|  |  |
| --- | --- |
| E:\nubip_logo_new_poisk_18_2.png | **СИЛАБУС ДИСЦИПЛІНИ**  **«ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ І КІБЕРБЕЗПЕКА»** |
| **Ступінь вищої освіти – Магістр** |
| **Спеціальність 123 – КОМП’ЮТЕРНА ІНЖЕНЕРІЯ** |
| **Освітня програма «Комп’ютерні системи і мережі»** |
| **Рік навчання 1, семестр 1,2**  **Форма навчання** денна |
| **Кількість кредитів ЄКТС 8** |
| **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 (1 семестр)** <https://elearn.nubip.edu.ua/course/view.php?id=1886> |

**ОПИС ДИСЦИПЛІНИ**

Навчальна дисципліна передбачає вивчення теоретичних основ проблеми зберігання, передачі, перетворення, закриття та відновлення інформації в організаціях і на підприємствах різних напрямків діяльності та різних форм власності, способів захисту від несанкціонованого доступу до інформації. Вивчаються методологічні, організаційні та наукові основи розробки апаратно-програмних засобів і систем збору та захисту інформації (ЗІ), забезпечення інформаційної безпеки процесів опрацювання, зберігання та поширення інформації в інформаційно-комунікаційних мережах з урахуванням сучасного стану та прогнозу розвитку методів, систем і засобів здійснення погроз з боку потенційних порушників.

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

ЗК 1. Здатність до абстрактного і системного мислення, аналізу та синтезу на основі логічних аргументів та достовірної інформації.

ЗК 6. Здатність використання інформаційних та комунікаційних технологій .

ЗК 7. Здатність використовувати нормативні правові документи в професійній діяльності.

ФК 1. Базові знання технічних характеристик, конструктивних особливостей, застосування правил експлуатації комп’ютерних систем, мереж та програмно-технічних засобів.

ФК 2. Здатність до проектування, дослідження, забезпечення ефективних режимів роботи роботизованих і мікроконтролерних комп’ютерних систем, комп’ютерних мереж, систем захисту інформації.

ФК 3. Здатність до розробки робочої проектної та технічної документації, оформлювання результатів завершених проектно-конструкторських робіт з проектування комп’ютерних систем.

ФК 4. Здатність розробляти та досліджувати алгоритмічне та програмне забезпечення комп’ютерних систем спеціалізованого призначення, Інтернет додатків, кіберфізичних систем з використанням сучасних методів і мов програмування, а також засобів і систем автоматизації проектування.

ФК 6. Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних і безпечних обчислень, брати участь в модернізації, реконфігурації та реконструкції комп’ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності.

ФК 8. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів для забезпечення захисту інформації.

ФК 9. Здатність оформляти отримані робочі результати у вигляді презентацій, науково-технічних звітів, статей і доповідей на науково-технічних конференціях.

ФК 11. Здатність аргументувати вибір методів розв’язування спеціалізованих задач, критично оцінювати отримані результати та захищати прийняті рішення.

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

ПРН 1. Знати і розуміти наукові і математичні положення, що лежать в основі функціонування комп’ютерних засобів, систем та мереж.

ПРН 4. Вміти застосовувати знання для розв’язування задач аналізу та синтезу апаратних і програмних засобів комп’ютерних систем захисту інформації, ІоТ систем.

ПРН 6. Вміти розробляти системне і прикладне програмне забезпечення для систем захисту інформації та ІоТ систем, мобільних систем, використовуючи сучасні технології програмування.

ПРН 9. Вміти оцінювати отримані результати та аргументовано захищати прийняті рішення.

**Зробимо курс корисним для вас. Якщо ви будете наполегливо працювати і докладати особливих зусиль, щоб не відставати від теоретичного та практичного матеріалу, ви отримаєте винагороду – як в короткостроковій перспективі, так і в набутті фахових компетентностей. Будь-ласка, широко використовуйте аудиторні заняття, відеоінструкції на ЕНК, вебінари, щоб переконатися, що рухаєтесь за графіком навчання**.

**СТРУКТУРА КУРСУ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Тема** | **Години**  (лекції/  лабораторні,) | | **Результати навчання** | **Завдання** | **Оцінювання** |
| **1 семестр** | | | | | |
| **Модуль 1. Механізми реалізації послуг безпеки.** | | | | | |
| Ризики порушення політики інформаційної безпеки (ІБ). Вимоги щодо безпеки інформаційно-комунікаційних систем (ІКС), ризики безпеки. | **4/4** | | Вміти застосовувати теоретичні знання та практичні навички для розв’язування задач аналізу та синтезу захищених ІКС, КМ та ІоТ систем, зокрема, для агропромислового комплексу країни. | Опитування у вигляді ессе з основних теоретичних питань. | **10** |
| Механізми реалізації послуг безпеки. Політика ІБ підприємства, зокрема у галузі АПК та його ІКС. | **4/4** | | Вміти здійснювати формалізований опис політик інформаційної безпеки для об’єктів захисту. | Здача лабораторної роботи.  Виконання самостійної роботи (Неформальна оn-line освіта на основі МВОК). | **20** |
| Аналіз моделей безпеки ІКС. | **4/4** | | Вміти аналізувати доцільність використовування різних моделей безпеки для конкретних ІКС. Вміти застосовувати знання та практичні навички для розв’язування задач аналізу та синтезу апаратних і програмних засобів ІКС, КМ та ІоТ систем. | Здача лабораторної роботи.  Опитування | **10**  **5** |
| Аналіз безпеки програмного забезпечення (ПЗ). | **4/4** | | Вміти розробляти програмне забезпечення для систем захисту інформації та ІоТ систем, мобільних систем, використовуючи сучасні технології програмування. Вміти аналізувати ПЗ з точки зору безпеки його використовування в ІКС. | Здача лабораторної роботи.  Опитування | **20**  **5** |
| **Модульний контроль** | | | | Підсумковий тест в ЕНК | **30** |
| **Модуль 2. Сучасні системи криптографічного захисту інформації.** | | | | | |
| Сучасні методи та моделі ідентифіка-ції та аутентифі-кації користувачів в ІКС. | **2/2** | | Знати методи та моделі ідентифікації та аутентифікації користувачів в ІКС. | Здача лабораторної роботи. | **15** |
| Сучасні системи криптографічного захисту інформації. | **4/4** | | Знати режими роботи сучасних криптосистем. Вміти розв’язувати практичні задачі по створенню надійних систем криптографічного захисту інформації, використовувати засоби асиметричної криптографії у банківській, комерційній та інших галузях, вміти проводити теоретичні та експериментальні дослідження в сучасних напрямках асиметричної криптографії, в задачах криптоаналізу систем та протоколів криптографії з відкритим ключем. | Опитування, розв’язання задачі | **10** |
| Апаратні системи криптографічного захист інформації. | **4/4** | | Здача лабораторної роботи.  Опитування. | **20**  **5** |
| Квантові та постквантові системи криптографічного захисту інформації. | **4/4** | | Знати основні переваги квантової криптографії, основи протоколу BB84. | Захист лабораторної роботи.  (Неформальна оn-line освіта на основі МВОК). | **20**  **10** |
| **Модульний контроль** | | | | Підсумковий тест в ЕНК. | **20** |
| **Всього** | | | |  | **70** |
| **Екзамен** | | | |  | **30** |
| **Всього за 1 семестр** | | | | | **100** |
| **2 семестр** | | | | | |
| **Модуль 1. Методи захисту інформації у автоматизованих системах.** | | | | | |
| Способи несанкціонованого зняття інформації. Методи та засоби блокування технічних каналів витоку інформації на об’єктах інформатизації. | **4/4** | | Вміти застосовувати знання для розв’язування задач аналізу технічних каналів витоку інформації на об’єктах інформатизації, зокрема для агропромислового комплексу країни. | Теоретичне опитування  Неформальна оn-line освіта на основі МВОК  Здача лабораторної роботи. | **15**  **15** |
| Методи та засоби захисту електромагнітної інформації. | **4/4** | | Знати методи та засоби захисту електромагнітної інформації. | Здача лабораторної роботи. | **10** |
| Методи захисту інформації у автоматизованих системах (АС). | **4/4** | | Вміти використовувати методи та засоби захисті інформації в АС різноманітного призначення, зокрема для галузі АПК. | Здача лабораторної роботи. | **20** |
| Методи захисту інформації у телекомуніка-ційних мережах та відкритих мережах зв’язку. | | **4/4** | Здатність застосовувати сучасні технології та методи захисту інформації в ІКС, телекомунікаційних мережах та відкритих мережах зв’язку, проводити командні роботи, пов’язані із розв’язанням комплексних завдань захисту інформації та кібербезпеки. | Здача лабораторної роботи. | **20** |
| Модульний контроль | | | | Підсумковий тест в ЕНК | **20** |
| **Модуль 2. Розгортання та використовування систем виявлення вторгнень.** | | | | | |
| Загальні принципи побудови захищених інформаційно-комунікаційних систем (ЗІКС) та КМ. | **2/2** | | Знати загальні принципи побудови захищених інформаційно-комунікаційних систем (ЗІКС) та комп’ютерних мереж (КМ). | Тестування та опитування.  Опитування. | **5**  **10** |
| ПЗ для адміністрування ЗІКС та КМ. | **4/4** | | Вміти використовувати сучасне програмне забезпечення для адміністрування ЗІКС та КМ. | Здача лабораторної роботи | **10** |
| Методи та моделі аудиту кібернетичної безпеки для об’єкту інформатизації. | **4/4** | | Знати та вміти використовувати для розв’язання практичних завдань методи аудиту кібернетичної безпеки для об’єктів інформатизації, зокрема, для підприємств у галузі АПК. | Здача лабораторної роботи. | **30** |
| Розгортання та використовування систем виявлення вторгнень (СВВ). Сканери вразливостей. Засоби виявлення аномалій у КМ. | **4/4** | | Вміти використовувати СВВ, сканери вразливостей, засоби виявлення аномалій у КМ. | Здача лабораторної роботи.  Неформальна оn-line освіта на основі МВОК. | **15**  **10** |
| Модульний контроль | | | | Підсумковий тест в ЕНК | **20** |
| **Всього за 2 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 |