедури ескалації допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача. .	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни. Здобувач здатний виконувати типові завдання за наданим алгоритмом, але потребує підтримки під час аналізу складних або неповних вихідних даних.	Задовільно / Зараховано (D)
60-66	Здобувач має певні знання, передбачені силабусом дисципліни, володіє основними положеннями на рівні, який визначається як мінімально допустимий. З використанням базових теоретичних положень з труднощами пояснює правила вирішення практичних, лабораторних або розрахунково-аналітичних завдань. Виконання практичних, лабораторних та індивідуальних завдань значною мірою формалізоване: є відповідність запропонованому алгоритму, але відсутнє глибоке розуміння взаємозв'язків між виявленням, тріажем, локалізацією, відновленням, документуванням і післяінцидентним аналізом.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни. Здобувач може відтворити базовий порядок дій під час реагування, але не демонструє достатньої самостійності в обґрунтуванні рішень.	Задовільно / Зараховано (E)

35-59	Здобувач може відтворити окремі фрагменти з курсу. Незважаючи на те, що окремі завдання навчальної дисципліни виконувались, працював пасивно, відповіді під час практичних і лабораторних робіт у більшості випадків є неповними, невірними або необґрунтованими. Цілісність розуміння матеріалу з дисципліни відсутня. Здобувач не може самостійно визначити критичність інциденту, послідовність реагування, вимоги до доказів, структуру звіту або заходи післяінцидентного вдосконалення системи ТЗІ.	**Низький** Не забезпечує практичної реалізації задач, що формуються під час вивчення дисципліни. Знання мають фрагментарний характер і не дозволяють виконувати професійні завдання без повторного опрацювання матеріалу.	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*
0-34	Здобувач повністю не виконав вимог силабусу навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними або відсутніми. Практичні, лабораторні та самостійні завдання не виконані або виконані на рівні, що не дозволяє оцінити сформованість результатів навчання. Здобувач не допущений до складання заліку або не може продемонструвати мінімально необхідні знання щодо управління інформаційними інцидентами в системах ТЗІ.	**Незадовільний** Здобувач не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни. Потребує повторного вивчення навчального матеріалу.	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) *В залікову книжку не проставляється*

ПОЛІТИКА ДОБРОЧЕСНОСТІ

Здобувач вищої освіти виконуючи самостійну або індивідуальну роботу повинен дотримуватись політики доброчесності.

У разі наявності плагіату в будь-яких видах робіт здобувача, він отримує незадовільну оцінку і повинен повторно виконати завдання, які передбачені у Силабусі.