

Затверджено
завідувач кафедри
СТКБ _____ Г. Гайдур
«31» _____ 08 2026 р.

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ПРИКЛАДНА ЗАГАЛЬНА ТЕОРІЯ СИСТЕМ КІБЕРБЕЗПЕКИ»

Лектор курсу			Гайдур Галина Іванівна, доктор технічних наук, професор		Контактна інформація лектора (e-mail), сторінка курсу		e-mail: g.haidur@duikt.edu.ua сторінка курсу https://classroom.google.com/c/ODY4MDA3MzExOTc4?cjc=24korurs	
Галузь знань			F Інформаційні технології		Рівень вищої освіти		Магістр	
Спеціальність			F5 Кібербезпека та захист інформації		Семестр		1	
Освітня програма			Інформаційна та кібернетична безпека		Тип дисципліни		Основна компонента освітньо-професійної програми	
Обсяг:	Кредитів ECTS	Годин	За видами занять:					
	3	90	Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка	
			18	-	18		54	
АНОТАЦІЯ КУРСУ								
Взаємозв'язок у структурно-логічній схемі								
Освітні компоненти, які передують вивченню			Основна					
Освітні компоненти для яких є базовою			Технології забезпечення безпеки мережевої інфраструктури, технології виявлення уразливостей мережевих ресурсів, організація проведення наукових досліджень, науково-технічний переклад					
Мета курсу:		Формування знань та вмінь щодо формування знань про теоретичні основи і практичні навички роботи з сучасними системами кібербезпеки,						
Компетентності відповідно до освітньої програми								
Soft- skills / Загальні компетентності (ЗК)					Hard-skills / Спеціальні компетентності (СК)			
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. КЗ5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).					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.

КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

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 впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно 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.

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

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.

КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

Програмні результати навчання (ПРН)

RH3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

RH5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

RH6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

RH7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

RH11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

RH16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

RH17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

RH23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Тема 1. Роль і місце систем кібербезпеки при функціонуванні інформаційних систем Знати: Концепцію «Імунних систем» і термінологію кібербезпеки. Роль і місце кібербезпеки в сучасному цифровому світі. Поширені загрози та вразливості в кіберсистемах. Формування компетенцій: К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: RH5, RH6, RH7, RH11, RH16, RH17, RP23 Рекомендовані джерела: 1-5	Лекція 1 2 год		Лекція-візуалізація.

Тема 1. Класифікація систем кібербезпеки. Знати: Уміти застосовувати предметну базу знань. Критично оцінювати результати дослідження Вміти: розв'язувати задачі, пов'язані з основними способами класифікації систем, описом вхідних, вихідних даних та можливих станів системи. Формування компетенцій: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН5, РН6, РН7, РН11, РН16, РН17, РП23 Рекомендовані джерела: 1-11	Практичне заняття 1 2 год	3	Практичне застосування методики експертних оцінок для класифікації систем кібербезпеки.
Тема 1. Роль і місце систем кібербезпеки в інформаційних системах організацій. Знати: поняття «корпоративна інформаційна система» як об'єкт захисту; превентивні, детективні та корективні заходи забезпечення кібербезпеки сучасного підприємства, поняття «подія безпеки», поняття «вразливість»; класифікація вразливостей; джерела даних щодо вразливостей; прийняті позначення вразливостей; зміст процесу управління вразливостями; мета управління вразливістю; ролі та обов'язки посадових осіб. Вміти: застосовувати методику управління вразливостями: здійснювати заходи підготовчого етапу; здійснювати початкове сканування вразливостей; визначати коригуючі дії або приймати ризик; здійснювати коригувальні дії; здійснювати перевірку (ресканування). Формування компетенцій: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН5, РН6, РН7, РН11, РН16, РН17, РП23 Рекомендовані джерела: 1-5	Самостійна робота 1 6 год	7	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Тема 2. Принципи та політики безпеки Знати: Основи принципів безпеки, які включають конфіденційність, цілісність і доступність. Моделі та політики контролю доступу. Політики та стандарти безпеки. Формування компетенцій: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН5, РН6, РН7, РН11, РН16, РН17, РП23 Рекомендовані джерела: 1-5	Лекція 2 2 год		Лекція-візуалізація

Тема 2. Застосування методу експертної оцінки для систем ІБ Знати: розв'язувати задачі, пов'язані з основними методами експертної оцінки. Вміти: стисло і зрозуміло висловлювати свої думки; акуратності і точності записів, уважності, дисциплінованості; приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки. набуттю навичок систематизації матеріалу, що вивчається Формування компетенцій: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН5, РН6, РН7, РН11, РН16, РН17, РП23 Рекомендовані джерела: 1-11	Практичне заняття 2 год	3	Вміти вирішувати задачі на основі методу експертних оцінок для класифікації систем кібербезпеки.
Тема 2. Принципи та політики безпеки Знати: Моделі та політики контролю доступу. Вміти: Застосовувати політики та стандарти безпеки в діяльності організацій. Формування компетенцій: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН5, РН6, РН7, РН11, РН16, РН17, РП23 Рекомендовані джерела: 1-6	Самостійна робота 2 год	7	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Тема 3. Безпека мережі організації Знати: Архітектуру мережі та протоколи. Поширені загрози мережевій безпеці та атаки. Технології мережевої безпеки та засоби протидії. Формування компетенцій: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН5, РН6, РН7, РН11, РН16, РН17, РП23 Рекомендовані джерела: 1-6	Лекція 2 год		Лекція-візуалізація
Тема 3. Безпека мережі організації Знати: знати топології мереж: кампусні, для малих організацій, хмарні, глобальні; Вміти: розробляти захищені мережі для організацій будь-якого типу з урахуванням стратегії, стандартів та протоколів кібербезпеки	Практичне заняття 3 год	3	Практичне застосування методів та засобів розробки, інтеграції мереж організацій на основі впроваджених стратегій і політик безпеки, з урахування стандартів кібербезпеки.

Формування компетенцій: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН5, РН6, РН7, РН11, РН16, РН17, РП23 Рекомендовані джерела: 1-7			
Тема 3. Безпека мережі організації Знати: знати топології мереж: кампусні, для малих організацій, хмарні глобальні; Вміти: розробляти захищені мережі для організацій будь-якого типу з урахуванням стратегії, стандартів та протоколів кібербезпеки Формування компетенцій: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН5, РН6, РН7, РН11, РН16, РН17, РП23 Рекомендовані джерела: 1-7	Самостійна робота 3 6 год	7	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Тема 4. Криптографія та шифрування Знати: Основи роль та місце криптографічних методів та засобів, симетричні та асиметричні алгоритми шифрування, цифрові підписи та сертифікати. Формування компетенцій: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН3, РН5, РН6, РН7, РН11, РН16, РН17, РП23 Рекомендовані джерела: 1-7	Лекція 4 2 год		Лекція-візуалізація
Тема 4. Криптографія та шифрування Знати: методи та засоби криптографічного захисту, на основі визначеної стратегії та політик безпеки організації. Вміти: вміти проводити оцінку ефективності криптографічних засобів, створювати цифровий підпис та сертифікат. Формування компетенцій: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН3, РН5, РН6, РН7, РН11, РН16, РН17, РП23 Рекомендовані джерела: 1-8	Практичне заняття 4 2 год	3	Практичне застосування методи та засоби криптографічного захисту, на основі визначеної стратегії та політик безпеки організації

Тема 4. Криптографія та шифрування Знати: Основи роль та місце криптографічних методів та засобів, симетричні та асиметричні алгоритми шифрування, цифрові підписи та сертифікати; методи та засоби криптографічного захисту, на основі визначеної стратегії та політик безпеки організації. Вміти: проводити оцінку ефективності криптографічних засобів, створювати цифровий підпис та сертифікат. Формування компетенцій: К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН5, РН6, РН7, РН11, РН16, РН17, РП23 Рекомендовані джерела: 8	Самостійна робота 4 6 год	2	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Тема 5. Оцінка безпеки та тестування на проникнення Знати: методику оцінки захищеності систем, огляд методології оцінки безпеки, методи сканування вразливостей і тестування на проникнення Звітування та стратегії пом'якшення. Формування компетенцій: К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН5, РН6, РН7, РН11, РН16, РН17, РП23 Рекомендовані джерела: 8	Лекція 5 2 год		Лекція-візуалізація
Тема 5. Оцінка безпеки та тестування на проникнення Знати: методику оцінки захищеності систем. Вміти: застосовувати методи сканування вразливостей і тестування на проникнення, створювати звіти. Формування компетенцій: К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН5, РН6, РН7, РН11, РН16, РН17, РП23 Рекомендовані джерела: 1-11	Практичне заняття 5 2 год	3	Практичне застосування методів сканування вразливостей
Тема 5. Оцінка безпеки та тестування на проникнення Знати: застосовувати методику оцінки захищеності систем. Вміти: застосовувати методи сканування вразливостей і тестування на проникнення, створювати звіти. Формування компетенцій: К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10	Самостійна робота 5 6 год	2	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

<u>Програмні результати навчання:</u> PH5, PH6, PH7, PH11, PH16, PH17, RP23 <u>Рекомендовані джерела:</u> 1-11			
Тема 6. Виявлення вторгнень та реагування на інциденти <u>Знати:</u> Системи виявлення та запобігання вторгненням (IDPS), реагування на інциденти та процедури врегулювання, криміналістичний аналіз та збір доказів. <u>Формування компетенцій:</u> K31, K32, K33, K34, K35, KФ1, KФ2, KФ3, KФ4, KФ5, KФ6, KФ7, KФ8, KФ9, KФ10 <u>Програмні результати навчання:</u> PH5, PH6, PH7, PH11, PH16, PH17, RP23 <u>Рекомендовані джерела:</u> 1-12	Лекція 6 2 год		Лекція-візуалізація
Тема 6. <u>Знати:</u> системи виявлення та запобігання вторгненням (IDPS), реагування на інциденти та процедури врегулювання, криміналістичний аналіз та збір доказів. <u>Вміти:</u> інтегрувати, супроводжувати системи виявлення та запобігання вторгненням (IDPS) на основі кращих світових практик. <u>Формування компетенцій:</u> K31, K32, K33, K34, K35, KФ1, KФ2, KФ3, KФ4, KФ5, KФ6, KФ7, KФ8, KФ9, KФ10 <u>Програмні результати навчання:</u> PH5, PH6, PH7, PH11, PH16, PH17, RP23 <u>Рекомендовані джерела:</u> 1-12	Практичне заняття 6 2 год	3	Практичне застосування систем виявлення та запобігання вторгненням (IDPS) на основі кращих світових практик.
Тема 6. Виявлення вторгнень та реагування на інциденти <u>Знати:</u> системи виявлення та запобігання вторгненням (IDPS), реагування на інциденти та процедури врегулювання, криміналістичний аналіз та збір доказів. <u>Вміти:</u> інтегрувати, супроводжувати системи виявлення та запобігання вторгненням (IDPS) на основі кращих світових практик. <u>Формування компетенцій:</u> K31, K32, K33, K34, K35, KФ1, KФ2, KФ3, KФ4, KФ5, KФ6, KФ7, KФ8, KФ9, KФ10 <u>Програмні результати навчання:</u> PH5, PH6, PH7, PH11, PH16, PH17, RP23 <u>Рекомендовані джерела:</u> 1-12	Самостійна робота 6 5 год	2	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

Тема 7. Безпека Web -додатків Знати: поширені вразливості веб-додатків (наприклад, ін'єкційні атаки, міжсайтовий сценарій), безпечні методи кодування та фреймворки, тестування та оцінка безпеки веб-додатків. Формування компетенцій: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН5, РН6, РН7, РН11, РН16, РН17, РП23 Рекомендовані джерела: 1-12	Лекція 7 2 год		Лекція-візуалізація
Тема 7. Безпека Web -додатків Знати: поширені вразливості Web--додатків (наприклад, ін'єкційні атаки, міжсайтовий сценарій), безпечні методи кодування та фреймворки, тестування та оцінка безпеки веб-додатків. Вміти: проводити оцінку безпеки Web--додатків на основних тестів безпеки Формування компетенцій: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН5, РН6, РН7, РН11, РН16, РН17, РП23 Рекомендовані джерела: 1-12	Практичне заняття 7 2 год	3	Практичне застосування застосування методів оцінки тестування Web-додатків.
Тема 7. Безпека Web -додатків Знати: Поширені вразливості Web--додатків (наприклад, ін'єкційні атаки, міжсайтовий сценарій), безпечні методи кодування та фреймворки, тестування та оцінка безпеки веб-додатків. Вміти: проводити оцінку безпеки Web-додатків на основ тестів безпеки Формування компетенцій: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН5, РН6, РН7, РН11, РН16, РН17, РП23 Рекомендовані джерела: 1-12	Самостійна робота 7 5 год	2	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Тема 8. Мобільна безпека та IoT Знати: Проблеми безпеки в мобільних пристроях і пристроях Інтернету речей, ландшафт загроз для мобільних пристроїв та Інтернету речей, Технології захисту мобільних пристроїв та IoT. Вміти: управляти доступом до інформаційних систем організацій.	Лекція 8 2 год		Лекція-візуалізація

<u>Формування компетенцій:</u> КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 <u>Програмні результати навчання:</u> РН5, РН6, РН7, РН11, РН16, РН17, РП23 <u>Рекомендовані джерела:</u> 1-12			
Тема 8. Мобільна безпека та IoT <u>Знати:</u> технології захисту мобільних пристроїв та IoT. <u>Вміти:</u> управляти доступом мобільних пристроїв до інформаційних систем організацій. <u>Формування компетенцій:</u> КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 <u>Програмні результати навчання:</u> РН5, РН6, РН7, РН11, РН16, РН17, РП23 <u>Рекомендовані джерела:</u> 1-12	Практичне заняття 8 2 год	3	Практичне застосування технології захисту мобільних пристроїв та IoT.
Тема 8. Мобільна безпека та IoT <u>Знати:</u> Проблеми безпеки в мобільних пристроях і пристроях Інтернету речей, ландшафт загроз для мобільних пристроїв та Інтернету речей, Технології захисту мобільних пристроїв та IoT. <u>Вміти:</u> управляти доступом мобільних пристроїв до інформаційних систем організацій. <u>Формування компетенцій:</u> КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 <u>Програмні результати навчання:</u> РН5, РН6, РН7, РН11, РН16, РН17, РП23 <u>Рекомендовані джерела:</u> 1-12	Самостійна робота 8 5 год	2	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Тема 9. Нові тенденції в кібербезпеці <u>Знати:</u> Поточні та нові технології кібербезпеки, розширені постійні загрози (APT) і цілеспрямовані атаки, майбутні напрямки досліджень і розробок у сфері кібербезпеки. <u>Формування компетенцій:</u> КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 <u>Програмні результати навчання:</u> РН5, РН6, РН7, РН11, РН16, РН17, РП23 <u>Рекомендовані джерела:</u> 12,13, 14-23	Лекція 9 2 год		Лекція-візуалізація

Тема 9. Нові тенденції в кібербезпеці Знати: Технології кібербезпеки на основі сучасних світових практик. Вміти: проводити аналіз новітніх технологій кібербезпеки, в тому числі технології ML. Формування компетенцій: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН5, РН6, РН7, РН11, РН16, РН17, РП23 Рекомендовані джерела: 1-3, 14-23	Практичне заняття 9 2 год	3	Практичне застосування технологій кібербезпеки на основі сучасних світових практик.
Тема 9. Нові тенденції в кібербезпеці Знати: напрямки досліджень і розробок у сфері кібербезпеки. Формування компетенцій: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН5, РН6, РН7, РН11, РН16, РН17, РП23 Рекомендовані джерела: 12,13, 14-23	Самостійна робота 9 год	2	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Навчальна лабораторія захисту кінцевих точок:

1. Комп'ютери:

DualCore Intel Pentium E2180, 2000 Ghz на МП ASUS P5JL SE/EPU, 1 Гб ОЗУ DDR2 – 13 од.

DualCore Intel Core 2 Duo, 2666 Mhz на МП ASUS P5E Deluxe, 4 Гб ОЗУ DDR2 – 4 од.– 17 шт.

2. Мультимедійна система Acer 113 – 1шт.

Програмно-апаратні комплекси:

1. ESET PROTECT Enterprise On-Prem: № ліцензії – А33-AMJ-UTU. Кількість пристроїв – 60.

Навчальна лабораторія реагування на кіберінциденти:

1. Комп'ютери Dell OptiPlex 3050/Core i5 7500T – 14 шт.

2. Мультимедійна система Acer 113 – 1 шт.

3. Набір серверів Server Dell PE R530 – 3шт.

4. Робочі станції Dell Precision Tower 3620 i7 – 14 шт. Dell OptiPlex 3050 i5;

5. Маршрутизатор Mikrotik CSS326-24G-2S+RM. – 1 шт.

6. Комутатор Mikrotik CSS326-24G-2S+ RM – 1шт.

Програмно-апаратні комплекси:

1. ESET PROTECT Enterprise On-Prem. № ліцензії – А33-AMJ-UTU, до 30.11.2026. Кількість пристроїв – 60.

2. IBM QRadar SIEM. № ліцензії – 31XX-SIEM-QRM-QVM. . Навчальна ліцензія

3. IBM i2 Analyst's Notebook Premium. Навчальна ліцензія

4. Tenable Nessus Professional. Навчальна ліцензія

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- ДСТУ EN ISO/IEC 15408-1:2022 (EN ISO/IEC 15408-1:2020, IDT; ISO/IEC 15408-1:2009, IDT) Інформаційні технології. Методи захисту. Критерії оцінювання. Частина 1. Вступ та загальна модель/

2. [ISO/IEC 27001:2013](#): an information security standard from the [International Organization for Standardization](#)
3. Guardium Tech Talk & Demo: Behind the Scenes of the Security Immune System <https://securityintelligence.com/events/guardium-tech-talk-demo-behind-scenes-security-immune-system/>
4. Cyberframework <https://www.nist.gov/cyberframework>
5. [COBIT](#): Control Objectives for Information and Related Technologies - a related framework from [ISACA](#).
6. Sabyasachi Pramanik, Debabrata Samanta, M. Vinay, Abhijit Guha, Cyber Security and Network Security. Released April 2022. Publisher(s): Wiley-Scrivener . ISBN: 9781119812494.
7. Jim Doherty Wireless and Mobile Device Security, 2nd Edition. Released March 2021. Publisher(s): Jones & Bartlett Learning. ISBN: 9781284211733
8. Massimo Bertaccini Cryptography Algorithms. Released March 2022. Publisher(s): Packt Publishing . ISBN: 9781789617139
9. Anil Kumar, Jafer Hussain, Anthony Chun Connecting the Internet of Things : IoT Connectivity Standards and Solutions. Released January 2023. Publisher(s): Apress
10. ISBN: 9781484288979
11. Andrew Hoffman Web Application Security . Released March 2020. Publisher(s): O'Reilly Media, Inc. ISBN: 9781492053118
12. Machine Learning for Computer and Cyber Security. Principles, Algorithms, and Practices. Editors Brij B. Gupta, Michael Shen. CRC Press, 2019. – 365 p.
13. A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments <https://csrc.nist.gov/publications/detail/sp/800-207a/draft>.
14. Гайдур Г. І., Шулімова Д. Д., Бойко А. О., Постніков Є. І. Модель забезпечення кібербезпеки інтернету речей. Телекомунікаційні та інформаційні технології. № 2 (2024). С 4-13. DOI: 10.31673/2412-4338.2024.020515
15. Гайдур, Г. І., Гахов, С. О., Марченко, В. В., & Гайдур, К. В. (2024). Концептуальна модель виявлення фішингових атак на основі використання методів опорних векторів. Сучасний захист інформації, 2(58), 24–33. <https://doi.org/10.31673/2409-7292.2024.020003>
16. Гайдур, Г. І., & Бригинець, А. А. (2024). Захист конфіденційних даних у сценаріях Amazon Elastic Block Store. Сучасний захист інформації, 1(57), 15–21. <https://doi.org/10.31673/2409-7292.2024.010002>.
17. Скибун, О. Ж., Гайдур, Г. І., & Гахов С. О. (2024). Аналіз використання концепції BYOD в корпоративних інформаційних системах. Сучасний захист інформації, 1(57), 50–56. <https://doi.org/10.31673/2409-7292.2024.010006> .
18. Легомінова, С.В., Гайдур Г.І. Аналіз сучасних загроз інформаційній безпеці організацій та формування інформаційної платформи протидії їм. Кібербезпека: освіта, наука, техніка. – 2023. - №2(22). – С. 564-67. DOI 10.28925/2663-4023.2023.22.5467
19. Ганченко М.І., Гайдур Г.І., Гахов С.О., Дмитрієв В.Є. “Актуальність та перспектива розвитку Privileged Access Management рішень.” Зв’язок. 2022. №1 (2022). С. 3-9. DOI: 10.31673/2412-9070.2022.010310 Доступ: <https://con.dut.edu.ua/index.php/communication/article/view/2578>
20. Гайдур Г. І., Гахов С. О., Бригинець А. А. Виявлення мережових аномалій з використанням алгоритмів нейронних мереж. Телекомунікаційні та інформаційні технології. № 1 (2023). С. 61-73. DOI: 10.31673/2412-4338.2023.016173
21. Гайдур Г. І. Гахов С. О, Сич М. В., Дмитрієв В. Є. Аналіз загроз мережевого трафіку рівнів моделі OSI для динамічного розрахунку RTO в контексті боротьби з DDOS атаками. Телекомунікаційні та інформаційні технології. № 3 (2023). С. 12-21. DOI: 10.31673/2412-4338.2023.031221
22. Haidur, H. The Method of Increasing the Efficiency of Signal Processing Due to the Use of Harmonic Operators // Zamrii, I., Haidur, H., Sobchuk, A., Zinchenko, K., Polovinkin, I. // 2022 IEEE 4th International Conference on Advanced Trends in Information Theory, ATIT 2022 - Proceedings, 2022, pp. 138–141.(Scopus)
23. Гайдур Г.І., Гахов С.О., Марченко В.В. Метод побудови динамічної моделі логічного об’єкта інформаційної системи та визначення закону його функціонування. Radioelectronic and Computer Systems, 2022, no. 1(101). С. 129-140. doi: 10.32620/reks.2022.1.10. (Категорія А, Scopus).

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, їх поглиблена проробка за рекомендованою літературою. - Усі завдання, передбачені програмою, мають бути виконані у встановлений термін. - Якщо студент відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача. - Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації аспірант повинен вказати джерело, використане в ході виконання завдання.			
* КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ			
Умовою допуску до підсумкового контролю є набрання студентом 60 балів у сукупності за всіма темами дисципліни			
Форми контролю	Види навчальної роботи		Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	Робота на заняттях, у т.ч.:		
	Виконання практичних робіт		27 балів
	Самостійна робота		33 бала
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, отримання міжнародного сертифікату за напрямом.		10 балів за рішенням викладача
ПІДСУМКОВЕ ОЦІНЮВАННЯ іспит	Метою іспиту є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання наукової роботи. Іспит проходить у письмовій формі.		40 балів
ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ			
бали	Критерії оцінювання	Рівень компетентності	Оцінка /затис в екзаменаційній відомості
90-100	Студент 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 Студент 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 студента в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивченні інших дисциплін, а також знання, набуті при самостійному поглибленому вивченні питань, що відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (А)
80-90	Студент демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі	Достатній	Добре /

	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.	Забезпечує студенту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивченні дисципліни	Зараховано (B)
75-81	Студент 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	Студент 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 розглядалися 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	Студент 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, студент 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	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у студента відсутня.	Низький Не забезпечує практичної реалізації задач, що формуються при вивченні дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) В залікову книжку не представляється
0-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі заліку.	Незадовільний Студент 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 представляється

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.