|  |  |
| --- | --- |
| E:\nubip_logo_new_poisk_18_2.png | **СИЛАБУС ДИСЦИПЛІНИ**  **«МЕТОДИ ТА ЗАСОБИ 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** | 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 (3 семестр)** |

**ОПИС ДИСЦИПЛІНИ**

Метою вивчення дисципліни «Методи та засоби захисту інформації» є ознайомлення з основними фізичними принципами, методами та засобами захисту інформації та пошуку розвідувальної апаратури, надання студентам знань з основ захисту інформації, принципів, методів та засобів несанкціонованого одержання інформації, а також створення протидії захисту інформації по каналах, на яких можливі її втрати. Вивчаються наступні питання: засоби несанкціонованого одержання інформації; методи протидії та захисту інформації від її несанкціонованого одержання; канали несанкціонованого одержання інформації; принципи та методи захисту інформації; механізми захисту інформації; методи захисту програмного забезпечення.

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

КЗ6. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

ФК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

ФК8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

ФК9. Здатність здійснювати професійну діяльність на

основі впровадженої системи управління інформаційною та/або кібербезпекою.

ФК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

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 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 12. Розробляти моделі загроз та порушника.

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

ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

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 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

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/  Лаборат-орні,) | **Результати навчання** | **Завдання** | **Оціню-вання** |
| **3 семестр** | | | | |
| **Модуль 1. Методи і засоби захисту інформації від витоку по технічних каналах (ТКВІ).** | | | | |
| Вступ до курсу. Причини, види та канали витоку інформації. Еволюційний розвиток методів та засобів захисту інформації (ЗІ). | **2/2** | Вміти вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів ЗІ та визначати ефективність ЗІ від витоку ТКВІ відповідно до вимог нормативних документів системи технічного захисту інформації.  Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем та виявляти небезпечні сигнали технічних засобів. | Теоретичне опитування. | **10** |
| Класифікація методів та засобів ЗІ від витоку. Первинні технічні заходи. Основні технічні заходи. | **4/4** | Здача лабораторної роботи. | **10** |
| Блокування каналів витоку інформації без використання спеціальних засобів ТЗІ. Застосуванням способів і схемних рішень із ЗІ, які не порушують основні технічні характеристики засобів забезпечення інформаційної діяльності. | **4/4** | Здача лабораторної роботи. | **10** |
| Основні технічні заходи ЗІ. Заходи щодо блокування ТКВІ з використанням пасивних засобів. | **6/4** | Здача лабораторної роботи. | **10** |
| Заходи щодо блокування ТКВІ з використанням активних засобів. Просторове електромагнітне зашумлення з використанням генераторів шуму або створення прицільних завад. Створення акустичних і вібраційних завад з використанням генераторів акустичного шуму. Придушення диктофонів в режимі запису з використанням пристроїв, що блокують роботу диктофонів. Пошук закладних пристроїв. | **6/4** | Здача лабораторної роботи. | **10**  **10** |
| Неформальна оn-line освіта на основі МВОК. | **20** |
| Модульний контроль | | | Підсумковий тест в ЕНК | **20** |
| **Модуль 2. Способи несанкціонованого доступу до інформації в комп'ютерних системах і захисту від нього.** | | | | |
| Способи несанкціонованого доступу до інформації в комп'ютерних системах і захисту від нього. Аутентифікація, авторизація і адміністрування дій користувачів. Аутентифікація користувачів за їх біометричними характеристиками, клавіатурним почерком та ін. | **4/4** | Вміти застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.  Вміти забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).  Вміти 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. | **5** |
| Методи захисту програмного забезпечення (ПЗ). Мотиви захисту ПЗ. Реєстраційні коди. Апаратні ключі. Захист від несанкціонованого копіювання. | **6/2** | Опитування  Здача лабораторної роботи. | **5**  **10** |
| Шкідливе програмне забезпечення. Захист від комп'ютерних вірусів. Технологія сигнатурного аналізу. Сигнатурні методи виявлення атак. Програмні закладки та методи захисту від них. Проблеми існування засобів зламу захистів ПЗ. Класифікація засобів зламу захистів ПЗ. Програмний інструментарій для зламу програмного забезпечення. | **5/2** | Опитування  Здача лабораторної роботи. | **5**  **20** |
| Методика обґрунтування вимог до захисту інформації. Методика вибору засобів і методів ЗІ. Методи визначення значень показників вразливості інформації. Методи оцінки ефективності систем ЗІ. | **4/2** | Здача лабораторної роботи. | **10** |
| Шляхи розвитку методів та засобів ЗІ. Аналіз досвіду ЗІ в країнах ЄС, США, Японії, КНР. Прогноз розвитку кіберзагроз та засобів ЗІ. | **4/2** | Здача лабораторної роботи.  Неформальна оn-line освіта на основі МВОК. | **10**  **15** |
| 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 |