Перелік коментарів та пропозицій, які були отримані до проєктів нових (оновлених) програм навчальних дисциплін

Ч.ч.	Назва дисципліни	Статус навчальної дисципліни	Перелік коментарів та пропозицій від стейкхолдерів	
			ТОВ «Консалтингова компанія СІДКОН»	ТОВ «Роберт Бош ЛТД»
1	Спеціальні вимірювання в галузі ТЗІ	Оновлюється	1. Відомо що інформаційна безпека досягається впровадженням відповідного набору заходів безпеки, який охоплює політику, процеси, процедури, організаційні структури й програмні та апаратні функції. Ці заходи безпеки необхідно розробити, впровадити, здійснювати моніторинг, переглядати та, за потреби, вдосконалювати для гарантування досягнення певного рівня безпеки та бізнес-цілей організації. На нашу думку необхідно додатково розглянуть звід практик щодо заходів технічного захисту інформації на підприємстві/організації, як це визначено в стандартах серії ISO/IEC 27000.	1. У навчальній програмі дисципліни рекомендується розглянути порядок зіставлення функціональних компонентів безпеки та довіри, визначених в ISO/IEC 15408, а також порядок виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99.
2	Моніторинг та аудит інформаційно-	Оновлюється	1. В рамках систем моніторингу інформаційно-комунікаційних систем можна було б розглянути центр управління інформаційної безпеки.	1. Було б доцільним розглянути тісний взаємозв'язок бізнес-стратегій з процесами розробки та управління операційною безпекою.

	комунікаційних систем		2. Було б доцільним розглянути системи автоматизації моніторингу інформаційної безпеки. 3. Треба було більш детально розглянути у курсі лабораторних робіт питання протоколювання процесів у центрі інформаційної безпеки та ведення системного журналу.	2. Треба було б провести дослідження центру управління безпекою за допомогою передових практик та стандартів (наприклад, ITIL, COBIT та PCI DSS). 3. Було б доцільним навести ефективність впровадження навчання та інформування користувачів та персоналу аспектів інформаційної безпеки.
3	Комплексні системи безпеки	Оновлюється	1. Потенційно додасть об'єктивності вивчення більшої кількості інтегрованих систем безпеки з оптимальною деталізацією параметрів. 2. Було б доцільним до складу лабораторного курсу включити вивчення сучасних українських систем безпеки з розширеною екосистемою, що дасть можливість вважати їх комплексними системами безпеки з адаптацією до масштабу об'єкта.	
4	Кіберфізична безпека об’єктів критичної інфраструктури	Нова	1. Розробити лабораторні роботи по системам забезпечення сталості та неперервності виробничих процесів. 2. Оновити тематику практичних занять новими інтегрованими видами захисту інформації.	1. Надати поглиблені знання та уміння по системам забезпечення сталості та неперервності технологічних процесів.

5	Управління доступом до інформаційних ресурсів	Нова	1. Більше детально освітити існуючі інтелектуальні мережі з аналізом забезпечення вимог по безпечному доступу до інформаційних ресурсів. 2. З урахування воєнного стану в Україні доцільно більш детальніше розкрити відповідні вимоги до системи управління доступу до інформаційних ресурсів користувачів мережі.	1) було б доцільно розглянути більш детально тенденції удосконалення системи управління доступом до інформаційних ресурсів з урахуванням розвитку технологічної бази інтелектуальної мережі для прогнозування можливих загроз і ризиків інформаційної безпеки у майбутньому; 2) було б доцільно більш детально освітити різні моделі систем управління доступом до інформаційних ресурсів з урахуванням мирного та військового стану держави.

Консультант  Є.В. Василіу