СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ: ПРОЕКТУВАННЯ, ВПРОВАДЖЕННЯ, СУПРОВІД

Галузь знань	12 Інформаційні технології
Шифр та назва спеціальності	125 Кібербезпека
Назва освітньо-професійної програми	Кібербезпека та захист інформації
Рівень вищої освіти	Перший (бакалаврський)
Факультет	Інформаційних технологій та кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	ОК-25 ОПП «Кібербезпека та захист інформації»
Форма навчання	Денна

Викладач

Онацький Олексій Віталійович
onatsky@meta.ua

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

Загальна інформація про дисципліну

Анотація до дисципліни	Забезпечення безпеки інформації у інформаційно-комунікаційних системах здійснюється шляхом створення та впровадження комплексних систем захисту інформації. Комплексна система захисту інформації – це сукупність організаційних та інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації від несанкціонованого доступу. У дисципліні висвітлюються основні поняття щодо, комплексних систем захисту інформації, інформаційних ресурсів з обмеженим доступом та необхідності захисту інформації від несанкціонованого

	доступу та розповсюдження. Принципи проектування та етапи створення комплексних систем захисту інформації.
Мета дисципліни	– ознайомлення студентів з принципами побудови системи захисту та етапи створення комплексних систем захисту інформації з застосуванням існуючої нормативної бази в Україні; – розвиток у студентів практичних навичок у послідовності розробки КСЗІ; – підготовка висококваліфікованих фахівців, здатних ставити завдання на виконання етапів створення КСЗІ.
Компетентності, формуванню яких сприяє дисципліна	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. 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.).
Результати навчання	ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. 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. ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та кібербезпеки. ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. ПРН 11. Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах. ПРН 12. Розробляти моделі загроз та порушника. ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень. 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 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). ПРН 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту. ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем. ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки. ПРН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів. ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем. ПРН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.

	ПРН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки. ПРН 36. Виявляти небезпечні сигнали технічних засобів. ПРН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах. ПРН 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
Обсяг дисципліни	Загальний обсяг дисципліни: 6 кредитів ЄКТС 150 годин. Для денної форми навчання: лекції – 34 годин, практичні заняття – 24 години, лабораторні заняття – 24 годин, самостійна робота – 68 годин.
Форма підсумкового контролю	Екзамен
Терміни викладання дисципліни	Дисципліна викладається у 1-му та 2-му семестрі

Програма дисципліни	
Тема 1.	***Введення в курс. Базові принципи, поняття та терміни у сфері технічного захист інформації.*** Питання передпроектної організації захисту інформації. Основні принципи побудови системи захисту. Аналіз погроз інформації в системах телекомунікації.
Тема 2.	***Системний підхід до вирішення проблеми захисту інформації. Принципи побудови системи захисту.*** Системно-концептуальний похід до захисту інформації в автоматизованих системах. Комплексна система захисту інформації. Основні вимоги до комплексної системи захисту інформації.
Тема 3.	***Основні етапи створення систем захисту інформації.*** Основи, напрямки й етапи побудови систем захисту інформації. Матриця інформаційної безпеки. Подання елементів матриці.
Тема 4.	***Технічна модель IT-безпеки стандарту ISO/IEC 15408.*** Функціональні вимоги безпеки, адекватності, профілю захисту та проекту.
Тема 5.	***Структура й завдання органів, що здійснюють захист інформації.*** Структура й завдання органів, що здійснюють захист інформації. Структура служби інформаційної безпеки. Типовий перелік завдань служби захисту інформації.
Тема 6.	***Питання оцінки ефективності й проектування систем захисту.*** Загальний похід до оцінки ефективності систем додаткового захисту. Основний критерій захищеності. Способи завдання вихідних параметрів для оцінки захищеності. Метод статистичної оцінки. Метод експертної оцінки.
Тема 7.	***Програмно-технічні методи й засоби захисту інформації.*** Програмно-технічні методи й засоби захисту інформації. Служби та механізми захисту.
Тема 8.	***Апаратні засоби захисту інформації.*** Функції контролю й керування систем захисту інформації. Інтеграція механізмів захисту.
Тема 9.	***Етапи створення КСЗІ. Порядок проведення робіт із створення КСЗІ в ІТС.*** Нормативні документи ТЗІ, які визначають порядок створення КСЗІ в ІТС. Етапи створення КСЗІ.
Тема 10.	***Формування вимог до КСЗІ та її завдань. Обґрунтування необхідності створення КСЗІ.*** Обґрунтування необхідності створення КСЗІ і призначення СЗІ. Наказ про порядок проведення робіт зі створення КСЗІ. Наказ про створення СЗІ. Положення про СЗІ. Перелік інформації, що підлягає обробленню в ІТС та потребує захисту.
Тема 11.	***Категоріювання ІТС.*** Категоріювання ІТС. Наказ про призначення комісії з категоріювання. Акт категоріювання.
Тема 12.	***Обстеження середовищ функціонування ІТС.*** Наказ про призначення комісії з обстеження. Акт обстеження. Формуляр ІТС.

Тема 13.	***Опис моделі порушника політики безпеки інформації.*** Категорії порушників. Специфікація моделі порушника за мотивами здійснення порушень, рівнем кваліфікації, показником можливостей використання засобів та методів подолання системи захисту, часом дії, місцем дії.
Тема 14.	***Опис моделі загроз для інформації. Формування завдання на створення КСЗІ.*** Перелік загроз з визначенням порушень властивостей інформації та ІТС. Загрози конфіденційності, цілісності, доступності, спостереженості інформації. Формування завдань та варіанту побудови КСЗІ. Оформлення звіту за результатами проведеної роботи.
Тема 15.	***Розробка політики безпеки інформації в ІТС. Вибір варіанту КСЗІ.*** Методичні вказівки щодо структури та змісту Плану захисту інформації в АС. Документальне оформлення політики безпеки. Порядок проведення відновлювальних робіт і забезпечення неперервного функціонування ІТС. Календарний план робіт із захисту інформації в ІТС.
Тема 16.	***Складання технічного завдання на створення КСЗІ. Введення КСЗІ в дію та оцінка захищеності інформації в ІТС.*** Розробка технічного завдання на створення комплексної системи захисту інформації. Пуско-налагоджувальні роботи. Попередні випробування КСЗІ. Протокол попередніх випробувань КСЗІ в ІТС. Акт завершення попередніх випробувань КСЗІ в ІТС.
Тема 17.	***Дослідна експлуатація КСЗІ. Державна експертиза КСЗІ.*** Порядок розроблення та оформлення програм і методик випробувань. Акт завершення дослідної експлуатації КСЗІ в ІТС. Акт завершення робіт зі створення КСЗІ в ІТС. Порядок організації та проведення експертизи. Етапи роботи Експерта. Складу супровідної документації КСЗІ згідно вимог НД ТЗІ.

Список рекомендованих джерел

1. Про внесення змін до Закону України “Про інформацію” № 2938-VI від 13.01.2011. – Відомості Верховної Ради України 2011, № 32, ст. 313. – (Серія видань “Законодавство України”)
2. Закон України “Про захист персональних даних” № 2297-VI від 01.06.2010. – Відомості Верховної Ради України 2010, № 34, ст. 481. – (Серія видань “Законодавство України”).
3. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” № 80/94-ВР від 05.07.1994. – Відомості Верховної Ради України 1994, № 31, ст. 286. – (Серія видань “Законодавство України”).
4. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. – Затверджено наказом ДСТСЗІ СБ України № 125 від 8.11.2005. – (Серія видань “Нормативний документ”).
5. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. – Затверджено наказом ДСТСЗІ СБ України № 22 від 28.04.99. – (Серія видань “Нормативний документ”).
6. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – Затверджено наказом ДСТСЗІ СБ України № 22 від 28.04.1999. – (Серія видань “Нормативний документ”).
7. НД ТЗИ 1.1-003-99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа. – (Серія видань “Нормативний документ”).
8. Положення про Державну експертизу в сфері технічного захисту інформації. – Затверджено наказом Адміністрації ДССЗЗІ України № 93

від 16.05.07. – Офіційний вісник України. – 2007. – № 52, ст. 2153. – (Серія видань “Нормативний документ”).

9. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. – Затверджено наказом Адміністрації ДССЗЗІ України № 65 від 12 березня 2011. – (Серія видань “Нормативний документ”).

10. 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.

11. Кононович В.Г., Гладиш С.В. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. Частина 4: навч. посіб. – Одеса: ОНАЗ ім. О.С. Попова, 2009.

12. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спеціальності 125 "Кібербезпека" спеціалізації "Системи технічного захисту інформації" / І. Є. Антіпов, А. М. Олейніков, Ю. В. Ликов и др. ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків : ХНУРЕ, 2019. – 216 с.

13. Яремчук Ю. Є. Комплексні системи захисту інформації : навчальний посібник / Вінниця : ВНТУ, 2018. – 118 с.

Інформація про консультації

Щопонеділка у вересні-грудні 2023 року з 14^{30} до 15^{00} год., ауд. 248 або зум – доц. О. В. Онацький

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		***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.
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 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.**