|  |  |
| --- | --- |
| E:\nubip_logo_new_poisk_18_2.png | **СИЛАБУС ДИСЦИПЛІНИ** **«Безпека безпровідних, мобільних та хмарних технологій»** |
| **Ступінь вищої освіти – бакалавр** |
| **Спеціальність 125 – КІБЕРБЕЗПЕКА** |
| **Освітня програма «КІБЕРБЕЗПЕКА»** |
| **Рік навчання 2 семестр 1****Форма навчання** денна |
| **Кількість кредитів ЄКТС 5** |
| **Мова викладання** українська |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| **Лектор курсу** |  **Блозва Андрій Ігорович, к пед.н., доцент**https://nubip.edu.ua/sites/default/files/imagecache/120x160/dsc_7629_0.jpg |
| **Контактна інформація лектора (e-mail)** | **Кафедра комп'ютерних систем і мереж,****корпус. 15, к. 207, тел. 5278724****e-mail andriy.blozva****@nubip.edu.ua** |
| **Сторінка курсу в eLearn**  | **ЕНК (1 семестр)**  |

**ОПИС ДИСЦИПЛІНИ**

Навчальна дисципліна передбачає вивчення загальних принципів та стандартів побудови комп’ютерних мереж, технологій локальних комп’ютерних мереж, протоколів стеку TCP/IP, питань маршрутизації в ІР-мережах, технологій глобальних мереж та мереж доступу, мережевих операційних систем та мережевого програмного забезпечення.

 **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 7 Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

ФК 8 Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку

ФК 11 Здатність виконувати моніторинг процесів функціонування Інформаційних, інформаційнотелекомунікаційних (автоматизованих) систем згід

ФК. 13 Здатність розробляти апаратне, алгоритмічне та програмне забезпечення, компоненти комп’ютерних систем захисту інформації

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

ПРН 1 Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;

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

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

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

ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;

ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;

ПРН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційнотелекомунікаційних системах;

ПРН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз;

**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. Концепція динамічної маршрутизації** |
| Центр моніторингу те керування безпекою | **2/2** | Введення в основи моніторингу, та спеціалізованих структурах керування безпекою | **Виконання лабораторної роботи** | **10** |
| Бездротові технології та їх протоколи | **2/2** | Вивчення технологій Wi-Fi, Bluetooth, LTE.  | **Виконання лабораторної роботи** | **10** |
| Хмарні технології та основи побудови інфраструктури | **2/2** | Основи побудови інфраструктури SaaS, PaaS, IaaS. | **Виконання лабораторної роботи** | **10** |
| Мережеві протоколи та служби | **2/2** | Знати основні мережеві протоколи та принцип їх роботи | **Виконання лабораторної роботи** | **10** |
| Мережева інфраструктура для бездротових мереж | **2/2** | Побудова бездротової мережі на основі різних пристроїв та технологій | **Виконання лабораторної роботи** | **10** |
| Самостійна робота  | **20** | Проходження додаткового курсу у мережевій академії CISCO | **Проходження додаткового матеріалу** | **50** |
| **Модуль 2 Забезпечення активної безпеки комп’ютерної мережі** |
| Принципи забезпечення безпеки у бездротових мережах | **2/2** | Знати як відбуваються атаки, види їх. Програмне забезпечення, яке найчастіше використовується для атак | **Виконання лабораторної роботи** | **10** |
| Мережеві атаки. Поглиблений розбір. | **2/2** | Знати спеціалізовані атаки: атаки на незахищені сервіси, ін’єкції, атаки міжмережевого скриптингу та інші  | **Виконання лабораторної роботи** | **10** |
| Захист периметру хмарних ресурсів | **2/2** | Авторизація, автентифікація та облік, принципи BYOD | **Виконання лабораторної роботи** | **10** |
| Криптографія та інфраструктура загальних ключів | **2/2** | Методи хешування, шифрування, види ключів та захищені з’єднанні | **Виконання лабораторної роботи** | **10** |
| Захист та аналіз кінцевих пристроїв | **2/2** | Знання систем виявлення вторгнень на стороні хоста, загальна система оцінки уразливостей | **Виконання лабораторної роботи** | **10** |
| Самостійна робота  | **20** | Проходження додаткового курсу у мережевій академії CISCO | **Проходження додаткового матеріалу** | **50** |
| **Модуль 3 Аналітика мережі, виявлення потенційних вторгнень** |
| Моніторинг безпеки бездротових мереж | **4/4** | Проводити документування подій у мережі, автоматизація записів. Вміння читати та орієнтуватися у записах можливих загроз. | **Виконання лабораторної роботи** | **20** |
| Аналіз даних вторгнень | **4/4** | Вміння працювати із програмними продуктами аналізу можливих вторгень  | **Виконання лабораторної роботи** | **20** |
| Реагування на інциденти та їх обробка | **2/2** | Розуміння системи VERIS, та орієнтуватися у групах CSIRT | **Виконання лабораторної роботи** | **10** |
| Самостійна робота  | **20** | Проходження додаткового курсу у мережевій академії CISCO | **Проходження додаткового матеріалу** | **50** |
| **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 |