Програма ЄДКІ спеціальності 125 Кібербезпека (2023 рік)

|  |  |  |  |
| --- | --- | --- | --- |
| **Код** | **Найменування розділу/ підрозділу/ теми** | **Дисципліна** | **Викладач** |
| **CS1** | **ЗАКОНОДАВЧА ТА НОРМАТИВНО-ПРАВОВА БАЗА, ДЕРЖАВНІ ТА МІЖНАРОДНІ ВИМОГИ, ПРАКТИКИ І СТАНДАРТИ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ ТА/АБО КІБЕРБЕЗПЕКИ** |    |   |
| **CS1.1** | **Законодавча та нормативно-правова база України в галузі інформаційної та /або кібербезпеки** |   |   |
| **CS**1.1.1 | ЗУ «Про інформацію», «Про науково-технічну інформацію» | Нормативно-правове забезпечення ІБ (НПЗ ІБ) | Сєчкін І.А. |
| **CS**1.1.2 |  ЗУ «Про захист інформації в інформаційнокомунікаційних системах», «Про основні засади забезпечення кібербезпеки України» |
| **CS1.1.3** | ЗУ «Про державну таємницю». «Про захист персональних даних» |
| **CS1.1.4** | Постанова КМУ від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» |
| **CS1.1.5** | Державні Стандарти України в галузі інформаційної та/або кібербезпеки |
| ДСТУ 3396.0,1,2-97  | СТЗІ | Магро В.І. |
| ДСТУ ISO/ІЕС 15408-1:2017  | НПЗ ІБ | Тимофєєв Д.С. |
| **CS1.1.6.** | Нормативні документи з технічного захисту інформації | КСЗІ, СТЗІ, НПЗ ІБ |   |
| НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу» | Комплексні системи захисту інформації | Кручінін О.В. |
| НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу» |
| **CS1.2** | **Міжнародні стандарти в галузі інформаційної та /або кібербезпеки** |   |   |
| **CS1.2.1** | Регламенти ЄС в галузі кібербезпеки |  | Тимофєєв Д.С. |
| Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій» |  |
| **CS1.2.2** | ISO 27001, ISO 27002, ISO 27003 | Управління інформаційною безпекою |
| ISO/IEC 15408- 2, ISO/IEC 15408-3 |  |
| **CS2** | **ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНІЙ ТА/АБО КІБЕРБЕЗПЕЦІ** |   |   |
| **CS2.1** | **Інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці** |   |   |
| **CS2.1.1** | Мережева модель OSI. Основні протоколи стеку TCP/IP | Мережеві технології і протоколи | Святошенко В.О. |
| **CS2.1.2** | Віртуалізація (принципи, гіпервізори) | Інформаційні технології | Олішевський І.Г. |
| **CS2.1.3** | Архітектура комп'ютерів | Архітектура комп’ютерів | Ткаченко С.М. |
| **CS2.2** | **Методи і засоби обробки інформації** |   |   |
| **CS2.2.1** | Алгоритмізація та програмування (без прив'язки до конкретної мови програмування) | Програмування і алгоритмічні мови | Алєксєєв О.М.  |
| **CS2.2.2** | Основи об'єктно-орієнтованого програмування (Класи, Методи, Перевантаження, Наслідування, Узагальнення) |
| **CS2.2.3** | Методи сортування та пошуку даних | Інформаційні технології | Олішевський І.Г. |
| **CS2.3** | **Операційні системи** | Операційні системи | Святошенко В.О.  |
| **CS2.3.1** | Архітектура операційних систем |
| **CS2.3.2** | Процеси і потоки в операційних системах |
| **CS2.3.3** | Керування пам'яттю в операційних системах |
| **CS2.3.4** | Файлові системи |
| **CS2.3.5** | Захисні механізми операційних систем |
| **CS3** | **БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ** | Кіберзахист (Кіберперації) | Мешков В.І.- (Ковальова Ю.В. ) |
| **CS3.1** | **Захист інформації, що обробляється та зберігається в ІКС** |
| **CS3.1.1** | Процедури ідентифікації, автентифікації, авторизації користувачів |
| **CS3.1.2** | Резервування інформації та компонентів ІКС |
| **CS3.2** | **Програмні та програмно-апаратні комплекси ЗЗІ** |
| **CS3.2.1** | Антивіруси, міжмережеві екрани (призначення, архітектура, функції) |
| **CS3.2.2** | IPS, IDS (призначення, архітектура, функції) |
| **CS3.2.3** | Системи контролю та управління доступом в ІКС (Active Directory, ACL) |
| **CS3.3** | **Відновлення функціонування ІКС після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження** |
| **CS3.3.1** | Організаційно-технічні заходи відновлення функціонування ІКС |
| **CS3.3.2** | Журнал аудиту подій |
| **CS3.3.3** | Політики резервного копіювання даних |
| **CS3.4** | **Моніторинг процесів функціонування ІКС** |
| **CS3.4.1** | Джерела інформації про події та типи подій, що аналізуються в системах моніторінгу |
| **CS3.4.2** | Система візуалізації та управління подіями (SIEM) |
| **CS3.4.3** | Аналіз подій |
| **CS3.5** | **Механізми безпеки комп'ютерних мереж** |
| **CS3.5.1** | Протоколи безпеки на канальному рівні |
| **CS3.5.2** | Протоколи безпеки на мережному рівні (IPSec)  |
| **CS3.5.3** | Протоколи безпеки на транспортному/сеансовому рівні (SSL/TLS) |
| **CS3.5.4** | Протоколи безпеки прикладного рівня (HTTPS) |
| **CS3.5.5** | Протоколи автентифікації прикладного рівня (RADIUS) |
| **CS3.5.6** | Віртуальні приватні мережі (VPN) |
| **CS4** | **КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ** | Комплексні системи захисту інформації | Кручінін О.В. |
| **CS4.1** | **Проєктування, створення, супровід КСЗІ** |
| **CS4.1.1** | Дослідження середовищ функціонування ІС – середовища користувачів, обчислювальної системи, фізичного середовища, інформаційного середовища та побудова моделі загроз |
| **CS4.1.2** | Вибір методів та засобів забезпечення необхідного рівня ІБ |
| **CS4.2** | **Моделі загроз та моделі порушника** |
| **CS4.2.1** | Загрози цілісності |
| **CS4.2.2** | Загрози доступності |
| **CS4.2.3** | Загрози конфіденційності |
| **CS4.2.4** | Загрози через технічні канали |
| **CS4.2.5** | Загрози автентичності |
| **CS4.3** | **Оцінка захищеності інформації в ІКС** |
| **CS5** | **УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА / АБО КІБЕРБЕЗПЕКОЮ** | Управління інформаційною безпекою | Тимофєєв Д.С. |
| **CS5.1** | **Управління кіберінцидентами** |
| **CS5.1.1** | Поняття кіберінцидента / кібератаки |
| **CS5.1.2** | Розслідування кіберінцидентів / кібератак |
| **CS5.2** | **Управління ризиками в інформаційній та / або кібербезпеці** |
| **CS5.2.1** | Ризики інформаційної безпеки |
| **CS5.2.2** | Аналіз та оцінка ризику. Прийняття ризику. Зменшення ризику. Страхування (перекладання) ризику |
| **CS5.3** | **Політика інформаційної безпеки** |
| **CS5.3.1** | Розробка політик ІБ під час забезпечення бізнес-процесів |
| **CS5.3.2** | Дотримання політик ІБ під час забезпечення бізнес-процесів |
| **CS6** | **КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ** |   |   |
| **CS6.1** | **Математичні основи криптографії та стеганографії** | Спеціальні розділи з математики | Кагадій Т.С. |
| **CS6.1.1** | Модулярні обчислення |
| **CS6.1.2** | Елементи теорії чисел. Алгоритм Евкліда. Теорема Ейлера. Теореми Ферма. Обчислення у скінченних полях |
| **CS6.1.3** | Умови стійкості шифрів |
| **CS6.1.4** | Однонаправлені функції, функції гешування |
| **CS6.1.5** | Псевдовипадкові послідовності в криптосистемах |
| **CS6.1.6** | Обчислення в системі чисел з плаваючою точкою |
| **CS6.2** | **Симетричні криптосистеми** | Прикладна криптологія | Бабець Д.В. |
| **CS6.2.1** | Модель симетричної криптосистеми |
| **CS6.2.2** | Класичні методи шифрування. Шифр Цезаря, Вернама. Квадрат Полібія. Шифр гамування |
| **CS6.2.3** | Блокові шифри. DES, AES, ДСТУ ГОСТ 28147-2009, ДСТУ 7624:2014 (довжина ключів, довжина блоку вхідного тексту, кількість раундів, крипостійкість, режими роботи згідно з  |
| ДСТУ ISO/IEC 10116:2019) |
| **CS6.2.4** | Потокові шифри. RC4, STRUMOK. (довжина ключів, крипостійкість) |
| **CS6.3** | **Асиметричні криптосистеми** |
| **CS6.3.1** | Модель асиметричної криптосистеми |
| **CS6.3.2** | Шифри RSA, Ель Гамаля (EG) |
| **CS6.3.3** | Генерація спільних секретних ключів Діффі-Хеллмана (DH) |
| **CS6.3.4** | Електронний цифровий підпис DSA |
| **CS6.4** | **Цифрова стеганографія** | Цифрова стеганографія | Герасіна О.В. |
| **CS6.4.1** | Поняття цифрової стеганографії |
| **CS6.4.2** | Модель стеганосистеми. Основні вимоги до стеганосистеми |
| **CS6.4.3** | Відкриті, напівзакриті, закриті стеганосистеми |
| **CS6.4.4** | Поняття ЦВЗ, класифікація |
| **CS6.4.5** | Метод модифікації найменшого значущого біта |
| **CS7** | **ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ** |   |   |
| **CS7.1** | **Технічні канали витоку інформації** | Системи технічного захисту інформації | Магро В.І. |
| **CS7.1.1** | Вібро-акустичний канал витоку інформації |
| **CS7.1.2** | Електричний канал витоку інформації |
| **CS7.1.3** | Електромагнітний канал витоку інформації |
| **CS7.1.4** | Оптичний та оптоелектронний канал витоку інформації |
| **CS7.1.5** | Параметричний канал витоку інформації |
| **CS7.2** | **Методи та засоби технічного захисту інформації** |
| **CS7.2.1** | Пасивні методи та засоби захисту інформації від витоку технічними каналами |
| **CS7.2.2** | Активні методи та засоби захисту інформації від витоку технічними каналами |
| **CS7.2.3** | Методи пошуку та блокування засобів негласного отримання інформації |
| **CS7.2.4** | Методи та засоби технічного захисту інформації від витоку вібро-акустичними каналами |
| **CS7.2.5** | Методи та засоби технічного захисту інформації від витоку електромагнітними та електричними каналами |
| **CS7.2.6** | Методи та засоби технічного захисту інформації від витоку оптичними та оптоелектронними каналами |
| **CS7.2.7** | Методи та засоби технічного захисту інформації від витоку параметричними каналами |
| **CS7.2.8** | Системи відеоспостереження, охоронних сигналізацій, контролю доступу | Технічні системи охорони об'єктів | Кручінін О.В. |