СИЛАБУС ДИСЦИПЛІНИ «ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ 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	 **Касаткін Дмитро Юрійович, к.пед.н., доцент** (Портфоліо НПП)
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем, мереж та кібербезпеки корпус. 15, к. 207, тел. 5278199** **e-mail d.kasatkin@nubip.edu.ua**
Сторінка курсу в eLearn	**ЕНК (4 семестр)**

ОПИС ДИСЦИПЛІНИ

Навчальна дисципліна передбачає вивчення організаційних методів захисту, організаційно-технічних та організаційно-правових заходів, наукового підходу до організації захисту інформації; планування захисту; керування системою захисту; безперервності процесу захисту інформації; мінімальної достатності організації захисту; системного підходу до організації та проектування систем та методів захисту інформації; комплексного підходу до організації захисту інформації; відповідності рівня захисту цінності інформації; гнучкість захисту; багатозональності захисту, що передбачає розміщення джерел інформації в зонах з контрольованим рівнем її безпеки; обмеження числа осіб, які допускаються до захищеної інформації; особиста відповідальність персоналу за збереження довіреної інформації.

Навчальна дисципліна забезпечує формування ряду фахових компетентностей:

Загальні компетентності:

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.

Спеціальні (фахові, предметні) компетентності (СК):

СК 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.

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

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

СК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

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

СК8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

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

В результаті вивчення навчальної дисципліни студент набуде певні програмні результати (РН), а саме

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/або кібербезпеки.

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 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 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

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.

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
1 семестр				
Модуль 1. Системи управління інформаційною безпекою.				
Система національного законодавства України та міжнародного законодавства у сфері кібербезпеки.	**2/2**	Вміти діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.	Теоретичне опитування Здача лабораторної роботи	**6**
Системи управління інформаційною безпекою. Основні принципи побудови СУІБ.	**2/2**	Знати та вміти 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.	Опитування. Здача лабораторної роботи	**8**
Основи управління інформаційними ризиками.(Ч.1+Ч.2)	**4/4**	Вміти здійснювати оцінювання ризиків інформаційної безпеки та управління такими ризиками.	Опитування Здача лабораторної роботи	**8**
Напрямки побудови СУІБ. Політика ІБ організації.	**2/2**	Вміти застосовувати законодавчу та нормативно-правову базу для побудови СУІБ, а також розробляти політику ІБ організації.	Здача лабораторної роботи	**8**
Фізична безпека організації та устаткування. Управління комп'ютерами та мережами. Управління доступом. Вимоги до інформаційних систем.	**2/2**	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки	Здача лабораторної роботи	**6**
Управління інцидентами в СУІБ. Питання безперервності функціонування організації.	**2/2**	Здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.	Опитування Здача лабораторної роботи	**8**
Внутрішній аудит СУІБ.	**2/2**	Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно з встановленою політикою інформаційної та\або кібербезпеки.	Опитування Здача лабораторної роботи	**8**
Самостійна роботп	**48**	Поняття системи управління інформаційною безпекою. Сутність політики інформаційної безпеки. Основні принципи побудови системи управління інформаційною безпекою. Напрямки побудови системи управління інформаційною безпекою. Заходи щодо організації захисту інформації. Класифікація інформації. Маркування інформації. Поводження з інформаційними ресурсами. Політика контролю доступу. Доступ до мереж та послуг мережі.	Опитування	**10**

		Управління доступом користувача. Поняття контрольованої зони. Поняття інформаційних ризиків. Поняття оцінки ризиків інформаційної безпеки.		
Модульний контроль			Підсумковий тест в ЕНК	**30**
Модуль 2. Впровадження системи управління інформаційною безпекою.				
Методика впровадження СУІБ.	**2/2**	Вміти впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.	Опитування	**5**
Розробка документа політики інформаційної безпеки та цілей СУІБ. Управління інформаційними активами. .(Ч.1+Ч.2)	**4/4**	Вміти розробляти політики інформаційної безпеки та цілей СУІБ. Здійснювати управління інформаційними активами.	Опитування Здача лабораторної роботи.	**10**
Впровадження системи управління інформаційними ризиками.	**2/2**	Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.	Здача лабораторної роботи.	**10**
Розробка та обґрунтування заходів з обробки та зниженню інформаційних ризиків.	**2/2**	Вміти розробляти та обґрунтовувати заходів з обробки та зниження інформаційних ризиків.	Здача лабораторної роботи.	**10**
Структура документації СУІБ та порядок її розробки. Розробка управлінських процедур.	**2/2**	Вміти застосовувати законодавчу та нормативно-правову базу для розробки документації СУІБ та управлінських процедур.	Здача лабораторної роботи.	**5**
Розробка плану безперервності функціонування організації. Розробка процедур реагування на надзвичайні ситуації. Розробка процедур переходу на аварійний режим. Введення в дію СУІБ.	**2/2**	Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.	Здача лабораторної роботи.	**10**
Самостійна робота	**42**	Сутність оброблення ризиків інформаційної безпеки. Організаційні ролі, відповідальності та повноваження. Цілі інформаційної безпеки та планування їх досягнення. Поняття створення та оновлення документованої інформації. Контроль документованої інформації. Робоче планування та контроль. Оцінювання результативності інформаційної безпеки. Внутрішній аудит інформаційної безпеки. Перегляд системи управління інформаційною безпекою. Корегувальні дії по відношенню до системи управління інформаційною безпекою. Дії вищого керівництва організації з управління по відношенню до систем управління інформаційною безпекою.		**10**

		Зобов'язання вищого керівництва організації по відношенню до систем управління інформаційною безпекою.		
Модульний контроль			Підсумковий тест в ЕНК	**30**
Всього за семестр				**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 «26» квітня 2023 р. протокол № 10):

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. Мужанова Т. М. Організаційне забезпечення інформаційної безпеки підприємства: основні засад / Т. М. Мужанова // Сучасний захист інформації. – 2016. №2. - с.78-82. - Режим доступу: http://nbuv.gov.ua/UJRN/szi_2016_2_13.
2. Правовий захист інформації: Навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса: Фенікс, 2015. – 264 с., іл.
3. Національний стандарт, який відповідає ISO/IEC 27001; Cor 1:2014, IDT) Information technology — Security techniques — Information security management systems — Requirements (Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги).
4. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
5. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2017. – 120 с.