



Силабус курсу

Нормативно-правове забезпечення кібербезпеки

Ступінь вищої освіти – бакалавр

Галузь знань – 12 Інформаційні технології

Спеціальність – 125 Кібербезпека та захист інформації

Освітньо-професійна програма – Кібербезпека

Рік навчання: II, Семестр: V

Кількість кредитів: 5 Мова викладання: українська

Керівник курсу

д.ю.н., доцент **Колесніков Андрій Павлович**

Контактна інформація

a.kolesnikov@wunu.edu.ua

Опис 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.

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.

Структура курсу

Години (лек. / лабор.)	Тема	Результати навчання	Завдання
4/2	Тема 1. Система правового регулювання кібербезпеки в Україні	Розуміння ієрархії нормативно-правових актів у сфері кібербезпеки, знання повноважень суб'єктів забезпечення кібербезпеки	Опитування, тести, завдання
2/2	Тема 2. Правове регулювання критичної інформаційної інфраструктури	Знання критеріїв віднесення об'єктів до КІІ, розуміння процедур категоризації та вимог до захисту	Опитування, тести, завдання
2/2	Тема 3. Кіберзлочинність: кримінально-правові аспекти	Вміння кваліфікувати кіберзлочини, знання санкцій та особливостей призначення покарань	Опитування, тести, завдання
2/2	Тема 4. Процесуальні аспекти розслідування кіберзлочинів	Розуміння особливостей проведення слідчих дій при розслідуванні кіберзлочинів, знання процесуальних гарантій	Опитування, тести, завдання
2/2	Тема 5. Правове регулювання захисту персональних даних у кіберпросторі	Знання прав суб'єктів персональних даних, обов'язків володільців даних та особливостей їх трансферу	Опитування, тести, завдання
2/2	Тема 6. Правові засади електронного урядування та цифровізації	Розуміння правового регулювання електронного документообігу та електронних довірчих послуг	Опитування, тести, завдання
2/4	Тема 7. Секторальне регулювання кібербезпеки	Знання особливостей правового регулювання кібербезпеки у різних галузях економіки	Опитування, тести, завдання
2/2	Тема 8. Правове забезпечення кібероборони	Розуміння правових засад кібероборони та особливостей правового режиму воєнного стану у кіберпросторі	Опитування, тести, завдання
2/2	Тема 9. Правове регулювання кіберстрахування	Знання правових основ кіберстрахування та особливостей договірних відносин	Опитування, тести, завдання
2/2	Тема 10. Правові аспекти реагування на кіберінциденти	Розуміння процедур реагування на кіберінциденти та обов'язків щодо повідомлення	Опитування, тести, завдання
2/2	Тема 11. Правове регулювання аудиту та сертифікації в сфері кібербезпеки	Знання системи технічного регулювання, сертифікації та аудиту у сфері кібербезпеки	Опитування, тести, завдання
2/2	Тема 12. Правові засади кібергігієни та кіберосвіти	Розуміння правового забезпечення кіберосвіти та регулювання безпеки дітей в Інтернеті	Опитування, тести, завдання
2/2	Тема 13. Актуальні проблеми та перспективи розвитку законодавства про кібербезпеку	Знання викликів регулювання нових технологій та перспектив розвитку законодавства	Опитування, тести, завдання
2/2	Тема 14. Міжнародне право кібербезпеки	Розуміння міжнародних угод у сфері кібербезпеки та особливостей їх імплементації	Опитування, тести, завдання

Літературні джерела

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 дотриманням 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). р. 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*. Elk, 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

Політика оцінювання

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 оцінювання	Модульний контроль 1	Поточне оцінювання	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 та 20 тестів по 2 бали кожен	визначається як середнє арифметичне з оцінок на практичних заняттях (тема 8-14)	2 теоретичні питання по 30 балів та 20 тестів по 2 бали кожен	Оцінка визначається 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. ПОТОЧНЕ ОПИТУВАННЯ МОДУЛІВ 1 І 3 (по 10% кожен)

Критерії оцінювання поточного опитування:

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 слабе 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 - слабо 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 поверхнєве розуміння принципів правового регулювання критичної інфраструктури, обмежено розуміє кримінально-правові аспекти кіберзлочинності та міжнародно-правові засади кібербезпеки.

1-15 балів - слабо 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 студентів:

ECTS	Бали	Зміст
A	90-100	відмінно

B	85-89	добре
C	75-84	добре
D	65-74	задовільно
E	60-64	достатньо
FX	35-59	незадовільно з можливістю повторного складання
F	1-34	незадовільно з обов'язковим повторним курсом