СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ОРГАНІЗАЦІЯ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ»

Лектор курсу	Ахрамович Володимир Миколайович, доктор технічних наук, професор, кафедри систем інформаційного та кібернетичного захисту	**Контактна інформація лектора (e-mail), сторінка курсу в Moodle**	**e-mail:**12z@ukr.net; **сторінка курсу в Moodle –** http://dl.dut.edu.ua/course/view.php?id=1195
Галузь знань	12 Інформаційні технології	**Рівень вищої освіти**	Магістри
Спеціальність	Кібербезпека	**Семестр**	1,2
Освітня програма	Доктор філософії кібербезпеки	**Тип дисципліни**	Професійної та практичної підготовки

Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	5	150	18	-	36		66

АНОТАЦІЯ КУРСУ

Взаємозв'язок у структурно-логічній схемі

Освітні компоненти, які передують вивченню	Методологія наукових досліджень кібербезпеці
Освітні компоненти для яких є базовою	

Мета курсу:	Формування системи теоретичних знань та практичних навичок щодо можливих небезпек і ступеня ризику втрат інформації, одержання практичних навичок щодо забезпечення захисту програмної продукції. засвоєння пошукувачами понять про науку з області захисту інформації, відомостей про математичні моделі захисту інформації сучасної науки, розуміння процесу наукової діяльності в області захисту і, оволодіння методологічними та методичними основами наукового дослідження в галузі систем захисту..

Компетентності відповідно до освітньої програми

Soft- skills / Загальні компетентності (ЗК)	**Hard-skills / Спеціальні компетентності (СК)**
ЗК 1 Уміння критичної самооцінки – здатність визначати та задовольняти потреби особистого та наукового розвитку, бути критичним і самокритичним ЗК-3. Знання інформаційних технологій – здатність використовувати інформаційні і комунікаційні технології для впровадження проектів в інформаційній та безпековій сферах.	ФК-1. Інтегративна компетентність ФК-3. Організаційно-комунікативна компетентність ФК-4. Професійна компетентність ФК-5. Загальнонаукова компетентність ФК-6. Політехнічна компетентність ФК-7. Інженерна компетентність

ЗК-4. Навички керування проектами – здатність демонструвати своєчасність та спланованість у дослідженні, здатність до адаптації та дії в новій ситуації, здатність розробляти та управляти проектами.	ФК-8. Ділова компетентність

Програмні результати навчання (ПРН)

ПРН-5. Уміти розробляти логічні схеми, складати план-проспекти та технічні завдання на виконання наукових досліджень.ПРН 9. Уміти здійснювати вибір методів і засобів захисту інформації з обмеженим доступом на обєктах інформаційної діяльності.
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-18. Уміти аналізувати існуючі технології, методи і засоби застосування шкідливого програмного забезпечення, нівелювання уразливостей мережевих та Web-ресурсів.
ПРН-20. Уміти визначати і вирішувати етичні питання при проведенні досліджень та пошуку відмінностей у шкідливому програмного забезпечення, уразливостях мережевих та Web-ресурсів.
ПРН-21. Уміти аналізувати та розробляти алгоритми, методики, моделі та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки.
ПРН-22. Уміти розробляти та впроваджувати дослідницькі проекти в галузі знань «інформаційні технології» спеціальності «кібербезпека» для забезпечення безпеки мережевої інфраструктури.
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. Коротка історія захисту інформації. Сучасні загрози інформаційній безпеці. Правові проблеми. Нормативно-методичні проблеми. Технічні проблеми.	Лекція 1 2 год.	10	Лекція-візуалізація

Організаційні проблеми. Проблеми метрології та регламенту в системі ТЗІ. Доктрина національної безпеки України в інформаційній сфері. 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 .***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:***ЗК1, ЗК3, ФК-1, ФК-5. ***Результати навчання:***ПРН-13, ПРН-25. ***Рекомендовані джерела:*** 3-5,8.	Практичне заняття 1 2 год. . Самостійна робота		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 Нормативні документи системи ТЗІ УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". від 28 грудня 2021 року № 685/2021. Історичні етапи науки про захист інформації. Доктрина національної безпеки України в інформаційній сфері.
Тема 2. ***Витоки акустичним, електромагнітним, радіоканалами. Побічні електромагнітні випромінювання***	Лекція 2 2 год 7	10	Лекція-візуалізація

Знати: Класифікацію витоку інформації. Акустичні та віброакустичні канали витоку інформації, електромагнітні, радіоканали, візуальні методи, фотографування, відеозйомка, спостереження. Побічні електромагнітні випромінювання та боротьбу з ними. .***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:***ЗК1, ЗК3, ЗК4,ФК-1, ФК-4, ФК-5, , ФК-7. . ***Результати навчання:***ПРН-13, ПРН-17, ПРН-18, ПРН-24, ПРН-25. ***Рекомендовані джерела:*** 1,3-7,8,11,17,20,24,25.	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.
	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***	Лекція 3 2 год	7	Лекція-візуалізація

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:*** 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:***ЗК1, ЗК3, ЗК4,ФК-1, ФК-4, ФК-5, , ФК-7. . ***Результати навчання:***ПРН-13, ПРН-17, ПРН-18, ПРН-24, ПРН-25. ***Рекомендовані джерела:*** 1,3-7,8,11,17,20,24,25.	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,
	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	Практичне заняття 4 2 год		Системи та обладнання СКУД. Обгрунтування та реалізція системи захисту СКУД на об'єктах інформаційної діяльності.

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:***ЗК1, ЗК3, ЗК4,ФК-1, ФК-4, ФК-5, , ФК-7. . ***Результати навчання:***ПРН-13, ПРН-17, ПРН-18, ПРН-24, ПРН-25. ***Рекомендовані джерела:*** 3-6,16,41,44, 45.	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.	Лекція 5 2 год.	10	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

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 пристроїв.Дослідження приміщень на предмет наявності акустичного і віброакуст ичного каналу витоку інформації ***<u>Формування компетенцій:</u>***ЗК1, ЗК3, ФК-1, ФК-4, ФК-5, ФК-7, ФК-8 ***<u>Результати навчання:</u>***ПРН-5, ПРН-13, ПРН-17, ПРН-21, ПРН-24,ПРН-25, ПРН-31,ПРН-32 ***<u>Рекомендовані джерела:</u>*** 1,7 ,11,17,20, 21,24,29,33,34,38,39,41,42.	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
	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*** ***<u>Знати</u>***: Аналіз моделей захисту інформації в інформаційних мережах держави. Аналіз побудови основних моделей захисту інформації.	Лекція 7 2 год	10	Лекція-візуалізація

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 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.	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. 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.

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:***ЗК1, ЗКЗ, ЗК4, ФК-1, ФК-3, ФК-4, ФК-5,ФК-6, ФК-7, ФК-8 ***Результати навчання:***ПРН-5, ПРН=13, ПРН13, ПРН-17, ПРН-18, ПРН-20, ПРН-21, ПРН-22, ПРН-24, ПРН-25, ПРН-31, ПРН-32, ***Рекомендовані джерела:*** 2,4,6,9,14,19,22,27,28,31,37,45	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 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	Практичне заняття 12 2 год	10*	Особливості функціонування Web серверів. Підсистема розмежування доступу. Підсистема антивірусного захисту. Підсистема контролю цілісності. Підсистема виявлення 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-

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:***ЗК1, ЗК3, ЗК4, ФК-1, ФК-3, ФК-4, ФК-5,ФК-6, ФК-7, ФК-8 ***Результати навчання:***ПРН-5, ПРН=13, ПРН13, ПРН-17, ПРН-18, ПРН-20, ПРН-21, ПРН-22, ПРН-24, ПРН-25, ПРН-31, ПРН-32, ***Рекомендовані джерела:*** 2,4,6,9,14,19,22,27,28,31,37,45			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

Закони України:

1. Закон України «Про інформацію» від 02.10.1992 № 2657-XII
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР
3. Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII
4. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-ДСТУ 3396.0-96 ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?artid=38911&cat_id=3 8836.
5. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

Укази президента:

6. № 685/2021Указ президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України».

7. Указ президента України №685/2021. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". від 28 грудня 2021 року

Постанова Кабінету Міністрів України

8. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373
9. Постанова Кабінету міністрів України «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтня 2016 р. № 736[1]
10. Постанова Кабінету Міністрів України "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" від 19.06.2010 № 518.

Нормативні документи

11. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу
12. НД 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. https://zakon.rada.gov.ua/rada/show/v0215519-13.
13. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ ПЕМВН-95). http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id =101798&cat_id-89734&ctime=1344500065981
14. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ЕОТ-95). http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art id=120206&cat id=89769&ctime=1421836194327.
15. НД ТЗІ 1.5-001-2000 Радіовиявлювачі. Класифікація. Загальні технічні вимоги.
16. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106342.

Основна

17. Technical Guide to Information Security Testing and Assessment. Recommendations of the National Institute of Standards and Technology. Karen Scarfone. Murugiah Souppaya. Amanda Cody. Angela Orebaugh. NIST Special Publication 800-115. (Sep. 2008). 80 p. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.
18. Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology. Paul Cichonski. Tom Millar. Tim Grance. Karen Scarfone. Special Publication 800-61 Revision 2 https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.
19. 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.
20. Бабак В. П. Теоретические основы защиты информации / Бабак В. П., Ключников А. А. – НАН Украины, Ин-т проблем безопасности АЭС.– Чернобыль (Киев.обл.): Ин-т проблем безопасности АЭС, 2018.– с.776
21. Богуш В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. – К. : "МК-Прес", 2018. – 432 с.
22. Ленков С. В. Методы и средства защиты информации. В 2-х томах /Ленков С. В., Перегудов Д. А., Хорошко В. А.– К.: Арий,2018.
23. Максименко Г.А., Хорошко В.А. Методы выявления, обработки и идентификации сигналов радиозакладных устройств. К: ПолиграфКонсалтинг, 2020. 317 с.

24. Пащенко Р.Е. Красношапка І.В. Максюта Д.В. Генерування та формування сигналів. Харків: ХУПС. 2019. 200 с.
25. Хорев А.А. Техническая защита информации/ учеб. пособие для студентов вузов/ в 3-х томах. − т. 1: Технические каналы утечки информации. - М.: НПЦ «Аналитика», 2018. - 436 с.

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.	30 балів

	Іспит проходить у письмовій формі.	
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 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.	**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 дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (А)
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 (В)
75 -	Аспірант в загальному добре володіє матеріалом, знає основні положення матеріалу, що	**Достатній**	Добре / Зараховано (С)

	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.	Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	
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. Цілісність розуміння матеріалу з дисципліни у аспіранта відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В заліковv 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 заліковv книжку не проставляється*