АНОТАЦІЯ
до дисципліни **«Управління інформаційною безпекою комп'ютерних систем»**

Мета дисципліни: Отримання студентами необхідних знань щодо принципів створення комплексних систем захисту інформації (КСЗІ) в інформаційних, комунікаційних та інформаційно-телекомунікаційних системах (ІТС), здійснення комплексу заходів, спрямованих на розроблення і впровадження інформаційних технологій, які забезпечують обробку інформації в ІТС згідно з вимогами, встановленими нормативно-правовими актами та нормативними документами у сфері захисту інформації, а також принципів проведення експертизи КСЗІ, отримання студентами необхідних базових знань з організації та проведення аудиту інформаційної безпеки в інформаційно-телекомунікаційних системах різного призначення.

Значна увага приділяється засвоєнню принципів, задач системи управління інформаційною безпекою, вивченню нормативної та правової бази з питань організації та проведення аудиту інформаційної безпеки в ІТС різного призначення, методик оцінки інформаційних ризиків.

Завдання дисципліни: Формування комплексу знань та умінь щодо менеджменту інформаційної безпеки, набуття студентами теоретичних знань та практичних навичок щодо управління інформаційною безпекою в ІТС для реалізації встановленої політики безпеки.

Результати навчання дисципліни

В результаті вивчення дисципліни студент повинен **знати:**

– як складати та впроваджувати політики інформаційної безпеки;
– як організовувати інформаційну безпеку, її внутрішню організацію, політику щодо мобільного обладнання та віддаленої роботи;
– як забезпечувати безпеку людських ресурсів перед наймом, протягом найму та за припинення чи зміні умов найму;
– криптографічні засоби захисту;
– як застосовувати засоби забезпечення безпеки експлуатації, зокрема безпечні процедури експлуатації та відповідальності, захисту від зловмисного коду, резервне копіювання, ведення журналів аудиту та моніторинг, управління технічною вразливістю, розгляд аудиту інформаційних систем;
– як застосовувати засоби забезпечення безпеки комунікацій: управління безпекою мережі та обміну інформацією;
– як застосовувати засоби забезпечення безпеки для інформаційних систем: вимоги щодо безпеки для інформаційних систем, безпека в процесах розроблення та підтримки, дані для тестування системи;
– як застосовувати засоби забезпечення вимог щодо відносин з постачальниками: інформаційна безпека у взаємовідносинах з постачальниками, управління наданням послуг постачальником.

В результаті вивчення дисципліни студент повинен **вміти:**

– складати та впроваджувати політики інформаційної безпеки;
– організовувати інформаційну безпеку, її внутрішню організацію, політику щодо мобільного обладнання та віддаленої роботи;
– забезпечувати безпеку людських ресурсів перед наймом, протягом найму та за припинення чи зміні умов найму;
– застосовувати заходи управління ресурсами СУІБ: відповідальність за ресурси СУІБ, класифікація інформації та поводження з носіями;
– застосовувати заходи контролю доступу, зокрема, бізнес-вимоги до контролю доступу, управління доступом користувача, відповідальності користувача та контроль доступу до систем і прикладних програм;
– застосовувати криптографічні засоби захисту, розробляти політику використання криптографічних засобів;
– забезпечувати заходи фізичної безпеки та безпеки інфраструктури: зони безпеки, обладнання;
– застосовувати засоби забезпечення безпеки експлуатації, зокрема безпечні процедури експлуатації та відповідальності, захисту від зловмисного коду, резервне копіювання, ведення журналів аудиту та моніторинг, управління технічною вразливістю, розгляд аудиту інформаційних систем;
– застосовувати засоби забезпечення безпеки комунікацій: управління безпекою мережі та обміну інформацією;
– застосовувати засоби забезпечення безпеки для інформаційних систем: вимоги щодо безпеки для інформаційних систем, безпека в процесах розроблення та підтримки, дані для тестування системи;
– застосовувати засоби забезпечення вимог щодо відносин з постачальниками: інформаційна безпека у взаємовідносинах з постачальниками, управління наданням послуг постачальником.

Перелік компетентностей, що вдосконалюватимуться/набуватимуться

Загальні: КЗ2, КЗ3, КЗ6.

Спеціальні: КС1, КС2, КС5, КС6, КС10, КС12.

Вивчення навчальної дисципліни передбачає досягнення студентом таких прикладних результатів навчання (ПР): ПР3, ПР4, ПР5, ПР8, ПР9, ПР10.

Формат дисципліни

Формат – змішана дисципліна, що передбачає проведення лекцій, лабораторних занять та консультацій.

Обсяг дисципліни

Вид заняття	**Загальна кількість годин**
лекції заняття	**32**
лабораторні заняття	**32**
самостійна робота	**71**
Всього за дисципліну	**135**

Пререквізити. Студенти повинні володіти базовими знаннями з таких дисциплін: Архітектура та проєктування програмного забезпечення, Тестування програмного забезпечення, Комп'ютерні мережі, Операційні системи, Веб-технології.

Характеристика навчальної дисципліни – **вибіркова**. Вона належить до вибіркових дисциплін циклу професійної підготовки освітньої програми «Інформаційні системи та технології» першого (бакалаврського) рівня вищої освіти. Галузь знань 12 «Інформаційні технології», спеціальності 126 «Інформаційні системи та технології». Викладається у 7 семестрі (четвертий курс) обсягом 4,5 кредити ECTS. Формою підсумковою контролю є **залік**.