Міністерство освіти і науки України
Національний університет «Чернігівська політехніка»
Навчально-науковий інститут електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

СИЛАБУС
Нормативно-правове забезпечення інформаційної безпеки

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Ткач Ю.М.
(підпис) (прізвище та ініціали)

«_26_» серпня 2024 р.

Розробник (-и): Ларченко М.О., доцент, кандидат юридичних наук, доцент _____
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Силабус навчальної дисципліни обговорено на засіданні кафедри кібербезпеки та математичного моделювання

Протокол від «26» серпня 2024 р. № 7

Узгоджено з гарантом освітньої програми: _____ Ткач Ю.М.
(підпис) (прізвище та ініціали)

---

1. Загальна інформація про дисципліну.

Тип дисципліни	*Вибіркова*
Мова викладання	українська
Рік навчання та семестр	2024-2025 навчальний рік, І семестр, ОП Кібербезпека за спеціальністю 125 Кібербезпека та захист інформації галузь знань 12 Інформаційні технології
Викладач (-і)	Ларченко Марина Олександрівна, доцент кафедри кібербезпеки та математичного моделювання, кандидат юридичних наук.
Профайл викладача (-ів)	https://mmi.stu.cn.ua/personal-kafedry/
Контакти викладача	Т.м. +38067 296 74 99, E-mail: urlinka2006@gmail.com

2. Анотація курсу.

Дисципліна **"Нормативно-правове забезпечення інформаційної безпеки"** є вибірковою частиною програми підготовки магістрів ОП **Кібербезпека** за спеціальністю 125 Кібербезпека та захист інформації 12 Інформаційні технології. Курс надає ґрунтовні знання та практичні навички щодо нормативно-правового регулювання інформаційної безпеки, правових аспектів кіберзахисту та міжнародних стандартів у сфері захисту інформації.

Загальна тематика курсу охоплює: основи правового регулювання інформаційної безпеки; міжнародні та національні нормативні акти у сфері кібербезпеки (ISO/IEC 27001, GDPR, NIST, Закон України "Про основні засади забезпечення кібербезпеки України" тощо); правові аспекти захисту інформації в державному та приватному секторах; відповідальність за кіберзлочини та інформаційні правопорушення; етичні аспекти діяльності в сфері кібербезпеки; регулювання обігу персональних даних та конфіденційної інформації.

Підхід до викладання орієнтований на поєднання теоретичних знань із практичними кейсами, аналізом законодавчих ініціатив, судової практики та міжнародного досвіду у сфері нормативно-правового забезпечення кібербезпеки. Особлива увага приділяється розумінню юридичних наслідків порушень у сфері інформаційної безпеки та практичному застосуванню нормативно-правових актів.

Курс готує фахівців, здатних аналізувати правові аспекти кіберзахисту, розробляти нормативні документи для забезпечення інформаційної безпеки, оцінювати ризики та відповідальність у сфері цифрових технологій.

3. Мета та цілі курсу.

Мета курсу – формування у студентів системного розуміння нормативно-правових аспектів інформаційної безпеки, забезпечення захисту інформації та відповідальності за правопорушення у кіберпросторі, а також розвиток практичних навичок застосування міжнародних і національних стандартів кібербезпеки в реальних умовах.

Цілі курсу:

Здатність аналізувати та застосовувати нормативно-правові акти у сфері інформаційної безпеки та кіберзахисту.

Здатність здійснювати правову експертизу інформаційних систем та оцінювати їх відповідність вимогам законодавства і міжнародних стандартів.

Здатність розробляти та впроваджувати політики кібербезпеки відповідно до нормативно-правових вимог.

Здатність оцінювати правові ризики у сфері кібербезпеки та пропонувати заходи щодо їх мінімізації.

Здатність визначати юридичну відповідальність за правопорушення у сфері інформаційної безпеки та кіберзлочини.

Здатність використовувати міжнародний досвід та найкращі практики у сфері нормативно-правового забезпечення кібербезпеки.

Здатність ефективно взаємодіяти з державними органами та приватними структурами у питаннях правового регулювання інформаційної безпеки.

Здатність аналізувати судову практику у сфері інформаційної безпеки та формувати юридично обґрунтовані висновки щодо її застосування.

4. Результати навчання:

Розуміти та застосовувати національні та міжнародні нормативно-правові акти у сфері інформаційної безпеки та кіберзахисту.

Аналізувати правові вимоги щодо захисту інформації, персональних даних та критичної інфраструктури.

Ідентифікувати та оцінювати правові ризики, пов’язані з інформаційною безпекою та кіберзлочинністю.

Застосовувати правові механізми забезпечення інформаційної безпеки в державному та приватному секторах.

Розробляти та впроваджувати політики інформаційної безпеки відповідно до вимог законодавства та міжнародних стандартів (ISO/IEC 27001, GDPR, NIST тощо).

Оцінювати юридичні аспекти кіберінцидентів та процесуального оформлення цифрових доказів.

Формувати правові висновки щодо відповідальності за порушення у сфері інформаційної безпеки та кіберзлочинності.

Взаємодіяти з державними регуляторами та правоохоронними органами з питань дотримання нормативно-правових вимог у сфері інформаційної безпеки.

Аналізувати судову практику щодо правозастосування у сфері кібербезпеки та використовувати її у професійній діяльності.

Розробляти правові стратегії кіберзахисту та забезпечувати відповідність інформаційних систем вимогам законодавства.A1.B1. Формувати й оновлювати базу знайдених матеріалів для подальшого її використання в роботі.

5. Пререквізити. Відсутні.

6. Обсяг курсу:

Вид заняття	Загальна кількість годин
Лекції	16/6
Практичні заняття	16/6
Самостійна робота	88/108
Індивідуальне завдання – розрахунково-графічна робота	
Всього кредитів	4

Лекційні, практичні заняття, розрахунково-графічна робота, самостійна робота – з використанням системи дистанційного навчання Moodle, Teams, рекомендованих джерел, відеоматеріалів тощо.

7. Тематика курсу.

Лекції (16/6 годин):

1. Правові засади інформаційної безпеки (2 години)
   Основні поняття та принципи нормативно-правового забезпечення інформаційної безпеки.
   Національні та міжнародні стандарти у сфері кібербезпеки (ISO/IEC 27001, NIST, GDPR).
   Державна політика України у сфері захисту інформації та кібербезпеки.
2. Законодавство України у сфері інформаційної безпеки (2 години)
   Закон України «Про основні засади забезпечення кібербезпеки України».
   Закон «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах».
   Регулювання доступу до інформації: державна, службова, конфіденційна інформація.
3. Міжнародне регулювання інформаційної безпеки (2 години)
   Конвенція про кіберзлочинність (Будапештська конвенція).
   Директиви ЄС у сфері захисту персональних даних (GDPR, NIS Directive).
   Співробітництво міждержавних структур у сфері кібербезпеки (Європол, Інтерпол, ENISA).
4. Юридична відповідальність за порушення у сфері інформаційної безпеки (2 години)
   Кримінальна, адміністративна та цивільно-правова відповідальність за кіберзлочини.
   Види кіберзлочинів та їхня кваліфікація згідно з Кримінальним кодексом України.
   Судова практика щодо кіберзлочинності.

5. Правові механізми захисту персональних даних (2 години)
   Законодавство України та міжнародні стандарти захисту персональних даних (GDPR).
   Правові механізми захисту інформаційної приватності.
   Відповідальність за порушення норм обробки персональних даних.
6. Нормативне регулювання використання криптографічного захисту інформації (2 години)
   Законодавчі вимоги щодо використання криптографічних засобів захисту.
   Державна експертиза у сфері криптографічного захисту інформації.
   Сертифікація та стандартизація криптографічних засобів.
7. Регулювання діяльності у сфері критичної інформаційної інфраструктури (2 години)
   Законодавчі вимоги щодо захисту критичної інфраструктури.
   Національна система кіберзахисту об'єктів критичної інфраструктури.
   Відповідальність операторів критичної інформаційної інфраструктури.
8. Аудит та оцінка відповідності інформаційної безпеки (2 години)
   Нормативно-правові вимоги до проведення аудиту інформаційної безпеки.
   Основні стандарти та методики аудиту кібербезпеки (ISO 27001, NIST).
   Впровадження заходів відповідності та управління ризиками.

Практичні (16/6 годин):

1. Аналіз законодавчих актів України та міжнародних норм у сфері інформаційної безпеки (2 години)
2. Розробка політики інформаційної безпеки організації відповідно до нормативних вимог (2 години)
3. Практичне застосування GDPR: кейси з аналізу персональних даних та прав користувачів (2 години)
4. Аналіз судової практики щодо кіберзлочинів та порушень у сфері інформаційної безпеки (2 години)
5. Юридичні аспекти розслідування кіберзлочинів: оформлення цифрових доказів (2 години)
6. Практичний аналіз відповідності організації вимогам кібербезпеки (ISO 27001, NIST) (2 години)
7. Юридична експертиза документів з криптографічного захисту інформації (2 години)
8. Оцінка ризиків та правових наслідків порушень у сфері інформаційної безпеки (2 години)

Розрахунково-графічна робота (РГР)

Тема: Аналіз нормативно-правових вимог у сфері інформаційної безпеки та розробка політики безпеки організації.

РГР передбачає дослідження законодавчих і нормативних актів (ISO 27001, GDPR, національні закони) та їх застосування до конкретного кейсу. Студенти аналізують вимоги інформаційної безпеки, розробляють політику захисту інформації, оцінюють ризики та моделюють заходи захисту. Робота включає підготовку пояснювальної записки та графічних схем (модель загроз, структура політики безпеки тощо).

Самостійна робота (88/108 годин):

Самостійна робота охоплює теоретичне опрацювання матеріалів, аналіз нормативно-правових документів та виконання практичних завдань.

Основні види діяльності:

1. Опрацювання законодавчих і нормативних актів (ISO/IEC 27001, NIST, GDPR, ЗУ «Про захист інформації в інформаційно-комунікаційних системах» тощо) – 20 годин.
2. Аналіз судової та адміністративної практики у сфері інформаційної безпеки (розгляд кейсів щодо порушень законодавства, відповідальності за кіберзлочини) – 12 годин.
3. Підготовка аналітичного звіту щодо правових аспектів інформаційної безпеки – 10 годин.

4. Виконання розрахунково-графічної роботи (РГР) (аналіз нормативних вимог, розробка політики безпеки) – 24 години.
5. Практичні кейси з розробки внутрішніх політик безпеки (підготовка політики управління доступом, реагування на інциденти, аудит безпеки) – 10 годин.
6. Підготовка до тестування та підсумкової атестації (вивчення контрольних питань, робота з додатковими джерелами) – 12 годин.

Робота передбачає активне використання нормативних баз, аналіз практичних ситуацій та розробку рекомендацій щодо впровадження заходів інформаційної безпеки.

8. Система оцінювання та вимоги

Загальна система оцінювання курсу	Оцінювання курсу базується на **накопичувальній системі** та включає: **поточний контроль** (оцінювання практичних занять) – 40 балів, **проміжний модульний контроль** – 10 балів, **виконання індивідуального завдання (РГР)** – 10 балів **та підсумковий контроль** – 40 балів. Оцінювання кожного виду діяльності здійснюється окремо відповідно до **досягнення навчальних цілей**.
Вимоги до РГР, КР, КП тощо	**Критерії оцінювання РГР:** 1) відповідність завдання вимогам курсу – **2 балів;** 2) обґрунтування вибору стандартів та методів захисту – **2 балів;** 3) якість аналізу ризиків та оцінка відповідності – **2 балів;** 4) оформлення роботи, відповідність методичним рекомендаціям – **2 балів;** 5) своєчасність здачі роботи – **2 бали.**
Практичні (лабораторні) заняття	Оцінка кожного практичного заняття здійснюється за наступними критеріями: 1) виконання практичного завдання – **3 бали;** 2) аналіз отриманих результатів – **1 бал**; 3) належне оформлення звіту – **1 бал.**
Умови допуску до підсумкового контролю	1. Виконання та захист **не менше 50% практичних робіт або усні відповіді на запитання** (щонайменше 4 із 8). 2. Проходження проміжного модульного контролю. 3. Виконання **розрахунково-графічної роботи** (РГР).

Розподіл балів, які отримують здобувачі вищої освіти

Модуль за тематичним планом дисципліни та форма контролю		Кількість балів
Змістовий модуль 1. Основи нормативно-правового забезпечення інформаційної безпеки		**30/30**
1	Вступ до нормативно-правового регулювання інформаційної безпеки.	**5/5**
2	Міжнародні стандарти та нормативні акти у сфері інформаційної безпеки (ISO/IEC 27001, NIST, GDPR).	**5/5**
3	Законодавство України у сфері захисту інформації (ЗУ «Про захист інформації в інформаційно-комунікаційних системах», Кримінальний кодекс України, ЗУ «Про кібербезпеку»).	**5/5**
4	Політика інформаційної безпеки в організаціях: правові аспекти та вимоги.	**15/15**
Змістовий модуль 2. Юридичні механізми забезпечення та відповідальність за порушення інформаційної безпеки		**30/30**

1	Державне регулювання інформаційної безпеки: роль НБУ, ДССЗЗІ, Кіберполіції.	**5/5**
2	Правове регулювання кіберзлочинності та відповідальність за правопорушення у сфері інформаційної безпеки.	**15/15**
3	Захист персональних даних: міжнародні та національні правові механізми.	**5/5**
4	Аудит та контроль відповідності заходів інформаційної безпеки законодавчим вимогам.	**5/5**
Усього поточний і проміжний модульний контроль		**60/60**
Семестровий контроль (Диференційований залік)		**40/40**
Разом		**0…100**

Шкала оцінювання результатів навчання

Оцінка в балах	**Оцінка ECTS**	**Оцінка за національною шкалою (диференційований залік)**	
		для екзамену (диференційованого заліку), курсового проєкту (роботи), практики, атестації	для заліку
90 – 100	**A** (*відмінно*)	відмінно	зараховано
82-89	**B** (*дуже добре*)	добре	
75-81	**C** (*добре*)		
66-74	**D** (*задовільно*)	задовільно	
60-65	**E** (*достатньо*)		
0-59	**FX** (*незадовільно*)	незадовільно з можливістю повторного складання	незараховано з можливістю повторного складання

9. Обладнання та програмне забезпечення.

При вивченні курсу використовується сучасне програмне забезпечення для аналізу нормативно-правового забезпечення інформаційної безпеки, оцінки відповідності стандартам та правовим нормам у сфері кібербезпеки.

Апаратне забезпечення:

Персональні комп’ютери або ноутбуки з доступом до інтернету.

Операційні системи: Windows 10/11 Pro, Linux (Ubuntu) або macOS.

Програмне забезпечення:

ISO/IEC 27001 Toolkit – для аналізу стандартів інформаційної безпеки.

NIST Security Content Automation Protocol (SCAP) Tools – для оцінки відповідності міжнародним стандартам.

COBIT Framework – для управління інформаційними ризиками та аудитів безпеки.

OneTrust, TrustArc – для аналізу відповідності законодавству (GDPR, PDPA тощо).

MS Word, LaTeX – для підготовки нормативної документації та аналітичних звітів.

Moodle, Microsoft Teams – для дистанційного навчання, тестування та обговорення правових аспектів інформаційної безпеки.

10. Політики курсу.

У випадку, якщо здобувач протягом семестру не виконав у повному обсязі всіх видів навчальної роботи, має невідпрацьовані лабораторні роботи або не набрав мінімально необхідну кількість балів (25), він не допускається до складання диференційованого заліку під час семестрового контролю, але має право ліквідувати академічну заборгованість у порядку, передбаченому «Положенням про поточне та підсумкове оцінювання знань здобувачів НУ "Чернігівська політехніка"». Повторне складання заліку з метою підвищення позитивної оцінки не дозволяється. У випадку повторного складання заліку всі набрані протягом семестру бали анулюються, а повторний диференційований залік складається у вигляді тестування.

До загальної політики курсу відноситься дотримання принципів відвідування занять у відповідності до затвердженого розкладу, а також вільного відвідування лекційних занять для осіб, які отримали на це дозвіл відповідно до «Порядку надання дозволу на вільне відвідування занять здобувачам вищої освіти НУ «Чернігівська політехніка»». Запорукою успішного вивчення дисципліни є активність та залучення під час проведення лабораторних/практичних та лекційних занять – відповіді на запитання викладача (як один з елементів поточного контролю), задавання питань для уточнення незрозумілих моментів, вирішення практичних завдань. Консультації відбуваються в аудиторіях університету у відповідності до затвердженого розкладу або ж особистих чи групових консультацій (через вбудований форум) на сторінці курсу в системі дистанційного навчання НУ «Чернігівська політехніка».

Політика дедлайнів

Своєчасність здачі лабораторної роботи оцінюється в 0,5 балу за кожну лабораторну роботу. Своєчасність здачі РГР оцінюється в 1 бал. Відповідно, максимальна оцінка за невчасно здані роботи зменшується на зазначену кількість балів. Виключенням може бути наявність поважних причин несвоєчасної здачі зазначених робіт (хвороба, участь в зазначений час в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом тощо).

Політика користування ноутбуками / смартфонами

Прохання до здобувачів тримати смартфони переведеними у беззвучний режим протягом лекційних та практичних занять, так як дзвінки, переписки та спілкування у соціальних мережах відволікають від проведення занять як викладача, так й інших здобувачів. Ноутбуки, планшети та смартфони не можуть використовуватися в аудиторіях під час занять та під час проведення підсумкового контролю (за виключенням проходження тестового контролю в системі Moodle).

Політика заохочень та стягнень

За результатами навчальної, наукової або організаційної діяльності здобувачів вищої освіти за курсом їм можуть нараховуватися додаткові бали – до 10 балів, у залежності від вагомості досягнень. Види позанавчальної діяльності, за якими здобувачі вищої освіти заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, участь у науково-практичних конференціях, винаходи, патенти, авторські свідоцтва за напрямами курсу.

Політика академічної доброчесності

Академічна доброчесність повинна бути забезпечена під час проходження даного курсу, зокрема при виконанні лабораторних, контрольних та розрахунково-графічних робіт (КР/КП) (принципи описані у Кодексі академічної доброчесності НУ «Чернігівська політехніка»). Списування під час проміжного та підсумкового контролів, виконання практичних завдань на замовлення, підказки вважаються проявами академічної недоброчесності. Від усіх слухачів курсу очікується дотримання академічної доброчесності у зазначених вище моментах. До здобувачів вищої освіти, у яких було виявлено порушення академічної доброчесності, застосовуються різноманітні дисциплінарні заходи (включаючи повторне проходження певних етапів).

Правила перезарахування кредитів

Кредити, отримані в інших закладах вищої освіти, а також результати навчання у неформальній та/або інформальній освіті, можуть бути перезараховані викладачем у

відповідності до положення «Порядок визначення академічної різниці та перезарахування навчальних дисциплін у НУ «Чернігівська політехніка»». Визнання результатів навчання у неформальній освіті розповсюджується на окремі змістові модулі (теми) навчальної дисципліни.

11. Рекомендовані джерела та література:

1. Правове регулювання національної безпеки : навчальний посібник / О. Г. Боднарчук, О. І. Боднарчук, М. В. Глух, А. В. Гарбінська-Руденко ; Державний податковий університет. – Ірпінь, 2024. – 202 с. URL: https://dpu.edu.ua/images/Documents/NAUKA/Naukova%20biblioteka/Navcalno-metodicna%20literatura/N/Pravove%20reguluvanna%20nacionalnoi%20bezpeki.pdf

2. Про Стратегію інформаційної безпеки: Указ Президента України «Про рішення Ради національної безпеки і оборони України» від 15 жовтня 2021 р. № 685/2021. Відомості Верховної Ради України. 2021. № 685/2021.

3. Про національну безпеку: Закон України 21 червня 2018 р. № 2469-VIII. Відомості Верховної Ради України. 2018. № 31. Ст. 241 (із змінами).

4. Гузь М.В. Становлення та розвиток світових стандартів інформаційної безпеки. – Київ: НПУ імені М. П. Драгоманова, 2018. – 15 с. [Електронний ресурс]. Режим доступу: http://enpuir.npu.edu.ua/bitstream/handle/123456789/23381/Guz.pdf

5. Баран М.В. Адміністративно-правове забезпечення інформаційної безпеки в Україні: дисертація на здобуття ступеня доктора філософії за спеціальністю 081 «Право» / Львівський державний університет внутрішніх справ. Львів. 2022. 242 с. URL: https://dspace. lvduvs.edu.ua/bitstream/1234567890/5076/1/baran_d.pdf

6. Бєлов Д., Громовчук М. Правовий простір держави: конституційно-правовий аспект. Науковий вісник Ужгородського національного університету. Серія Право. 2021. Випуск 66. С. 46–50.

7. Бєлов Д.М., Белова М.В. Система захисту прав і свобод людини і громадянина: доктринальні та нормативні основи. Науковий вісник Ужгородського національного університету. Серія «Право». 2022. Вип. 74. С. 85–90.

8. Денисюк Ж.З., Яковлєв О.В. Формування інформаційної культури суспільства в умовах цифровізації. Вісник Національної академії керівних кадрів культури і мистецтв. № 2. 2021. С. 18–22.

9. Дзьобань О., Данильян О. Права і свободи людини: інформаційний вимір. Вісник Національного юридичного університету імені Ярослава Мудрого. № 3 (58). Серія: філософія, філософія права, політологія, соціологія. 2023. С. 6–22.

10. Захаренко К.В. Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири: дисертація на здобуття наукового ступеня доктора політичних наук за спеціальністю 23.00.02 «Політичні інститути та процеси» / Національний педагогічний університет імені М. Драгоманова, Львівський національний університет імені Івана Франка. Львів. 2021. 423 с. URL: https://lnu.edu.ua/wp-content/uploads/2021/04/dis_zakharenko.pdf

11. Квіткін П.В., Дятлова І.В., Петрова Л.О. Інформаційна безпека особистості: теоретико-методологічний аналіз. Вісник Національного юридичного університету імені Ярослава Мудрого. № 4 (51). Серія: філософія, філософія права, політологія, соціологія. 2021. С. 46–62. 459 Юридичний науковий електронний журнал.

12. Мельничук В., Горохова Л. Критичне мислення як складова інформаційної безпеки. Вісник Львівського університету. Випуск 29. Серія філософські науки. 2022. С. 7–13.

13. Тихомиров О. Ідея інформаційної гігієни в контексті інформаційної безпеки і захисту інформаційних прав людини. Науковий юридичний журнал «Правові новели». № 20. 2023. С. 59–65. URL: http://legalnovels.in.ua/journal/20_2023/8.pdf.

14. Хитра О.Л. Інформаційна безпека людини як базова аксіологічна константа. Modern information technologies and their implementation in the processes of social and technical project

management. Abstracts of IV International Scientific and Practical Conference. Boston. USA. 17–18 February 2020. P. 150–153. URL: https://isg-konf.com/wp-content/uploads/2020/02/IV-Conference-BostonUSA.pdf#page=151

15. Byelov D., Novak O. Communal property disposal: actual issues. Visegrad Journal on Human Rights. Issue 1. 2022. P. 33–39.

16.Diptiben Ghelani. Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. American Journal of Science, Engineering and Technology. 2022. P. 1–7.

17.Yuchong Li, Qinghui Liu. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports. 7. 2021. P. 1–11.

18. Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). *The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda*. The TQM Journal, 33(2), 39-59. https://www.emerald.com/insight/content/doi/10.1108/TQM-09-2020-0202/full/html

19. Chapple, M., Stewart, J. M., & Gibson, D. (2021). *(ISC)² CISSP Certified Information Systems Security Professional Official Study Guide* (9th ed.). Wiley. https://books.google.com/books/about/ISC_2_CISSP_Certified_Information_System.html?id=kSw0EAAAQBAJ

20. Calder, A. (2019). *ISO/IEC 27001:2013 A Pocket Guide* (2nd ed.). IT Governance Publishing.