|  |  |
| --- | --- |
| E:\nubip_logo_new_poisk_18_2.png | **СИЛАБУС ДИСЦИПЛІНИ** **«ТЕОРІЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»** |
| **Ступінь вищої освіти – Бакалавр** |
| **Спеціальність 125 – КІБЕРБЕЗПЕКА** |
| **Освітня програма «Кібербезпека»** |
| **Рік навчання 2, семестр 4****Форма навчання** денна |
| **Кількість кредитів ЄКТС 4** |
| **Мова викладання** українська |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| **Лектор курсу** |  C:\Users\Alex\Desktop\aIMG_4137.JPG**Бакалинський Олександр Олегович** **(портфоліо)** |
| **Контактна інформація лектора (e-mail)** | **Кафедра комп'ютерних систем і мереж,****корпус. 15, к. 207, тел. 5278724****e-mail baov@meta.ua** |
| **Сторінка курсу в eLearn**  | **ЕНК (4 семестр)**  |

**ОПИС ДИСЦИПЛІНИ**

Метою викладання навчальної дисципліни є формування у майбутніх фахівців системи спеціальних знань та сучасного мислення в галузі інформаційної безпеки, наукового підходу при наданні консультацій та розроблянні пропозицій, здатності надання практичних рекомендацій щодо прийняття управлінських рішень, а також здатності до опрацювання проектів нормативно-правових документів на відповідність чинним міжнародним нормам щодо забезпечення інформаційної безпеки.

В результаті вивчення дисципліни слухачі отримують знання з сучасних методів протидії загрозам інформаційної безпеки, з природи, основних видів ризиків інформаційної безпеки; актуальних проблеми управління ризиками інформаційної безпеки. Заняття будуть спрямовані на формування умінь з використання методів та засобів оцінювання ризиків інформаційної безпеки; планування та здійснення конкретних заходів щодо протидії та нейтралізації загроз інформаційної безпеки; з підготовки та надання пропозицій щодо удосконалення нормативних та розпорядчих документів з питань забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; з використання знань й умінь в прогнозуванні, виявленні та оцінюванні можливих загроз інформаційної безпеки, дестабілізуючих чинників.

**Навчальна дисципліна забезпечує формування ряду фахових компетентностей**:

**ФК1**. 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.

**ФК9**. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

**ФК12**. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно

з встановленою політикою інформаційної та/або кібербезпеки.

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

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

**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 33.** Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;

**ПРН 44.** 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;

**ПРН** **46.** Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

**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** | **Оціню-вання** |
| **1 семестр** |
| **Модуль 1. Природа й основні види ризиків у сфері інформаційної безпеки.** |
| Природа й основні види ризиків у сфері інформаційної безпеки. Основні елементи управління ризиками. | **8.4** | Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;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. | Теоретичне опитуванняТестування | **20****20** |
| Процес та етапи управління ризиками. | **6/4** | Теоретичне опитуванняТестування | **20****10** |
| Модульний контроль  | Підсумковий тест в ЕНК | **30** |
| **Модуль 2. Інструментальні засоби управління ризиками інформаційної безпеки.** |
| Міжнародний стандарт ISO/IEC 27005 «Інформаційна технологія. Методи та засоби забезпечення безпеки інформації». | **2/2** | Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки | Опитування Здача лабораторної роботи | **5****10** |
| Використання стандарту BSI 100-3 «Аналіз ризиків на основі IT-Grundschutz». | **2/2** | Опитування Здача лабораторної роботи | **5****10** |
| Стандарти NIST 800-39 «Управління ризиками інформаційної безпеки». та NIST 800-30 «Настанови стосовно управління ризиком». | **2/2** | ОпитуванняЗдача лабораторної роботи | **5****10** |
| Впровадження процесу управління ризиками інформаційної безпеки | **4/6** | 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  | **25** |
| Модульний контроль | Підсумковий тест в ЕНК | **30** |
| **Модуль 3. Види аналізу ризиків проектів.**  |
| Застосування методів ідентифікування ризиків інформаційної безпеки. | **0/4** | 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; | Тестування та опитування.Здача лабораторної роботи. | **5****10** |
| Види аналізу ризиків проектів. Застосування методів аналізу ризиків інформаційної безпеки. | **0/2** | ОпитуванняЗдача лабораторної роботи. | **5****10** |
| Оцінювання ризиків. Табличний метод визначення оцінок ризиків інформаційної безпеки. | **2/2** | Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класівЗдійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. | Здача лабораторної роботи. | **10** |
| Застосування методів атестування ризиків інформаційної безпеки. | **0/2** | Здача лабораторної роботи. | **10** |
| Основні перспективні напрями розвитку інформаційних технологій захисту інформації. Заходи та засоби обробляння ризиків інформаційної безпеки. | **0/2** | Здача лабораторної роботи. | **10** |
| Технічні, прикладні, системні програмні засоби підтримання та захисту інформації. Програмні засоби оцінювання ризиків інформаційної безпеки. | **0/4** |  | Здача лабораторної роботи. | **10** |
| Модульний контроль | Підсумковий тест в ЕНК | **30** |
| **Всього за 1 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 |