Анотація вибіркових дисциплін

076 Підприємництво та торгівля

Освітньо-професійна програма: Інформаційні технології в підприємницькій діяльності

Дисципліна	Технології захисту інформації
Курс	III
Циклова комісія	Інженерії програмного забезпечення, телекомунікацій та економічної кібернетики
Що буде вивчатися (мета і завдання)	Основна мета дисципліни – ознайомити з принципами побудови та використання програмних та програмно-апаратних засобів для захисту програмного забезпечення та іншої інформації в комп'ютерних системах. Головна задача дисципліни – надати основні відомості з принципів побудови систем захисту інформації та методів протидії спробам несанкціонованого доступу до неї з боку сторонніх осіб, привласнення привілей тощо.
Чому це цікаво/треба вивчати	Особлива увага буде приділена, окрім природних способів виявлення і своєчасного усунення причин (шкоди), також і спеціальним способам захисту інформації від порушень працездатності систем. Особливо, від загроз реалізація яких виконується при постійній участі людини та після розробки відповідних комп’ютерних програм без безпосередньої участі людини.
Чому можна навчитися (результати навчання)	Після вивчення дисципліни здобувач освіти повинен вміти: • виконати аналіз безпеки комп'ютерної системи та усунути можливі шляхи несанкціонованого доступу; • здійснити організаційні та програмні заходи щодо підвищення рівня безпеки зберігання інформації; • виконувати адміністрування прав доступу до комп’ютерної системи з метою перешкоди призначення невиправданих привілей; • виконувати постійний моніторинг з пошуку програмних закладок та каналів витоку інформації; • використовувати основні прийоми та програмні засоби хакерів для перевірки надійності захисту інформації та стійкості його щодо хакерських атак.
Як можна користуватися набутими знаннями і уміннями (компетентності)	Після вивчення дисципліни студент повинен знати: • об'єкти програмного забезпечення, на які можливі атаки з боку комп'ютерних хакерів, та методи здійснення несанкціонованого доступу до інформації; • принципи функціонування вбудованих засобів захисту комп'ютерних систем (BIOS) та шляхи протидії спробам їх взлому; • принципи функціонування систем захисту, призначення привілей, зберігання паролів та автентифікація користувачів в операційних системах WINDOWS та UNIX, методи хакерів з

	несанкціонованого проникнення до інформації, привласнення привілей адміністратора тощо; • методи несанкціонованого зйому та навмисного пошкодження інформації та засоби протидії цим спробам; • методи побудови захисту окремих програмних продуктів; • основні прийоми і програмні засоби для аналізу та дизасемблювання програмних продуктів з метою їх подальшого несанкціонованого використання, методи захисту від дизасемблювання.
Форма проведення занять	Лекція, практична та лабораторні роботи робота
Форма контролю	Залік