СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ ПРОБЛЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ»

Лектор курсу	Ахрамович Володимир Миколайович, доктор технічних наук, професор, професор кафедри систем інформаційного та кібернетичного захисту	**Контактна інформація лектора (e-mail), сторінка курсу в Moodle**	**e-mail:**ptbd_dut@ukr.net; **сторінка курсу в Moodle –** http://dl.dut.edu.ua/course/view.php?id=1195
Галузь знань	12 Інформаційні технології	**Рівень вищої освіти**	Доктор філософії
Спеціальність	125 Кібербезпека	**Семестр**	1,2
Освітня програма	Доктор філософії кібербезпеки	**Тип дисципліни**	Обов'язковий компонент освітньо-наукової програми. Здобуття глибинних знань зі спеціальності.

Обсяг:	Кредитів ECTS	За видами занять:				
		Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	4	18	-	36		66

АНОТАЦІЯ КУРСУ

Взаємозв'язок у структурно-логічній схемі

Освітні компоненти, які передують вивченню	Основи наукових досліджень та організація науки, Методологія наукових досліджень кібербезпеки
Освітні компоненти для яких є базовою	Вибіркові компоненти

Мета курсу:	Формування системи теоретичних знань та практичних навичок щодо можливих небезпек і ступеня ризику втрат інформації, а також практичних навичок щодо забезпечення технічного захисту інформації. Засвоєння здобувачами понять про науку з області технічного захисту інформації, відомостей про математичні моделі та методи захисту інформації, розуміння процесу наукової діяльності в області захисту і оволодіння методологічними та методичними основами наукового дослідження в галузі систем захисту інформації.

Компетентності відповідно до освітньої програми

Soft- skills / Загальні компетентності (ЗК)	**Hard-skills / Спеціальні компетентності (СК)**
ЗК-3. Знання інформаційних технологій – здатність використовувати інформаційні і комунікаційні технології для впровадження проектів в інформаційній та безпековій сферах.	ФК-1. Інтегративна компетентність ФК-4. Професійна компетентність ФК-5. Загальнонаукова компетентність ФК-6. Політехнічна компетентність

	ФК-7. Інженерна компетентність
Програмні результати навчання (ПРН)	
ПРН-5. Уміти розробляти логічні схеми, складати план-проспекти та технічні завдання на виконання наукових досліджень. ПРН-13. Уміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх в усній та/або письмових формах перед фаховою і нефаховою аудиторією. ПРН-17. Уміти підтримувати комплексні системи інформаційної та кібербезпеки в стані, необхідному для вирішення завдань захисту інформації. ПРН-21. Уміти аналізувати та розробляти алгоритми, методики, моделі та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки. ПРН-24. Уміти здійснювати науково-технічне супроводження заходів з формування і коригування програмних комплексів забезпечення безпеки та захисту інформації на об'єктах інформаційної діяльності. ПРН-25. Уміти визначати можливості для підприємницької та громадської діяльності за напрямом захисту інформації, організації й забезпечення інформаційної та кібербезпеки об'єктів інформаційної діяльності. ПРН-31. Уміти проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та кібербезпеки об'єктів інформаційної діяльності. ПРН-32. Уміти обґрунтовувати раціональні шляхи щодо захисту інформації на об'єктах інформаційної діяльності та інформації, що циркулює в ІТ системах та мережах.	

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Змістовий модуль 1. «Теоретичні та практичні проблеми захисту інформації»			
Тема 1. ***Моделі та способи захисту інформації в ТЗІ*** ***Знати***: Проблеми захисту інформації в Україні. Коротку історію захисту інформації. Сучасні загрози інформаційній безпеці. Правові проблеми. Нормативно-методичні проблеми. Технічні проблеми. Організаційні проблеми. Проблеми метрології та регламенту в системі ТЗІ. Доктрину інформаційної безпеки України. Затверджено Указом Президента України від 25 лютого 2017 року. № 47/2017 Закон України «Про основні засади забезпечення кібербезпеки України». (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) Закон України «Про національну безпеку України» від 21 червня 2018 року Національні інтереси України в інформаційній сфері. Актуальні загрози національним інтересам та національній безпеці України в	Лекція 1 2 год. Практичне заняття 1 2 год. .	7	Лекція-візуалізація Загальні положення. Мета та принципи Доктрини. Національні інтереси України в інформаційній сфері. Актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері. Пріоритети державної політики в інформаційній сфері. Механізм реалізації Доктрини. Прикінцеві положення. Закон «Про основні засади забезпечення кібербезпеки України». визначає правові та організаційні основи забезпечення захисту життєво

інформаційній сфері. Пріоритети державної політики в інформаційній сфері. .***Вміти:*** обгрунтовувати та реалізовувати системи захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності, здійснювати вибір методів і засобів захисту інформації з обмеженим доступом на обєктах інформаційної діяльності, здійснювати оцінку систем захисту інформації автоматизованої системи своєму призначенню відповідно до вимог діючих стандартів та нормативних документів, володіти вмінням формувати технології розроблення комплексів захисту інформації з обмеженим доступом та охорони обєктів інформаційної діяльності, розробляти проекти комплексів засобів захисту та охорони обєктів інформаційної діяльності. ***Формування компетенцій:*** ЗК3, ФК-1, ФК-5. ***Результати навчання:***ПРН-13, ПРН-25. ***Рекомендовані джерела:*** 7,8,11,12,16,17,20-26,29-33.			важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. Закон України «Про національну безпеку України» визначає основи та принципи національної безпеки і оборони, цілі та основні засади державної політики, що гарантуватимуть суспільству і кожному громадянину захист від загроз. Як вказується, цим Законом запроваджується всеосяжний підхід до планування у сферах національної безпеки і оборони.
	Самостійна робота		Історичні етапи науки про захист інформації. Доктрина національної безпеки України в інформаційній сфері. Закон України «Про національну безпеку України». Закон «Про основні засади забезпечення кібербезпеки України».
Тема 2. ***Витоки акустичним, електромагнітним, радіоканалами. Побічні електромагнітні випромінювання*** ***Знати***: фізичні основи. Середовища поширення сигналів. Розуміти роль фізичних процесів у появі каналів витоку інформації, знати їх класифікацію та характеристики; знати і вміти застосовувати основні методи, алгоритми і технічні засоби захисту інформації; Акустичні та віброакустичні канали витоку інформації, електромагнітні, радіоканали, візуальні методи, фотографування, відеозйомка, спостереження. Побічні електромагнітні випромінювання та боротьбу з ними. .***Вміти:*** виявляти методи та засоби несанкціонованого доступу до інформації та її руйнування; використовувати підходи до формування моделі загроз; підходи до формування моделі порушника та моделі опису цінності інформації: базові поняття; адитивна модель цінності інформації; порядкова шкала цінностей;	Лекція 2 2 год 7	7	Лекція-візуалізація
	Практичне заняття 2 2 год		Запис звуку, підслуховування і прослуховування; акустоелектричні –канали отримання інформації через звукові хвилі з подальшою передачею її через мережі електроживлення; віброакустичні - сигнали, що виникають за допомогою перетворення інформативного акустичного сигналу при впливі його на будівельні конструкції і інженерно-технічні комунікації приміщень, які захищаються; оптичні. електромагнітні - копіювання полів шляхом зняття індуктивних наводок; радіовипромінювання або електричні сигнали від впроваджених в технічні засоби і приміщення спеціальних електронних пристроїв знімання мовної інформації «закладних пристроїв», які модульовані інформативним сигналом.

модель решітки цінностей; MLS решітка; підходи та моделі оцінки збитків автоматизованої системи та ризику її функціонування; обгрунтовувати та реалізовувати системи захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності на основі правових, організаційних інженерно-технічних заходів до засобів захисту; вміти застосовувати отримані теоретичні знання на практиці при розробленні та впровадженні інформаційно-комунікаційних систем та систем технічного захисту інформації; ***Формування компетенцій:*** ЗК3, ФК-1, ФК-4, ФК-5, ФК-7. ***Результати навчання:*** ПРН-13, ПРН-17, ПРН-24, ПРН-25. ***Рекомендовані джерела:*** 7,8,11,12,16,17,20-26,29-33.	Самостійна робота		Реалізація системи захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності, здійснення вибіру методів і засобів захисту інформації з обмеженим доступом на обєктах інформаційної діяльності, здійснення оцінки систем захисту інформації автоматизованої системи відповідно до вимог діючих стандартів та нормативних документів.
Тема 3. ***Сучасні технології перехоплення інформації. Програмні засоби ТЗІ*** ***Знати***: аналіз та класифікацію сучасних технічних засобів негласного отримання інформації. Загальні відомості про закладні устрої. Класифікація закладних пристроїв. Загальні характеристики закладних пристроїв. Радіозакладні перевипромінюючі ЗНОІ. Радіозакладки. Акустичні закладні устрої. Програмні засоби засобів перехоплення інформації та пошуку закладних пристроїв. .***Вміти:*** використовувати комплекс нормативно-правової бази, в тому числі основні концепції, які визначають сучасний стан та подальший розвиток національної та, як її складової, інформаційної безпеки України; застосовувати сучасні прилади, що використовують для блокування каналів витоку інформації; виявляти та блокувати канали витоку акустичної та каналів витоку	Лекція 3 2 год	7	Лекція-візуалізація
	Практичне заняття 3 2 год		Класифікація програмних засобів засобів перехоплення інформації. Програмні засоби закладних пристроїв, для знімання акустичної, інформації, та за електромагнітними і радіоканалами. Класифікація програмних засобів засобів пошуку закладних пристроїв . Програмні засоби індикаторів поля, радіочастотомів і інтерсепторів. Програмні засоби сканерів приймачів і аналізаторів спектру;. нелінійних радіолокаторів,

електромагнітної інформації; використовувати методики пошуку радіозакладних пристроїв; дотримуватися вимог нормативних документів, що визначають правила обробки інформації з обмеженим доступом засобами обчислювальної техніки; механізми та засоби захисту від шкідливих програмних засобів. ***Формування компетенцій:*** ЗК3, ФК-1, ФК-4, ФК-5, ФК-7. ***Результати навчання:***ПРН-13, ПРН-17, ПРН-24, ПРН-25. ***Рекомендовані джерела:*** 7,8,11,12,16,17,20-26,29-33..	Самостійна робота		Галузь використання. Нормативні посилання. Класифікація пристроїв негласного отримання інформації. Реалізація системи захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності, здійснення вибіру методів і засобів захисту інформації з обмеженим доступом на обєктах інформаційної діяльності, здійснення оцінки систем захисту інформації автоматизованої системи відповідно до вимог діючих стандартів та нормативних документів.
Тема 4.***Контроль доступу*** ***Знати***: Загальні положення. Системи та обладнання СКУД. Організацію	Лекція 4 2 год	7	Лекція-візуалізація
проведення перевірок стану СКУД та ТЗІ. Права посадових осіб УРТЗІ НПУ, що здійснюють перевірку стану СКУД та ТЗІ. Порядок проведення перевірок стану СКУД та ТЗІ. Кваліфікація порушень СКУД. Висновки перевірок стану СКУД та критерії їх складання. .***Вміти:*** обгрунтовувати та реалізовувати системи захисту СКУД на об'єктах інформаційної діяльності, здійснювати вибір методів і засобів захисту інформації з обмеженим доступом на обєктах інформаційної діяльності, розробляти проекти комплексів засобів захисту та охорони обєктів інформаційної діяльності. Використовувати положення про державний контроль за станом технічного захисту інформації. Затверджено Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.05.2007 N 87. Зареєстровано в Міністерстві юстиції України 10 липня 2007 р. за N 785/14052; положення про контроль за станом технічного захисту інформації в органах і підрозділах Національної поліції України. Наказ від29.02.2016 № 139. Зареєстровано в Міністерстві юстиції України 23 березня 2016 р. за № 431/28561. ***Формування компетенцій:*** ЗК3, ФК-1, ФК-4, ФК-5, ФК-7. ***Результати навчання:***ПРН-13, ПРН-17, ПРН-24, ПРН-25. ***Рекомендовані джерела:*** 7,8,11,12,16,17,20-26,29-33..	Практичне заняття 4 2 год		Системи та обладнання СКУД. Обгрунтування та реалізція системи захисту СКУД на об'єктах інформаційної діяльності.
	Самостійна робота		Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.05.2007 N 87. Зареєстровано в Міністерстві юстиції України 10 липня 2007 р. за N 785/14052; положення про контроль за станом технічного захисту інформації в органах і підрозділах Національної поліції України. Наказ від29.02.2016 № 139. Зареєстровано в Міністерстві юстиції України 23 березня 2016 р. за № 431/28561.

Тема 5 ***Організація пошуку засобів негласного отримання інформації та концепції пошуку цифрових засобів*** ***Знати***: Математичні моделі перетворення безперервних сигналів у цифровий вид. Дискретизація за часом. Обмеження енергетичного спектра по частоті. Удосконалення методу перетворення сигналу..Аналіз існуючих автоматизованих комплексів пошуку засобів негласного отримання інформації та концепції пошуку цифрових засобів. Сучасна тенденція розвитку. Розробка концепції пошуку цифрових засобів негласного отримання інформації ***Вміти***: Розробляти методики для локалізації засобів негласного отримання інформації автоматизованими програмними комплексами та застосування методу пасивної радіолокації для локалізації засобів негласного отримання інформації на основі побічного електромагнітного випромінювання. Методики для локалізації засобів негласного отримання інформації автоматизованими програмними комплексами. Застосування методу пасивної радіолокації для локалізації засобів негласного отримання інформації на основі побічного електромагнітного випромінювання. Кластеризацію на основі мультиагентного підходу. Експериментальна перевірка результатів. Проводити комплексних спеціальних перевірок приміщень. Застосовувати методику виконання робіт на підготовчому етапі. Методологія і порядок інструментального пошуку ЗП. Пошук закладних пристроїв з радіочастотним каналом передачі інформації. Сканування радіочастотного діапазону, аналіз радіоелектронної обстановки в приміщенні, виявлення радіовипромінювальних ЗП за допомогою ПАК DigiScan. Пошук пасивних та закладних пристроїв, що використовують низькочастотні магнітні випромінювання і дослідження приміщень на предмет наявності акустичного і віброакустичного каналу витоку інформації. Пошук закладних пристроїв, що використовують низькочастотні магнітні випромінювання. Пошук пасивних закладних	Лекція 5 2 год.	7	Лекція-візуалізація
	Практичне заняття 5 2 год.		Удосконалення методу перетворення сигналу..Аналіз існуючих автоматизованих комплексів пошуку засобів негласного отримання інформації та концепції пошуку цифрових засобів.
	Практичне заняття 6 2 год.		Методики для локалізації засобів негласного отримання інформації автоматизованими програмними комплексами. Застосування методу пасивної радіолокації для локалізації засобів негласного отримання інформації на основі побічного електромагнітного випромінювання
	Лекція 6 2 год.		Лекція-візуалізація
	Практичне заняття 7 2 год.		Пошук закладних пристроїв, що використовують низькочастотні магнітні випромінювання. Пошук пасивних закладних пристроїв.Дослідження приміщень на предмет наявності акустичного і віброакуст ичного каналу витоку інформації

пристроїв.Дослідження приміщень на предмет наявності акустичного і віброакуст ичного каналу витоку інформації ***Формування компетенцій:*** ЗК3, ФК-1, ФК-4, ФК-5, ФК-7 ***Результати навчання:***ПРН-5, ПРН-13, ПРН-17, ПРН-21, ПРН-24,ПРН-25, ПРН-31,ПРН-32 ***Рекомендовані джерела:*** 17,8,11,12,16,17,20-26,29-33..	Самостійна робота		Радіозакладні перевипромінюючі ЗНОІ. Радіозакладки. Акустичні закладні устрої
Змістовий модуль 2. «Теоретичні та практичні проблеми захисту інформації в мережах»			
Тема 6. ***Аналіз уразливості систем захисту інформації з обмеженим доступом*** ***Знати***: Аналіз моделей захисту інформації в інформаційних мережах держави. Аналіз побудови основних моделей захисту інформації. Стратегія технічного захисту інформації в захищених інформаційно-телекомунікаційних системах. Комплексна узагальнена математична модель захисту інформації в мережах загального користування. Концептуальні моделі захисту інформації для технологій стаціонарного, стільникового, супутникового зв'язку. Концептуальна модель захисту інформації для технологій стаціонарного зв'язку. Концептуальна модель захисту інформації для технологій стільникового зв'язку. Концептуальна модель захисту інформації для технологій супутникового зв'язку. ***Вміти***: Застосовувати методологію синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу на державні інформаційні ресурси. Постановка проблеми. Визначення множини станів СІБ. Вибір стратегій КБз. Оптимізація стратегій КБз та оцінювання РЗ. Прогнозування розвитку динаміки процесу КБн. Оптимізація ресурсів КБз та оцінювання РЗ. Блок аналізу ефективності СІб конфіденційність цілісність доступність. Багатоагентне моделювання для дослідження механізмів захисту інформації в мережі Інтернет. Використання заснованого на многоагентних технологіях моделювання процесів забезпечення безпеки Інтернет. Середовище моделювання. Використання міжмережевих екранів. Особливості функціонування міжмережевих екранів. Основні компоненти міжмережевих	Лекція 7 2 год	8	Лекція-візуалізація
	Лекція 8 2 год		Лекція-візуалізація
	Лекція 9 2 год		Лекція-візуалізація
	Практичне заняття 8 4 год		Особливості функціонування міжмережевих екранів. Основні компоненти міжмережевих екранів. Фільтруючі маршрути-затори. Шлюз сеансового рівня. Шлюзи рівня додатків.

екранів.Фільтруючі маршрутизатори. Шлюз сеансового рівня. Шлюзи рівня додатків. Підсилена аутентифікація. Адміністрування і система збору статистики. Основні схеми мережевого захисту на базі міжмережевих екранів. Міжмережевий екран – фільтруючий маршрутизатор. Міжмережевий екран на основі двупортового шлюза. Міжмережевий екран на основі екранованого шлюза. Міжмережевий екран – екранована підмережа. Застосування міжмережевих екранів для організації віртуальних корпоративних мереж. Типові рішення з застосування міжмережевих екранів для захисту інформаційних ресурс. Захист програм за допомогою мереж Петрі. Основні поняття про мережі Петрі. Захист програм за допомогою мереж Петрі. Злом програм, захищених за допомогою мереж Петрі. ***Формування компетенцій:*** ЗКЗ, ФК-1, ФК-4, ФК-5,ФК-6, ФК-7 ***Результати навчання:*** ПРН-5, ПРН-13, ПРН-17, ПРН-21, ПРН-24, ПРН-25, ПРН-31, ПРН-32, ***Рекомендовані джерела:*** 1-6,9,10,12,14-16,26-28			Підсилена аутентифікація. Адміністрування і система збору статистики. Основні схеми мережевого захисту на базі міжмережевих екранів. Міжмережевий екран – фільтруючий маршрутизатор. Міжмережевий екран на основі двупортового шлюза. Міжмережевий екран на основі екранованого шлюза. Міжмережевий екран – екранована підмережа. Застосування міжмережевих екранів для організації віртуальних корпора-тивних мереж. Типові рішення з застосування міжмережевих екранів для захисту інформаційних ресурс.
	Практичне заняття 9 2 год		Основні поняття про мережі Петрі. Захист програм за допомогою мереж Петрі. Злом програм, захищених за допомогою мереж Петрі.
	Практичне заняття 10 2 год		Визначення множини станів СІБ. Вибір стратегій КБз. Оптимізація стратегій КБз та оцінювання РЗ. Прогнозування розвитку динаміки процесу КБн. Оптимізація ресурсів КБз та оцінювання РЗ. Блок аналізу ефективності СІб конфіден-ційність цілісність доступність
	Практичне заняття 11 2 год		Використання заснованого на многоагентних технологіях моделювання процесів забезпечення безпеки Інтернет. Середовище моделювання
	Самостійна робота		Використання міжмережевих екранів. Захист програм за допомогою мереж Петрі. Методологія синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу на державні інформаційні ресурси Багатоагентне моделювання для дослідження механізмів захисту інформації в мережі Інтернет
Тема 7. ***Моделі та способи захисту інформації в соціальних мережах Знати***: Особливості функціонування Web серверів. Підсистема розмежування доступу. Підсистема антивірусного захисту. Підсистема	Практичне заняття 12 2 год	8*	Особливості функціонування Web серверів. Підсистема розмежування доступу. Підсистема антивірусного захисту. Підсистема контролю цілісності. Підсистема виявлення

контролю цілісності. Підсистема виявлення вторгнень. Підсистема аналізу захищеності. Підсистема криптографічного захисту. Підсистема управління засобами захисту Web-порталу. Аналіз математичних моделей захисту інформації у соціальних мережах Огляд комп'ютерних впливів. Аналіз математичних моделей впливів на системи захисту інформації у соціальних мережах. Засоби захисту. Ієрархія захисту баз даних. Метод моделювання нестаціонарних процесів в системах захисту інформації. Аналіз протоколів роботи та протоколів обміну даних пристроїв в мережі Z-Wave , JavaScript API, з метою недопущення втручання в роботу пристроїв захисту інформації. Використання криптографії. ***Вміти:*** володіти вмінням методу оцінювання захисту інформації в соціальних мережах з урахуванням довіри між користувачами та інтенсивності передачі інформації. Основні параметри довіри. Математична модель захисту інформації при лінійних параметрах зовнішних впливів. Математична модель захисту інформації від довіри між користувачами при нелінійних параметрах зовнішних впливів. Визначення фазового портрету системи захисту інформації. Модель зовнішніх впливів. Визначення фазового портрету системи захисту інформації з урахуванням зовнішніх впливів. ***Формування компетенцій:*** ЗКЗ, ФК-1, ФК-4, ФК-5,ФК-6, ФК-7 ***Результати навчання:*** ПРН-5, ПРН-13, ПРН-17, ПРН-21, ПРН-24, ПРН-25, ПРН-31, ПРН-32, ***Рекомендовані джерела:*** 1-6,9,10,12,14-16,26-28			вторгнень. Підсистема аналізу захищеності. Підсистема криптографічного захисту. Підсистема управління засобами захисту Web-порталу.
	Практичне заняття 13 2 год		Концептуальна модель захисту інформації для технологій стаціонарного зв'язку. Концептуальна модель захисту інформації для технологій стільникового зв'язку. Концептуальна модель захисту інформації для технологій супутникового зв'язку
	Практичне заняття 14 2 год		Огляд комп'ютерних впливів. Аналіз математичних моделей впливів на системи захисту інформації у соціальних мережах
	Практичне заняття 15 2 год		Методи та засоби захисту інформації в соціальних мережах. Засоби захисту. Ієрархія захисту баз даних. Метод моделювання нестаціонарних процесів в системах захисту інформації. Аналіз протоколів роботи та протоколів обміну даних пристроїв в мережі Z-Wave , JavaScript API, з метою недопущення втручання в роботу пристроїв захисту інформації. Використання криптографії
	Практичне заняття 16 2 год		Основні параметри довіри. Математична модель захисту інформації при лінійних параметрах зовнішних впливів
	Практичне заняття 17 4 год		Математична модель захисту інформації при нелінійних параметрах зовнішних впливів. Визначення фазового портрету системи захисту інформації.
	Самостійна робота		Особливості функціонування Web серверів. Аналіз математичних моделей впливів на системи захисту інформації у соціальних мережах. Розробка методу оцінювання захисту інформації в соціальних мережах з урахуванням довіри між користувачами та інтенсивності передачі інформації. Визначення фазового портрету системи захисту інформації з урахуванням зов-нішніх впливів.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- Мультимедійний проектор;
- Комп'ютерне обладнання, мережа Інтернет ауд. 423.
- Навчальна лабораторія засобів контролю доступу «HIKVISION»
- Навчальна лабораторія технічного захисту інформації «PIAC»

- Програмне забезпечення. Windows XP, 8,10, Microsoft Office.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Андон П. І. Атаки на відмову в мережі Інтернет: опис проблеми та підходів до її вирішення / П. І. Андон, О. П. Ігнатенко. – К. : Ін-т ПС, 2018. – 52 с. – (Препринт / НАН України, Ін-т програмних систем).
2. Артемов В. Ю. Нормативно-правовий довідник з охорони інформації в Україні. У 4-х томах / Артемов В. Ю., Лєнков О. С., Пашков А. С., Стаднік О. М., Хорошко В. О. – К.: Вид. ДУІКТ, 2018. Бабак В. П. Теоретичні основи захисту інформації / Бабак В. П., Ключников А. А. – НАН Україні, Ін-т проблем безпеки АЕС.– Чорнобиль (Київ.обл.): Ін-т проблем безпеки АЕС, 2018.– с.776
3. Ахрамович В.М. Інформаційна безпека: навч. посіб. К.:ДП «Інформ.-аналіт. Агенство», 2019.-276с.
4. Ахрамович В.М. Методологічні основи захисту інформації в соціальних мережах. Дисертація на на здобуття наукового ступеня доктора технічних наук, спеціальність 05.13.21 «Системи захисту інформації» К.,2021.-302с.
5. Богуш В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. – К. : "МК-Прес", 2018. – 432 с.
6. Гайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Гайворонський, О. М. Новиков. За заг. ред. академіка НАН України М. З. Згуровського. – К. : Видавнича група BHV, 2019. – 608 с.
7. Гайдук О.В. Радіотелекомунікаційні технології: радіопередавальні та радіоприймальні пристрої. – Ніжин: ТОВ «Видавництво «Аспект-Полігаф»», 2017. – 320 с.
8. Голубенко О. Л. Політика інформаційної безпеки / О. Л. Голубенко, В. О. Хорошко, О. С. Петров та ін. – Луганськ : СНУ ім. В.Даля, 2019 – 376 с.
9. Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень : монографія / Р. В. Грищук. – Житомир : Рута, 2017. – 280 с.
10. Домарев В. В. Безпека інформаційних технологій. Системний підхід / В. В. Домарев. – К. : ООО "ТИД "ДС", 2017. – 992 с.
11. Емельянов С. Л. Проблеми захисту інформації від витоку та шляхи її вирішення / Ємельянов С. Л.– Одеса: Фенікс, 2019. – с. 624
12. Єжова Л.Ф. Управління інформаційною безпекою. В 2-х томах / Л.Ф. Єжова, І.О. Мачалін, Я.В. Невойт, В.О. Хорошко. – К.: Вид. ДУІКТ, 2017.
13. Зайцев Д.А. Математичні моделі дискретних систем: Навчальний посібник // Одеса: ОНАЗ ім. О.С. Попова, 2019. – 40 с.
14. Зайцев Д.А. Мережі Петрі і моделювання систем: Навчальній посібник // , Одеса: ОНАЗ ім. О.С. Попова, 2017
15. Згуровський М.З. Основи системного аналізу / М.З. Згуровський, Н.Д. Панкратова. – К:ВНУ, 2017. – 544 с.
16. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Захист інформації технічними засобами: Навчальний посібник / За редакцією Ю.Ф. Каторіна - СПб: Одеса: ОНАЗ ім. О.С. Попова 2018. - 416 с.
17. Козлова К.В. Кількісна оцінка захисту радіоелектронних об’єктів / К.В. Козлова, В.О. Хорошко // Захист інформації. – 2017. – №1. – С. 30-32.
18. Корченко А. Г. Побудова систем захисту інформації на нечітких множинах. Теорія і практичне рішення : монографія / А. Г. Корченко. – К. : "МК-Прсс", 2019. – 320 с.
19. Коханович Г. Ф., Бабак В.П., Фисенко В.М. Спеціальний радіомоніторинг. Київ: МК-Прес, 2007. 384 с.
20. Лаптев О.А. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. Дисертація на на здобуття наукового ступеня доктора технічних наук, спеціальність 05.13.21 «Системи захисту інформації» К.,2020.-393с.
21. Лаптєв О.А., Савченко В.А., Шуклін Г.В. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності Навчальній посібник Київ – 2020.-126с.

22. Ленков С. В. Методи та засоби захисту інформації : монографія [в 2-х т.] Т. 2. Інформаційна безпека / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. – К. : Арій, 2018. – 344 с.
23. Ленков С.В. Методи та засоби захисту інформації. В 2-х томах. Том 1. Несанкціоноване отримання інформації / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко; під ред. В.А. Хорошко. – К.: Арій, 2018. – 464 с.
24. Максименко Г.А., Хорошко В.А. Методи виявлення, обробка та ідентифікації сигналів радіозакладних приладів. К: ПоліграфКонсал-тинг, 2020. 317 с.
25. Мірошніков В.В., Мілих М.Л., Чумак О.І. Системи передачі цифрової інформації: К.: УНДІЗ, 2021. 82 с.
26. Олейник А.А. Субботин С.А. Мультиагентная кластеризация с прямой связью между агентами. Адаптивні системи автоматичного управління. К.: КПІ, 2018. № 13 (33). С. 118 – 128.
27. Онищенко Ю.М. Тексти лекцій з дисципліни «Засоби передавання інформації в системах технічного захисту інформації». Харків: ХНУВС, 2019. (Електронний варіант).
28. Пащенко Р.Е. Красношапка І.В. Максюта Д.В. Генерування та формування сигналів. Харків: ХУПС. 2019. 200 с.
29. Пащенко Р.Е. Красношапка І.В. Максюта Д.В. Генерування та формування сигналів. Харків: ХУПС. 2018. 200 с.
30. Пухов Г.Е. Дифференциальные спектры и модели. К.: Наукова думка, 2020. 184 с.
31. Радзієвський В. Г. Сирота А. А. Теоретичні засади радіоелектронної розвідки. Закрите акціонерне товариство Видавництво Харків: ХУПС, 2019. 432с.
32. Самохвалов Ю.Я., Темніков В.О., Хорошко В.О. Організаційно-технічне забезпечення захисту інформації / За ред. проф. В.О.Хорошка – К.: Видавництво НАУ, 2020. – 208с.

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 пошукувач 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 пошукувач повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату студент отримує за завдання 0 балів.
- Пошукувач, 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 пошукувач видаляється з заняття, за заняття отримує 0 балів.

***КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ**

Умовою допуску до підсумкового контролю є набрання студентом 30 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання

ПОТОЧНИЙ КОНТРОЛЬ	• 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 бал
	•	
Додаткова оцінка	• Участь у наукових конференціях, підготовка наукових публікацій, отримання міжнародного сертифікату за напрямом.	Звільняється від екзамену
РУБІЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)	• Модульний контроль № 1 «Теоретичні та практичні проблеми пошуку закладних цифрових пристроїв»	максимальна оцінка – 15 балів
	Модульний контроль № 2 «Теоретичні та практичні проблеми захисту інформації в мережах»»	максимальна оцінка – 15 балів
	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо.	Звільняється від іспиту
	Метою іспиту є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Іспит проходить у письмовій формі.	30 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо.	Звільняється від іспиту
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***екзамен***	Метою екзамену є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання наукової роботи. Екзамен проходить у письмовій формі.	30 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** /*запис в екзаменаційній відомості*
90-100	Аспірант 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	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції аспіранта в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших	Відмінно / Зараховано (А)

	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 аспірант проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що відносяться до дисципліни, яка вивчається.	
82-89	Аспірант 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 аспіранту 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	Аспірант 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)
64-74	Аспірант 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	Аспірант 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, аспірант 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	Аспірант може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни аспірант виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені	Незадовільно з можливістю повторного складання) / Не

	Цілісність розуміння матеріалу з дисципліни у аспіранта відсутні.	дисципліни	зараховано (FX) *В залікову книжку не проставляється*
1-34	Аспірант повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Аспірант не допущений до здачі заліку.	**Незадовільний** Аспірант 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*