Технології захисту інформаційних систем

Заплановані результати навчання:

Мета вивчення навчальної дисципліни: формування системи теоретичних знань здобувачів вищої освіти щодо сучасних методів та засобів забезпечення інформаційної безпеки, порядку проєктування, впровадження та супроводження комплексної системи захисту інформації, системи управління інформаційною безпекою, підготовки фахівців, здатних аналізувати, обирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки та цілісності даних відповідно до розв'язуваних прикладних завдань.

Основні завдання навчальної дисципліни: є оволодіння необхідними теоретичними знаннями курсу та основними напрямами їх застосування, а саме знати та вміти: визначати чинники уразливості інформаційних систем, загрози інформаційної безпеки, забезпечувати безпеку інформаційних систем, здійснювати її моніторинг, розробляти і впроваджувати заходи щодо запобігання порушення захисту інформації і доступу до даних, встановлювати, налагоджувати та супроводжувати технічні засоби захисту інформації.

Компетентності:

загальні:

КЗ 4. Здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах;

КЗ 8. Здатність оцінювати та забезпечувати якість виконуваних робіт у сфері ІСТ.

фахові:

КС 3. Здатність до забезпечення надійності та безпеки на всіх етапах життєвого циклу інформаційних систем;

КС 4. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики і техніки кібербезпеки під час виконання функціональних завдань та обов'язків;

КС 12. Здатність працювати зі сховищами великих даних, і використовувати інструментальні засоби інтеграції різнотипних даних у наборах великої розмірності, здійснювати їх інтелектуальну обробку і створювати прикладні інформаційні продукти.

Програмні результати навчання:

ПР 4. Демонструвати знання стандартів, методів, і технологій управління проєктами створення, розгортання та розвитку інформаційних систем, основ управління ризиками та якістю проєктів інформаційних систем, світового досвіду планування управління проєктами інформаційних систем;

ПР 8. Визначати чинники уразливості інформаційних систем, загрози інформаційної безпеки, забезпечувати безпеку інформаційних систем, здійснювати її моніторинг, розробляти і впроваджувати заходи щодо запобігання порушення захисту інформації і доступу до даних, встановлювати, налагоджувати та супроводжувати технічні засоби захисту інформації;

ПР 14. Практикувати прийняття рішень у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування; демонструвати соціальну відповідальність за результати прийняття стратегічних рішень.

Програма навчальної дисципліни

Тема 1. Основні поняття безпеки інформаційних систем

Тема 2. Криптографічний захист інформації

Тема 3. Безпека програм та даних

Тема 4. Мережева та веббезпека

Тема 5. Етапи проєктування комплексної системи захисту інформації

Трудомісткість:

Загальна кількість годин 90 год

Кількість кредитів 3,0

Форма семестрового контролю екзамен