**Додаток 1**

**Інформація про дисципліну вільного вибору студента**

|  |  |  |
| --- | --- | --- |
| Назва дисципліни | Основи кібербезпеки | |
| Семестр | 5 | |
| Кафедра | Комп’ютерної інженерії та кібербезпеки | |
| Факультет | Факультет інформаційно-комп’ютерних технологій | |
| Короткий опис дисципліни | Дисципліна включає лекції, практичні заняття, модульні контрольні роботи та самостійну роботу. Програмою дисципліни передбачено виконання індивідуального завдання, що представляє собою самостійне дослідження студента, який оформив індивідуальний графік навчання та є альтернативним варіантом виконання практичних занять з дисципліни. Також, при вивченні дисципліни передбачено проходження курсу «Основи кібербезпеки» в межах Мережевої академії Cisco Житомирської політехніки. | |
| Мета й ціль дисципліни | Метою викладання навчальної дисципліни є ознайомлення студентів з сутністю, задачами, принципами та сучасними інформаційними технологіями кібербезпеки, методологічними та законодавчими основами організації, планування та впровадження систем захисту інформації на підприємствах, а також основними аспектами практичної діяльності по їх створенню, забезпеченню функціонуванню та оцінці ефективності з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників.  Ціль дисципліни полягає у набутті студентами знань, умінь і здатностей (компетенцій) щодо побудови, експлуатації та розробки систем кіберзахисту інформації в кіберпросторі для ефективного вирішення завдань професійної діяльності. | |
| Результати навчання (навички, що отримає студент після курсу) | Результатом вивчення дисципліни є набуття студентами таких компетенцій:   * здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо безпечного здійснення професійної діяльності; * здатність здійснювати проектування (розробку) систем, технологій і засобів кіберзахисту при здійсненні професійної діяльності; * здатність прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави, суспільству організації та дестабілізуючі чинники в роботі систем управління. | |
| Перелік тем | **Тема 1.** Теоретичні основи та нормативно-правове забезпечення кіберзахисту.  **Тема 2.** Загрози безпеці інформаційних систем.  **Тема 3.** Моделі загроз та порушника в кіберпросторі.  **Тема 4.** Основи криптографічних методів кіберзахисту.  **Тема 5.** Методи та засоби захисту інформації від несанкціонованого доступу.  **Тема 6.** Методи та засоби технічного захисту інформації.  **Тема 7.** Захист інформації в розподілених інформаційних системах.  **Тема 8.** Програмні методи і засоби кіберзахисту | |
| Система оцінювання  (як розподіляється 100 балів за курс) | <https://docs.google.com/spreadsheets/d/1vK5isGb4Ix1YVEdgBZRlbbS3HnCoO8eZ8R9-5YwmES0/edit#gid=2090047754> | |
| Форма контролю | залік | |
| Лектор | IMG_3153 (1).JPG | **Лобанчикова Н.М.**, к.т.н., доц., доцент кафедри комп’ютерної інженерії та кібербезпеки |