СИЛАБУС ДИСЦИПЛІНИ «БЕЗПЕКА ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ»

Ступінь вищої освіти - Бакалавр
Спеціальність 125 - Кібербезпека
Освітня програма «Кібербезпека»
Рік навчання 3, семестр 5
Форма навчання - денна_(денна, заочна**)**
Кількість кредитів ЄКТС 4
Мова викладання українська_(українська, англійська)

Лектор дисципліни	**МАМЧЕНКО Сергій Миколайович, д.пед. н., професор** 
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем і мереж та кібербезпеки** **корпус. 15, к. 207, тел. 527-87-24** **e-mail s.mamchenko@nubip.edu.ua**
Сторінка дисципліни в eLearn	**https://elearn.nubip.edu.ua/course/view.php?id=4784**

ОПИС ДИСЦИПЛІНИ

(до 1000 друкованих знаків)

Навчальна дисципліна є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в області кібербезпеки. На базі здобутих знань та умінь фахівець зможе вирішувати професійні задачі, що базуються на сучасних технологіях та методах захисту інформації у сучасних інформаційно-комунікаційних системах та мережах. Метою викладання дисципліни є розкриття сучасних методів захисту інформації в інформаційно- комунікаційних системах та мережах і ознайомлення з особливостями їх апаратної та програмної реалізацій. Дисципліна передбачає вивчення: видів загроз інформації в інформаційно-комунікаційних системах; програмних та програмно-апаратних комплексів засобів захисту інформації; відновлення функціонування інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов; моніторинг процесів функціонування інформаційно-комунікаційних систем; механізми безпеки комп'ютерних мереж.

Компетентності ОП:

загальні компетентності (ЗК):

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

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

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

Спеціальні (фахові, предметні) компетентності (СК):

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.

СК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (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.).

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

ПРН3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

ПРН4. 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.

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

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

ПРН14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

ПРН17. 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.

ПРН20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомуні каці йних 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.

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

ПРН29. 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.

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

ПРН31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

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

ПРН51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.

ПРН52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

СТРУКТУРА КУРСУ

Тема	Години (лекції/ Лабора	Результати навчання	Завдання	Оціню вання
5 семестр				
Модуль 1. Основні поняття щодо безпеки інформації в інформаційно-комунікаційних системах.				
Тема 1. Модель взаємодії елементів інформаційно - комунікаційної системи.	**2/2**	**- Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. - 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. - Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. - Аналізувати проекти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних. - Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень. - 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. - Здійснювати**	**1. Підготовка до лабораторної роботи. 2. Виконання лабораторної роботи. 3. Захист звітів з лабораторної роботи.**	**10**
Тема 2. Побудова систем управління інформаційною безпекою інформаційно-комунікаційних систем.	**2/2**			**15**
Тема 3. Процедури ідентифікації, автентифікації, авторизації користувачів.	**2/2**			**15**
Тема 4. Модель загроз безпеці інформації в інформаційно - комунікаційних системах.	**2/2**			**15**
Тема 5. Модель порушника безпеки інформації в інформаційно - комунікаційних системах.	**2/2**			**15**
Тема 6. Моделі управління доступом в інформаційно - комунікаційних системах.	**2/2**			**15**
Тема 7. Моделі безпеки інформації в інформаційно-комунікаційних системах.	**2/2**			**15**

Модуль 2. Методи та засоби забезпечення безпеки інформації в інформаційно-комунікаційних системах.				
Тема 1. Методи та засоби забезпечення інформаційної безпеки інформаційно – комунікаційних систем	**2/2**	**- Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних(автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-**	**1. Підготовка до лабораторної роботи.**	**10**
Тема 2. Фізична безпека інформаційно - комунікаційних систем.	**2/2**	**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.** **- Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.** **- Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.** **- Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.** **- Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично- сигнатурних).** **- Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно- телекомунікаційних системах.** **- Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.**	**2. Виконання лабораторної роботи.** **3. Захист звітів з лабораторної роботи.**	**10**
Тема 3. Основні підсистеми комплексу засобів захисту в інформаційно - комунікаційних системах.	**2/2**			**15**
Тема 4. Системи виявлення вторгнень та системи запобігання вторгненням.	**2/2**			**15**
Тема 5. Реєстрація подій в інформаційно-комунікаційних системах.	**2/2**			**10**
Тема 6. Моніторинг процесів функціонування інформаційно - комунікаційних систем.	**2/2**			**15**
Тема 7. Механізми безпеки комп'ютерних мереж.	**2/2**			**15**
Тема 8. Внутрішній аудит безпеки інформації в інформаційно - комунікаційних системах.	**2/2**			**10**
Всього за семестр				**0,7*(100+ 100)/2 = 70**
Екзамен			**Тест, теоретичні**	**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)

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

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

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. Кормич Б.А. Інформаційна безпека: організаційно-правові основи. / Б.А. Кормич. - К., Принт. 2004. -169 с.
4. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Василіу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. - К. : ЦП «Компринт» О.В., 2020. - 444 с.
5. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. - Х.: Вид. ХНЕУ, 2010. - 316 с.

6. Браіловський М.М. Захист інформації у банківській діяльності / М.М. Браіловський, Г.П. Лазарєв, В.О. Хорошко. - К.: ТОВ “ПоліграфКонсалтинг”, 2010. - 216 с.
7. 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.
8. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. - Х. : Вид. ХНЕУ, 2013. - 476 с. (Укр. мов.).
9. Основи інформаційної безпеки / С. В. Кавун, О. А. Смірнов, В. Ф. Столбов - Кіровоград : Вид. КНТУ, 2012. - 414 с.