СИЛАБУС ДИСЦИПЛІНИ «ПРОВЕДЕННЯ РОЗСЛІДУВАНЬ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Ступінь вищої освіти – бакалавр
Спеціальність 125 – Кібербезпека
Освітня програма «Кібербезпека»
Рік навчання 4, семестр 8
Форма навчання денна
Кількість кредитів ЄКТС 5
Мова викладання українська

Лектор курсу	**Лахно Валерій Анатолійович, д.т.н., професор (портфоліо)** 
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем, мереж та кібербезпеки корпус. 15, к. 207, тел. 0445278724 e-mail lva964@nubip.edu.ua**
Сторінка курсу в eLearn	**ЕНК (8 семестр)**

ОПИС ДИСЦИПЛІНИ

Завдання навчальної дисципліни «Проведення розслідувань інцидентів інформаційної безпеки» - є теоретична та практична підготовка здобувачів до проведення розслідувань інцидентів інформаційної безпеки в різних установах та на підприємствах, зокрема АПК.

Місце і роль дисципліни в системі підготовки фахівців відповідно до навчального плану. Дана навчальна дисципліна є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в області кібербезпеки.

Набуття компетентностей:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності:

КЗ2. Знання та розуміння предметної області та розуміння професії.

КЗ4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ5. Здатність до пошуку, оброблення та аналізу інформації.

КЗ8. Здатність до абстрактного і системного мислення, аналізу та синтезу.

Спеціальні (фахові) компетентності:

СК4. Здатність забезпечувати неперервність бізнесу згідно 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.).

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

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.

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

ПРН7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;

ПРН8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;

ПРН9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;

ПРН25. 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;

ПРН42. 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/ лабора-торні)	Результати навчання	Завдання	Оціню-вання
1 семестр				
Модуль 1.				
Вступ, мета та цілі дисципліни. Аудити інформаційної безпеки	**2/0**	Ознайомитися з цілями та метою дисципліни, її важливість в системі підготовки фахівця з кібербезпеки	Опитування.	-
Системи менеджменту інформаційної безпеки (СМІБ) за вимогами ISO/IEC 27001.	**4/4**	Вміти застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.	Захист лабораторної роботи	**7**
Комплексний аудит інформаційної безпеки. Реалізація програми аудиту	**4/4**	Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки	Захист лабораторної роботи.	**7**
Оцінка діяльності з управління інформаційною безпекою організації.	**4/4**	Вміти вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.	Захист лабораторної роботи.	**7**
Системи менеджменту інцидентами інформа-ційної безпеки. Етапи управління інцидентами інформаційної безпеки ISO/IEC 27035	**4/4**	Вміти визначати показники ефективності процесу управління інцидентами інформаційної безпеки.	Захист лабораторної роботи.	**7**
Концепція та структура автоматизованої системи управління інцидентами інформаційної безпеки	**2/4**	Вміти забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.	Захист лабораторної роботи.	**7**
Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT. Програмні рішення у розслідуваннях інцидентів інформаційної безпеки \ кібербезпеки	**4/4**	Вміти впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки	Захист лабораторної роботи.	**7**

Модульний контроль	**0/2**		Підсумковий тест в ЕНК.	**28**
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

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. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 «Кібербезпека» / Корченко О.Г., Шелест М.Є., Казмірчук С.В. та ін. – Ніжин: ТПК «Орхідея», 2019. – 408 с.

2. Аудит та управління інцидентами інформаційної безпеки: навч. посіб / Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін. – К: НА СБУ, 2014. – 190 с.

3. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.

4. ISO/IEC 27001:2013 «Система управління інформаційною безпекою. Вимоги».

5. ISO/IEC 27032:2012 «Інформаційні технології – Методи забезпечення безпеки - Керівництво з кібербезпеки».

6. ISO/IEC 27035:2011 «Інформаційні технології. Методи забезпечення безпеки. Управління інцидентами інформаційної безпеки».