СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«АНАЛІЗ ЕФЕКТИВНОСТІ СИСТЕМ КІБЕРНЕТИЧНОГО ЗАХИСТУ»

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="2">Рижаков Микола Миколайович, PhD, ст. викладач кафедри технічних систем кіберзахисту</td><td>Контактна інформація лектора (e-mail), сторінка курсу в GWE</td><td colspan="2">e-mail: m.ruzhakov@duikt.edu.ua
сторінка курсу в Classroom: https://classroom.google.com/c/Nzk0MDk1MTYyNjA2?cjc=6bqzpimg
код доступу – 6bqzpimg</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="2">12 Інформаційні технології</td><td>Рівень вищої освіти</td><td colspan="2">Магістр</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="2">Кібербезпека</td><td>Семестр</td><td colspan="2">1,2</td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="2">Технічні системи інформаційного та кібернетичного захисту</td><td>Тип дисципліни</td><td colspan="2">Вибіркова компонента освітньо-наукової програми</td></tr>
<tr><td rowspan="2">Обсяг:</td><td>Кредитів ECTS</td><td>Годин</td><td colspan="5">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>Самостійна підготовка: 96</td></tr>
<tr><td colspan="8">АНОТАЦІЯ КУРСУ</td></tr>
<tr><td colspan="8">Взаємозв’язок у структурно-логічній схемі</td></tr>
<tr><td colspan="3">Освітні компоненти, які передують вивченню</td><td colspan="5">Стандарти кібербезпеки та захисту конфіденційної інформації.
Технологія створення та застосування комплексів захисту інформації з обмеженим доступом та охорони об’єктів інформаційної діяльності</td></tr>
<tr><td colspan="3">Освітні компоненти для яких є базовою</td><td colspan="5">Кваліфікаційна робота</td></tr>
<tr><td>Мета курсу:</td><td colspan="7">Формування знань та вмінь щодо застосування аналітичних, розрахункових та експериментальних методів для оцінки захищеності інформаційних систем, а також розробки та супроводу систем аудиту і моніторингу ефективності комплексів технічного та кібернетичного захисту на об'єктах інформаційної діяльності.</td></tr>
<tr><td colspan="8">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="4">Soft-skills / Загальні компетентності (ЗК)</td><td colspan="4">Hard-skills / Спеціальні компетентності (СК)</td></tr>
<tr><td colspan="4">ЗК1. Здатність застосовувати знання у практичних ситуаціях.
ЗК2. Здатність проводити дослідження на відповідному рівні.
ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
ЗК7. Вміння виявляти, ставити та вирішувати проблеми.
ЗК9. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК10. Здатність застосовувати кращі практики у професійній діяльності.</td><td colspan="4">КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх</td></tr>
</table>

	впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

Програмні результати навчання (РН)

КЗ1. Здатність застосовувати знання у практичних ситуаціях.
КЗ2. Здатність проводити дослідження на відповідному рівні.
КЗ3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
КЗ7. Вміння виявляти, ставити та вирішувати проблеми.
КЗ9. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
КЗ10. Здатність застосовувати кращі практики у професійній діяльності.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Тема 1. Основи теорії оцінки ефективності систем кіберзахисту.			
Лекція 1. Теоретичні основи та загальна методологія оцінки ефективності систем кіберзахисту. ***Знати***: теоретичні основи, базові поняття, принципи та загальну методологію оцінки ефективності систем кібернетичного захисту. ***Формування компетенцій:*** КЗ2, КЗ3, КЗ7, КФ3, КФ5. ***Результати навчання:*** РН19, РН20, РН22. ***Рекомендовані джерела:*** 1,5,7.	Лекція 1 2 год	1	Лекція-візуалізація
Пз 1. Визначення цілей, завдань та базових показників оцінювання захищеності для умовного об'єкта. ***Знати***: теоретичні основи, базові поняття, принципи та загальну методологію оцінки ефективності систем кібернетичного захисту. ***Вміти***: визначати цілі та завдання оцінювання, класифікувати методи аналізу систем захисту відповідно до специфіки об'єкта. ***Формування компетенцій:*** КЗ2, КЗ3, КЗ7, КФ3, КФ5. ***Результати навчання:*** РН19, РН20, РН22. ***Рекомендовані джерела:*** 1,5,7.	Практичне заняття 1 2 год	2	Практичні навички постановки задачі оцінювання ефективності КСЗІ.
Знати: еволюцію підходів до оцінки захищеності інформаційних систем. ***Вміти***: визначати підхід до оцінки захищеності інформаційних	Самостійна робота 1 8 год	-	Самостійна підготовка. Вивчення еволюції підходів до оцінки захищеності інформаційних систем.

систем. ***Формування компетенцій:*** К32, К33, К37, КФ3, КФ5. ***Результати навчання:*** РН19, РН20, РН22. ***Рекомендовані джерела:*** 1,5,7.			
Тема 2. Критерії та метрики ефективності інформаційної безпеки (KPI, KRI, KCI).			
Лекція 2. Ключові показники ефективності, ризику та контролю у сфері кібербезпеки. ***Знати***: ключові показники ефективності (KPI), показники ризику (KRI) та показники контролю (KCI) у сфері кібербезпеки.. ***Вміти***: розробляти, впроваджувати та аналізувати систему метрик для комплексної оцінки поточного стану захищеності організації. ***Формування компетенцій:*** К31, К33, К34, КФ4, КФ9. ***Результати навчання:*** РН9, РН14, РН19, РН22. ***Рекомендовані джерела:*** 3,5,7.	Лекція 2 2 год	1	Лекція-візуалізація.
Лб 1. Розробка та налаштування дашборду метрик інформаційної безпеки (KPI/KRI) у спеціалізованому ПЗ. ***Знати***: ключові показники ефективності (KPI), показники ризику (KRI) та показники контролю (KCI) у сфері кібербезпеки.. ***Вміти***: розробляти, впроваджувати та аналізувати систему метрик для комплексної оцінки поточного стану захищеності організації. ***Формування компетенцій*:** К31, К33, К34, КФ4, КФ9. ***Результати навчання:*** РН9, РН14, РН19, РН22. ***Рекомендовані джерела:*** 3,5,7.	Лабораторне заняття 1 2 год	5	Практичні навички візуалізації та контролю метрик ефективності.
Знати: ключові показники ефективності (KPI), показники ризику (KRI) та показники контролю (KCI) у сфері кібербезпеки.. ***Вміти***: вимірювати рівень захищеності за ISO/IEC 27004. ***Формування компетенцій*:** К31, К33, К34, КФ4, КФ9. ***Результати навчання:*** РН9, РН14, РН19, РН22. ***Рекомендовані джерела:*** 3,5,7.	Самостійна робота 2 8 год	-	Самостійна підготовка. Опрацювання міжнародних стандартів щодо вимірювання ефективності ІБ (наприклад, ISO/IEC 27004).
Тема 3. Аналітичні методи оцінки ефективності систем захисту.			
Лекція 3. Математичні та аналітичні моделі оцінки надійності та стійкості систем захисту. ***Знати*** сутність, можливості та види аналітичних і розрахункових методів оцінки ефективності інформаційної безпеки. ***Вміти***: застосовувати математичні та аналітичні моделі для розрахунку показників надійності, безвідмовності та стійкості систем захисту. ***Формування компетенцій:*** К32, К33, К37, КФ3, КФ5. ***Результати навчання:*** РН19, РН20, РН22. ***Рекомендовані джерела:*** 1,3,8.	Лекція 3 2 год	1	Лекція-візуалізація.

Пз. 2 Практичний розрахунок показників безвідмовності та стійкості засобів захисту з використанням аналітичних моделей. ***Знати*** сутність, можливості та види аналітичних і розрахункових методів оцінки ефективності інформаційної безпеки. ***Вміти***: застосовувати математичні та аналітичні моделі для розрахунку показників надійності, безвідмовності та стійкості систем захисту. ***Формування компетенцій:*** КЗ2, КЗ3, КЗ7, КФ3, КФ5. ***Результати навчання:*** РН19, РН20, РН22. ***Рекомендовані джерела:*** 1,3,8.	Практичне заняття 2 2 год	2	Практичні навички розрахунку показників безвідмовності та стійкості засобів захисту з використанням аналітичних моделей.
Аналіз методів теорії ймовірностей та марковських ланцюгів у контексті кібербезпеки. ***Знати*** сутність та можливості методів теорії ймовірностей та марковських ланцюгів у контексті кібербезпеки. ***Вміти***: аналізувати методи теорії ймовірностей та марковських ланцюгів у контексті кібербезпеки. ***Формування компетенцій:*** КЗ2, КЗ3, КЗ7, КФ3, КФ5. ***Результати навчання:*** РН19, РН20, РН22. ***Рекомендовані джерела:*** 1,3,8.	Самостійна робота 3 8 год	-	Самостійна підготовка. Дослідження методів теорії ймовірностей та марковських ланцюгів у контексті кібербезпеки.
Тема 4. Експериментальні методи перевірки захищеності (Penetration Testing).			
Лекція 4. Експериментальні методи оцінки: інструментальне сканування та тестування на проникнення. ***Знати***: принципи, види та етапи застосування експериментальних методів оцінки (тестування на проникнення, інструментальне сканування). ***Вміти***: застосовувати експериментальні методи для практичної перевірки ефективності засобів кіберзахисту в реальних умовах. ***Формування компетенцій:*** КЗ1, КЗ2, КЗ7, КФ3, КФ5, КФ9. ***Результати навчання:*** РН6, РН19, РН20, РН22. ***Рекомендовані джерела:*** 4,11,12.	Лекція 4 2 год	1	Лекція-візуалізація.
Лб. 2. Проведення інструментального сканування мережі та верифікація ефективності налаштувань міжмережевого екрану. ***Знати***: принципи, види та етапи застосування експериментальних методів оцінки (тестування на проникнення, інструментальне сканування). ***Вміти***: застосовувати експериментальні методи для практичної перевірки ефективності засобів кіберзахисту в реальних умовах. ***Формування компетенцій:*** КЗ1, КЗ2, КЗ7, КФ3, КФ5, КФ9. ***Результати навчання:*** РН6, РН19, РН20, РН22. ***Рекомендовані джерела:*** 4,11,12.	Лабораторне заняття 2 2 год	5	Практичні навички експериментальної перевірки дієвості механізмів захисту.

Знати: методології проведення тестування на проникнення як інструменту оцінки ефективності (PTES, OSSTMM). ***Вміти***: застосовувати методології проведення тестування на проникнення як інструменту оцінки ефективності (PTES, OSSTMM). ***Формування компетенцій:*** КЗ1, КЗ2, КЗ7, КФ3, КФ5, КФ9. ***Результати навчання:*** РН6, РН19, РН20, РН22. ***Рекомендовані джерела:*** 4,11,12.	Самостійна робота 4 8 год	-	Самостійна підготовка. Вивчення методологій проведення тестування на проникнення як інструменту оцінки ефективності (PTES, OSSTMM).
Тема 5. Моделювання загроз та оцінка ризиків як базис ефективності КСЗІ.			
Лекція 5. Моделювання загроз та кількісна/якісна оцінка ризиків інформаційної безпеки. ***Знати***: сучасні методики моделювання загроз та підходи до кількісної і якісної оцінки ризиків інформаційної безпеки. ***Вміти***: будувати моделі загроз, аналізувати ризики та оцінювати адекватність впроваджених механізмів захисту поточним векторам атак. ***Формування компетенцій:*** КЗ2, КЗ3, КЗ7, КФ5. ***Результати навчання:*** РН6, РН9, РН10, РН16, РН20. ***Рекомендовані джерела:*** 3,8,10.	Лекція 5 2 год	1	Лекція-візуалізація.
Пз 3. Побудова моделі загроз та розрахунок рівня ризику для оцінки адекватності існуючої КСЗІ. ***Знати***: сучасні методики моделювання загроз та підходи до кількісної і якісної оцінки ризиків інформаційної безпеки. ***Вміти***: будувати моделі загроз, аналізувати ризики та оцінювати адекватність впроваджених механізмів захисту поточним векторам атак. ***Формування компетенцій:*** КЗ2, КЗ3, КЗ7, КФ5. ***Результати навчання:*** РН6, РН9, РН10, РН16, РН20. ***Рекомендовані джерела:*** 3,8,10.	Практичне заняття 3 2 год	2	Практичні навички моделювання загроз та прив'язки ризиків до ефективності контролів безпеки.
Знати: сучасні фреймворки моделювання загроз (STRIDE, PASTA) та методологій оцінки ризиків (NIST SP 800-30). ***Вміти***: аналізувати сучасні фреймворки моделювання загроз (STRIDE, PASTA) та методологій оцінки ризиків (NIST SP 800-30). ***Формування компетенцій:*** КЗ2, КЗ3, КЗ7, КФ5. ***Результати навчання:*** РН6, РН9, РН10, РН16, РН20. ***Рекомендовані джерела:*** 3,8,10.	Самостійна робота 5 8 год	-	Самостійна підготовка. Дослідження сучасних фреймворків моделювання загроз (STRIDE, PASTA) та методологій оцінки ризиків (NIST SP 800-30).
Тема 6. Аудит ефективності системи управління інформаційною безпекою (СУІБ).			
Лекція 8. Стандарти та процедури проведення внутрішнього і зовнішнього аудиту СУІБ. ***Знати***: стандарти, етапи та процедури проведення внутрішнього і зовнішнього аудиту СУІБ (зокрема ISO/IEC 27007, ISO/IEC 27008).	Лекція 8 2 год	1	Лекція-візуалізація.

Вміти: планувати аудит, збирати свідчення та формувати об'єктивну звітність щодо ефективності функціонування процесів СУІБ. ***Формування компетенцій*:** КЗ1, КЗ4, КФ4, КФ9, КФ12. ***Результати навчання:*** РН9, РН14, РН16, РН20. ***Рекомендовані джерела:*** 1,5,6.			
Пз. 4. Складання програми, плану та аудиторських чек-листів для перевірки процесів СУІБ. ***Знати***: стандарти, етапи та процедури проведення внутрішнього і зовнішнього аудиту СУІБ (зокрема ISO/IEC 27007, ISO/IEC 27008). ***Вміти***: складати плани та проводити підготовку документації для аудиту ефективності. ***Формування компетенцій*:** КЗ1, КЗ4, КФ4, КФ9, КФ12. ***Результати навчання:*** РН9, РН14, РН16, РН20. ***Рекомендовані джерела:*** 1,5,6.	Практичне заняття 4 2 год	2	Практичні навички планування та підготовки документації для аудиту ефективності
Лб 3. Проведення імітаційного аудиту налаштувань безпеки операційної системи та формування звіту про невідповідності. ***Знати***: стандарти, етапи та процедури проведення внутрішнього і зовнішнього аудиту СУІБ (зокрема ISO/IEC 27007, ISO/IEC 27008). ***Вміти***: збирати свідчення та формувати об'єктивну звітність щодо ефективності функціонування процесів СУІБ. ***Формування компетенцій*:** КЗ1, КЗ4, КФ4, КФ9, КФ12. ***Результати навчання:*** РН9, РН14, РН16, РН20. ***Рекомендовані джерела:*** 1,5,6.	Лабораторне заняття 3 2 год	5	Практичні навички технічного аудиту та оцінки відповідності стандартам.
Знати: стандарти, етапи та процедури проведення внутрішнього і зовнішнього аудиту СУІБ (зокрема ISO/IEC 27007, ISO/IEC 27008). ***Вміти***: планувати аудит, збирати свідчення та формувати об'єктивну звітність щодо ефективності функціонування процесів СУІБ. ***Формування компетенцій*:** КЗ1, КЗ4, КФ4, КФ9, КФ12. ***Результати навчання:*** РН9, РН14, РН16, РН20. ***Рекомендовані джерела:*** 1,5,6.	Самостійна робота 6 8 год	-	Самостійна підготовка. Опрацювання стандартів ISO/IEC 27007 та 27008 щодо настанов з аудиту СУІБ.
Тема 7. Оцінка ефективності засобів технічного захисту інформації (ТЗІ).			
Лекція 7. Критерії та методики оцінки ефективності комплексів технічного захисту інформації. ***Знати***: критерії та нормативні методики оцінки ефективності комплексів технічного захисту інформації (акустичного, електромагнітного тощо).	Лекція 7 2 год	1	Лекція-візуалізація.

Вміти*:** проводити інструментальні вимірювання, аналізувати результати та розраховувати показники захищеності об'єктів інформаційної діяльності. ***Формування компетенцій: КЗ1, КЗ2, КЗ4, КФ5, КФ8. ***Результати навчання:*** РН6, РН13, РН19, РН20, РН22. ***Рекомендовані джерела:*** 1,2,9.			
Пз 5. Розрахунок показників ефективності захисту мовної інформації від витоку акустичним та віброакустичним каналами. ***Знати***: критерії та нормативні методики оцінки ефективності комплексів технічного захисту інформації (акустичного, електромагнітного тощо). ***Вміти*:** проводити розрахунок показників ефективності захисту мовної інформації від витоку акустичним та віброакустичним каналами. ***Формування компетенцій:*** КЗ1, КЗ2, КЗ4, КФ5, КФ8. ***Результати навчання:*** РН6, РН13, РН19, РН20, РН22. ***Рекомендовані джерела:*** 1,2,9.	Практичне заняття 5 2 год	2	Практичні навички оцінки захищеності об'єктів від витоку технічними каналами.
Поглиблене вивчення нормативних документів (НД ТЗІ) щодо критеріїв оцінки ефективності засобів ТЗІ. ***Знати***: нормативні документи (НД ТЗІ) щодо критеріїв оцінки ефективності засобів ТЗІ. ***Вміти*:** виділяти критерії оцінки ефективності засобів ТЗІ. ***Формування компетенцій:*** КЗ1, КЗ2, КЗ4, КФ5, КФ8. ***Результати навчання:*** РН6, РН13, РН19, РН20, РН22. ***Рекомендовані джерела:*** 1,2,9.	Самостійна робота 7 8 год		Самостійна підготовка. Поглиблене вивчення нормативних документів (НД ТЗІ) щодо критеріїв оцінки ефективності засобів ТЗІ.
Тема 8. Ефективність підсистем криптографічного захисту та управління доступом.			
Лекція 8. Критерії стійкості криптоалгоритмів та ефективність систем управління доступом (IAM, PAM). ***Знати*:** показники стійкості криптографічних алгоритмів та критерії ефективності систем управління ідентифікацією та доступом (IAM, PAM). ***Вміти***: аналізувати надійність реалізації криптографічного захисту та ефективність налаштувань підсистем розмежування доступу. ***Формування компетенцій*:** КЗ1, КЗ2, КЗ3, КФ5, КФ8. ***Результати навчання*:** РН6, РН13, РН19, РН20. ***Рекомендовані джерела*:** 1,2,9.	Лекція 8 2 год	1	Лекція-візуалізація.
Пз 6. Аналіз надійності та ефективності політик парольного захисту та багатофакторної автентифікації. ***Знати*:** показники стійкості криптографічних алгоритмів та критерії ефективності систем управління ідентифікацією та доступом (IAM, PAM).	Практичне заняття 6 2 год	2	Практичні навички оцінки якості налаштувань систем розмежування доступу.

Вміти: аналізувати надійність реалізації криптографічного захисту та ефективність налаштувань підсистем розмежування доступу. ***Формування компетенцій*:** КЗ1, КЗ2, КЗ3, КФ5, КФ8. ***Результати навчання*:** РН6, РН13, РН19, РН20. ***Рекомендовані джерела*:** 1,2,9.			
Лб 4. Практична перевірка стійкості реалізації криптографічного захисту (наприклад, TLS-з'єднань) інструментальними засобами. ***Знати*:** показники стійкості криптографічних алгоритмів та критерії ефективності систем управління ідентифікацією та доступом (IAM, PAM). ***Вміти***: перевіряти стійкість реалізації криптографічного захисту (наприклад, TLS-з'єднань) інструментальними засобами. ***Формування компетенцій*:** КЗ1, КЗ2, КЗ3, КФ5, КФ8. ***Результати навчання*:** РН6, РН13, РН19, РН20. ***Рекомендовані джерела*:** 1,2,9.	Лабораторне заняття 4 2 год	5	Практичні навички аналізу криптографічних протоколів на ефективність.
Знати*:** показники стійкості криптографічних алгоритмів та критерії ефективності систем управління ідентифікацією та доступом (IAM, PAM). ***Вміти: оцінювати продуктивність систем криптографічного захисту та управління ключами (KMS). ***Формування компетенцій*:** КЗ1, КЗ2, КЗ3, КФ5, КФ8. ***Результати навчання*:** РН6, РН13, РН19, РН20. ***Рекомендовані джерела*:** 1,2,9.	Самостійна робота 8 8 год		Самостійна підготовка. Оцінка продуктивності систем криптографічного захисту та управління ключами (KMS).
Тема 9. Інструментальний моніторинг ефективності (SIEM-системи та SOC).			
Лекція 9. Архітектура систем моніторингу подій безпеки (SIEM) та оцінка роботи SOC. ***Знати***: архітектуру систем моніторингу подій безпеки (SIEM) та принципи оцінки ефективності роботи центрів операційної безпеки (SOC). ***Вміти***: аналізувати повноту збору логів, налаштовувати правила кореляції та оцінювати ефективність автоматизованого виявлення аномалій. ***Формування компетенцій*:** КЗ1, КЗ2, КЗ7, КФ3, КФ9 ***Результати навчання*:** РН6, РН14, РН16, РН20. ***Рекомендовані джерела*:** 1,5,12.	Лекція 9 2 год	1	Лекція-візуалізація.
Пз 7. Розробка та оптимізація правил кореляції подій безпеки для підвищення ефективності виявлення інцидентів. **Знати**: архітектуру систем моніторингу подій безпеки (SIEM) та принципи оцінки ефективності роботи центрів операційної безпеки (SOC). **Вміти**: розробляти і налаштовувати правила кореляції та	Практичне заняття 7 2 год	2	Практичні навички аналізу та налаштування логіки SIEM-систем.

оцінювати ефективність автоматизованого виявлення аномалій. **Формування компетенцій:** К31, К32, К37, КФ3, КФ9 **Результати навчання:** РН6, РН14, РН16, РН20. **Рекомендовані джерела:** 1,5,12.			
Вивчення показників ефективності (SLA) та метрик роботи центрів операційної безпеки (SOC). **Знати**: архітектуру систем моніторингу подій безпеки (SIEM) та показників ефективності (SLA) та метрик роботи центрів операційної безпеки (SOC). **Вміти**: аналізувати показники ефективності (SLA) та метрик роботи центрів операційної безпеки (SOC). **Формування компетенцій:** К31, К32, К37, КФ3, КФ9 **Результати навчання:** РН6, РН14, РН16, РН20. **Рекомендовані джерела:** 1,5,12.	Самостійна робота 9 8 год		Самостійна підготовка. Вивчення показників ефективності (SLA) та метрик роботи центрів операційної безпеки (SOC).
Тема 10. Оцінка готовності до реагування на інциденти кібербезпеки.			
Лекція 10. Метрики оцінки процесу реагування на інциденти (MTTD, MTTR) та кібернавчання ***Знати***: метрики оцінки ефективності процесу реагування на інциденти (MTTD, MTTR) та методики проведення кібернавчань. ***Вміти***: розраховувати час виявлення та реагування на інциденти, об'єктивно аналізувати готовність організації до протидії кібератакам. ***Формування компетенцій:*** К31, К32, К37, КФ4, КФ9. ***Результати навчання:*** РН9, РН10, РН14, РН16, РН20, РН22. ***Рекомендовані джерела:*** 5,7,12.	Лекція 10 2 год	1	Лекція-візуалізація.
Лб 5. Моделювання інциденту кібербезпеки та розрахунок часових метрик (MTTD, MTTR) у тестовому середовищі. ***Знати***: метрики оцінки ефективності процесу реагування на інциденти (MTTD, MTTR) та методики проведення кібернавчань. ***Вміти***: виявляти та реагувати на інциденти, об'єктивно аналізувати готовність організації до протидії кібератакам. ***Формування компетенцій*:** К31, К32, К37, КФ4, КФ9. ***Результати навчання:*** РН9, РН10, РН14, РН16, РН20, РН22. ***Рекомендовані джерела:*** 5,7,12.	Лабораторне заняття 5 2 год	5	Практичні навички оцінки операційної готовності та швидкості реакції на інциденти
Знати: методики проведення кібернавчань. ***Вміти***: готувати сценарії для проведення командно-штабних кібернавчань (Tabletop exercises). ***Формування компетенцій*:** К31, К32, К37, КФ4, КФ9. ***Результати навчання:*** РН9, РН10, РН14, РН16, РН20, РН22. ***Рекомендовані джерела:*** 5,7,12.	Самостійна робота 10 8 год		Самостійна робота. Підготовка сценаріїв для проведення командно-штабних кібернавчань (Tabletop exercises).
Тема 11. Економічна ефективність систем кіберзахисту.			
Лекція 11. Фінансові метрики оцінки інвестицій у кібербезпеку (ROSI, ALE, SLE).	Лекція 11 2 год	1	Лекція-візуалізація.

Знати: фінансові метрики оцінки інвестицій у кібербезпеку (ROSI - Return on Security Investment, ALE - Annualized Loss Expectancy, SLE). ***Вміти***: розраховувати економічну доцільність впровадження нових засобів захисту та обґрунтовувати бюджет на кібербезпеку. ***Формування компетенцій*:** КЗ1, КЗ3, КЗ4, КФ4, КФ5. ***Результати навчання:*** РН9, РН10, РН16, РН19, РН20. ***Рекомендовані джерела:*** 3,8,10.			
Пз. 8. Практичний розрахунок показника повернення інвестицій у кібербезпеку (ROSI) для обґрунтування закупівлі нових засобів захисту. ***Знати***: фінансові метрики оцінки інвестицій у кібербезпеку (ROSI - Return on Security Investment, ALE - Annualized Loss Expectancy, SLE). ***Вміти***: розраховувати економічну доцільність впровадження нових засобів захисту та обґрунтовувати бюджет на кібербезпеку. ***Формування компетенцій:*** КЗ1, КЗ3, КЗ4, КФ4, КФ5. ***Результати навчання:*** РН9, РН10, РН16, РН19, РН20. ***Рекомендовані джерела:*** 3,8,10.	Практичне заняття 8 2 год	2	Практичні навички фінансово-економічного обґрунтування рішень з інформаційної безпеки
Знати:методи оцінки вартості інформаційних активів та можливих збитків від порушення конфіденційності, цілісності, доступності. ***Вміти***: застосовувати методи оцінки вартості інформаційних активів та можливих збитків від порушення конфіденційності, цілісності, доступності. ***Формування компетенцій:*** КЗ1, КЗ3, КЗ4, КФ4, КФ5. ***Результати навчання:*** РН9, РН10, РН16, РН19, РН20. ***Рекомендовані джерела:*** 3,8,10.	Самостійна робота 11 8 год		Самостійна робота. Аналіз методів оцінки вартості інформаційних активів та можливих збитків від порушення конфіденційності, цілісності, доступності.
Тема 12. Безперервне вдосконалення комплексної системи захисту інформації.			
Лекція 12. Цикл постійного покращення (PDCA) та модернізація архітектури КСЗІ. ***Знати***: процеси постійного покращення (цикл PDCA) та методики адаптації архітектури КСЗІ до нових технологічних викликів. ***Вміти***: розробляти практичні рекомендації щодо модернізації, оптимізації та підвищення загальної ефективності системи кібернетичного захисту. ***Формування компетенцій*:** КЗ1, КЗ3, КЗ4, КЗ7, КФ4, КФ9, КФ12. ***Результати навчання*:** РН9, РН14, РН16, РН19, РН20, РН22. ***Рекомендовані джерела*:** 5,6,7.	Лекція 12 2 год	1	Лекція-презентація, експрес-опитування здобувачів
Пз. 9. Розробка плану заходів щодо підвищення ефективності та модернізації КСЗІ за результатами попереднього оцінювання.	Практичне заняття 9 2 год	2	Практичні навички формування управлінських рішень щодо вдосконалення системи безпеки

Знати: процеси постійного покращення (цикл PDCA) та методики адаптації архітектури КСЗІ до нових технологічних викликів. ***Вміти***: розробляти план заходів щодо підвищення ефективності та модернізації КСЗІ за результатами попереднього оцінювання.. ***Формування компетенцій*:** К31, К33, К34, К37, КФ4, КФ9, КФ12. ***Результати навчання*:** РН9, РН14, РН16, РН19, РН20, РН22. ***Рекомендовані джерела*:** 5,6,7.			
Лб 6. Автоматизована перевірка налаштувань інфраструктури (Compliance Check) та генерація звіту про ефективність застосованих політик. ***Знати***: процеси постійного покращення (цикл PDCA) та методики адаптації архітектури КСЗІ до нових технологічних викликів. ***Вміти***: проводити автоматизовані перевірки налаштувань інфраструктури (Compliance Check) та генерувати звіти про ефективність застосованих політик. ***Формування компетенцій*:** К31, К33, К34, К37, КФ4, КФ9, КФ12. ***Результати навчання*:** РН9, РН14, РН16, РН19, РН20, РН22. ***Рекомендовані джерела*:** 5,6,7.	Лабораторне заняття 6 2 год	5	Практичні навички автоматизації процесів безперервного контролю ефективності)
	Самостійна робота 12 8 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Комп'ютерне обладнання, мультимедійний проектор, мережа Інтернет.
Спеціалізоване програмне забезпечення для інструментального аудиту та моніторингу: мережеві сканери (Nmap, Nessus/OpenVAS), системи збору та кореляції подій безпеки (навчальні розгортання SIEM-систем, наприклад, Splunk або Elastic Security), інструменти автоматизованого compliance-чекінгу.
Програмні засоби для аналітики та моделювання: табличні процесори (Excel/Google Sheets) для розрахунку економічної ефективності (ROSI, ALE) та метрик (KPI/KRI), програмне забезпечення для побудови моделей загроз і ризиків.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Сучасні інформаційні технології в кібербезпеці [моногр.] / А.С. Довбиш, В.К. Ободяк, І.В. Шелехов. – Суми: СумДУ, 2021. – 348 с. https://essuir.sumdu.edu.ua/bitstream-download/123456789/82619/3/Obodiak_kiberbezpeka.pdf
2. Технології захисту інформації в інформаційно-телекомунікаційних системах [навч. посіб.] / А.В. Жилін, О.М. Шаповал, О.А. Успенський. – К.: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с. https://ela.kpi.ua/server/api/core/bitstreams/d99a0045-e907-4d17-afc1-5431f67d2444/content
3. Hubbard D. W., Seiersen R. How to Measure Anything in Cybersecurity Risk. Режим доступу: https://duikt.edu.ua/ua/lib/1/category/726/view/2077
4. Weidman G. Penetration Testing: A Hands-On Introduction to Hacking. Режим доступу: https://duikt.edu.ua/ua/lib/1/category/742/view/1846
5. ДСТУ ISO/IEC 27004:2019 (ISO/IEC 27004:2016, IDT). Інформаційні технології. Методи захисту. Менеджмент інформаційної безпеки. Моніторинг, вимірювання, аналізування та оцінювання.
6. ДСТУ ISO/IEC 27007:2022 (ISO/IEC 27007:2020, IDT). Інформаційна безпека, кібербезпека та захист конфіденційності. Настанови щодо аудиту систем управління інформаційною безпекою.
7. NIST Special Publication 800-55 Rev. 1. Performance Measurement Guide for Information Security. National Institute of Standards and Technology. Режим доступу: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-55r1.pdf
8. NIST Special Publication 800-30 Rev. 1. Guide for Conducting Risk Assessments. National Institute of Standards and Technology. Режим доступу: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

9. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Режим доступу: https://tzi.com.ua/downloads/2.5-004-99.pdf
10. CIS RAM (Center for Internet Security Risk Assessment Method). Режим доступу: https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method
11. OSSTMM 3 (The Open Source Security Testing Methodology Manual). ISECOM. Режим доступу: https://www.isecom.org/OSSTMM.3.pdf
12. База знань MITRE ATT&CK® (для моделювання ефективності виявлення загроз). Режим доступу: https://attack.mitre.org/

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов'язкове відвідування лекцій і практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, проведення тестових розрахунків рівнів сигналів для їх подальшого аналізу, поглиблене вивчення матеріалу за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо здобувач відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультується з викладачем.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації здобувач повинен вказати джерело, використане в ході виконання завдання.

***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	***Робота на заняттях,*** *у т.ч.:*	
	присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 1 бала
	звіт про виконання практичного завдання	за кожен звіт максимум 1 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, отримання міжнародного сертифікату за напрямом.	10-15 балів
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Залік***	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання наукової роботи. Залік проходить у письмовій формі.	40 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	Критерії оцінювання	Рівень компетентності	**Оцінка** */запис в екзаменаційній відомості*
90-100	Здобувач демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об'єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або Здобувач проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції здобувача в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (A)
82-89	Здобувач демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	**Достатній** Забезпечує здобувачу самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені дисципліни	Добре / Зараховано (B)
75-81	Здобувач в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (C)
67-74	Здобувач засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача.	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-66	Здобувач має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, Здобувач з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)

35-59	Здобувач може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни здобувач виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у Здобувача відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*
0-34	Здобувач повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Здобувач не допущений до здачі заліку.	**Незадовільний** Здобувач не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	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.