СИЛАБУС КОМПОНЕНТИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

«ПРИКЛАДНА ЗАГАЛЬНА ТЕОРІЯ СИСТЕМ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ»

Лектор курсу			**Гайдур Галина Іванівна**, доктор технічних наук, професор		**Контактна інформація лектора (e-mail), сторінка курсу в Moodle**	**e-mail:** ikbdut@gmail.com; **сторінка курсу в Moodle –** https://dn.dut.edu.ua/course/view.php?id=446	
Галузь знань			12 Інформаційні технології		**Рівень вищої освіти**	Магістр	
Спеціальність			125 Кібербезпека та захист інформації		**Семестр**	9	
Освітня програма			Управління інформаційною та кібернетичною безпекою		**Тип дисципліни**	Основна компонента освітньо-професійної програми	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	4	120	18	-	36		66

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. **КЗ4.** Здатність оцінювати та забезпечувати якість виконуваних робіт.	**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. **КФ6.** Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки

	організації. **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.

Програмні результати навчання (ПРН)

РН5. 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.

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН16. 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.

РН17. 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.

РН23. 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 інформаціних систем ***<u>Знати</u>***: Концепцію «Імунних систем» і термінологію кібербезпеки. Роль і місце кібербезпеки в сучасному цифровому світі. Поширені загрози та вразливості в кіберсистемах. ***<u>Формування компетенцій:</u>*** КЗ1, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***<u>Програмні результати навчання:</u>*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***<u>Рекомендовані джерела:</u>*** 1-5	Лекція 1 2 год	5	Лекція-візуалізація.
Тема 1. Класифікація систем кібербезпеки. ***<u>Знати</u>***: *Уміти застосовувати предметну базу знань. Критично оцінювати результати дослідження* ***<u>Вміти:</u>*** *розв'язувати задачі, пов'язані з основними способами класифікації систем, описом вхідних, вихідних даних та можливих станів системи.* ***<u>Формування компетенцій:</u>*** КЗ1, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***<u>Програмні результати навчання:</u>*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***<u>Рекомендовані джерела:</u>*** 1-11	Практичне заняття 1 4 год		Практичне застосування методики експертних оцінок для класифікації систем кібербезпеки.
Тема 1. Роль і місце систем кібербезпеки в інформаціних системах організацій. ***<u>Знати:</u>*** 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. ***<u>Вміти:</u>*** застосовувати методику управління вразливостями: здійснювати заходи підготовчого етапу; здійснювати початкове сканування вразливостей; визначати коригуючі дії або приймати ризик; здійснювати коригувальні дії; здійснювати перевірку (рескануванння). ***<u>Формування компетенцій:</u>*** КЗ1, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***<u>Програмні результати навчання:</u>*** РН5, РН6, РН7, РН11, РН16, РН17,	Самостійна робота 1 10 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

РП23 ***<u>Рекомендовані джерела:</u>*** 1-5			
Тема 2. Принципи та політики безпеки ***<u>Знати:</u>*** Основи принципів безпеки, які включають конфіденційність, цілісність і доступність. Моделі та політики контролю доступу. Політики та стандарти безпеки. ***<u>Формування компетенцій:</u>*** КЗ1, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***<u>Програмні результати навчання:</u>*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***<u>Рекомендовані джерела:</u>*** 1-5	Лекція 2 2 год	5	Лекція-візуалізація
Тема 2. Застосування методу експертної оцінки для систем ІБ ***<u>Знати:</u>*** розв'язувати задачі, пов'язані з основними методу експертної оцінки. ***<u>Вміти:</u>*** 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 ***<u>Формування компетенцій:</u>*** КЗ1, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***<u>Програмні результати навчання:</u>*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***<u>Рекомендовані джерела:</u>*** 1-11	Практичне заняття 4 год		Вміти вирішувати задачі на основі методу експертних оцінок для класифікації систем кібербезпеки.
Тема 2. Принципи та політики безпеки ***<u>Знати</u>***: Моделі та політики контролю доступу. ***<u>Вміти:</u>*** Застосовувати політики та стандарти безпеки в діяльності організацій. ***<u>Формування компетенцій:</u>*** КЗ1, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***<u>Програмні результати навчання:</u>*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***<u>Рекомендовані джерела:</u>*** 1-6	Самостійна робота 2 10 год		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, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***Програмні результати навчання:*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***Рекомендовані джерела:*** 1-6	Лекція 3 2 год	5	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 ***Формування компетенцій:*** КЗ1, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***Програмні результати навчання:*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***Рекомендовані джерела:*** 1-7	Практичне заняття 3 4 год		Практичне застосування методів та засобів розробки, інтеграції мереж організацій на основі впроваджених стратегій і політик безпеки, з урахування стандартів кібербезпеки.
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, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***Програмні результати навчання:*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***Рекомендовані джерела:*** 1-7	Самостійна робота 3 10 год		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, КЗ 4, КФ2, КФ3, КФ4., КФ6, КФ 8 ***Програмні результати навчання:*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***Рекомендовані джерела:*** 1-7	Лекція 4 2 год	5	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, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***Програмні результати навчання:*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***Рекомендовані джерела:*** 1-8	Практичне заняття 4 4 год		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:*** КЗ1, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***Програмні результати навчання:*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***Рекомендовані джерела:*** 8	Самостійна робота 4 11 год		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:*** КЗ1, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***Програмні результати навчання:*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***Рекомендовані джерела: 8***	Лекція 5 2 год	5	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:*** КЗ1, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***Програмні результати навчання:*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***Рекомендовані джерела:*** 1-11	Практичне заняття 5 4 год		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:*** КЗ1, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***Програмні результати навчання:*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***Рекомендовані джерела:*** 1-11	Самостійна робота 5 11 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Тема 6. Виявлення вторгнень та реагування на інциденти ***Знати:***. Системи виявлення та запобігання вторгненням (IDPS), реагування на інциденти та процедури врегулювання, криміналістичний аналіз та збір доказів. ***Формування компетенцій:*** КЗ1, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***Програмні результати навчання:*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***Рекомендовані джерела:*** 1-12	Лекція 6 2 год	5	Лекція-візуалізація
Тема 6. ***Знати:*** системи виявлення та запобігання вторгненням (IDPS), реагування на інциденти та процедури врегулювання, криміналістичний аналіз та збір доказів. ***Вміти:*** інтегрувати, супроводжувати системи виявлення та запобігання вторгненням (IDPS) на основі кращих світових практик. ***Формування компетенцій:*** КЗ1, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***Програмні результати навчання:*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***Рекомендовані джерела:*** 1-12	Практичне заняття 6 4 год		Практичне застосування систем виявлення та запобігання вторгненням (IDPS) на основі кращих світових практик.
Тема 6. Виявлення вторгнень та реагування на інциденти ***Знати:*** системи виявлення та запобігання вторгненням (IDPS), реагування на інциденти та процедури врегулювання, криміналістичний аналіз та збір доказів. ***Вміти:*** інтегрувати, супроводжувати системи виявлення та запобігання вторгненням (IDPS) на основі кращих світових практик. ***Формування компетенцій:*** КЗ1, КЗ 4, КФ2, КФ3, КФ4., КФ6	Самостійна робота 6 11 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

Програмні результати навчання: РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***Рекомендовані джерела:*** 1-12			
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, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***Програмні результати навчання:*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***Рекомендовані джерела:*** 1-12	Лекція 7 2 год	5	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, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***Програмні результати навчання:*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***Рекомендовані джерела:*** 1-12	Практичне заняття 7 4 год		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, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***Програмні результати навчання:*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***Рекомендовані джерела:*** 1-12	Самостійна робота 7 11 год		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	5	Лекція-візуалізація

Формування компетенцій: КЗ1, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***Програмні результати навчання:*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***Рекомендовані джерела:*** 1-12			
Тема 8. Мобільна безпека та IoT ***Знати:*** технології захисту мобільних пристроїв та IoT. ***Вміти:*** управляти доступом мобільних пристроїв до інформаційних систем організацій. ***Формування компетенцій:*** КЗ1, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***Програмні результати навчання:*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***Рекомендовані джерела:*** 1-12	Практичне заняття 8 4 год		Практичне застосування технології захисту мобільних пристроїв та IoT.
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 мобільних пристроїв до інформаційних систем організацій. ***Формування компетенцій:*** КЗ1, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***Програмні результати навчання:*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***Рекомендовані джерела:*** 1-12	Самостійна робота 8 11 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Тема 9. Нові тенденції в кібербезпеці ***Знати:*** Поточні та нові технології кібербезпеки, розширені постійні загрози (APT) і цілеспрямовані атаки, майбутні напрямки досліджень і розробок у сфері кібербезпеки. ***Формування компетенцій:*** КЗ1, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***Програмні результати навчання:*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***Рекомендовані джерела:*** 12,13	Лекція 9 2 год	5	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, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***Програмні результати навчання:*** РН5, РН6, РН7, РН11, РН16, РН17,	Практичне заняття 9 4 год		Практичне застосування технологій кібербезпеки на основі сучасних світових практик.

РП23 ***Рекомендовані джерела:*** 1-3			
Тема 9. Нові тенденції в кібербезпеці ***Знати:*** напрямки досліджень і розробок у сфері кібербезпеки. ***Формування компетенцій:*** КЗ1, КЗ 4, КФ2, КФ3, КФ4., КФ6 ***Програмні результати навчання:*** РН5, РН6, РН7, РН11, РН16, РН17, РП23 ***Рекомендовані джерела:*** 12,13	Самостійна робота 9 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Комп‘ютерне обладнання, мережа Інтернет ауд. 420, програмні комплекси Nessus Professional, Tenable.sc, IBM QRadar SIEM та IBM QRadar Vulnerability Manager.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. 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 ISBN: 9781484288979
10. Andrew Hoffman Web Application Security . Released March 2020. Publisher(s): O'Reilly Media, Inc. ISBN: 9781492053118
11. Machine Learning for Computer and Cyber Security. Principles, Algorithms, and Practices. Editors Brij B. Gupta, Michael Shen. CRC Press, 2019. – 365 p.
12. 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

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 студент повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату студент отримує за завдання 0 балів.
- Студент, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.
- За використання телефонів і комп'ютерних засобів без дозволу викладача, порушення дисципліни студент видаляється з заняття, за заняття отримує 0 балів.

* КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є набрання студентом 45 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 0,5 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.	Звільняється від іспиту
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***іспит***	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання наукової роботи. Іспит проходить у письмовій формі.	55 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** /*запис 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 вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (А)
82 - 89	Студент демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі	**Достатній**	Добре / Зараховано (В)

	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 вивчені дисципліни	
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 (С)
64-74	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 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)
60-63	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 (Е)
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 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*
1-34	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 проставляється*