СИЛАБУС ДИСЦИПЛІНИ «ПРОУКТУВАННЯ, ВПРОВАДЖЕННЯ, СУПРОВІД КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ»

Ступінь вищої освіти – Бакалавр
Спеціальність 125 – КІБЕРБЕЗПЕКА
Освітня програма «Кібербезпека»
Рік навчання 2, семестр 3
Форма навчання денна
Кількість кредитів ЄКТС 5
Мова викладання українська

Лектор курсу	**Кулініч Олег Миколайович, к.т.н., доцент.**
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем, мереж та кібербезпеки корпус. 15, к. 207, тел. 0445278724 e-mail o.kulinich@nubip.edu.ua**
Сторінка курсу в eLearn	**ЕНК (4 семестр)** https://elearn.nubip.edu.ua/course/view.php?id=3403

ОПИС ДИСЦИПЛІНИ

Навчальна дисципліна передбачає вивчення організаційних та інженерно-технічних заходів, спрямованих на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу. Знайомство з базовими організаційними заходами для комплексних систем захисту інформації, а також інженерно-технічними заходами. Засвоєння функціональних можливостей та методів побудови комплексних систем захисту інформації, опановування необхідними прийомами та практичними навичками при налаштуванні та конфігуруванні сучасного мережевого обладнання.

Навчальна дисципліна забезпечує формування ряду фахових компетентностей:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 8. Здатність до абстрактного і системного мислення, аналізу та синтезу.

Спеціальні (фахові, предметні) компетентності (СК):

СК1. 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.

СК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

СК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

СК4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

СК5. Здатність забезпечувати захист інформації, що обробляється в інформаційнотелекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

СК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

СК9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

СК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

СК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

СК13. Здатність розробляти апаратне, алгоритмічне та програмне забезпечення, компоненти комп'ютерних систем захисту інформації.

У результаті вивчення навчальної дисципліни студент набуде певні програмні результати, а саме

ПРН6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

ПРН10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

ПРН11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.

ПРН13. Аналізувати проекти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних.

ПРН16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.

ПРН20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.

ПРН21. 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.

ПРН22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

ПРН23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

ПРН25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та

інформаційнотелекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

ПРН28. 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.

ПРН30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.

ПРН35. 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.

ПРН36. Виявляти небезпечні сигнали технічних засобів.

ПРН37. 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.

ПРН38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційнотелекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.

ПРН50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

Зробимо курс корисним для вас. Якщо ви будете наполегливо працювати і докладати особливих зусиль, щоб не відставати від матеріалу, ви отримаєте винагороду – як в короткостроковій перспективі, так і в набутті фахових компетентностей. Будь-ласка, широко використовуйте аудиторні заняття, відеоінструкції, вебінари, щоб переконатися, що рухаєтесь за графіком навчання.

СТРУКТУРА КУРСУ

Тема	**Години** (лекції/ Лабораторні,)	**Результати навчання**	**Завдання**	**Оцінювання**
4 семестр				
Модуль 1. Порядок проведення робіт із створення комплексної системи захисту інформації.				
Тема 1. Нормативнометодичне забезпечення з питань побудови КСЗІ та проведення їх державної експертизи.	**4/2**	- Вміти критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.	1. Підготовка до лабораторної роботи. 2. Виконання лабораторної роботи.	**15**

Тема 2. Формування загальних вимог до КСЗІ в ІТС.	**4/4**	- Вміти виконувати аналіз та декомпозицію інформаційнотелекомунікаційних систем. - Вміти виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. - Аналізувати проекти інформаційнотелекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних. - Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів. - Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах. - 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. - Вирішувати задачі управління процедурами ідентифікації,	3. Захист звітів з лабораторної роботи.	**15**
Тема 3. Порядок та приклад розробки акту обстеження ІТС.	**4/2**			**15**
Тема 4. Поняття моделі загроз та моделі порушника.	**2/4**			**15**
Тема 5. Типове положення про службу захисту інформації в автоматизованій системі.	**4/2**			**15**
Тема 6. Етапи створення комплексної системи захисту інформації в ІТС.	**2/4**	автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки. - Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на		**15**

Тема 7. Технічне завдання на створення та експлуатацію КСЗІ в складі ІТС.	**2/4**	основі моделей управління доступом (мандатних, дискреційних, рольових). - 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. - Виявляти небезпечні сигнали технічних засобів. - Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризикорієнтованому контролі доступу до інформаційних активів.		**10**
Модуль 2. Визначення відповідності комплексної системи захисту інформації технічному завданню.				
Тема 1. Критерії оцінки захищеності інформації в ІТС (частина 1)	**4/4**	- 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. - Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем. - 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. - 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.	1. Підготовка до лабораторної роботи. 2. Виконання лабораторної роботи. 3. Захист звітів з лабораторної роботи.	**15**
Тема 2. Критерії оцінки захищеності інформації в ІТС (частина 2)	**4/4**			**15**
Тема 3. Критерії гарантій захищеності інформації в ІТС.	**4/4**			**15**
Тема 4. Методика та порядок проведення випробувань КСЗІ.	**2/4**			**15**
Тема 5. Спеціальні дослідження основних та додаткових ТЗ.	**4/2**			**10**
Тема 6. Порядок ліцензування господарської діяльності.	**2/3**			**10**

Тема 7. Ліцензування діяльності в галузі ТЗІ.		- Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційнотелекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. - Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистичносигнатурних). - Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.		**10**
Тема 8. Експертиза комплексної системи захисту інформації.	**3/2**			**10**
Всього за семестр				**0,7*(100+ 100)/2 = 70**
Екзамен			**Тест, теоретичні питання, задача**	**30**
Всього за курс				**100**

ПОЛІТИКА ОЦІНЮВАННЯ

Політика щодо дедлайнів та перескладання:	Дедлайни визначені в ЕНК. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний, стажування або відрядження).
Політика щодо академічної доброчесності:	Списування під час самостійних робіт, тестування та екзаменів заборонені (в т.ч. із використанням мобільних девайсів).
Політика щодо відвідування:	Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в дистанційній on-line формі за погодженням із деканом факультету)

ШКАЛА ОЦІНЮВАННЯ СТУДЕНТІВ

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл.1 «Положення про екзамени та заліки у НУБіП України» (наказ про уведення в дію від 27.12.2019 р. № 1371):

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів заліків**	
	Екзаменів	**Заліків**
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

Рекомендована література

Основна:

1. НД ТЗІ 3.7-003 -2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» // Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. Київ. 2005. – С. 22.
2. Закон України «Про захист інформації в автоматизованих системах» // Відомості Верховної Ради України, 1994. - № 31. – С. 286.
3. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.].Вінниця : ВНТУ, 2018. - 118 с.
4. Проєктування комплексних систем захисту інформації. Підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020. 320 с

Допоміжна

1. Кузнецов О.О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2011. – 510 с.
2. Постанова Кабінету Міністрів України від 08 жовтня 1997 року № 1126 "Про затвердження Концепції технічного захисту інформації в Україні".
3. Постанова Кабінету Міністрів України від 27 листопада 1998 року № 1893 "Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію".
4. Постанова Кабінету Міністрів України від 19 липня 2006 року № 1000 "Деякі питання обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію".

5. Постанова Кабінету Міністрів України від 29 березня 2006 року № 373 "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах".

6. Постанова Кабінету Міністрів України від 12 серпня 2009 року № 869 "Про затвердження загальних вимог до програмних продуктів, які закуповуються та створюються на замовлення державних органів".

7. Указ Президента України від 27 вересня 1999 року № 1229 "Про затвердження Положення про технічний захист інформації в Україні".

8. Наказ Адміністрації Держспецзв'язку від 16 травня 2007 року № 93 "Про затвердження Положення про державну експертизу в сфері технічного захисту інформації", зареєстрований в Міністерстві юстиції України 16 липня 2007 року за № 820/14087.

9. Наказ Адміністрації Держспецзв'язку від 26 березня 2007 року № 45 "Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації", зареєстрований в Міністерстві юстиції України 10 квітня 2007 року за № 320/13587.

10. Державний стандарт України ДСТУ 3396.0-96 "Захист інформації. Технічний захист інформації. Основні положення".

11. Державний стандарт України ДСТУ 3396.1-96 "Захист інформації. Технічний захист інформації. Порядок проведення робіт".

12. Державний стандарт України ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни та визначення".

13. Державні будівельні норми України ДБН А.2.2-2-96 "Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва".

14. Нормативний документ системи технічного захисту інформації НД ТЗІ 1.1-002-99 "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу".

15. Нормативний документ системи технічного захисту інформації НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу".

16. Нормативний документ системи технічного захисту інформації НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі".

17. Нормативний документ системи технічного захисту інформації НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу".

18. Нормативний документ системи технічного захисту інформації НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні

функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу".

19. Нормативний документ системи технічного захисту інформації НД ТЗІ 3.6-001-2000 "Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу".

20. Нормативний документ системи технічного захисту інформації НД ТЗІ 3.7-001-99 "Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі".

21. Нормативний документ системи технічного захисту інформації НД ТЗІ 2.5-008-2002 "Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2".

22. Нормативний документ системи технічного захисту інформації НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі".

23. Нормативний документ системи технічного захисту інформації НД ТЗІ 2.5-010-2003 "Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу".

24. Нормативний документ системи технічного захисту інформації НД ТЗІ 3.6-003-2016 "Порядок проведення робіт зі створення та атестації комплексів технічного захисту інформації".

25. Нормативний документ системи технічного захисту інформації НД ТЗІ 2.7 -009-09 "Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу".

Інформаційні ресурси

1. АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ [Електронний ресурс] – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=81998&cat_id=38835