|  |  |
| --- | --- |
| E:\nubip_logo_new_poisk_18_2.png | **СИЛАБУС ДИСЦИПЛІНИ**  **«ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ»** |
| **Ступінь вищої освіти – Бакалавр** |
| **Спеціальність 123 – КОМП’ЮТЕРНА ІНЖЕНЕРІЯ** |
| **Освітня програма «Комп’ютерна інженерія»** |
| **Рік навчання 4, семестр 8**  **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 (1 семестр)** <https://elearn.nubip.edu.ua/course/view.php?id=2773> |

**ОПИС ДИСЦИПЛІНИ**

Навчальна дисципліна передбачає вивчення основ використання засобів та методів захисту інформації у комп’ютерних системах та мережах, дослідження проблем зберігання, опрацювання, пошуку, передачі, перетворення, закриття та відновлення інформації в організаціях і на підприємствах різних напрямків діяльності та різних форм власності, способів захисту від несанкціонованого доступу до інформаційних ресурсів.

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

ЗК 1. Здатність до абстрактного мислення, аналізу і синтезу.

ЗК 2. Здатність вчитися і оволодівати сучасними знаннями.

ЗК 3. Здатність застосовувати знання у практичних ситуаціях.

ЗК 7. Вміння виявляти, ставити та вирішувати проблеми.

ФК 2. Здатність використовувати методи фундаментальних і прикладних дисциплін для опрацювання, аналізу і синтезу результатів професійних досліджень.

ФК 3. Здатність розробляти алгоритмічне та програмне забезпечення, компоненти комп’ютерних систем та мереж, Інтернет додатків, кіберфізичних систем з використанням сучасних методів і мов програмування, а також засобів і систем автоматизації проектування.

ФК 4. Здатність проектувати, впроваджувати та обслуговувати комп’ютерні системи та мережі різного виду та призначення.

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

ФК 12. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп’ютерних систем, мереж та їхніх компонентів шляхом використання аналітичних методів і методів моделювання;

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

ФК 14. Здатність проектувати системи та їхні компоненти з урахуванням усіх аспектів їх життєвого циклу та поставленої задачі, включаючи створення, налаштування, експлуатацію, технічне обслуговування та утилізацію.

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

ПРН 2. Знати основи професійно-орієнтованих дисциплін спеціальності.

ПРН 3. Мати знання та навички щодо проведення експериментів, збору даних та моделювання в комп’ютерних системах.

ПРН 4. Мати знання з новітніх технологій в галузі комп’ютерної інженерії.

ПРН 6. Вміти застосовувати знання для ідентифікації, формулювання і розв’язування технічних задач спеціальності, використовуючи відомі методи.

ПРН 7. Вміти застосовувати знання для розв’язування задач аналізу та синтезу засобів, характерних для спеціальності.

ПРН 9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп’ютерних систем та мереж для вирішення технічних задач спеціальності.

ПРН 11. Вміти здійснювати пошук інформації в різних джерелах для розв’язання задач комп’ютерної інженерії.

ПРН 14. Вміти поєднувати теорію і практику, а також приймати рішення та виробляти стратегію діяльності для вирішення завдань спеціальності з урахуванням загальнолюдських цінностей, суспільних, державних та виробничих інтересів.

**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. Політика інформаційної безпеки.** | | | | |
| Об’єкт, предмет, зміст, завдання та структура курсу. | **2/2** | Вміти здійснювати пошук інформації в різних джерелах для розв’язання задач комп’ютерної інженерії, пов’язаних із дисципліною. | Теоретичне опитування | **10** |
| Властивості інформації з точки зору проблематики її захисту. | **2/2** | Вміти виконувати аналіз зв’язків між інформаційними процесами на локальних та віддалених обчислювальних системах. | Здача лабораторної роботи. | **10** |
| Поняття загрози інформації. Класифікація загроз. Порушники безпеки. | **2/2** | Вміти розробляти моделі загроз та порушника. | Здача лабораторної роботи. | **10** |
| Ризики порушення політики інформаційної та кібернетичної безпеки (КБ) об’єкту інформатизації (ОБІ). | **2/2** | Використовувати методи та принципи моделювання організаційно-технічних систем і операцій, проводити аналіз оптимальних планів.  Вміти здійснювати пошук інформації в різних джерелах для розв’язання | Здача лабораторної роботи. | **10** |
| Вимоги щодо захисту інформації та КБ інформаційно-комунікаційних систем (ІКС) та комп’ютерних мереж (КМ) ОБІ. | **4/4** | Вміти застосовувати знання для ідентифікації, формулювання і розв’язування технічних задач, пов’язаних із захистом інформації та забезпечення кібернетичної безпеки ОБІ. | Здача лабораторної роботи. | **10** |
| Моделей безпеки комп’ютерних систем. | **4/4** | Вміти діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.  Вміти впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. | Здача лабораторної роботи. | **10** |
| Механізми реалізації послуг безпеки. | **4/4** |  | **10** |
| Політики інформаційної безпеки компанії. | **4/4** | Здача лабораторної роботи.  Неформальна оn-line освіта на основі МВОК. | **10** |
| Модульний контроль | | | Підсумковий тест в ЕНК | **20** |
| **Модуль 2. Методи та засоби захисту інформації у ІКС.** | | | | |
| Канали витоку інформації. | **2/2** | Вміти застосовувати знання для розв’язування задач аналізу та синтезу засобів захисту інформації. | Тестування та опитування. | **5** |
| Методи, які застосовуються для захисту мовної інформації від несанкціонованого прослуховування. Активні і пасивні методи. | **4/4** | Опитування  Здача лабораторної роботи. | **5**  **10** |
| **Основи сучасної**  **криптографії і питання шифрування.**  **Криптографія і криптосистеми.**  Історія криптографії, основні терміни і вимоги, що пред'являються до криптосистем. | **2/2** | Вміти вирішувати задачі захисту інформації, що обробляється в ІКС з використанням сучасних методів та засобів криптографічного захисту інформації.  Вміти виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в ІКС. | Опитування | **5** |
| Симетричні криптосистеми і системи шифрування. Перестановки. Системи підстановок. Гамування. Блокові шифри. Датчики ПВЧ. Багатоалфавітні системи. Системи одноразового використання. Датчики М-послідовностей. Стандарт шифрування даних ДЕСТ 28147-89. | **6/6** | Здача лабораторної роботи.  Неформальна оn-line освіта на основі МВОК. | **10**  **15** |
| **Засоби автентифікації даних і управління ключами шифрування.**  Безповоротні або односторонні функції. Засоби для розподілу ключів.  Алгоритм RSA. Гарантована оцінка захищеності алгоритму RSA. Практична реалізація RSA.  Криптосистема Ель-Гамаля.  Криптосистеми на основі еліптичних рівнянь. | **6/6** | Знати основні системи з відкритим ключем.  Вміти виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в ІКС. | Здача лабораторної роботи. | **10**  **10** |
| Електронний підпис. Можливі порушення захисту повідомлень. Засоби автентифікації користувачів. Електронний підпис на основі алгоритму RSA. Цифрова сигнатура. Хеш-функції. Управління ключами. Генерація ключів. Накопичення ключів. Розподіл ключів. | **4/4** | Здача лабораторної роботи. | **10** |
| Модульний контроль | | | Підсумковий тест в ЕНК | **20** |
| **Всього за 1 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 |