МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Декан факультету комп'ютерних інформаційних технологій

Ігор ЯКИМЕНКО _____
"29" _____ 2025 р.

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи

Віктор ОСТРОВЕРХОВ _____
"29" _____ 2025 р.

# РОБОЧА ПРОГРАМА

з дисципліни

# "НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ"

Ступінь вищої освіти – бакалавр
Галузь знань – 12 Інформаційні технології
Спеціальність — 125 Кібербезпека та захист інформації
Освітньо-професійна програма – Кібербезпека

Кафедра кібербезпеки

| Форма навчання | Курс | Семестр | Лекції | Лабораторні | ІРС | Тренінг | СРС | Разом | Екзамен |
|---|---|---|---|---|---|---|---|---|---|
| Денна | 3 | 5 | 30 | 30 | 4 | 8 | 78 | 150 | 5 |

29.08.2025

Тернопіль: ЗУНУ, 2025

Робоча програма складена на основі освітньо-професійної програми підготовки бакалавра галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека та захист інформації, освітньо-професійної програми Кібербезпека, затвердженої Вченою радою ЗУНУ, протокол № 10 від 23.06.2023 р.

Робочу програму склав доцент кафедри теорії права та конституціоналізму, д.ю.н., доцент Андрій КОЛЕСНІКОВ

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 1 від 26.08 2025 р.

Завідувач кафедри Василь ЯЦКІВ

Гарант ОПП Михайло КАСЯНЧУК

# СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
## *“Нормативно-правове забезпечення кібербезпеки”*

## 1. Опис дисципліни
## “Нормативно-правове забезпечення кібербезпеки”

| Дисципліна “Нормативно-правове забезпечення кібербезпеки” | Галузь знань, спеціальність, ступінь вищої освіти | Характеристика навчальної дисципліни |
|---|---|---|
| Кількість кредитів ECTS – 5 | Галузь знань: 12 Інформаційні технології | Нормативна дисципліна циклу загальної підготовки, мова навчання українська |
| Кількість залікових модулів – 5 | Спеціальність 125 Кібербезпека та захист інформації | Рік підготовки: *денна – 3* Семестр: *денна – 5* |
| Кількість змістовних модулів – 2 | Ступінь вищої освіти – бакалавр | Лекції: *Денна – 30 год.* Практичні заняття: *Денна – 30 год.* |
| Загальна кількість годин – 150 | | Самостійна робота: *Денна – 78 год.* Тренінг: *Денна – 8 год.* |
| Тижневих годин: 10 год. з них аудиторних – 4 год. | | Вид підсумкового контролю – *екзамен* |

## 2. Мета й завдання дисципліни
## *“Нормативно-правове забезпечення кібербезпеки”*

### 2.1. Мета вивчення дисципліни

Метою викладання навчальної дисципліни “Нормативно-правове забезпечення кібербезпеки” є формування у студентів комплексного розуміння правових основ забезпечення кібербезпеки в Україні, оволодіння теоретичними знаннями щодо нормативно-правового регулювання кіберпростору та набуття практичних навичок застосування законодавства у сфері кібербезпеки, захисту критичної інформаційної інфраструктури та протидії кіберзлочинності.

### 2.2. Завдання вивчення дисципліни

Одним з основних завдань курсу є формування у студентів спеціальності "Кібербезпека та захист інформації" навичок застосування нормативно-правових актів для забезпечення кібербезпеки та протидії кіберзлочинності.

Теоретична та практична підготовка фахівців з питань кібербезпеки здійснюється згідно наступних питань:

– система правового регулювання кібербезпеки в Україні;

– правове регулювання критичної інформаційної інфраструктури;

– кіберзлочинність: кримінально-правові аспекти;
– процесуальні аспекти розслідування кіберзлочинів;
– правове регулювання захисту персональних даних у кіберпросторі;
– правові засади електронного урядування та цифровізації;
– секторальне регулювання кібербезпеки;
– правове забезпечення кібероборони;
– правове регулювання кіберстрахування;
– правові аспекти реагування на кіберінциденти;
– правове регулювання аудиту та сертифікації в сфері кібербезпеки;
– правові засади кібергігієни та кіберосвіти;
– актуальні проблеми та перспективи розвитку законодавства про кібербезпеку;
– міжнародне право кібербезпеки.

**2.3. Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни**

КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

**2.4. Передумови для вивчення дисципліни**

Успішне засвоєння студентами матеріалу навчального курсу передбачає наявності знань з політології, української мови за професійним спрямуванням, основ кібербезпеки.

**2.5. Результати навчання**

ПРН7. Діяти на основі законодавчої та нормативно правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

ПРН8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

ПРН16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно правових документів.

ПРН27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно телекомунікаційних (автоматизованих) системах.

ПРН36. Виявляти небезпечні сигнали технічних засобів.

ПРН37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

## 3. Програма навчальної дисципліни
## *“Нормативно-правове забезпечення кібербезпеки”*

### Змістовний модуль 1. Основи правового регулювання кібербезпеки та протидія кіберзлочинності

### ТЕМА 1. СИСТЕМА ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Ієрархія нормативно-правових актів у сфері кібербезпеки. Конституційні засади забезпечення кібербезпеки. Закон України "Про основні засади забезпечення кібербезпеки України". Стратегія кібербезпеки України: цілі, завдання, принципи. Роль і повноваження суб'єктів забезпечення кібербезпеки.

### ТЕМА 2. ПРАВОВЕ РЕГУЛЮВАННЯ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Поняття та критерії віднесення об'єктів до критичної інформаційної інфраструктури. Процедура категоризації об'єктів критичної інформаційної інфраструктури. Вимоги до захисту критичної інформаційної інфраструктури. Обов'язки суб'єктів господарювання-власників об'єктів КІІ. Державний нагляд у сфері захисту критичної інформаційної інфраструктури.

### ТЕМА 3. КІБЕРЗЛОЧИННІСТЬ: КРИМІНАЛЬНО-ПРАВОВІ АСПЕКТИ

Система кіберзлочинів у Кримінальному кодексі України. Злочини у сфері комп'ютерної інформації (Розділ XVI КК України). Кваліфікуючі ознаки кіберзлочинів. Особливості призначення покарання за кіберзлочини. Звільнення від кримінальної відповідальності у сфері кібербезпеки. Міжнародне співробітництво у боротьбі з кіберзлочинністю.

### ТЕМА 4. ПРОЦЕСУАЛЬНІ АСПЕКТИ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Особливості досудового розслідування кіберзлочинів. Слідчі дії при розслідуванні кіберзлочинів. Процесуальні гарантії при проведенні негласних слідчих дій. Тимчасовий доступ до електронної інформації. Міжнародна правова допомога у кримінальних справах про кіберзлочини.

**ТЕМА 5. ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У КІБЕРПРОСТОРІ**

Закон України "Про захист персональних даних": основні положення. Права суб'єктів персональних даних у цифровому середовищі. Обов'язки володільців персональних даних. Трансферт персональних даних до третіх країн. Відповідальність за порушення законодавства про захист персональних даних. GDPR та його вплив на українське законодавство.

**ТЕМА 6. ПРАВОВІ ЗАСАДИ ЕЛЕКТРОННОГО УРЯДУВАННЯ ТА ЦИФРОВІЗАЦІЇ**

Концепція розвитку електронного урядування в Україні. Правове регулювання електронного документообігу. Електронні довірчі послуги: правовий статус та вимоги. Кваліфіковані електронні підписи та печатки. Правові аспекти функціонування державних електронних реєстрів. Кібербезпека в системі електронного урядування.

**ТЕМА 7. СЕКТОРАЛЬНЕ РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ**

Кібербезпека у банківській сфері: вимоги НБУ. Регулювання кібербезпеки у сфері телекомунікацій. Кібербезпека в енергетичному секторі. Правові вимоги до кібербезпеки у сфері охорони здоров'я. Регулювання кібербезпеки в транспортній галузі. Особливості забезпечення кібербезпеки у сфері освіти.

**Змістовний модуль 2. Спеціальні режими правового регулювання та перспективи розвитку законодавства про кібербезпеку**

**ТЕМА 8. ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРОБОРОНИ**

Поняття кібероборони та її правові засади. Повноваження сил оборони у кіберпросторі. Правовий режим воєнного стану та кібербезпека. Міжнародне гуманітарне право у кіберпросторі. Співробітництво з НАТО та ЄС у сфері кібероборони. Правові аспекти кібероперацій та активної кіберзахисту. Цивільно-військове співробітництво у сфері кібербезпеки.

**ТЕМА 9. ПРАВОВЕ РЕГУЛЮВАННЯ КІБЕРСТРАХУВАННЯ**

Поняття та види кіберстрахування. Правові основи функціонування ринку кіберстрахування в Україні. Типові умови договорів кіберстрахування. Страхові випадки та виключення з покриття. Врегулювання збитків від кіберінцидентів. Роль кіберстрахування у забезпеченні кібербезпеки.

**ТЕМА 10. ПРАВОВІ АСПЕКТИ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ**

Система реагування на кіберінциденти в Україні. Обов'язки щодо повідомлення про кіберінциденти. Координація дій при ліквідації наслідків кіберінцидентів. Правові засади діяльності CERT-UA. Міжнародна координація при реагуванні на кіберінциденти. Документування кіберінцидентів для правових цілей.

**ТЕМА 11. ПРАВОВЕ РЕГУЛЮВАННЯ АУДИТУ ТА СЕРТИФІКАЦІЇ В СФЕРІ КІБЕРБЕЗПЕКИ**

Система технічного регулювання у сфері кібербезпеки. Обов'язкова та добровільна сертифікація засобів кібербезпеки. Акредитація органів з оцінки відповідності. Аудит інформаційної безпеки: правові засади. Міжнародні стандарти кібербезпеки та їх статус в Україні. Визнання зарубіжних сертифікатів відповідності.

**ТЕМА 12. ПРАВОВІ ЗАСАДИ КІБЕРГІГІЄНИ ТА КІБЕРОСВІТИ**

Концепція кібергігієни: правові та етичні аспекти. Правове забезпечення кіберосвіти та підвищення кіберграмотності. Відповідальність освітніх закладів за кібербезпеку. Регулювання дитячої безпеки в Інтернеті. Права та обов'язки провайдерів Інтернет-послуг щодо безпеки користувачів. Саморегулювання в IT-індустрії.

**ТЕМА 13. АКТУАЛЬНІ ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ЗАКОНОДАВСТВА ПРО КІБЕРБЕЗПЕКУ**

Виклики регулювання штучного інтелекту та машинного навчання. Правові аспекти квантових технологій та постквантової криптографії. Регулювання блокчейн-технологій та криптовалют з позицій кібербезпеки. IoT та промислові системи управління: правові виклики. Кібербезпека в умовах гібридних загроз. Перспективи гармонізації українського та європейського законодавства.

**ТЕМА 14. МІЖНАРОДНЕ ПРАВО КІБЕРБЕЗПЕКИ**

Міжнародні угоди та конвенції у сфері кібербезпеки. Будапештська конвенція про кіберзлочинність: положення та імплементація. Європейська нормативна база кібербезпеки (NIS Directive, Cybersecurity Act). Міжнародне співробітництво у сфері кібербезпеки. Дипломатичні аспекти кіберконфліктів.

## 4. Структура залікового кредиту дисципліни
## *“Нормативно-правове забезпечення кібербезпеки”*

денна форма навчання

| | Кількість годин | | | | | |
|---|---|---|---|---|---|---|
| | Лекції | Практичні заняття | Самостійна робота | Індивідуальна робота | Тренінг | Контрольні заходи |
| Змістовий модуль 1. Основи правового регулювання кібербезпеки та протидія кіберзлочинності | | | | | | |
| Тема 1. Система правового регулювання кібербезпеки в | 4 | 2 | 6 | 2 | 4 | Опитування, тести, |

| | | | | | | |
|---|---|---|---|---|---|---|
| Україні | | | | | | завдання |
| Тема 2. Правове регулювання критичної інформаційної інфраструктури | 2 | 2 | 6 | | | Опитування, тести, завдання |
| Тема 3. Кіберзлочинність: кримінально-правові аспекти | 2 | 2 | 6 | | | Опитування, тести, завдання |
| Тема 4. Процесуальні аспекти розслідування кіберзлочинів | 2 | 2 | 6 | | | Опитування, тести, завдання |
| Тема 5. Правове регулювання захисту персональних даних у кіберпросторі | 2 | 2 | 6 | | | Опитування, тести, завдання |
| Тема 6. Правові засади електронного урядування та цифровізації | 2 | 2 | 6 | | | Опитування, тести, завдання |
| Тема 7. Секторальне регулювання кібербезпеки | 2 | 4 | 6 | | | Опитування, тести, завдання |
| Змістовний модуль 2. Спеціальні режими правового регулювання та перспективи розвитку законодавства про кібербезпеку | | | | | | |
| Тема 8. Правове забезпечення кібероборони | 2 | 2 | 6 | | | Опитування, тести, завдання |
| Тема 9. Правове регулювання кіберстрахування | 2 | 2 | 5 | | | Опитування, тести, завдання |
| Тема 10. Правові аспекти реагування на кіберінциденти | 2 | 2 | 5 | | | Опитування, тести, завдання |
| Тема 11. Правове регулювання аудиту та сертифікації в сфері кібербезпеки | 2 | 2 | 5 | 2 | 4 | Опитування, тести, завдання |
| Тема 12. Правові засади кібергігієни та кіберосвіти | 2 | 2 | 5 | | | Опитування, тести, завдання |
| Тема 13. Актуальні проблеми та перспективи розвитку законодавства про кібербезпеку | 2 | 2 | 5 | | | Опитування, тести, завдання |
| Тема 14. Міжнародне право кібербезпеки | 2 | 2 | 5 | | | Опитування, тести, завдання |
| Разом | 30 | 30 | 78 | 4 | 8 | |

## 5. Тематика лабораторних робіт

***“Нормативно-правове забезпечення кібербезпеки”***

**Змістовний модуль 1. Основи правового регулювання кібербезпеки та протидія кіберзлочинності**

**ЛАБОРАТОРНА РОБОТА 1. СИСТЕМА ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ**

*Мета: проаналізувати ієрархію та взаємозв'язок нормативно-правових актів у сфері кібербезпеки, дослідити повноваження суб'єктів забезпечення кібербезпеки*

**Завдання для лабораторної роботи:**

Завдання 1. Робота з нормативно-правовими актами Проаналізувати статтю 1 Закону України "Про основні засади забезпечення кібербезпеки України":

- виписати та пояснити 10 основних термінів і понять з даної статті;
- порівняти визначення терміну "кібербезпека" у цьому Законі та пріоритетів забезпечення кібербезпеки України у Стратегії кібербезпеки України 2021 року;
- знайти аналогічні терміни у законодавстві ЄС (NIS2 Directive) та порівняти їх визначення з українськими;

Завдання 2. Дослідницький кейс. У 2023 році відбулася кібератака на енергетичну компанію, яка призвела до відключення електроенергії у декількох районах міста на 6 годин.

- визначити, які суб'єкти забезпечення кібербезпеки мають реагувати на цю ситуацію згідно з чинним законодавством;
- описати повноваження кожного з цих суб'єктів у даній ситуації;
- встановити, які документи повинні бути складені та куди направлені;

Завдання 3. Практичне завдання. Використовуючи відкриті джерела (офіційні сайти державних органів):

- знайти та проаналізувати структуру Державної служби спеціального зв'язку та захисту інформації України;
- скласти схему підпорядкування органів у сфері кібербезпеки в Україні;
- визначити контактну інформацію регіонального підрозділу, який відповідає за кібербезпеку у вашому регіоні;

## ЛАБОРАТОРНА РОБОТА 2. ПРАВОВЕ РЕГУЛЮВАННЯ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

*Мета: засвоїти процедури категоризації об'єктів КІІ, вимоги до їх захисту та особливості державного нагляду*

**Завдання для лабораторної роботи:**

Завдання 1. Робота з нормативно-правовими актами. Проаналізувати Постанову КМУ № 943 від 09.10.2020:

- виписати всі критерії, за якими об'єкт може бути віднесений до КІІ (пункти 3-4 Порядку);
- дослідити процедуру подання заяви про віднесення об'єкта до КІІ: які документи потрібні, строки розгляду, підстави для відмови;
- порівняти українські критерії КІІ з аналогічними критеріями у NIS2 Directive ЄС, виявити спільні та відмінні риси;

Завдання 2. Дослідницький кейс. Приватний банк має власний дата-центр, який обслуговує 500 тисяч клієнтів та здійснює близько 2 млн транзакцій на день. У банку працює онлайн-банкінг, мобільний застосунок та система платіжних карток. Відключення системи на понад 2 години може призвести до значних фінансових збитків.

- визначити, чи підпадає цей об'єкт під критерії КІІ згідно з українським законодавством;

- якщо так, то до якої категорії він має бути віднесений та які вимоги до нього застосовуватимуться;
- описати процедуру, яку має пройти банк для офіційного визнання його об'єктом КІІ;

Завдання 3. Практичне завдання. Використовуючи відкриті дані:

- знайти інформацію про ведення реєстру об'єктів КІІ України;
- проаналізувати структуру розподілу об'єктів КІІ за галузями в Україні;
- знайти та вивчити публічну інформацію про один конкретний випадок віднесення об'єкта до КІІ (з ЗМІ або офіційних повідомлень);

**ЛАБОРАТОРНА РОБОТА 3. КІБЕРЗЛОЧИННІСТЬ: КРИМІНАЛЬНО-ПРАВОВІ АСПЕКТИ**

*Мета: навчитися кваліфікувати кіберзлочини, визначати санкції та аналізувати особливості призначення покарань*

**Завдання для лабораторної роботи:**

Завдання 1. Робота з нормативно-правовими актами. Проаналізувати статті 361, 361¹, 361², 362, 363, 363¹ КК України:

- скласти таблицю складів кіберзлочинів з вказанням об'єкта та санкцій за кожну статтю;
- дослідити кваліфікуючі ознаки у частинах 2-4 статей 361 та 362 КК України, пояснити їх зміст;
- порівняти санкції за різні види кіберзлочинів у межах українського КК (наприклад, ст. 361 vs ст. 362);

Завдання 2. Дослідницький кейс. 19-річний студент створив шкідливу програму-вірус та поширив її через соціальні мережі. Вірус заблокував роботу комп'ютерів у 15 малих підприємствах, вимагаючи викуп у розмірі 200 доларів за розблокування. Загальна сума збитків склала 50 тисяч гривень. Студент зізнався у скоєному та повністю відшкодував збитки.

- визначити, які обставини можуть пом'якшити або обтяжити покарання;
- проаналізувати можливість застосування звільнення від кримінальної відповідальності;
- вказати орієнтовний розмір покарання з урахуванням усіх обставин;

Завдання 3. Практичне завдання. Використовуючи Єдиний державний реєстр судових рішень (reyestr.court.gov.ua):

- знайти 3 реальні судові рішення за статтями 361-363 КК України за останні 2 роки;
- проаналізувати фактичні обставини справ та призначені покарання;
- порівняти суворість покарань та виявити тенденції в судовій практиці щодо кіберзлочинів;

**ЛАБОРАТОРНА РОБОТА 4. ПРОЦЕСУАЛЬНІ АСПЕКТИ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ**

*Мета: вивчити особливості проведення слідчих дій при розслідуванні кіберзлочинів та процесуальні гарантії*

**Завдання для лабораторної роботи:**

Завдання 1. Робота з нормативно-правовими актами. Проаналізувати статті 264-1 "Тимчасовий доступ до речей і документів" та 290-294 КПК України (обшук):

- виписати процесуальні вимоги до проведення тимчасового доступу до електронної інформації (підстави, порядок, строки);
- дослідити особливості обшуку при розслідуванні кіберзлочинів: що можна вилучати, як забезпечити збереження цифрових доказів;
- порівняти процедуру отримання тимчасового доступу до речей і документів та до електронних носіїв інформації - в чому відмінності;

Завдання 2. Дослідницький кейс. Під час розслідування справи про шахрайство в інтернеті слідчий отримав інформацію, що підозрюваний зберігає докази злочину на своєму домашньому комп'ютері та в хмарному сховищі Google Drive. Також є підстави вважати, що він видаляє сліди своєї діяльності.

- описати процедуру отримання судового дозволу на кожну з цих дій;
- проаналізувати, як забезпечити збереження доказів, якщо є ризик їх знищення;
- вказати процесуальні гарантії прав підозрюваного під час цих слідчих дій;

Завдання 3. Практичне завдання. Використовуючи відкриті джерела та судову практику:

- знайти в реєстрі судових рішень ухвалу суду про дозвіл на обшук у справі про кіберзлочин;
- проаналізувати, які обґрунтування наводив слідчий для отримання дозволу;
- знайти інформацію про технічні засоби, які використовуються правоохоронними органами України для вилучення цифрових доказів (з офіційних джерел МВС, СБУ);

## ЛАБОРАТОРНА РОБОТА 5. ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У КІБЕРПРОСТОРІ

*Мета: засвоїти права суб'єктів персональних даних, обов'язки володільців та особливості трансферту даних*

**Завдання для лабораторної роботи:**

Завдання 1. Робота з нормативно-правовими актами. Проаналізувати статті 8, 14, 15 Закону України "Про захист персональних даних":

- виписати всі права суб'єкта персональних даних, передбачені статтею 8, та пояснити зміст кожного права;
- дослідити обов'язки володільця персональних даних згідно зі статтями 14-15, систематизувати їх за етапами обробки даних;
- порівняти українські права суб'єктів персональних даних з правами, передбаченими статтями 15-22 GDPR - які додаткові права має суб'єкт даних за європейським регулюванням;

Завдання 2. Дослідницький кейс. Інтернет-магазин одягу збирає персональні дані покупців: ПІБ, номер телефону, електронну пошту, адресу доставки. Також сайт використовує cookies для відстеження поведінки користувачів та показує їм персоналізовану рекламу. Дані зберігаються на серверах у США. Один з клієнтів звернувся з вимогою видалити всі його персональні дані.

- визначити, які вимоги законодавства України має дотримувати інтернет-магазин;
- проаналізувати правомірність передачі персональних даних до США;
- описати процедуру, яку має виконати магазин у відповідь на вимогу клієнта про видалення даних;

- вказати відповідальність за можливі порушення законодавства про захист персональних даних;

Завдання 3. Практичне завдання. Використовуючи реальні веб-сайти українських компаній:

- знайти та проаналізувати політики конфіденційності 3-х різних українських інтернет-магазинів або сервісів;
- перевірити їх відповідність вимогам Закону України "Про захист персональних даних";
- знайти на сайті Уповноваженого ВРУ з прав людини інформацію про розгляд скарг щодо порушень у сфері захисту персональних даних;

**ЛАБОРАТОРНА РОБОТА 6. ПРАВОВІ ЗАСАДИ ЕЛЕКТРОННОГО УРЯДУВАННЯ ТА ЦИФРОВІЗАЦІЇ**

*Мета: вивчити правове регулювання електронного документообігу та електронних довірчих послуг*

**Завдання для лабораторної роботи:**

Завдання 1. Робота з нормативно-правовими актами. Проаналізувати статті 1, 6, 7 Закону України "Про електронні довірчі послуги":

- виписати та пояснити основні терміни з статті 1: кваліфікований електронний підпис, кваліфікований сертифікат, довірча особа;
- дослідити вимоги до надавачів кваліфікованих електронних довірчих послуг згідно зі статтею 6;
- порівняти вимоги до простого, удосконаленого та кваліфікованого електронного підпису за статтею 7 - скласти порівняльну таблицю;

Завдання 2. Дослідницький кейс. Державна установа планує перейти на повністю електронний документообіг. Всі службові документи, накази, листування з іншими органами мають бути в електронній формі з електронними підписами. Установа також планує надавати електронні послуги громадянам через власний портал.

- визначити, які типи електронних підписів має використовувати установа для різних видів документів;
- описати процедуру отримання кваліфікованих сертифікатів для співробітників установи;
- проаналізувати вимоги до системи електронного документообігу з точки зору кібербезпеки;
- вказати, які додаткові зобов'язання виникають у установи при наданні електронних послуг громадянам;

Завдання 3. Практичне завдання. Використовуючи офіційні електронні ресурси:

- зайти на портал "Дія" (diia.gov.ua) та проаналізувати, які електронні послуги надаються громадянам;
- вивчити процедуру отримання електронного підпису громадянином через "Дію" або ЦСК "Україна";
- знайти на сайті Мінцифри перелік акредитованих надавачів електронних довірчих послуг в Україні та порівняти їх послуги;

**ЛАБОРАТОРНА РОБОТА 7. СЕКТОРАЛЬНЕ РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ**

*Мета: дослідити особливості правового регулювання кібербезпеки у різних галузях економіки*

**Завдання для лабораторної роботи:**

Завдання 1. Робота з нормативно-правовими актами. Проаналізувати Постанову НБУ № 95 від 28.09.2017 (розділи 2-4):

- виписати основні вимоги до організації інформаційної безпеки у банках згідно з розділом 2;
- дослідити вимоги до управління доступом та аутентифікації в банківських системах (розділ 3);
- порівняти вимоги НБУ до банків з загальними вимогами Закону "Про основні засади забезпечення кібербезпеки України" - виявити специфічні банківські вимоги;

Завдання 2. Дослідницький кейс. Регіональний енергетичний оператор, який забезпечує електроенергією 200 тисяч споживачів, планує модернізацію своєї IT-інфраструктури. Планується впровадження smart-мережі з інтелектуальними лічильниками, системи дистанційного управління підстанціями та мобільного додатка для споживачів.

- визначити, які нормативні вимоги до кібербезпеки має дотримуватись оператор;
- проаналізувати, чи підпадає цей об'єкт під критерії критичної інформаційної інфраструктури;
- описати основні кіберризики smart-мережі та правові вимоги до їх мінімізації;
- вказати, які органи здійснюють нагляд за кібербезпекою в енергетичному секторі;

Завдання 3. Практичне завдання. Використовуючи офіційні сайти регуляторів:

- знайти на сайті НБУ актуальні рекомендації або вимоги щодо кібербезпеки для банків ;
- вивчити на сайті НКРЗІ інформацію про вимоги до кібербезпеки телекомунікаційних операторів;
- проаналізувати структуру та повноваження НКРЕКП (енергетичний регулятор) у сфері кібербезпеки енергетики;

**Змістовний модуль 2. Спеціальні режими правового регулювання та перспективи розвитку законодавства про кібербезпеку**

**ЛАБОРАТОРНА РОБОТА 8. ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРОБОРОНИ**

*Мета: вивчити правові засади кібероборони та особливості правового режиму воєнного стану у кіберпросторі*

**Завдання для лабораторної роботи:**

Завдання 1. Робота з нормативно-правовими актами. Проаналізувати Доктрину інформаційної безпеки України (розділи 4-5):

- виписати основні загрози у кіберпросторі, визначені Доктриною, та класифікувати їх за сферами впливу;

- дослідити повноваження сил безпеки і оборони у кіберпросторі згідно з розділом 5;
- порівняти цілі державної політики у сфері кібербезпеки до 2022 року з реальними викликами воєнного стану - які пріоритети змінились;

Завдання 2. Дослідницький кейс. Під час активних бойових дій противник здійснив масштабну кібератаку на енергетичну інфраструктуру, що призвело до відключення електроенергії у декількох областях. Одночасно зафіксовано DDoS-атаки на державні сайти та поширення дезінформації через соціальні мережі.

- визначити, які органи мають реагувати на цю ситуацію відповідно до законодавства про воєнний стан;
- проаналізувати правові можливості обмеження доступу до інтернет-ресурсів в умовах воєнного стану;

Завдання 3. Практичне завдання. Використовуючи відкриті джерела та офіційні повідомлення:

- знайти та проаналізувати публічні заяви РНБО або Генштабу ЗСУ щодо кібероборони з початку 2022 року;
- вивчити діяльність IT Army of Ukraine як прикладу цивільно-військового співробітництва у кіберпросторі;
- дослідити інформацію про міжнародну підтримку України у сфері кібероборони (через сайти партнерів);

## ЛАБОРАТОРНА РОБОТА 9. ПРАВОВЕ РЕГУЛЮВАННЯ КІБЕРСТРАХУВАННЯ

*Мета: вивчити правові основи кіберстрахування та особливості договірних відносин*

**Завдання для лабораторної роботи:**

Завдання 1. Робота з нормативно-правовими актами. Проаналізувати статті 979-987 Цивільного кодексу України (страхування відповідальності):

- виписати основні принципи страхування відповідальності, які можуть застосовуватись до кіберстрахування;
- дослідити поняття "страховий випадок" та "страхове відшкодування" в контексті можливих кіберінцидентів;
- порівняти обов'язкове та добровільне страхування за ЗУ "Про страхування" - визначити, до якого виду належить кіберстрахування;

Завдання 2. Дослідницький кейс. IT-компанія з розробки мобільних додатків уклала договір кіберстрахування. Через вразливість у їх додатку хакери отримали доступ до персональних даних 50 тисяч користувачів. Компанії довелося сплатити штрафи регуляторам, компенсації потерпілим та витрати на відновлення репутації загальною сумою 2 млн грн.

- визначити, які види збитків може покривати кіберстрахування згідно з українським законодавством;
- проаналізувати можливі виключення зі страхового покриття у такій ситуації;
- описати процедуру врегулювання страхового випадку: документи, строки, обов'язки сторін;
- вказати особливості доказування причинно-наслідкового зв'язку при кіберінцидентах;

Завдання 3. Практичне завдання. Використовуючи відкриті джерела та сайти страхових компаній:

- знайти пропозиції українських страхових компаній з кіберстрахування (мінімум 3 компанії);
- порівняти умови покриття, страхові суми та виключення у різних страховиків;
- дослідити статистику Нацкомфінпослуг щодо розвитку ринку кіберстрахування в Україні;

**ЛАБОРАТОРНА РОБОТА 10. ПРАВОВІ АСПЕКТИ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ**

*Мета: засвоїти процедури реагування на кіберінциденти та обов'язки щодо повідомлення*

**Завдання для лабораторної роботи:**

Завдання 1. Робота з нормативно-правовими актами. Проаналізувати статтю 1 Закону України "Про основні засади забезпечення кібербезпеки України":

- виписати та пояснити 10 основних термінів і понять з даної статті;
- класифікувати ці терміни за категоріями (наприклад: суб'єкти, об'єкти, процеси, загрози);
- проаналізувати, які з цих термінів є найбільш важливими для розуміння системи кібербезпеки України та обґрунтувати свою думку;

Завдання 2. Дослідницький кейс. У 2023 році відбулася кібератака на енергетичну компанію, яка призвела до відключення електроенергії у декількох районах міста на 6 годин.

- визначити, які суб'єкти забезпечення кібербезпеки мають реагувати на цю ситуацію згідно з чинним законодавством;
- описати повноваження кожного з цих суб'єктів у даній ситуації;
- встановити, які документи повинні бути складені та куди направлені;

Завдання 3. Практичне завдання. Використовуючи відкриті джерела (офіційні сайти державних органів):

- знайти та проаналізувати структуру Державної служби спеціального зв'язку та захисту інформації України;
- скласти схему підпорядкування органів у сфері кібербезпеки в Україні;
- визначити контактну інформацію регіонального підрозділу, який відповідає за кібербезпеку у вашому регіоні;

**ЛАБОРАТОРНА РОБОТА 11. ПРАВОВЕ РЕГУЛЮВАННЯ АУДИТУ ТА СЕРТИФІКАЦІЇ В СФЕРІ КІБЕРБЕЗПЕКИ**

*Мета: вивчити систему технічного регулювання, сертифікації та аудиту у сфері кібербезпеки*

**Завдання для лабораторної роботи:**

Завдання 1. Робота з нормативно-правовими актами. Проаналізувати Закон України "Про технічні регламенти та оцінку відповідності" (статті 1, 6-8):

- виписати та пояснити основні поняття з статті 1: технічний регламент, оцінка відповідності, сертифікація, акредитація;
- дослідити принципи технічного регулювання згідно зі статтею 6 та їх застосування у сфері кібербезпеки;

- порівняти обов'язкову та добровільну оцінку відповідності за статтями 7-8 - визначити переваги та недоліки кожного виду для засобів кібербезпеки;

Завдання 2. Дослідницький кейс. ІТ-компанія розробила новий програмний засіб захисту від шкідливого ПЗ для корпоративних мереж. Компанія планує продавати цей продукт державним установам та об'єктам критичної інфраструктури. Також планується експорт до країн ЄС.

- визначити, чи підлягає цей засіб обов'язковій сертифікації в Україні;
- описати процедуру отримання сертифіката відповідності для цього продукту;
- проаналізувати додаткові вимоги для продажу державним установам;
- вказати можливості взаємного визнання українських сертифікатів у ЄС;

Завдання 3. Практичне завдання. Використовуючи офіційні реєстри та бази даних:

- знайти в реєстрі сертифікатів відповідності ДП "УкрНДНЦ" приклади сертифікованих засобів ТЗІ;
- проаналізувати структуру ринку акредитованих органів з оцінки відповідності у сфері кібербезпеки;
- вивчити на сайті Національного агентства з акредитації України (NAAU) процедуру акредитації лабораторій для випробувань засобів ТЗІ;

## ЛАБОРАТОРНА РОБОТА 12. ПРАВОВІ ЗАСАДИ КІБЕРГІГІЄНИ ТА КІБЕРОСВІТИ

*Мета: дослідити правове забезпечення кіберосвіти та регулювання безпеки дітей в Інтернеті*

**Завдання для лабораторної роботи:**

Завдання 1. Робота з нормативно-правовими актами. Проаналізувати Концепцію розвитку цифрових компетентностей (розділи 2-3):

- виписати ключові цифрові компетентності, визначені в Концепції, та їх зв'язок з кібербезпекою;
- дослідити заходи з розвитку цифрової грамотності населення згідно з розділом 3;
- порівняти завдання для загальної та професійної освіти у сфері цифрових компетентностей - виявити специфіку кожного рівня;

Завдання 2. Дослідницький кейс. У школі планується запровадження програми з основ кібербезпеки для учнів 8-11 класів. Програма включатиме навчання безпечної поведінки в Інтернеті, захист персональних даних, розпізнавання фішингу та соціальної інженерії. Також планується створення шкільної мережі Wi-Fi з доступом для учнів.

- визначити правові вимоги до змісту освітньої програми з кібербезпеки;
- проаналізувати обов'язки школи щодо захисту персональних даних учнів при використанні цифрових технологій;
- описати вимоги до забезпечення безпеки дітей при користуванні шкільною мережею;

Завдання 3. Практичне завдання. Використовуючи офіційні освітні ресурси:

- вивчити ресурси Національної онлайн-платформи з цифрової грамотності "Дія.Цифрова освіта" щодо кібербезпеки;

- дослідити діяльність громадських організацій України, які займаються цифровою грамотністю та кіберосвітою (через їх офіційні сайти);

**ЛАБОРАТОРНА РОБОТА 13. АКТУАЛЬНІ ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ЗАКОНОДАВСТВА ПРО КІБЕРБЕЗПЕКУ**

*Мета: проаналізувати виклики регулювання нових технологій та перспективи розвитку законодавства*

**Завдання для лабораторної роботи:**

Завдання 1. Робота з нормативно-правовими актами. Проаналізувати Закон України "Про віртуальні активи" (статті 1, 15-16):

- виписати основні поняття з статті 1, пов'язані з кібербезпекою: віртуальний актив, постачальник послуг віртуальних активів, криптографічний ключ;
- дослідити вимоги до забезпечення кібербезпеки постачальниками послуг віртуальних активів згідно зі статтями 15-16;
- проаналізувати, які нові виклики для кібербезпеки створюють віртуальні активи;

Завдання 2. Дослідницький кейс. Українська IT-компанія розробляє систему штучного інтелекту для медичної діагностики, яка буде використовуватись у лікарнях для аналізу медичних зображень. Система збирає та обробляє персональні дані пацієнтів, використовує машинне навчання та може приймати рішення, що впливають на лікування.

- визначити, які правові виклики виникають при регулюванні такої AI-системи в контексті кібербезпеки;
- проаналізувати застосування вимог GDPR та українського законодавства про захист персональних даних до AI;
- вказати необхідність адаптації українського законодавства до вимог AI Act ЄС;

Завдання 3. Практичне завдання. Використовуючи офіційні джерела та аналітичні матеріали:

- знайти інформацію про законопроекти щодо регулювання штучного інтелекту в Україні;
- проаналізувати звіти міжнародних організацій (НАТО, ЄС, ООН) щодо перспектив розвитку законодавства про кібербезпеку;

**ЛАБОРАТОРНА РОБОТА 14. МІЖНАРОДНЕ ПРАВО КІБЕРБЕЗПЕКИ**

*Мета: вивчити міжнародні угоди у сфері кібербезпеки та особливості їх імплементації*

**Рекомендовані для опрацювання нормативно-правові акти:**

- Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція) від 23.11.2001
- Закон України "Про ратифікацію Конвенції про кіберзлочинність" від 07.09.2005 № 2824-IV
- Регламент ЄС 2019/881 про кіберсертифікацію (Cybersecurity Act)
- Угода про асоціацію між Україною та ЄС

**Завдання для лабораторної роботи:**

Завдання 1. Робота з нормативно-правовими актами. Проаналізувати Будапештську конвенцію про кіберзлочинність (статті 2-6, 23-25):

- виписати склади кіберзлочинів, визначені у статтях 2-6 Конвенції, та порівняти їх з відповідними статтями КК України;
- дослідити принципи міжнародного співробітництва у кримінальних справах згідно зі статтями 23-25;
- проаналізувати, які зобов'язання взяла на себе Україна при ратифікації Конвенції та ступінь їх виконання;

Завдання 2. Дослідницький кейс. Громадянин України, перебуваючи в Польщі, здійснив кібератаку на сервери французької компанії, використовуючи ботнет, що включав комп'ютери у США та Німеччині. Збитки склали 2 млн євро. Підозрюваний затриманий у Варшаві за запитом французької прокуратури.

- визначити юрисдикцію для розслідування цього кіберзлочину згідно з міжнародним правом;
- проаналізувати процедуру видачі підозрюваного відповідно до Будапештської конвенції;
- описати механізми міжнародного співробітництва у збиранні цифрових доказів у різних країнах;
- вказати роль України у цій справі як держави громадянства підозрюваного;

Завдання 3. Практичне завдання. Використовуючи офіційні джерела міжнародних організацій:

- вивчити на сайті ЄС інформацію про співпраці України з європейськими агенціями кібербезпеки (ENISA, Europol);
- дослідити участь України у міжнародних навчаннях та ініціативах з кібербезпеки (через сайти НАТО, ООН, ОБСЄ);

## 6. Самостійна робота

Метою виконання самостійної роботи є поглиблене вивчення аспектів правового регулювання кібербезпеки та набуття навичок самостійного аналізу нормативно-правових актів.

Виконання самостійної роботи необхідно починати з вивчення відповідних розділів підручників, навчальних посібників, наукових джерел тощо, що наведені у переліку рекомендованої літератури, а також додаткової літератури і практичних матеріалів, які студент повинен знайти і опрацювати самостійно.

**Тема: Правове регулювання кібербезпеки у конкретній галузі економіки (за вибором студента)**

**Завдання:**

1. Оберіть одну з галузей економіки (банківська сфера, телекомунікації, енергетика, транспорт, охорона здоров'я, освіта) та зберіть нормативно-правові акти, що регулюють кібербезпеку у цій галузі. Проаналізуйте не менше 5 документів різного рівня (закони, постанови, накази регуляторів).

2. Проведіть аналіз правових вимог до забезпечення кібербезпеки у обраній галузі. Систематизуйте вимоги за категоріями: технічні, організаційні, кадрові, документальні. Визначте специфічні особливості регулювання саме цієї галузі.

3. Вивчіть міжнародний досвід правового регулювання кібербезпеки у обраній галузі. Порівняйте українські вимоги з аналогічними вимогами у 2-3 країнах ЄС або інших розвинених країнах (використовуючи доступні переклади та аналітичні матеріали).

4. Проаналізуйте судову практику та випадки притягнення до відповідальності за порушення вимог кібербезпеки у обраній галузі. Знайдіть та опрацюйте не менше 3 реальних справ з Єдиного державного реєстру судових рішень.

5. Підготуйте аналітичний звіт, який має містити аналіз нормативної бази, порівняння з міжнародною практикою, аналіз судових рішень та рекомендації щодо вдосконалення правового регулювання кібербезпеки у обраній галузі.

## 7. Тренінг з дисципліни

Метою проведення тренінгу є формування та розвиток практичних навичок правового аналізу відповідності організацій вимогам законодавства про критичну інформаційну інфраструктуру. Тренінг проводиться у формі комплексного аналізу конкретної організації (об'єкт студент обирає самостійно з переліку галузей: банківська сфера, енергетика, телекомунікації, транспорт, охорона здоров'я, водопостачання) щодо відповідності критеріям віднесення до КІІ та вимогам забезпечення кібербезпеки. За результатами аналізу формується правовий висновок з обґрунтуванням висновків та рекомендацій, підтверджених посиланнями на нормативно-правові акти та публічно доступну інформацію про організацію.

Завдання тренінгу:

1. Обрати конкретну організацію з однієї з галузей (бажано українську компанію з доступною публічною інформацією)
2. Зібрати та проаналізувати інформацію про організацію: сфера діяльності, кількість користувачів/споживачів, географія діяльності, технічна інфраструктура, критичність для суспільства
3. Провести правовий аналіз відповідності організації критеріям віднесення до КІІ згідно з чинним законодавством України
4. Визначити категорію КІІ (у разі відповідності критеріям) та проаналізувати вимоги до забезпечення кібербезпеки для цієї категорії
5. Оцінити поточний стан кібербезпеки організації (на основі публічно доступної інформації)
6. Підготувати правовий висновок з рекомендаціями щодо приведення діяльності організації у відповідність до вимог законодавства про КІІ

## 8. Засоби оцінювання та методи демонстрування результатів навчання

В процесі вивчення дисципліни “Нормативно-правове забезпечення кібербезпеки” використовуються методи оцінювання навчальної роботи студента:

– поточне тестування та опитування;

– підсумкове оцінювання по кожному змістовному модулю;

– оцінювання виконання тренінгу;

– оцінювання виконання самостійної роботи;

– екзамен

## 9. Критерії, форми поточного та підсумкового контролю

В процесі вивчення дисципліни “Нормативно-правове забезпечення кібербезпеки” рівень підготовки студентів оцінюється шляхом здачі іспиту. Іспит виставляється відповідно до затвердженої шкали:

| Модуль 1 | | Модуль 2 | | Модуль 3 | Модуль 4 | Модуль 5 |
|---|---|---|---|---|---|---|
| 10% | 10% | 10% | 10% | 5% | 15% | 40% |
| Поточне опитування | Модульний контроль 1 | Поточне опитування | Модульний контроль 2 | Тренінг | Самостійна робота | Екзамен |
| визначається як середнє арифметичне з оцінок на практичних заняттях (тема 1-7) | 2 теоретичні питання по 30 балів (– max 60 балів) та 20 тестів по 2 бали кожен (– max 40 балів) | визначається як середнє арифметичне з оцінок на практичних заняттях (тема 8-14) | 2 теоретичні питання по 30 балів (– max 60 балів) та 20 тестів по 2 бали кожен (– max 40 балів) | Оцінка визначаєтьс я відповідно критеріїв оцінювання | Оцінка визначається відповідно критеріїв оцінювання | 1. Тестові завдання (10 тестів по 2 бали) – max 20 балів. 2. Теоретичне питання (2) – max 80 балів. |

1. КРИТЕРІЇ ОЦІНЮВАННЯ ПОТОЧНОГО ОПИТУВАННЯ МОДУЛІВ 1 І 2 (по 10% кожен)

**90–100 балів** – у повному обсязі володіє навчальним матеріалом з нормативно-правового забезпечення кібербезпеки, вільно та аргументовано викладає особливості правового регулювання критичної інформаційної інфраструктури, глибоко розуміє питання кримінально-правових аспектів кіберзлочинності, демонструє системні знання щодо процесуальних аспектів розслідування кіберзлочинів, розуміє специфіку захисту персональних даних у кіберпросторі та правові засади електронного урядування.

**75–89 балів** – достатньо повно володіє теоретичним матеріалом з нормативно-правового забезпечення кібербезпеки, але при викладанні окремих питань щодо правового регулювання критичної інфраструктури або особливостей кримінального переслідування за кіберзлочини не вистачає достатньої глибини аргументації, допускаються несуттєві неточності в розумінні специфіки застосування міжнародного права кібербезпеки.

**65–74 бали** – в цілому володіє навчальним матеріалом та викладає основний зміст тем про правове регулювання кібербезпеки, але без глибокого аналізу практичних аспектів застосування законодавства у сфері кібербезпеки, допускаючи суттєві неточності в розумінні принципів категоризації об'єктів критичної інформаційної інфраструктури та процесуальних особливостей розслідування кіберзлочинів.

**60–64 бали** – не в повному обсязі володіє матеріалом з основ правового регулювання кібербезпеки, фрагментарно викладає особливості правового статусу суб'єктів забезпечення кібербезпеки, недостатньо розкриває зміст питань щодо забезпечення захисту персональних даних у цифровому середовищі.

**1–59 балів** – не володіє навчальним матеріалом з основних концепцій нормативно-правового забезпечення кібербезпеки, не може пояснити структуру системи правового регулювання кібербезпеки в Україні, не розуміє специфіки кримінально-правової кваліфікації кіберзлочинів та процесуальних особливостей їх розслідування.

2. МОДУЛЬНІ КОНТРОЛІ 1-2 (по 10% кожен)

**Структура модульного контролю:**

- 2 теоретичні питання (по 30 балів кожне = 60 балів)
- 20 тестів (по 2 бали = 40 балів)

**Критерії оцінювання теоретичного питання (30 балів):**

**25–30 балів** – демонструє комплексне розуміння системи правового регулювання кібербезпеки в Україні, вільно оперує знаннями про ієрархію нормативно-правових актів у сфері кібербезпеки, аналізує особливості правового статусу об'єктів критичної інформаційної інфраструктури, розуміє специфіку кримінально-правової та процесуальної регламентації боротьби з кіберзлочинністю, знає міжнародно-правові засади кібербезпеки, наводить конкретні приклади з практики правозастосування.

**15–24 балів** – володіє основним теоретичним матеріалом про нормативно-правове забезпечення кібербезпеки, але не завжди може встановити зв'язки між різними рівнями правового регулювання, недостатньо аналізує практичні аспекти застосування законодавства у сфері кібербезпеки, може мати прогалини в знаннях щодо особливостей секторального регулювання або міжнародного співробітництва.

**5–14 балів** – поверхнево викладає матеріал про окремі аспекти правового регулювання кібербезпеки, плутає різні категорії нормативно-правових актів, не може пояснити принципи категоризації об'єктів критичної інфраструктури, має слабке розуміння кримінально-правових аспектів кіберзлочинності, не розуміє специфіки міжнародного права кібербезпеки.

**1–4 балів** – не володіє матеріалом про нормативно-правове забезпечення кібербезпеки, не може назвати основні законодавчі акти у сфері кібербезпеки, не розуміє їх ієрархії та сфери застосування в контексті забезпечення кібербезпеки України.

**Критерії оцінювання тестів (40 балів):**

- **2 бали** – правильна відповідь на тест
- **0 балів** – неправильна відповідь

3. ТРЕНІНГ (5%)

**Тема: "Правовий аналіз відповідності організації вимогам законодавства про критичну інформаційну інфраструктуру"**

**90–100 балів** – демонструє високопрофесійні навички правового аналізу критеріїв віднесення об'єктів до критичної інформаційної інфраструктури, ефективно застосовує нормативно-правові акти для оцінки відповідності конкретної організації, проводить глибокий аналіз правових вимог до забезпечення кібербезпеки, створює обґрунтований правовий висновок з посиланнями на відповідні норми законодавства, підготовлює структуровані та

практично орієнтовані рекомендації щодо приведення діяльності у відповідність до вимог законодавства.

**75–89 балів** – ефективно проводить правовий аналіз з використанням релевантних нормативно-правових актів, демонструє хороші навички застосування критеріїв віднесення до КІІ, створює якісний правовий висновок, підготовлює добрі рекомендації з незначними недоліками в правовому обґрунтуванні або структурі.

**65–74 бали** – базово використовує правові критерії для аналізу, правовий аналіз поверхневий, висновок стандартний без глибокого правового обґрунтування, рекомендації мають прийнятну якість, але відсутні посилання на конкретні норми законодавства.

**60–64 бали** – слабко застосовує критерії віднесення до КІІ, правовий аналіз неглибокий, висновок примітивний, правові рекомендації низької якості з недостатнім обґрунтуванням нормами права.

**1–59 балів** – не вміє ефективно застосовувати законодавство про критичну інформаційну інфраструктуру, не може провести правовий аналіз відповідності, не здатен створити обґрунтований правовий висновок, не може підготувати якісні правові рекомендації.

4. САМОСТІЙНА РОБОТА (15%)

**Завдання: "Правове регулювання кібербезпеки у конкретній галузі економіки"**

**90–100 балів** – створює високоякісне комплексне дослідження правового регулювання кібербезпеки у обраній галузі, ефективно збирає та аналізує нормативно-правові акти різного рівня, проводить професійний порівняльний аналіз з міжнародною практикою, всебічно аналізує судову практику у відповідній сфері, демонструє глибоке розуміння специфіки галузевого регулювання, підготовлює структурований аналітичний звіт з обґрунтованими правовими висновками та практичними рекомендаціями щодо вдосконалення законодавства.

**75–89 балів** – підготовлює якісне правове дослідження з належним рівнем аналізу, використовує релевантні нормативно-правові акти та методи порівняльно-правового аналізу, демонструє хороші навички правового аналізу, може мати незначні недоліки в окремих компонентах дослідження або систематизації судової практики.

**60–74 балів** – створює базове правове дослідження з поверхневим аналізом, обмежено використовує нормативно-правові джерела та порівняльно-правові методи, аналіз судової практики недостатній, є суттєві недоліки в структурі звіту та правовому обґрунтуванні висновків.

**1–59 балів** – не може створити якісне правове дослідження галузевого регулювання кібербезпеки, неефективно використовує нормативно-правові джерела та методи правового аналізу, слабкі навички правової систематизації, звіт не відповідає стандартам правового дослідження, відсутні обґрунтовані правові висновки та рекомендації.

5. ІСПИТ (40%)

**Структура іспиту:**

- 10 тестових завдань (по 2 бали = 20 балів)
- 2 теоретичні питання (по 40 балів = 80 балів)

**Критерії оцінювання теоретичного питання (40 балів):**

**34–40 балів** – демонструє системні знання з усіх аспектів нормативно-правового забезпечення кібербезпеки, самостійно та правильно аналізує комплексні питання правового регулювання критичної інформаційної інфраструктури, розуміє особливості кримінально-правової та процесуальної регламентації боротьби з кіберзлочинністю, аналізує правові засади електронного урядування та захисту персональних даних, розуміє специфіку міжнародного права кібербезпеки, демонструє глибоке знання судової практики, пропонує обґрунтовані рішення з урахуванням доктринальних джерел та практики правозастосування.

**26–33 балів** – володіє основним правовим матеріалом, достатньо глибоко аналізує основні аспекти застосування законодавства у сфері кібербезпеки, розуміє принципи функціонування системи правового регулювання, може мати незначні прогалини в знаннях окремих спеціальних нормативно-правових актів або деталей їх застосування, загалом здатен встановлювати зв'язки між різними рівнями правового регулювання кібербезпеки.

**16–25 балів** – володіє базовим правовим матеріалом, але недостатньо глибоко аналізує практичні аспекти застосування законодавства, може плутати окремі категорії нормативно-правових актів у сфері кібербезпеки, має поверхневе розуміння принципів правового регулювання критичної інфраструктури, обмежено розуміє кримінально-правові аспекти кіберзлочинності та міжнародно-правові засади кібербезпеки.

**1–15 балів** – слабко володіє правовим матеріалом, не може пояснити основні принципи правового регулювання кібербезпеки, плутає базові поняття та категорії, не розуміє структури системи забезпечення кібербезпеки в Україні, не здатен проводити правовий аналіз ситуацій у сфері кібербезпеки.

**Критерії оцінювання тестів (20 балів):**

- **2 бали** – правильна відповідь на тест
- **0 балів** – неправильна відповідь

Шкала оцінювання:

| За шкалою Університету | За національною шкалою | За шкалою ECTS |
|---|---|---|
| 90-100 | відмінно | A (відмінно) |
| 85-89 | добре | B (дуже добре) |
| 75-84 | | C (добре) |
| 65-74 | задовільно | Д (задовільно) |
| 60-64 | | E (достатньо) |
| 35-59 | незадовільно | FX (незадовільно з можливістю повторного складання) |
| 1-34 | | F (незадовільно з обов’язковим повторним курсом) |

## 11. Інструменти, обладнання та програмне забезпечення, використання

**яких передбачає навчальна дисципліна**

| № п/п | Найменування | Номер теми |
|---|---|---|
| 1 | Технічне забезпечення: мультимедійний проєктор, ноутбук, проєкційний екран | 1-14 |
| 2 | Базове програмне забезпечення: ОС Windows. Стандартне програмне забезпечення базових інформаційних технологій: MS Office (Word, Excel, PowerPoint, Microsoft Visio). Телекомунікаційне програмне забезпечення (Internet Explorer, Google Chrome,Viber тощо). | 1-14 |
| 3 | Комунікаційна навчальна платформа (Moodle) для організації дистанційного навчання (за необхідності). | 1-14 |
| 4 | Комунікаційне програмне забезпечення Zoom для проведення занять в режимі on-line (за необхідності). | 1-14 |

## РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

### Нормативно-правові акти


1. Деякі питання документування управлінської діяльності. Постанова КМУ від 17.01.2018 № 55.
2. Деякі питання електронної взаємодії електронних інформаційних ресурсів. Положення від 08.09.2016 № 606
3. Деякі питання об'єктів критичної інформаційної інфраструктури. Постанова КМУ від 18.08.2021 № 868
4. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі. Постанова КМУ від 04.04.2023 № 299
5. Додатковий протокол до Конвенції про кіберзлочинність щодо криміналізації актів расистського та ксенофобського характеру від 28.01.2003
6. Доктрина інформаційної безпеки України, затверджена Указом Президента від 25.02.2017 № 47/2017
7. Кодекс України про адміністративні правопорушення. Закон України від 07.12.1984 № 8073-X
8. Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція) від 23.11.2001
9. Конституція України. Закон від 28.06.1996 № 254к/96-ВР
10. Концепція розвитку штучного інтелекту в Україні. Розпорядження КМУ від 02.12.2020 № 1556-р
11. Кримінальний кодекс України. Закон від 05.04.2001 № 2341-III
12. Кримінальний процесуальний кодекс України. Закон України від 13.04.2012 № 4651-VI
13. Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі від 03.07.2023 № 570
14. Про акредитацію органів з оцінки відповідності. Закон України від 17.05.2001 № 2407-III
15. Про віртуальні активи. Закон України (ще не набрав чинності)
16. Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню). Закон України від 18.12.2018 № 2657-VIII
17. Про електронні документи та електронний документообіг. Закон України від 22.05.2003 № 851-IV

18. Про електронні комунікації. Закон України від 16.12.2020 № 1089-IX
19. Про електронну ідентифікацію та електронні довірчі послуги. Закон України від 05.10.2017 № 2155-VIII
20. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури. Постанова КМУ; від 19.06.2019 № 518
21. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури. Постанова КМУ від 19.06.2019 № 518
22. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України. Постанова Правління НБУ від 28.09.2017 № 95
23. Про затвердження Порядку здійснення нагляду за додержанням законодавства про захист персональних даних. Постанова КМУ від 08.01.2014 № 11
24. Про затвердження Порядку формування переліку об'єктів критичної інформаційної інфраструктури. Постанова КМУ від 09.10.2020 № 943
25. Про затвердження Правил надання та отримання телекомунікаційних послуг. Постанова КМУ від 11 квітня 2012 р. № 295
26. Про затвердження Технічного регламенту щодо вимог до засобів електронної ідентифікації в контексті схеми електронної ідентифікації та процедури, що застосовуються для визначення рівня довіри до засобів електронної ідентифікації. Постанова КМУ від 16.05.2025 № 577
27. Про захист персональних даних. Закон України від 01.06.2010 № 2297-VI
28. Про національну безпеку України. Закон України від 21.06.2018 № 2469-VIII
29. Про обов'язкове страхування цивільно-правової відповідальності власників наземних транспортних засобів. Закон України від 21.05.2024 № 3720-IX (як приклад обов'язкового страхування)
30. Про оборону України. Закон України від 06.12.1991 № 1932-XII
31. Про оперативно-розшукову діяльність. Закон України від 18.02.1992 № 2135-XII
32. Про організаційно-технічну модель кіберзахисту, Постанова КМУ від 29 грудня 2021 р. № 1426
33. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 № 2163-VIII
34. Про правовий режим воєнного стану. Закон України від 12.05.2015 № 389-VIII
35. Про ратифікацію Конвенції про кіберзлочинність. Закон України від 07.09.2005 № 2824-IV
36. Про ринок електричної енергії. Закон України від 13.04.2017 № 2019-VIII
37. Про страхування. Закон України від 18.11.2021 № 1909-IX
38. Про технічні регламенти та оцінку відповідності. Закон України від 15.01.2015 № 124-VIII
39. Про цифровий порядок денний України. Проект Закону України
40. Регламент ЄС 2016/679 (GDPR)

41. Стратегія воєнної безпеки України. Указ Президента України від 25.03.2021 № 121/2021
42. Стратегія кібербезпеки України. Указ Президента від 14.09.2021 № 447/2021
43. Цивільний кодекс України. Закон України від 16.01.2003 № 435-IV

Наукові джерела

1. Бенескул А.В. Нормативно-правове закріплення застосування цифрових технологій для забезпечення кримінологічної безпеки суспільства. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО*. 2023. Випуск 78: частина 2. С. 145-151
2. Вдовенко С., Даник Ю., Фараон С. Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення. *CS&CS*. 2019. Issue 1(13). p. 17-29.
3. Горінов П.В., Драпушко Р.Г. Сучасні виклики адміністративно-правових засад кібербезпеки України в умовах воєнного стану. *Юридичний науковий журнал*. 2023. № 1. С. 267-270.
4. Колесніков А. П. Особливості захисту інформації в діяльності органів здійснення правосуддя. *Економіка. Фінанси. Право*. 2024. № 5. С. 8–12. DOI: https://doi.org/10.37634/efp.2024.5.1.
5. Колесніков А. П., Біловус Л. І. Цифровізація державних послуг: тенденції та перспективи. *Економічний дискурс*. 2021. № 3–4. С. 139–146. DOI: https://doi.org/10.36742/2410-0919-2021-2-14.
6. Колесніков А. П., Карапетян О. М. Штучний інтелект: переваги та загрози використання. *Ефективна економіка*. 2023. № 8. DOI: https://doi.org/10.32702/2307-2105.2023.8.9
7. Колесніков А. П. Цифрове суспільство в Україні: стан та вектори безпечного розвитку. *Економічна безпека та фінансові розслідування: концепти, прагматика, інструментарій забезпечення* : кол. монографія. Тернопіль : Економічна думка ; ТНЕУ, 2019. С. 55–70.
8. Колесніков А., Зяйлик М. Економіко-правові засади розвитку кіберзлочинності та методів боротьби з нею. *Актуальні проблеми правознавства***.** 2017. № 1. С. 26–29. DOI: https://doi.org/10.35774/app2017.01.026.
9. Скіцько О.І., Ширшов Р.А. Нормативно-правове забезпечення кібербезпеки об'єктів критичної інфраструктури. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2024. № 2. С. 73-79
10. Скіцько О.І., Ширшов Р.А. Нормативно-правове забезпечення кібероборони України: сучасний стан. *Юридичний вісник*. 2024. № 3. С. 244-250
11. Третяк Ю. І. Нормативно-правове регулювання кібербезпеки в Україні. *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична*. 2024. Випуск 40. С. 280-289.
12. Kolesnikov A. Cybersecurity as a necessary condition for the functioning of the justice administration system. *Підприємництво, господарство і право*. 2023. № 5. С. 101–107. DOI: https://doi.org/10.32849/2663-5313/2023.5.15.
13. Kolesnikov A., Oliynychuk O. Information Security Strategy: New Challenges and Prospects for Ukraine. *National security in modern world. Legal, technological and social communication aspects*. Ełk, 2021. Pp. 37–44.

14. Onishchenko N. M., Teremetskyi V. I., Kolesnikov A. P., Kovalchuk O. Ya., Shabalin A. V., Romas M. I. Protection of confidential medical information in Ukraine: problems of legal regulation. *Georgian Medical News*. 2024. № 4. Pp. 161–168. URL: https://www.geomednews.com/Articles/2024/4_2024/161-168.pdf