Вступ

Дисципліна “Безпека програмного забезпечення” відіграє ключову роль у підготовці фахівців з кібербезпеки, оскільки саме програмне забезпечення часто є об’єктом атак. Знання методів захисту коду, виявлення вразливостей, протидії реверс-інжинірингу, запобігання несанкціонованому копіюванню та використанню є необхідними для ефективного захисту інформаційних систем. Формування таких компетентностей дасть змогу майбутнім фахівцям не лише реагувати на загрози, а й проактивно створювати безпечне програмне забезпечення. Вивчення такої дисципліни забезпечує глибоке розуміння принципів безпеки на рівні коду та архітектури, що є фундаментом професійної діяльності у сфері кіберзахисту.

У практикумі містяться настанови щодо виконання лабораторних робіт. До кожної роботи подано: короткі теоретичні відомості, сформульовані завдання, контрольні запитання, а також взірці виконання завдань з детальним поясненням. Контрольні запитання дають змогу провести самооцінку глибини засвоєного теоретичного матеріалу, а покрокові інструкції до виконання індивідуальних завдань лабораторних робіт – розширити і закріпити лекційний матеріал, здобути практичні навички щодо забезпечення інформаційної безпеки та захисту програмного забезпечення. Перелік тем лабораторних робіт та їх оцінювання визначаються робочою програмою навчальної дисципліни.

Практикум призначений насамперед на студентів вищих навчальних закладів, для підготовки здобувачів вищої освіти за першим (бакалаврським) рівнем галузі знань F “Інформаційні технології” спеціальності F5 “Кібербезпека та захист інформації”.