|  |  |
| --- | --- |
| E:\nubip_logo_new_poisk_18_2.png | **СИЛАБУС ДИСЦИПЛІНИ**  **«КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ»** |
| **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** | https://nubip.edu.ua/sites/default/files/imagecache/120x160/dsc_7616.jpg**Лахно Валерій Анатолійович, д.т.н., професор**  **(**[**портфоліо**](https://docs.google.com/document/d/1EQrGnT_fG6QJS2EHVPvmUM1-v61S3DXGkUoVhCRrO8k/edit?usp=sharing)**)** |
| **Контактна інформація лектора (e-mail)** | **Кафедра комп'ютерних систем і мереж,**  **корпус. 15, к. 207, тел. 5278724**  **e-mail lva964**[**@nubip.edu.ua**](mailto:nklimenko@nubip.edu.ua) |
| **Сторінка курсу в eLearn** | **ЕНК (4 семестр)** |

**ОПИС ДИСЦИПЛІНИ**

Метою викладання дисципліни є формування у студентів знань з організації комплексних систем захисту інформації (КСЗІ) на підприємстві. Завдання дисципліни: вивчення сутності та завдань комплексної системи захисту інформації (КСЗІ); вивчення принципів організації та етапів розробки КСЗІ, факторів, що впливають на організацію КСЗІ; визначення та нормативне закріплення складу інформації, яка підлягає захисту; визначення об'єктів захисту; аналіз і оцінка загроз безпеці інформації: виявлення та оцінка джерел, способів і результатів дестабілізуючого впливу на інформацію; визначення потенційних каналів і методів несанкціонованого доступу до інформації, визначення можливостей несанкціонованого доступу до інформації, яка підлягає захисту; визначення компонентів і умов функціонування КСЗІ, розробка моделі, технологічного та організаційної побудови КСЗІ; кадрове, матеріально-технічне та нормативно-методичне забезпечення функціонування КСЗІ; призначення, структура і зміст управління КСЗІ, вивчення принципів і методів планування, сутності і змісту контролю функціонування КСЗІ; вивчення особливостей управління КСЗІ в умовах надзвичайних ситуацій; вивчення складу методів і моделей оцінки ефективності КСЗІ.

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

ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

ФК 13. Здатність досліджувати проблему в галузі комп’ютерних та інформаційних технологій, визначати їх обмеження.

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

ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

ПРН 11. Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах.

ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних.

ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.

ПРН 21. 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.

ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

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 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 35. 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.

ПРН 36. Виявляти небезпечні сигнали технічних засобів.

ПРН 37. 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.

ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН 45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.

ПРН 50. 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/  Лабора-торні,) | **Результати навчання** | **Завдання** | **Оціню-вання** |
| **8 семестр** | | | | |
| **Модуль 1. Системний метод при вирішенні завдань забезпечення комплексного захисту інформації.** | | | | |
| Мета комплексного захисту інформації (ЗІ) та способи її забезпечення. Системний метод при вирішенні завдань забезпечення комплексного захисту інформації. | **2/2** | Вміти здійснювати пошук інформації в різних джерелах для розв’язання задач комплексного захисту інформації (ЗІ). | Теоретичне опитування. | **10** |
| Визначення можливих каналів витоку інформації. Визначення об'єктів та елементів захисту. Оцінка загроз технічних розвідок (ТР) та інших джерел загроз безпеці інформації, що захищається. | **2/2** | Вміти розробляти моделі загроз та порушника. Знати базові технічні засоби захисту інформації. | Здача лабораторної роботи. | **10** |
| Вибір методів і засобів захисту інформації. Технічний захист інформації. Види інформації, що захищається технічними засобами. Демаскуючі ознаки об'єктів захисту і їх класифікація. Канали витоку інформації (оптичний, акустичний, радіоелектронний). методи захисту від несанкціонованого перехоплення мовної, візуальної, оптичної, радіоелектронної інформації. | **2/2** |
| Фізичний захист інформації. Принципи, сили, кошти та умови організаційного захисту інформації. Організація внутрішньо об'єктного і пропускного режиму підприємства. | **2/2** | Використовувати методи та принципи організації системи охорони підприємства (Фізична охорона, пожежна та охоронна сигналізація, охоронне телебачення, системи обмеження доступу). | Здача лабораторної роботи. | **10** |
| Організація системи охорони підприємства (Фізична охорона, пожежна та охоронна сигналізація, охоронне телебачення, системи обмеження доступу). | **2/2** |
| Організація аналітичної роботи із запобігання перехопленню конфіденційної інформації. Напрямки та методи роботи з персоналом, що володіє конфіденційною інформацією. Визначення політики захисту інформації на підприємстві. | **2/2** | Вміти застосовувати знання для Організація аналітичної роботи із запобігання перехопленню конфіденційної інформації. | Здача лабораторної роботи. | **10** |
| Особливості організації комплексного захисту інформації, віднесеної в установленому порядку до державної таємниці. Визначення сил і засобів, необхідних для захисту інформації. | **2/2** |
| Особливості віднесення відомостей, що становлять службову, конфіденційну, комерційну та державну таємницю до різних ступенів і категорій доступу. | **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. | Здача лабораторної роботи. | **10** |
| Технологія визначення і класифікації складу і захищеності інформації. | **2/2** |
| Здача лабораторної роботи.  Неформальна оn-line освіта на основі МВОК. | **10**  **20** |
| Модульний контроль | | | Підсумковий тест в ЕНК | **20** |
| **Модуль 2. Побудова та управління комплексною системою захисту інформації..** | | | | |
| Розробка моделей комплексної системи захисту інформації. Визначення та розробка складу нормативно-технічної документації (НТД) щодо забезпечення захисту інформації, матеріально-технічне та нормативно-методичне забезпечення функціонування КСЗІ.. | **2/2** | Вміти застосовувати знання для розробки складу нормативно- НТД щодо забезпечення захисту інформації на підприємстві. | Тестування та опитування. | **5** |
| Структура і зміст технології управління комплексною системою захисту інформації. Планування та оперативне управління системою ЗІ. | **2/2** | Опитування  Здача лабораторної роботи. | **5**  **10** |
| Організація служби захисту інформації (СЗІ) та організаційне проектування діяльності СЗІ. Порядок створення СЗІ, склад нормативних документів, що регламентують діяльність служб захисту інформації. | **4/4** | Вміти вирішувати задачі по організації служби захисту інформації на підприємстві. | Здача лабораторної роботи.  Опитування | **20**  **5** |
| Забезпечення умов безперервності в інформаційній сфері організації. Роль ради директорів і виконавчих органів організації. Ідентифікація недоліків. Безперервність сервісів в мінливому середовищі та забезпечення КСЗІ. | **2/2** | Здача лабораторної роботи. | **10** |
| Здача лабораторної роботи.  Неформальна оn-line освіта на основі МВОК. | **10**  **15** |
| **Зміст і особливості методології оцінки ефективності КСЗІ. Основні моделі оцінки ефективності КСЗІ.** | **2/2** |
| Модульний контроль | | | Підсумковий тест в ЕНК | **20** |
| **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 |