**Інформація про дисципліну вільного вибору студента**

|  |  |  |
| --- | --- | --- |
| Назва дисципліни | Інфраструктура відкритих ключів | |
| Семестр | 7 | |
| Кафедра | Комп’ютерної інженерії та кібербезпеки | |
| Факультет | Факультет інформаційно-комп’ютерних технологій | |
| Короткий опис дисципліни | Дисципліна включає лекції, практичні заняття, лабораторні роботи, модульні контрольні роботи та самостійну роботу. Програма базується на використанні сучасного програмного забезпечення для впровадження та застосування знань щодо забезпечення інформаційної безпеки інфраструктури відкритих ключів в інформаційно-комунікаційних системах. | |
| Мета й ціль дисципліни | **Метою** викладання навчальної дисципліни є опанування загальними основами методології створення та аналізу різноманітних типових технологій побудови інфраструктури відкритих ключів(ІВК); опанування навичками проектування та впровадження базових варіантів ІВК; вивчення основних підходів до забезпечення інформаційної безпеки ІВК в організаціях різної форми власності; ґрунтовне ознайомлення студентів із основними нормативними документами в галузі ІВК та особливостями їх застосування на практиці; ознайомлення студентів із основними типами технологічних рішень направленими на забезпечення інформаційної безпеки ІВК. **Ціль** дисципліни полягає у набутті знань і навичок, необхідних для впровадження та застосування теоретичних знань щодо забезпечення інформаційної безпеки ІВК в майбутній професійній діяльності. | |
| Результати навчання (навички, що отримає студент після курсу) | В результаті вивчення дисципліни, студенти повинні:   * **знати:** основні вітчизняні нормативні документи в галузі захисту інформації та міжнародні стандарти з інформаційної безпеки, процеси які висуваються ними при побудові захищених систем, особливості підтвердження відповідності побудованого захисту; принципи побудови систем забезпечення інформаційної безпеки; основні типи, призначення та характеристики технологічних рішень, направлених на забезпечення інформаційної безпеки. * **вміти:** аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації; аналізувати та визначати можливість застосування технологій, методів та засобів технічного захисту інформації; виявляти небезпечні сигнали технічних засобів; вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю захищеності інформації від витоку технічними каналами; визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації. | |
| Перелік тем | **Тема 1.** Призначення інфраструктур відкритих ключів (ІВК) та сфери застосування.  **Тема 2.** Основні криптографічні примітиви та механізми інфраструктури відкритих ключів.  **Тема 3.** Теоретичні основи застосування ІВК.  **Тема 4.** Формати сертифікатів. Перелік відкликаних сертифікатів. Життєвий цикл сертифікатів. Процеси генерування, відкликання, призупинення дії та закінчення терміну дії сертифікатів.  **Тема 5.** Відкликання сертифікатів. Механізми періодичної публікації. Переліки відкликаних сертифікатів. Переліки відкликаних сертифікатів органів сертифікації.  **Тема 6.** Розповсюдження інформації в ІВК. Публікація і сховища. Міждомнні сховища. Прямий доступ. Сховища, що використовуються колективно. Пограничне сховище. Проблеми, що виникають при реалізації ІВК.  **Тема 7.** Завдання та шляхи розгортання ІВК. Визначення завдання та шляхів розгортання ІВК. Критерії вибору .  **Тема 8.** Визначення політик безпеки. Проблеми вибору постачальника технології або сервісів PKI.  **Тема 9.** Планування і створення інфраструктури. Управління і адміністрування ІВК. Особливості розгортання інфраструктури відкритих ключів.  **Тема 10.** Нормативно-законодавча база. Закони України у сфері створення і використання ІВК.  **Тема 11.** Державне регулювання в сфері розроблення і впровадження інфраструктур відкритих ключів і відповідних криптосистем.  **Тема 12.** Типові технології використання інфраструктури відкритих ключів в інформаційно-комунікаційних системах. | |
| Система оцінювання  (як розподіляється 100 балів за курс) | Відвідування лекцій – 0,25 балів кожна (16 лекцій),  Практичні заняття – 1 бали кожне (16 практичних),  Лабораторні роботи – 2 бали кожна (16 л.р),  Контрольна робота – 10 балів кожна (4 МКР),  Самостійна робота – 4 бали кожна (2 СРС). | |
| Форма контролю |  | |
| Лектор |  |  |