ОСНОВИ КІБЕРБЕЗПЕКИ

Циклова комісія, яка забезпечує викладання
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА АВТОМАТИЗАЦІЇ

Викладач	Боюн Неоніла Олександрівна
Семестр	6-й
Освітньо-професійний ступінь	Фаховий молодший бакалавр
Кількість кредитів ЄКТС	3
Форма контролю	Диференційований залік

ЗАГАЛЬНИЙ ОПИС ДИСЦИПЛІН

Мета вивчення освітнього компонента «Основи кібербезпеки» - є дослідження характеристик і тактик кіберзлочинців. Під час вивчення освітнього компоненту здобувачі освіти заглиблюються в технології, продукти і процедури професіоналів боротьби з кіберзлочинністю. Данна дисципліна допоможе розвинути навички, необхідні для роботи в якості ІТ-фахівця.

Завдання курсу: В процесі навчання здобувачі освіти охоплюють основні знання і навички у всіх областях безпеки в кіберпросторі - інформаційна безпека, системна безпека, мережна безпека, мобільна безпека, фізична безпека, етика і закони, пов'язані технології, використання технологій захисту і пом'якшення у захисті бізнесу.

Вміти: описати характеристики злочинців і героїв в сфері кібербезпеки; описати, які принципи конфіденційності, цілісності і доступності, пов'язані з станом даних і контрзаходами щодо кібербезпеки; описати тактику, методи та процедури, які використовуються кіберзлочинцями; описати, які технології, продукти і процедури використовуються для захисту конфіденційності та для забезпечення цілісності і високої доступності; пояснити, як професіонали кібербезпеки використовують технології, процеси та процедури для захисту всіх компонентів мережі; пояснити мету законів, пов'язаних з кібербезпекою.

Знати: характеристики злочинців і героїв в сфері кібербезпеки; принципи конфіденційності, цілісності і доступності, пов'язані з станом даних і контрзаходами щодо кібербезпеки; тактику, методи та процедури, які використовуються кіберзлочинцями; технології, продукти і процедури які використовуються для захисту конфіденційності та для забезпечення цілісності і високої доступності; як професіонали з кібербезпеки використовують технології, процеси та процедури для захисту всіх компонентів мережі; мету законів, пов'язаних з кібербезпекою.

Компетентнісний потенціал освітнього компонента (навчальної дисципліни) та результати навчання:

Інтегральна компетентність:

ІК1. Здатність вирішувати типові спеціалізовані задачі в галузі інформаційних технологій в процесі професійної діяльності або навчання, що вимагає застосування методів і технологій комп'ютерної інженерії та може характеризуватися певною невизначеністю умов; нести відповідальність за результати своєї діяльності, здійснювати контроль інших осіб у визначених ситуаціях.

Загальна компетентність:

ЗК3. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК4. Здатність застосовувати знання у практичних ситуаціях.

ЗК5. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК7. Здатність працювати в команді.

ЗК8. Здатність вчитися і оволодівати сучасними знаннями.

Спеціальна компетентність:

СК2. Здатність застосовувати на практиці фундаментальні концепції, парадигми і основні принципи функціонування апаратних, програмних та інструментальних засобів комп'ютерної інженерії.

СК3. Здатність вільно користуватись сучасними комп'ютерними та інформаційними технологіями, прикладними та спеціалізованими комп'ютерно інтегрованими середовищами для розробки, впровадження та обслуговування апаратних та програмних засобів комп'ютерної інженерії.

СК4. Здатність брати участь у розробці системного та прикладного програмного забезпечення засобів комп'ютерної інженерії з використанням ефективних алгоритмів, сучасних методів і мов програмування.

СК5. Здатність забезпечувати захист інформації в комп'ютерних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

СК6. Здатність брати участь у модернізації апаратних та програмних засобів комп'ютерної інженерії.

СК7. Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи.

СК8. Здатність здійснювати організацію робочих місць з урахуванням вимог охорони праці, їх технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

СК9. Здатність оформляти отримані робочі результати у вигляді презентацій, науково-технічних звітів.

СК10. Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати прийняті рішення.

Результати навчання (програмні результати навчання):

РН2. Знати і розуміти теоретичні положення, що лежать в основі функціонування апаратних та програмних засобів комп'ютерної інженерії.

РН3. Знати сучасні методи та технології для розв'язання прикладних задач комп'ютерної інженерії.

РН4. Застосовувати правові норми, норми з охорони праці, безпеки життєдіяльності у професійній діяльності.

РН6. Тестувати, діагностувати та обслуговувати апаратні та програмні засоби комп'ютерної інженерії.

РН9. Розробляти, тестувати, впроваджувати, експлуатувати програмне забезпечення для вбудованих і розподілених систем.

РН10. Здійснювати пошук інформації з різних джерел для розв'язання задач комп'ютерної інженерії.

РН11. Ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів комп'ютерної інженерії.

РН12. Поєднувати теорію і практику, знаходити та обґрунтовувати шляхи рішення типових задач у професійній діяльності з урахуванням виробничих інтересів.

РН15. Проводити інсталяцію та налаштування системного та прикладного програмного забезпечення, у тому числі програмних засобів захисту інформації з метою реалізації встановленої політики інформаційної безпеки.

Теми лекцій:

1. Вступ до кібербезпеки
2. Потреба у кібербезпеці.
3. Атаки, поняття та методи. Захист даних і конфіденційність.
4. Захист організації. Правові та етичні питання кібербезпеки, освіта і кар'єра.
5. Основи кібербезпеки
6. Світ експертів і злочинців.
7. Куб кібербезпеки.
8. Кібербезпека - загрози, вразливості та атаки.
9. Мистецтво захисту таємниць.
10. Мистецтво забезпечення цілісності.
11. Концепція п'яти дев'яток.
12. Захист домену кібербезпеки.
13. Як стати спеціалістом з кібербезпеки

Теми лабораторних занять

1. Робота с матеріалами Закону України «Про основні засади забезпечення кібербезпеки України».
2. Системи числення Симетричні криптологічні системи
3. Шифрування текстів. Основні принципи Алгоритми симетричного шифрування
4. Основи шифрування та дешифрування методом Цезаря Криптосистеми із відкритим ключем
5. Алфавітний підхід до визначення кількості інформації
6. Шифрування методом Гронсфельда.
7. Шифри складної заміни
8. Шифри Віжинера
9. Дослідження шифру “Подвійний квадрат”