

КІБЕРБЕЗПЕКА

Кредити та кількість годин: 4 ECTS; години: 12 лекційних, 12 практичних, 96 самостійна робота; залік.

I. Опис навчальної дисципліни

Цей курс спрямований на освоєння сутності та змісту кібербезпеки. У ході вивчення дисципліни розглядається роль і місце кібербезпеки у системі національної безпеки держави, надається аналіз побудови системи кібербезпеки, описується широке коло питань зі складових кібербезпеки, їх аналізу і дій для її всебічного забезпечення. Особливої уваги приділено технологіям дій у кіберпросторі та впровадженню організаційних і управлінських заходів кібербезпеки.

Основне завдання курсу дати студентам теоретичну та практичну підготовку з основ кібербезпеки, зокрема: тактику, методи та процедури, які використовуються кіберзлочинцями; принципи конфіденційності, цілісності і доступності, оскільки вони відносяться до станів даних і контрзаходів у сфері кібербезпеки; технології, продукти і процедури, які використовуються для захисту конфіденційності, цілісності та доступності; розуміння використовуваних фахівцями кібербезпеки технологій, процесів та процедур для захисту всіх компонентів мережі.

II. Мета та завдання навчальної дисципліни

Метою викладання дисципліни «Кібербезпека» є отримання знань та умінь, які необхідні для успішного виявлення вразливостей у кіберпросторі та усунення проблем безпеки шляхом розробки та впровадження захисних заходів.

Завданням вивчення дисципліни «Кібербезпека» є надання студентам необхідної теоретичної та практичної підготовки, а саме наступні вміння та знання:

- використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності в галузі кібербезпеки;
- аналізувати та виявляти загрози інформації, а також проводити реалізацію засобів захисту;
- аналізувати наслідки кібератак; знати різні категорії вразливостей програмного та апаратного забезпечення і систем безпеки;
- описати принципи конфіденційності, цілісності та доступності відносно стану даних та заходів протидії загрозам у сфері кібербезпеки;
- прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави, суспільству, організації та дестабілізуючі чинники в роботі систем управління;
- знати різні типи шкідливого програмного забезпечення;
- знати різні методи, якими використовують зловмисники для реалізації кібератак;
- знати засоби захисту та превентивних дій для запобігання реалізації кіберзагроз.

III. Результати навчання

Дисципліна «Кібербезпека», як обов'язкова компонента освітньої програми, забезпечує оволодіння студентами загальними та фаховими компетентностями і досягнення ними програмних результатів навчання за відповідною освітньо-професійною програмою «Національна безпека (за окремими сферами забезпечення і видами діяльності):

- критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

- застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
- реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
- вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
- проводити розслідування реалізованих кіберінцидентів;
- забезпечувати впровадження запобіжних заходів протидії кібератакам та кіберзагрозам.

IV. Програма навчальної дисципліни (структура дисципліни)

№	Теми
1	Кіберпростір, кібербезпека, кібератаки та кібертероризм. Основні поняття та визначення.
2	Методи та засоби соціального інжинірингу.
3	Напрями забезпечення кібербезпеки України. Основи міжнародної співпраці з питань кібербезпеки
4	Технологічні аспекти захисту інформації в інформаційно-телекомунікаційних системах. Ідентифікація, автентифікація, авторизація. Антивірусний захист.
5	Основи безпеки комп'ютерних мереж
6	Віртуальні приватні мережі (VPN) в інформаційно-телекомунікаційних системах.