



СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗАКОНОДАВСТВО В ОБЛАСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Галузь знань	12 Інформаційні технології
Шифр та назва спеціальності	125 Кібербезпека та захист інформації
Назва освітньо-професійної програми	Кібербезпека та захист інформації
Рівень вищої освіти	Перший (бакалаврський)
Факультет	Інформаційних технологій і кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	ОК-16 ОПП «Кібербезпека та захист інформації»
Форма навчання	Денна

Викладач

Кільдішев Віталій Йосипович
kildishev@ukr.net



Доцент кафедри Кібербезпеки та технічного захисту інформації,
кандидат технічних наук, доцент

Загальна інформація про дисципліну

Анотація до дисципліни Дисципліна «Законодавство в області інформаційної безпеки» базується на професійно-орієнтованих дисциплінах. Предметом вивчення навчальної дисципліни є міждержавні та вітчизняні стандарти систем інформаційної безпеки,

	інформаційна безпека держави, безпека інформаційних технологій, аналіз ризиків для оцінки реальних загроз порушення інформаційної безпеки, аудит безпеки інформаційних і комунікаційних систем.
Мета дисципліни	– формування основ знань, необхідних майбутнім фахівцям в області інформаційної безпеки; формування знань методології використання державних і галузевих законодавчих та нормативно-правових актів з питань інформаційної безпеки.
Компетентності, формуванню яких сприяє дисципліна	<p>КЗ2. Знання та розуміння предметної області та розуміння професії.</p> <p>КЗ4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p>КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.</p> <p>КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.</p> <p>КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).КФ11.</p> <p>КФ12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.</p>
Результати навчання	<p>ПРН 2. Організувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.</p> <p>ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.</p> <p>ПРН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.</p> <p>ПРН 5. Адаптуватися в умовах частотої зміни технологій професійної діяльності, прогнозувати кінцевий результат.</p> <p>ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.</p> <p>ПРН8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.</p> <p>ПРН10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.</p> <p>ПРН12. Розробляти моделі загроз та порушника.</p> <p>ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.</p>

ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.

ПРН 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних

ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.

ПРН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

Обсяг дисципліни Загальний обсяг дисципліни: 4 кредиту ЄКТС 120 годин

Форма підсумкового контролю Залік

Терміни викладання дисципліни Дисципліна викладається у 3-му семестрі

Програма дисципліни

Тема 1.	Основні цілі та задачі забезпечення інформаційної безпеки. Джерела загроз та засоби їх впливу на об'єкти інформаційної безпеки.
Тема 2.	Основні положення державної інформаційної політики. Основні напрями національної інформаційної політики.

Тема 3.	<i>Характеристика сучасної національної та міжнародної нормативної бази у сфері інформаційної безпеки.</i> Етапи розвитку нормативної бази у сфері інформаційної безпеки.
Тема 4.	<i>Основні положення законодавчої та нормативно-правової бази України щодо захисту інформації.</i> Основні елементи організаційної основи системи забезпечення інформаційної безпеки України.
Тема 5.	<i>Міжнародні стандарти з систем управління інформаційною безпекою.</i> Принципи управління інформаційною безпекою інформаційних систем.
Тема 6.	<i>Оцінка ризиків інформаційної безпеки.</i> Методи оцінки ризиків інформаційної безпеки.
Тема 7.	<i>Міжнародні стандарти з аудиту інформаційної безпеки.</i> Загальні принципи аудиту інформаційної безпеки.

Список рекомендованих джерел

1. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник – К.: «МК-Прес», - 2005. – 432 с.
2. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник / За ред. Кривуци В.Р – Київ: ООО "Д.В.К.", 2004 . – 508 с.
3. Тардаскіна Т. М. Менеджмент інформаційної безпеки в галузі зв'язку : [навч. посібник. Затверджено Міністерством освіти та науки України як посібник для вищих навчальних закладів. Лист № 1/11-7791 від 13 серпня 2010 року] / Т. М. Тардаскіна, В. Г. Кононович. – Одеса: ОНАЗ, 2010. – 268 с.
4. Президент України <http://www.president.gov.ua>
5. Верховна Рада України. <http://www.rada.gov.ua>
6. Кабінет Міністрів України <http://www.kmu.gov.ua>

Інформація про консультації

Щопонеділка у вересні-грудні 2024 року з 13⁰⁰ до 14³⁰ год., ауд. 250 або zoom – доц. В. Й. Кільдішев

Загальна схема оцінювання

Сума балів за всі види навчальної діяльності	Шкала ЄКТС	Оцінка за національною шкалою		Нарахування балів	Бали нараховуються таким чином:
		для іспиту	для заліку		
90-100	A	Відмінно	зараховано	Нарахування балів	<p><i>Оцінювання знань здобувачів вищої освіти здійснюється за 100-бальною шкалою і становить: за поточну успішність (участь у практичних заняттях, виконання практичних завдань та контрольних робіт) – до 60 балів, за результати екзамену – до 40 балів.</i></p>
82-89	B	Добре			
74-81	C				
64-73	D	Задовільно			
60-63	E				
35-59	FX	Незадовільно з можливістю повторного складання	Не зараховано з можливістю повторного складання		
0-34	F	Незадовільно з обов'язковим повторним вивченням дисципліни	Не зараховано з обов'язковим повторним вивченням дисципліни		

Політика опанування дисципліни

Відвідування: Здобувачі вищої освіти самостійно планують відвідування лекційних занять, що проводяться в межах дисципліни. Присутність на практичних заняттях, лабораторних заняттях та контрольних заходах (екзамен/залік) є обов'язковою. При проведенні занять в онлайн режимі, присутність здобувача враховується у разі відкритого вікна.

Дотримання принципів академічної доброчесності: Підготовка усіх завдань, письмових робіт і т. ін., що виконуються в межах дисципліни, здійснюється здобувачем вищої освіти самостійно, на засадах академічної доброчесності. Викладач має право для перевірки робіт застосовувати програму **Unicheck**.

Умови зарахування пропущених занять:

Інші умови: Навчально-методичні матеріали дисципліни розміщені на платформі Moodle, за посиланням <https://e-learning.suitt.edu.ua/course/view.php?id=929>