Національний юридичний університет імені Ярослава Мудрого

Військово-юридичний інститут

Кафедра кримінально-правової політики

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Запобігання кіберзлочинності»

Рівень вищої освіти – перший (бакалаврський) рівень

Ступінь вищої освіти – бакалавр

Галузь знань – 26 «Цивільна безпека»

Спеціальність – 262 «Правоохоронна діяльність»

Спеціалізація – «Правоохоронна діяльність»

Статус навчальної дисципліни – обов'язкова

Рік набору – 2024

Харків 2024

Робоча програма навчальної дисципліни «Запобігання кіберзлочинності» для здобувачів вищої освіти першого (бакалаврського) рівня вищої освіти галузі знань 26 «Цивільна безпека» спеціальності 262 «Правоохоронна діяльність» спеціалізації «Правоохоронна діяльність». Харків: Нац. юрид. ун-т імені Ярослава Мудрого, 2024. 25 с.

Розробники:
Таволжанський Олексій Володимирович,
кандидат юридичних наук, доцент, доцент кафедри кримінології
та кримінально-виконавчого права;
Оболенцев Валерій Федорович,
кандидат юридичних наук, доцент, доцент кафедри кримінології
та кримінально-виконавчого права

Затверджено на засіданні кафедри кримінології
та кримінально-виконавчого права
(протокол № 14 від 10 червня 2022 р.)

Завідувач кафедри – Головкін Богдан Миколайович, доктор юридичних наук, професор

Оновлену редакцію (зі змінами та доповненнями)
затверджено на засіданні кафедри кримінально-правової політики
(протокол № 10 від 30 травня 2023 р.)

Оновлену редакцію (зі змінами та доповненнями)
затверджено на засіданні кафедри кримінально-правової політики
(протокол № 10 від 11 червня 2024 р.)

Завідувач кафедри – Харитонов Сергій Олександрович, доктор юридичних наук, професор

Зміст

1. Опис навчальної дисципліни

Робоча програма навчальної дисципліни «Запобігання кіберзлочинності» розроблена відповідно до освітньо-професійної програми «Правоохоронна діяльність» першого (бакалаврського) рівня вищої освіти галузі знань 26 «Цивільна безпека» спеціальності 262 «Правоохоронна діяльність» спеціалізації «Правоохоронна діяльність».

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Рівень освіти, галузь знань, спеціальність, спеціалізація</td><td>Дидактична структура навчальної дисципліни</td></tr>
<tr><td>Денна форма навчання</td></tr>
<tr><td>Кількість кредитів ЄКТС – 4,0</td><td rowspan="12">Рівень освіти – перший (бакалаврський)

Галузь знань – 26 «Цивільна безпека»

Спеціальність – 262 «Правоохоронна діяльність»

Спеціалізація – «Правоохоронна діяльність»</td><td>Обов’язкова</td></tr>
<tr><td rowspan="2">Кількість модулів – 3</td><td>Період підготовки: 2024-2027</td></tr>
<tr><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 120</td><td>6</td></tr>
<tr><td>Лекції</td></tr>
<tr><td rowspan="5">Тижневих годин:
аудиторних – 2-4,
самостійної роботи здобувача вищої освіти – 2-6</td><td>30 год.</td></tr>
<tr><td>Практичні заняття</td></tr>
<tr><td>34 год.</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>56 год.</td></tr>
<tr><td>Види контролю:
поточний контроль;
підсумковий контроль знань (диференційований залік)</td></tr>
</table>

Мета навчальної дисципліни – забезпечити фундаментальну теоретичну і практичну підготовку фахівців з правоохоронної діяльності у сфері запобігання кіберзлочинам; оволодіння ними базовими знаннями, вміннями, навичками, комунікацією та автономією, які необхідні для розв’язування складних задач та практичних проблем охорони прав і свобод людини, громадянського суспільства і держави, протидії кіберзлочинності, забезпечення публічної безпеки і порядку тощо.

Завдання:

- формування системи теоретичних знань про інститут кібербезпеки, його змістовне наповнення;

- опанування інструментарієм інституту запобігання кіберзлочинам, базовими категоріями кібербезпеки;

- набуття вмінь щодо визначення стану кіберзлочинності: рівня, структури, динаміки та інших показників;

- вироблення навичок аналізу і дослідження прикладних проблем порядку формування та реалізації державної політики у сфері забезпечення кібербезпеки в контексті набуття (підтвердження) суб'єктивних прав та покладення на приватних осіб передбачених законом обов'язків;

- вироблення вміння щодо наведення характеристики класифікацій та видів кіберзлочинів, аналізу їх структури, визначення стадій та етапів, окреслення повноважень суб'єктів запобігання кіберзлочинам;

- розвиток навичок і умінь запровадження та застосування заходів запобігання кіберзлочинам.

Пререквізити: «Теорія права», «Конституційне право України», «Правові основи діяльності органів кримінальної юстиції», «Професійна відповідальність правоохоронця», «Адміністративне право», «Цивільне право», «Кримінальне право», «Міжнародне право», «Кримінологія», «Основи організації та ведення боротьби в електромагнітному середовищі та кіберпросторі», «Правові основи інформаційної безпеки у воєнній сфері».

Кореквізити: «Право національної безпеки України», «Криміналістика», «Інформаційно-аналітичне забезпечення правоохоронної діяльності».

Постреквізити: «Засоби зв'язку та програмно-технічні комплекси підрозділів Державної прикордонної служби України», «Правові основи розвідувальної та контррозвідувальної діяльності підрозділів Державної прикордонної служби України», «Запобігання та протидія організованій та транснаціональній злочинності».

2. Очікувані результати навчання

У результаті засвоєння навчальної дисципліни здобувач вищої освіти повинен демонструвати такі результати навчання:

РН НД-1	Аналізувати понятійний апарат у сфері кіберзахисту, детермінанти та зміст кіберзлочинності.
РН НД-2	Співвідносити міжнародний досвід у сфері запобігання кіберзлочинам.

РН НД-3	Дискутувати зі складних правових проблем застосування європейських стандартів забезпечення кібербезпеки.
РН НД-4	Здійснювати дослідження правового регулювання у віртуальній сфері.
РН НД-5	Обґрунтовано формулювати свою правову позицію щодо принципів забезпечення кібербезпеки.
РН НД-6	Генерувати нові ідеї та використовувати сучасні стандарти для вдосконалення законодавства у сфері запобігання кіберзлочинам.
РН НД-7	Здійснювати порівняльно-правовий аналіз національних актів з іншими актами, спрямованими на запобігання кіберзлочинам.
РН НД-8	Інтегрувати знання про сутність запобігання кіберзлочинам, його місце в забезпеченні кібербезпеки.
РН НД-9	Демонструвати розуміння змісту правового статусу суб'єктів забезпечення кібербезпеки, особливостей їх участі в запобіганні кіберзлочинам.
РН НД-10	Аналізувати змістовне наповнення етапів і стадій запобігання кіберзлочинам, визначати заходи запобігання кіберзлочинності.
РН НД-11	Демонструвати навички підготовки проєктів документів, спрямованих на забезпечення кібербезпеки, наводити їх обґрунтування.
РН НД-12	Демонструвати навички визначення стану кіберзлочинності.

Викладання навчальної дисципліни забезпечує формування у здобувача вищої освіти загальних і спеціальних компетентностей та досягнення результатів навчання, визначених стандартом вищої освіти відповідної спеціальності та освітньо-професійною програмою «Правоохоронна діяльність», а саме:

Загальних компетентностей:

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК4. Здатність використовувати інформаційні та комунікаційні технології.

ЗК5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК7. Здатність до адаптації та дії в новій ситуації.

ЗК8. Здатність приймати обґрунтовані рішення.

ЗК9. Здатність працювати в команді.

ЗК11. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати

різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

ЗК 1.1. Здатність удосконалювати свій професійний рівень та набувати нові знання.

ЗК 1.2. Здатність до пошуку альтернативних рішень у професійній діяльності.

ЗК 1.3. Здатність бути лідером, стимулювати на досягнення спільної мети, брати на себе відповідальність.

ЗК 1.5. Здатність до креативності у предметно-практичній діяльності.

Спеціальних компетентностей:

СК1. Усвідомлення функцій держави у сфері правоохоронної діяльності, способів та механізмів реалізації цих функцій.

СК3. Здатність до критичного мислення та системного аналізу правових явищ.

СК4. Здатність самостійно збирати та критично опрацьовувати, аналізувати та узагальнювати правову інформацію з різних джерел.

СК5. Здатність визначати придатні для юридичного аналізу факти, систематизувати одержані результати, встановлювати причинно-наслідкові зв’язки, формулювати аргументовані висновки та рекомендації.

СК8. Здатність ефективно застосовувати сучасну техніку та інформаційні технології, використовувати технічні засоби, спеціалізовані інформаційно-пошукові системи, бази та банки даних, а також відповідне програмне забезпечення для захисту прав і свобод людини, власності, суспільних відносин від протиправних посягань.

СК10. Здатність до аналізу та оцінки причин, умов та факторів, що впливають на вчинення кримінальних та адміністративних правопорушень.

СК11. Здатність визначати особу правопорушника, аналізувати кількісні та якісні показники злочинності.

СК16. Здатність забезпечувати кібербезпеку, економічну та інформаційну безпеку держави, об’єктів критичної інфраструктури.

СК18. Здатність вживати заходів з метою запобігання, виявлення та припинення кримінальних та адміністративних правопорушень, усунення загроз життю та здоров'ю фізичних осіб і публічній безпеці, що виникли внаслідок учинення правопорушення.

СК1.1. Здатність до реалізації міжнародних стандартів прав і свобод людини у правоохоронній діяльності.

СК1.2. Уміння виявляти проблеми правозастосування та пропонувати шляхи їх вирішення під час здійснення правоохоронної діяльності.

СК1.4. Здатність використовувати спеціальні знання в різних сферах правоохоронної діяльності.

СК1.5. Вміння визначати напрями і способи виявлення та протидії організованій та транснаціональній злочинності.

Програмних результатів навчання:

РН2. Вести міжособистісний діалог та превентивну комунікацію з метою виконання завдань професійної діяльності.

РН3. Розуміти та професійно застосовувати понятійний апарат права та правоохоронної діяльності.

РН4. Формулювати і перевіряти гіпотези, виокремлювати юридично значущі факти, виявляти причинно-наслідкові зв'язки в діях і явищах для прийняття оптимального рішення в конкретних ситуаціях.

РН5. Розробляти тексти, документи з питань професійної діяльності, вільно спілкуватися українською та іноземною мовами.

РН7. Взаємодіяти із суб'єктами забезпечення публічної (громадської) безпеки і порядку, а також здійснювати комунікацію з фізичними та юридичними особами з метою виконання завдань у сфері правоохоронної діяльності.

РН8. Здійснювати пошук інформації у доступних джерелах, аналізувати і оцінювати її для повного та всебічного встановлення обставин, необхідних для виконання професійних завдань.

РН9. Використовувати інформаційно-комунікаційні системи та інші інформаційні ресурси, у тому числі ті, що мають технічний та криптографічний

захист, поштовий зв’язок спеціального призначення, фельд’єгерський зв’язок, системи цифрового зв’язку суб’єктів сектору безпеки і оборони з метою виконання професійних завдань у сфері правоохоронної діяльності.

РН10. Виокремлювати юридично значущі факти і формувати обґрунтовані правові висновки.

РН11. Знати і розуміти сучасні правові доктрини, цінності та принципи функціонування національної правової системи.

РН12. Адаптуватися і ефективно діяти у стандартних професійних ситуаціях, а також у разі ускладнення оперативної обстановки, підвищення фізичного та психологічного навантаження.

РН14. Здійснювати пошук та аналіз новітньої інформації у сфері правоохоронної діяльності, мати навички саморозвитку та самоосвіти протягом життя, підвищення професійної майстерності, вивчення та використання передового досвіду у сфері правоохоронної діяльності.

РН15. Працювати самостійно та в команді при виконанні службових (посадових) обов’язків та під час розв’язання складних спеціалізованих задач у сфері правоохоронної діяльності.

РН17. Використовувати методи та засоби забезпечення публічної (громадської) безпеки та порядку, протидії злочинності, дотримуватися прав і свобод людини і громадянина, здійснювати заходи щодо попередження та припинення нелегальної (незаконної) міграції та інших загроз національній безпеці держави.

РН18. Застосовувати вогнепальну зброю та спеціальні засоби (штатне та бойове озброєння), фізичну силу; інформаційні системи та технології, технології захисту даних, методи обробки, накопичення та аналізу інформації, інформаційно-аналітичні системи, бази даних (в тому числі міжвідомчі та міжнародні), криміналістичні та оперативно-технічні засоби, безпілотну авіацію, іншу спеціальну та військову техніку і спорядження.

РН22. Оцінювати оперативну (бойову) обстановку, рівень потенційних загроз та викликів, прогнозувати їх розвиток, застосовувати тактичні методи

превентивного та силового втручання для запобігання та припинення правопорушень, усунення загроз внутрішньому безпековому середовищу, державному суверенітету та територіальній цілісності держави, у тому числі у взаємодії з іншими уповноваженими на це органами та громадою.

РН1.1. Виконувати оперативні завдання правоохоронної діяльності із залученням фахівців з інших галузей знань.

РН1.2. Демонструвати навички верифікації отриманої під час здійснення правоохоронної діяльності інформації.

РН1.4. Визначати професійні завдання і організовувати підлеглих для їх виконання, брати на себе відповідальність за отримані результати та здійснювати службові обов'язки у нестандартних ситуаціях за наявності неповної або обмеженої інформації.

РН1.5. Виявляти навички фізичної підготовленості; експлуатації й обслуговування техніки; тактичного планування, моделювання та прийняття оптимальних рішень в умовах невизначеності.

3. Зміст програми навчальної дисципліни

Модуль 1. Формування та реалізація державної політики у сфері кібербезпеки

Основні цілі, напрями та принципи державної політики у сфері кібербезпеки. Стратегія, напрямки сучасної політики у сфері кібербезпеки в Україні та зарубіжних країнах. Суб'єкти формування та реалізації політики у сфері кібербезпеки та кіберзахисту державних інформаційних ресурсів, інформації. Фактори, що впливають на державну політику у сфері кібербезпеки. Об'єкти кібербезпеки та кіберзахисту. Поняття об'єкта кібербезпеки та кіберзахисту. Процедура включення об'єкта до переліку об'єктів кібербезпеки та кіберзахисту. Суб'єкти забезпечення кібербезпеки. Поняття суб'єкта забезпечення кібербезпеки. Класифікація суб'єктів, діяльність яких спрямована на забезпечення кібербезпеки.

Кіберзлочинність в умовах повномасштабного російського вторгнення в Україну. Кіберзлочинність як елемент гібридної війни РФ проти України. Тенденції кіберзлочинності як способу ведення війни. Характеристика кіберзлочинів у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації. Поняття військових кіберзлочинів та їх характеристика.

Стан забезпечення кібербезпеки на сучасному етапі. Світовий досвід та тенденції у формуванні безпечного віртуального простору. Передумови та чинники кіберзагроз. Заходи забезпечення кібербезпеки. Концепція розвитку науки щодо запобігання кіберзлочинності в Україні на початку XXI століття. Методологічні особливості вивчення кіберпростору.

Міжнародний досвід у побудові безпечного кіберпростору. Базові міжнародні документи щодо запобігання кіберзлочинності. Кіберзлочинність та транснаціональна організована злочинність. Міжнародні акти про захист дітей від сексуальної експлуатації та сексуального насильства. Міжнародні та іноземні суб'єкти запобігання кіберзлочинності.

Модуль 2. Базові засади запобігання кіберзлочинам

Поняття і визначення кіберзлочину. Кіберзлочин як соціально-правове явище, особа кіберзлочинця, детермінація кіберзлочинності, запобігання кіберзлочинності. Запобігання кіберзлочинам як міжгалузева дисципліна. Класифікація кіберзлочинів. Запобігання кіберзлочинності на сучасному етапі розвитку України і в перспективі.

Кіберзлочинність та її вимірювання. Поняття кіберзлочинності та основні науково-практичні підходи щодо її розуміння і визначення. Кількісно-якісне вимірювання кіберзлочинності. Рівень кіберзлочинності. Структура кіберзлочинності. Кримінально-правові ознаки структури кіберзлочинності. Кримінологічні ознаки структури кіберзлочинності. Динаміка кіберзлочинності. Технічні фактори, які впливають на динаміку кіберзлочинності. Соціальні фактори, які впливають на динаміку кіберзлочинності. Правові фактори, які

впливають на динаміку кіберзлочинності. Географія кіберзлочинності. Топографія кіберзлочинності. Ціна кіберзлочинності.

Латентність кіберзлочинності. Структура латентної кіберзлочинності. Детермінація латентної кіберзлочинності. Загальна характеристика латентності сучасної кіберзлочинності в Україні, тенденції її розвитку.

Особа кіберзлочинця. Зміст поняття кіберзлочинець та основні підходи до його визначення. Структура особистості кіберзлочинця. Соціально-демографічні ознаки особистості кіберзлочинця. Морально-психологічні якості й особистісно-рольові властивості особистості кіберзлочинця. Соціальне і біологічне в особистості кіберзлочинця, їх співвідношення. Типологія кіберзлочинців. Наукове і практичне значення вивчення особистості кіберзлочинця та її типології.

Детермінанти кіберзлочинності. Умови формування кримінальної мотивації та мотивів. Умови реалізації мотивів і рішення про вчинення кіберзлочину. Поняття причини кіберзлочину. Умови, що сприяють вчиненню кіберзлочину. Умови формування кримінальної мотивації та мотивів. Умови реалізації мотивів і рішення про вчинення кіберзлочину.

Запобігання кіберзлочинності: поняття, зміст, значення. Поняття і система запобігання кіберзлочинності, класифікація запобіжних заходів. Загально соціальне, спеціально-кримінологічне та індивідуальне запобігання кіберзлочинності й окремих злочинів. Об’єкти запобігання кіберзлочинності. Суб’єкти запобігання кіберзлочинності та основні напрями їх діяльності. Прогнозування в сфері кіберзахисту. Поточне прогнозування. Короткострокове прогнозування. Середньострокове прогнозування. Перспективне прогнозування. Загальнодержавне планування. Регіональне планування. Відомче та галузеве планування. Головні етапи планування.

Модуль 3. Теорія окремих видів кіберзлочинів та їх запобігання

Підходи до класифікації кіберзлочинів. Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп’ютерних даних і систем (незаконний доступ, незаконне перехоплення, втручання в дані, втручання в

систему). Поняття та характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерної інформації. Основні кримінологічні риси особистості кіберзлочинців, які вчиняють злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему). Причини та умови злочинів проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему). Запобігання кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему).

Характеристика кіберзлочинів, пов'язаних з контентом (змістом даних), розміщеним у комп'ютерних мережах (зокрема злочинів, пов'язаних з дитячою порнографією). Характеристика кіберзлочинів, пов'язаних з контентом. Особистість кіберзлочинця, основні риси. Причини і умови кіберзлочинів, пов'язаних з контентом (змістом даних), розміщеним у комп'ютерних мережах (зокрема злочинів, пов'язаних з дитячою порнографією). Запобігання кіберзлочинам, пов'язаним із контентом (змістом даних), розміщеним у комп'ютерних мережах (зокрема злочинам, пов'язаним із дитячою порнографією).

Характеристика кіберзлочинів, пов'язаних з порушенням авторського права і суміжних прав. Поняття та характеристика кіберзлочинів, пов'язаних з порушенням авторського права і суміжних прав. Причини та умови кіберзлочинів, пов'язаних з порушенням авторського права і суміжних прав. Запобігання кіберзлочинам, пов'язаним з порушенням авторського права і суміжних прав.

Характеристика кіберзлочинів, зафіксованих в окремому протоколі (акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж). Поняття та характеристика кіберзлочинів, зафіксованих в окремому протоколі (акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж). Хуліганство у

віртуальній сфері. Запобігання кіберзлочинам проти громадського порядку та моральності.

Кіберзлочинність у сфері економіки. Поняття та характеристика кіберзлочинів у сфері економіки. Особистість кіберзлочинця, основні риси. Причини та умови кіберзлочинів у сфері економіки. Запобігання кіберзлочинам у сфері економіки. Характеристика кіберзлочинів, пов'язаних з використанням комп'ютера як засобу скоєння злочинів, а саме, як засобу маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо). Поняття та характеристика кіберзлочинів, пов'язаних із використанням комп'ютера як засобу скоєння злочинів. Особистість кібершахрая, основні риси. Причини і умови кіберзлочинів, пов'язаних із використанням комп'ютера як засобу скоєння злочинів, а саме, як засобу маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо). Запобігання кіберзлочинам, пов'язаним із використанням комп'ютера як засобу скоєння злочинів, а саме, як засобу маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо).

4. Обсяг і структура навчальної дисципліни

№ п/п	Дата проведення (згідно розкладу)	Тематика навчального курсу	Обсяг у годинах			
			Усього	У тому числі		
				Лекції	Практичні заняття, колоквіуми тощо	Самостій на робота
		Модуль 1. Формування та реалізація державної політики у сфері кібербезпеки.				
1.		Тема 1. Основні цілі, напрями та принципи державної політики у сфері кібербезпеки.	12	2	4	6
2.		Тема 2. Кіберзлочинність в умовах	8	2	2	4

		повномасштабного російського вторгнення в Україну.				
3.		Тема 3. Стан забезпечення кібербезпеки на сучасному етапі.	6	2	2	2
4.		Тема 4. Міжнародний досвід у побудові безпечного кіберпростору.	8	2	2	4
		Разом	*34*	*8*	*10*	*16*
		Модуль 2. Базові засади запобігання кіберзлочинам.				
5.		Тема 1. Поняття і визначення кіберзлочину.	6	2	2	2
6.		Тема 2. Кіберзлочинність та її вимірювання.	12	2	4	6
7.		Тема 3. Латентність кіберзлочинності.	6	2	2	2
8.		Тема 4. Особа кіберзлочинця.	6	2	2	2
9.		Тема 5. Детермінанти кіберзлочинності.	6	2	2	2
10.		Тема 6. Запобігання кіберзлочинності: поняття, зміст, значення.	8	2	2	4
		Разом	*44*	*12*	*14*	*18*
		Модуль 3. Теорія окремих видів кіберзлочинів та їх запобігання.				
11.		Тема 1. Підходи до класифікації кіберзлочинів.	6	2	2	2
12.		Тема 2. Характеристика кіберзлочинів, пов’язаних з контентом (змістом даних), розміщеним у	10	2	2	6

		комп'ютерних мережах (зокрема злочинів, пов'язаних з дитячою порнографією).				
13.		Тема 3. Характеристика кіберзлочинів, пов'язаних з порушенням авторського права і суміжних прав.	8	2	2	4
14.		Тема 4. Характеристика кіберзлочинів, зафіксованих в окремому протоколі (акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж).	8	2	2	4
15.		Тема 5. Кіберзлочинність у сфері економіки.	10	2	2	6
		Разом	*42*	*10*	*10*	*22*
		Усього годин / кредитів ECTS	**120/4,0**	**30**	**34**	**56**

5. Самостійна робота здобувачів вищої освіти

Самостійна робота здобувачів вищої освіти здійснюється у таких формах:

- підбір та аналітичне дослідження рекомендованої, нової навчальної та наукової літератури, тематичних законопроєктів, чинних актів законодавства України (релевантних змін до нього) та іноземних держав, статистичних даних, емпірики;

- підготовка до практичних занять;

- виконання практичних завдань; підготовка індивідуальних робіт (реферат, стаття, тези, есе й ін.);

- участь у конкурсах студентських наукових праць, турнірах;

- підготовка до всіх видів поточних контрольних випробувань (колоквіумів тощо);

- самотестування;

- підготовка до диференційованого заліку та ін.

Види індивідуальних робіт, вимоги до виконання та критерії їх оцінювання закріплені у Положенні про види та критерії оцінювання індивідуальних робіт здобувачів вищої освіти кафедри кримінально-правової політики.

6. Форми педагогічного контролю та засоби оцінювання результатів навчання

Оцінювання результатів засвоєння навчальної дисципліни «Запобігання кіберзлочинності» передбачає проведення поточного та підсумкового контролю і здійснюється на основі накопичувальної бально-рейтингової системи.

Поточний контроль знань включає:

- контроль якості засвоєння здобувачами вищої освіти програмного матеріалу навчальної дисципліни *на практичних заняттях* із застосуванням таких засобів: усне/письмове опитування, експрес-опитування; вирішення практичних завдань; участь у розробці кейсу; демонстрація презентації; захист есе, реферату тощо. У ході практичного заняття здобувач може отримати оцінку за чотирибальною шкалою (0, 1, 2, 3);

- контроль якості засвоєння здобувачами вищої освіти програмного матеріалу навчальної дисципліни, що проводиться наприкінці модулів у формі колоквіумів. Поточний контроль має на меті перевірку рівня підготовки здобувача у вивченні поточного матеріалу.

Впродовж семестру здобувачі вищої освіти виконують самостійну роботу, в тому числі, у формі підготовки *індивідуальної роботи*. Максимальна кількість балів за індивідуальну роботу – 10 балів.

Формою *підсумкового контролю* знань здобувачів вищої освіти з навчальної дисципліни *є диференційований залік*. Мінімальна оцінка результатів поточного контролю й індивідуальної роботи, за якої здобувач освіти може отримати залік, становить 60 балів.

7. Критерії оцінювання результатів навчання

Розподіл балів між формами організації освітнього процесу і видами контрольних заходів навчальної дисципліни «Запобігання кіберзлочинності» при підсумковому контролі у формі диференційованого заліку:

Поточний контроль						Індивідуальна робота здобувачів	Підсумкова оцінка знань (диференційований залік)
Модуль № 1		Модуль № 2		Модуль № 3			
п/з	колоквіум	п/з	колоквіум	п/з	колоквіум		
max 15	max 13	max 21	max 13	max 15	max 13	max 10	max 100

Критерії оцінювання (диференційований залік)

Вид контролю	**Кількість балів**	**Критерії (за кожною з оцінок)**
Поточний контроль на практичному занятті	Max 3	Відмінне засвоєння навчального матеріалу з теми, можливі окремі несуттєві недоліки.
	2	Добре засвоєння матеріалу з теми, але є окремі помилки.
	1	Задовільний рівень засвоєння матеріалу, значна кількість помилок.
	Min 0	Незадовільний рівень засвоєння матеріалу.
Колоквіум	Max 13	Відмінне засвоєння навчального матеріалу з тем, можливі окремі несуттєві недоліки.
	10	Результати опрацювання матеріалу високі, можлива незначна кількість несуттєвих помилок.
	7	Добре засвоєння матеріалу з тем, але є окремі помилки.
	4	Задовільний рівень засвоєння матеріалу, значна кількість помилок.
	1	Мінімальні результати, достатні для отримання позитивної оцінки.
	Min 0	Незадовільний рівень засвоєння матеріалу.

Оцінка індивідуальної роботи здобувачів вищої освіти: Реферат	Max 10	Питання плану реферату висвітлені повно. Проаналізовані представлені в навчальній та науковій літературі погляди щодо предмета дослідження; на основі їх порівняльної оцінки висловлене особисте ставлення автора до кожного з них, а також дана особиста оцінка запропонованим у літературі пропозиціям стосовно шляхів вирішення таких проблемних питань, які стосуються теми, та (або) висловлені власні пропозиції.

	7	Переважна більшість питань плану реферату висвітлена повно та точно. Одне з питань розкрито недостатньо повно або при його висвітленні допущена суттєва помилка. Проаналізовані основні літературні джерела, рекомендовані кафедрою при написанні роботи на відповідну тему.
	3	Питання плану теми висвітлені поверхово. При написанні реферату використана незначна кількість монографічних та нормативних джерел із числа рекомендованих кафедрою. При розкритті питань плану допущені грубі помилки.
	2	Робота оформлена з помилками та порушеннями кафедральних вимог щодо форми роботи. Робота містить методологічні та змістовні помилки, використано недостатню кількість джерел для обґрунтування дослідження та висновків. При захисті виникли труднощі щодо розкриття змісту теми, наведення аргументів стосовно окремих положень роботи та обґрунтованості і доведеності висновків.
	Min 0	Тема реферату не розкрита або в ній виявлено плагіат.
Стаття	10	Наукова стаття рецензується науковим керівником і зараховується публікація статті у фаховому науковому виданні.
Тези	5	Тези рецензуються науковим керівником і зараховується публікація тез доповіді на студентській науково-практичній конференції.
Есе	Max 5	Есе містить ключову ідею, що розкривається у змісті роботи на конкретних прикладах із судової практики, цитатах науковців з висловленням свого власного ставлення до досліджуваного питання.
	3	Есе фрагментарно розкриває ключову ідею, містить методологічні помилки, недостатнє обґрунтування досліджуваного питання.
	Min 0	Тема есе не розкрита або в ній виявлено плагіат.
Презентація	5	За допомогою програми Microsoft PowerPoint або за вибором здобувача вищої освіти іншого зручного програмного забезпечення підготовлено презентацію однієї з тем навчальної дисципліни, що вивчається. Подача матеріалу повинна бути динамічною, цікавою, ілюстративною, з використанням різних видів зображень. Презентація має містити не менше 10 слайдів та повністю розкривати питання.

Диференційований залік Зараховано	100	1. Всебічне, систематичне і глибоке знання матеріалу, передбаченого програмою навчальної дисципліни, у тому числі орієнтація в основних наукових доктринах і концепціях навчальної дисципліни. 2. Засвоєння основної та додаткової літератури, рекомендованої кафедрою. 3. Здатність до самостійного поповнення знань з навчальної дисципліни й використання отриманих знань у практичній роботі.
	90	1. Повне знання матеріалу, передбаченого програмою навчальної дисципліни. 2. Засвоєння основної літератури та знайомство з додатковою літературою, рекомендованою кафедрою. 3. Здатність до самостійного поповнення знань з дисципліни, розуміння їх значення для практичної роботи.
	85	1. Достатньо повне знання матеріалу, передбаченого програмою навчальної дисципліни, за відсутності у відповіді суттєвих помилок. 2. Засвоєння основної літератури, рекомендованої кафедрою. 3. Здатність до самостійного поповнення знань з дисципліни, розуміння їх значення для практичної роботи.
	75	1. Знання основного матеріалу, передбаченого програмою навчальної дисципліни, в обсязі, достатньому для подальшого навчання і майбутньої роботи за професією. 2. Засвоєння основної літератури, рекомендованої кафедрою. 3. Помилки й суттєві неузгодженості у відповіді на заліку за наявності знань для їх самостійного усунення або за допомогою викладача.
	70	1. Знання основного матеріалу, передбаченого програмою навчальної дисципліни, в обсязі, достатньому для подальшого навчання і майбутньої роботи за професією. 2. Ознайомлення з основною літературою, рекомендованою кафедрою. 3. Помилки у відповіді на заліку за наявності знань для усунення найсуттєвіших помилок за допомогою викладача.
	60	1. Прогалини в знаннях з певних частин основного матеріалу, передбаченого програмою навчальної дисципліни. 2. Наявність помилок у відповіді на питання на заліку.

Не зараховано	55	1. Відсутність знань значної частини основного матеріалу, передбаченого програмою навчальної дисципліни. 2. Неможливість продовжити навчання або здійснювати професійну діяльність без проходження повторного курсу з цієї дисципліни.

8. Педагогічний контроль для здобувачів вищої освіти

Шкала підсумкового педагогічного контролю (диференційований залік)

Оцінка за шкалою ECTS	Визначення	Оцінка за національною шкалою	Оцінка за 100-бальною шкалою, що використовується в НЮУ
A	**Відмінно** – відмінне виконання, лише з незначною кількістю помилок	зараховано	90 – 100
B	**Дуже добре** – вище середнього рівня з кількома помилками		80 – 89
C	**Добре** – у цілому правильна робота з певною кількістю незначних помилок		75 – 79
D	**Задовільно** – непогано, але зі значною кількістю недоліків		70 – 74
E	**Достатньо** – виконання задовольняє мінімальні критерії		60 – 69
FX	**Незадовільно** – потрібно попрацювати перед тим, як перескладати	не зараховано	35 – 59
F	**Незадовільно** – необхідна серйозна подальша робота, обов'язковий повторний курс		0 – 34

9. Навчально-методичне та інформаційне забезпечення навчальної дисципліни

Нормативно-правові акти

1. Конвенція про кіберзлочинність від 23.11.2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

2. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

3. Про Бюро економічної безпеки України : Закон України від 28.01.2021 р. № 1150-IX. URL: https://zakon.rada.gov.ua/laws/show/1150-20#Text

4. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII. URL:

https://zakon.rada.gov.ua/laws/show/2155-19#top

5. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України від 06.12.2019 р. № 361-IX. URL: https://zakon.rada.gov.ua/laws/show/361-20#Text

6. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

7. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

8. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

9. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text

10. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 р. № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text

11. Про організаційно-правові основи боротьби з організованою злочинністю : Закон України від 30.06.1993 р. № 3341-XII. URL: https://zakon.rada.gov.ua/laws/show/3341-12#Text

12. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

13. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

14. Стратегія кібербезпеки України. Безпечний кіберпростір – запорука успішного розвитку країни : затв. Указом Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

Література

Основна література

1. Богатирьов І. Г. Актуальні проблеми запобігання кіберзлочинності в Україні. *Економіка. Фінанси. Право*. 2022. № 10/1. С. 13–17.

2. Гавловський В. Д. Аналіз стану кіберзлочинності в Україні. *Інформація і право*. № 1(28)/2019. С. 108–117.

3. Захист прав, приватності та безпеки людини в інформаційну епоху : монографія / за заг. ред. В. Г. Пилипчука. Київ-Одеса : Фенікс, 2020. 260 с.

4. Тарасюк А. В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи : монографія. Київ; Одеса : Фенікс, 2020. 404 с.

5. V. Tsypko, K. I. Alieksieieva, I. A. Venger, O. V. Tavolzhanskyi, N. I. Galunets, A. V. Klyuchnik. Information policy of the enterprise as the basis for the reproduction of human potential in the structure of public social interaction. *Journal of Advanced Research in Law and Economics*. 2019. Vol. 10. Issue 6. P. 1664–1672.

6. Viacheslav V. Vapniarchuk, Iryna I. Puchkovska, Oleksii V. Tavolzhanskyi, Roman I. Tashian. Protection of ownership right in the court: the essence and particularities. *Asia life science*. Supplement 21(2), December 2019. Iss. 2. P. 863–879.

Додаткова література

1. O. E. Kostyuchenko, T. V. Kolesnik, Z. V. Bilous, O. V. Tavolzhanskyi. Robotization of manufacturing process: economic and social problems and legal ways of their solution. *Financial and credit activity: problems of theory and practice*. 2019. T. 3, № 30. P. 454–462.

2. Orlovskyi, Ruslan, Kharytonov, Sergiy, Samoshchenko, Igor, Us, Olha, Iemelianenko, Volodymyr. Countering Cybercrime Under Martial Law. *Journal of Cyber Security and Mobility*. 2023. T. 23, № 4. P. 626–241.

3. Ovcharenko, Mykola O., Tavolzhanskyi, Oleksii V., Radchenko, Tetiana M., Kulyk, Kateryna D., Smetanina, Nataliia V. Combating Illegal Drugs Trafficking Using

the Internet by Means of the Profiling Method. *Journal of Advanced Research in Law and Economics.* 2020. Vol. 11, n. 4. P. 1296–1304.

4. Гладка Н. М. Боротьба з кіберзлочинністю: напрями вдосконалення кримінального законодавства України. *Науковий вісник Ужгородського національного університету. Серія : Право*. 2020. Вип. 60. С. 139–142.

5. Кримінологія : підручник / за ред. Б. М. Головкіна. Харків : Право, 2020. 410 с.

6. Леонов Б. Д. Методичне забезпечення заходів з класифікації ідентифікації та фіксації кіберзлочинів. *Інформація і право*. 2021. № 1. С. 99–105.

7. Саєнко М. І. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Науковий вісник Ужгородського національного університету. Серія : Право*. 2021. Вип. 64. С. 386–391.

8. Таволжанський О. В. Інформаційна безпека України: стан правового забезпечення в контексті глобалізаційних процесів. *Журнал східноєвропейського права*. 2018. № 56. С. 90–105.

Інтернет-ресурси:

1. Офіційний веб-портал Верховної Ради України - https://www.rada.gov.ua/

2. Офіційний веб-портал Офісу Генерального прокурора - https://www.gp.gov.ua/

3. Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України - https://cip.gov.ua/ua

4. Офіційний веб-сайт Міністерства внутрішніх справ України - https://mvs.gov.ua/

5. Єдиний державний реєстр судових рішень - https://reyestr.court.gov.ua/

СЕНМК

Стандартизований електронний навчально-методичний комплекс кафедри кримінально-правової політики. URL:

https://library.nlu.edu.ua/senmk/itemlist/category/118-kafedra-kriminalnogo-prava-2.html

НЕІК

Навчальний електронний інформаційний комплекс «Запобігання кіберзлочинності». URL: https://neik.nlu.edu.ua/moodle/course/view.php?id=1250