# Анотація до навчальної дисципліни
# «ЗАПОБІГАННЯ КІБЕРЗЛОЧИНАМ»

| | |
|---|---|
| **Мета вивчення навчальної дисципліни** | формування системи наукових знань про правове регулювання запобігання кіберзлочинів, вивчення вітчизняних та зарубіжних підходів до розуміння змісту заходів забезпечення кібербезпеки, вироблення основних умінь і навичок застосування національного законодавства, активізація аналітичної діяльності студентів, проведення науково-дослідницької роботи, а також практичних навичок діяльності правника. |
| **Завдання навчальної дисципліни** | формування системи теоретичних знань про інститут кібербезпеки, його змістовне наповнення; опанування інструментарієм інституту запобігання кіберзлочинам, базовими категоріями кібербезпеки; визначення поняття, видів та стану кіберзлочинності: рівня, структури, динаміки та інших показників; аналіз і дослідження прикладних проблем порядку формування та реалізації державної політики в сфері забезпечення кібербезпеки, спрямованих на набуття (підтвердження) суб'єктивних прав та покладення на приватних осіб передбачених законом обов'язків; наведення характеристики, класифікацій та видів кіберзлочинів, аналіз їх структури, визначення стадій та етапів, окреслення повноважень суб'єктів запобігання кіберзлочинам; розвиток навичок і умінь запровадження та застосування заходів запобігання кіберзлочинам. |
| **У результаті вивчення навчальної дисципліни студенти повинні:** | **мати уявлення:**<br>про новітні досягнення науки в сфері запобігання кіберзлочинам;<br>закономірності виникнення і поширення кіберзлочинності;<br>**знати:**<br>основні принципи забезпечення кібербезпеки;<br>сукупність ознак структури особи кіберзлочинця; |

| | |
|---|---|
| | основні теорії пояснення причин кіберзлочинності;<br>засадничі положення державної політики забезпечення кіберзахисту та кібербезпеки;<br>**уміти:**<br>досліджувати рівень, структуру, динаміку кіберзлочинності;<br>характеризувати суспільні явища і процеси, що породжують та зумовлюють кіберзлочинність;<br>аналізувати законодавство, що визначає систему заходів запобігання різним формам і проявам кіберзлочинності;<br>надавати кримінологічну характеристику кримінальним правопорушенням у віртуальній сфері та пропонувати заходи запобігання їм;<br>**володіти навичками:**<br>аналізу та оцінювання стану кіберзлочинності в державі;<br>складання проєктів програм запобігання окремим видам кіберзлочинів.<br>Оволодіння навчальної дисципліни «Запобігання кіберзлочинам» сприятиме суттєвому підвищенню загального рівня підготовки правників, розвиткові аналітичних здібностей, удосконаленню володіння компетентностями, що забезпечить у подальшому їх належний професійний рівень. |
| **Зміст навчальної дисципліни:** | ***ЗМІСТОВИЙ МОДУЛЬ І:***<br>***«Формування та реалізація державної політики в сфері кібербезпеки».***<br>Тема 1. Основні цілі, напрями та принципи державної політики у сфері кібербезпеки.<br>Тема 2. Стан забезпечення кібербезпеки на сучасному етапі. |

| | |
|---|---|
| | ***ЗМІСТОВИЙ МОДУЛЬ ІІ:***<br>***«Базові засади запобігання кіберзлочинам».***<br>Тема 3. Поняття і визначення кіберзлочину.<br>Тема 4. Кіберзлочинність та її вимірювання.<br>Тема 5. Особа кіберзлочинця.<br>Тема 6. Запобігання кіберзлочинності: поняття, зміст, значення.<br><br>***ЗМІСТОВИЙ МОДУЛЬ ІІІ:***<br>***«Теорія окремих видів кіберзлочинів та їх запобігання».***<br>Тема 7. Підходи до класифікації кіберзлочинів. Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.<br>Тема 8. Характеристика кіберзлочинів пов'язаних з використанням комп'ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо)<br>Тема 9. Характеристика кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією) та інших кіберзлочинів<br>Тема 10. *Гібридна війна.* |