# ОСНОВИ КІБЕРБЕЗПЕКИ

**Вивчає:** кіберпростір і кібербезпеку — головні ознаки нової інформаційної цивілізації; національну систему кібербезпеки України; сутність та основні процедури управління кібербезпекою; кібератаки, загрози та їх властивості. Характеристика сучасних кібератак; дезінформацію як елемент кібератак. Сценарії розвитку та методи протидії; комп'ютерну вірусологію; соціальна інженерію; соціотехнічну безпеку: проблемні аспекти; безпеку спілкування в кіберпросторі; забезпечення інформаційної безпеки в діяльності суб'єктів господарювання; безпеку цифрового простору суб'єктів господарювання; безпеку Інтернету-речей; системи захисту інформації на проникнення; основні методи забезпечення кібербезпеки суб'єкта господарювання;

**Основна увага** приділяється формуванню необхідного рівня знань щодо правильного поводження з інформацією у кіберсфері та безпечної роботи із засобами комп'ютерної техніки в професійній діяльності; знанню про основні загрози в сучасному інформаційному просторі; аналізу поширених помилок користувачів та наслідки від атак зловмисників і кібершахраїв; вивченню базових правил захисту інформації на персональних електронних пристроях та в соціальних мережах; визначенню фейкових новин; опануванню основних рекомендацій щодо захисту власних даних, безпечного користування електронними пристроями та інформаційними ресурсами у сфері обліку, аналізу, контролю, аудиту, оподаткування, що характеризуються невизначеністю умов і вимог.

**У результаті опанування дисципліни здобувачі будуть уміти:**

- визначати основні положення, терміни та заходи, що стосуються кібергігієни на робочу місці;
- визначати основну нормативно-правову бази у сфері кібербезпеки та інформаційної безпеки;
- визначати особливості кібергігієни в системі публічної служби;
- визначати заходи кібергігієни для конкретної ситуації;
- оцінювати загрози та вживати заходів реагування на робочому місці;
- безпечно поводитись у кіберсфері;
- використовувати навички організації безпечного доступу до пристроїв і програм;
- використовувати навички правильного налаштування програмного забезпечення на робочому місці;
- використовувати навички критичного оцінювання інформації;
- використовувати різні типи зловмисного ПЗ (відомого як шкідливі програми) та їх симптоми; знати різні методи, якими нападники можуть проникнути в систему: соціальна інженерія, злам паролю Wi-Fi, фішинг та використання вразливостей, тощо.