

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Волинський національний університет імені Лесі Українки

Юридичний факультет

Кафедра цивільно-правових дисциплін

СИЛАБУС

нормативного освітнього компонента

НОРМАТИВНО-ПРАВОВА БАЗА КІБЕРБЕЗПЕКИ

підготовки бакалавра

спеціальності 125 Кібербезпека та захист інформації

освітньо-професійної програми Інформаційна безпека

Луцьк – 2024

**Силабус нормативного освітнього компонента НОРМАТИВНО-ПРАВОВА
БАЗА КІБЕРБЕЗПЕКИ** підготовки бакалавра, галузі знань 12 Інформаційні
технології, спеціальності 125 Кібербезпека та захист інформації, за освітньо-
професійною програмою Інформаційна безпека

Розробник:

доцент кафедри цивільно-правових дисциплін, канд. юрид. наук Книш Зоряна
Ігорівна

Погоджено

Гарант освітньо-професійної програми:



Чернящук Н.Л.

Силабус ОК затверджено на засіданні кафедри цивільно-правових дисциплін
протокол № 6 від 20.11.2024

Завідувач кафедри



А. В. Духневич

I. Опис освітнього компонента

Найменування показників	Галузь знань, спеціальність, освітньо-професійна програма, освітній рівень	Характеристика освітнього компонента
денна форма навчання	галузь знань 12 Інформаційні технології спеціальність 125 Кібербезпека та захист інформації освітньо-професійна програма Інформаційна безпека Освітній рівень: перший (бакалаврський)	Нормативний
Кількість годин/кредитів: 120/4		Рік навчання: 1
		Семестр: 1
		Лекції 32 год.
ІНДЗ: є		Практичні 36 год.
		Самостійна робота 72 год.
		Консультації 10 год.
		Форма контролю: залік
Мова навчання: українська		

II. Інформація про викладача

Книш Зоряна Ігорівна
Кандидат юридичних наук
Доцент кафедри цивільно-правових дисциплін
Контактна інформація: knysh.zoriana@vnu.edu.ua
Дні занять: <http://194.44.187.20/cgi-bin/timetable.cgi>

III. Опис освітнього компонента

1. Анотація

Освітній компонент «Нормативно-правова база кібербезпеки» відноситься до переліку нормативних дисциплін циклу професійної підготовки бакалавра спеціальності 125 Кібербезпека та захист інформації. Навчальна дисципліна являє собою систему взаємоузгоджених елементів навчального процесу, які зорієнтовані на ознайомлення здобувачів зі змістом основних нормативних актів, які визначають правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки та інформаційної безпеки, захисту інформації, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки та інформаційної безпеки, захисту інформації.

2. Пререквізити

При вивченні освітнього компонента «Нормативно-правова база кібербезпеки» використовуються теоретичні знання та набуті практичні навички пошуку, застосування та тлумачення норм права; користування персональним комп'ютером, роботою в мережі інтернет; загальні та фахові знання, отримані протягом першого семестру.

Постреквізити

Знання, уміння і навички, які сформуються в процесі вивчення дисципліни «Нормативно-правова база кібербезпеки» можуть бути використані здобувачами освіти при опануванні інших освітніх компонентів циклу загальної та професійної підготовки.

3. Мета і завдання освітнього компонента

Мета: формування знань про національну систему кібербезпеки та інформаційної безпеки та захисту інформації, правові засади їх забезпечення; вироблення навичок і вмінь пошуку, тлумачення і застосування норм права у цих сферах.

Завдання:

Сформувати у здобувачів освіти уміння та навички:

здійснювати критичний та системний аналіз правових явищ і застосовувати набуті знання у професійній діяльності;

розуміти особливості правового регулювання відносин у сфері забезпечення кібербезпеки, інформаційної безпеки держави та захисту інформації, забезпечення прав та свобод кожного громадянина України;

діяти на основі нормативно-правової бази України;

здійснювати самостійний пошук, аналіз та синтез правової інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

оволодівати сучасними знаннями, поєднувати юридичні навички з технологічними процесами інших галузей знань.

4. Результати навчання (Компетентності)

За підсумками вивчення освітнього компонента «Нормативно-правова база кібербезпеки» у здобувачів освіти повинен бути сформований відповідний набір компетентностей.

Інтегральна компетентність

Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та захисту інформації і/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

Загальні компетентності

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК 4. Здатність спілкуватися іноземною мовою.

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні.

ЗК 7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

ЗК 8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

Спеціальні (фахові, предметні) компетентності

СК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності.

СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною, кібербезпекою.

Після вивчення освітнього компонента здобувачі освіти повинні продемонструвати такі результати навчання:

РН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

РН 3. Застосовувати принципи неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.

РН 4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН 5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН 6. Адаптуватися в умовах часткої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

РН 9 Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

ПРН 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

5. Структура освітнього компонента

Назви змістових модулів і тем	Усього	Лек.	Практ.	Сам. роб.	Конс.	Форма контролю / бали
Змістовий модуль 1. Кібербезпека як складова системи захисту національної безпеки України						
Тема 1. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України.	10	2	2	6	1	ДС/Т 2
Тема 2. Правові основи забезпечення кібербезпеки України. Міжнародне співробітництво у сфері кібербезпеки.	9	2	2	6		РМГ/Д Б/Т 2
Тема 3. Захист прав, свобод і законних інтересів громадян України у кіберпросторі.	9	2	2	5	1	РЗ/К/Т 2
Тема 4. Об'єкти кібербезпеки та кіберзахисту	9	2	4	5	1	РМГ/Т 2
Тема 5-6. Правовий статус суб'єктів забезпечення кібербезпеки. Державна служба спеціального зв'язку та захисту інформації України	10	4	4	5		РМГ/Д С/Т 4
Модульна контрольна робота № 1						20
Разом за 1 модулем	47	12	14	27	3	32
Змістовий модуль 2.						
Інформаційна безпека як складова частина національної безпеки України						
Тема 7. Нормативно-правове регулювання інформаційних відносин в	9	2	2	5	1	РЗ/К/Т 2

Україні						
Тема 8. Нормативно-правове забезпечення інформаційної безпеки в Україні	8	2	2	5	1	ДС/Т 2
Тема 9. Забезпечення захисту прав і свобод людини в інформаційній сфері	8	2	2	5	1	РЗ/К/Т 2
Тема 10. Технологія blockchain як складова інформаційної безпеки	8	2	2	5	1	ДС/Т 2
Тема 11. Кібербезпека та захист персональних даних	7	2	2	5		РЗ/К/Т 2
Тема 12. Інформаційна безпека у системі електронного урядування	8	2	2	5	1	ДС/Р/Т 2
Тема 13. Захист інформації в системах електронного документообігу	7	2	2	5		ДС/Т 2
Модульна контрольна робота № 2						20
Разом за 2 модулем	55	14	14	35	5	34
Змістовий модуль 3.						
Відповідальність за порушення законодавства у сфері кібербезпеки						
Тема 14. Контроль за законністю заходів із забезпечення кібербезпеки України	9	2	4	5	1	ДС/Т 2
Тема 15. Відповідальність за порушення законодавства у сфері кібербезпеки	9	4	4	5	1	ДС/РЗ/ К/Т 2
Модульна контрольна робота № 3						20
Разом за 3 модулем	18	6	8	10	2	24
ІНДЗ						10
ВСЬОГО поточне оцінювання						100
Всього годин / Балів	150	32	36	72	10	100

6. Завдання для самостійного опрацювання

Самостійна робота є складовою частиною навчального процесу, від якої значною мірою залежить засвоєння навчального матеріалу, формування правової культури.

Навчальний матеріал освітнього компонента «Нормативно-правова база кібербезпеки», передбачений для засвоєння здобувачами освіти в процесі самостійної роботи, виноситься на підсумковий контроль поряд з навчальним матеріалом, який опрацьовувався під час аудиторних навчальних занять.

Під час організації навчальної самостійної роботи викладач ставить перед здобувачами освіти цілі, пов'язані з необхідністю засвоєння навчального матеріалу, і пропонує їм самостійно, досягнути цих цілей. Залежно від задуму він визначає час здійснення самостійної роботи в процесі навчальних занять, узгоджує її з іншими видами навчальної діяльності, пропонує конкретні завдання, проводить інструктаж щодо їх виконання, з'ясовує повноту, глибину та обсяг обов'язкового виконання завдань, здійснює допоміжні заходи з опосередкованого управління діяльністю здобувачів освіти і діагностики якості самостійної роботи (консультації, спостереження, співбесіди тощо).

Форми самостійної роботи здобувачів освіти з освітнього компонента «Нормативно-правова база кібербезпеки»:

- опрацювання теоретичних основ прослуханого лекційного матеріалу;
- вивчення окремих тем або питань, що передбачені для самостійного опрацювання;
- підготовка до лабораторних занять;
- підготовка до різних форм поточного контролю;

систематизація вивченого матеріалу дисципліни перед написанням модульної контрольної роботи;

підготовка реферативної доповіді або презентації;
пошук (підбір) джерел для підготовки презентацій за заданою тематикою.

IV. Політика оцінювання

Політика викладача щодо здобувача освіти

Під час формування лекційного матеріалу та завдань до лабораторних робіт, викладач створює умови для найбільш ефективного засвоєння здобувачем освіти знань в рамках пропонованого освітнього компонента. Досягненню відповідної мети слугує, зокрема визначення тих питань, що за рівнем складності можуть бути вивчені здобувачем освіти в рамках самопідготовки.

При цьому у процесі викладання освітнього компонента викладач використовує сучасні наукові методи, спрямовані зокрема на розвиток у здобувачів освіти критичного мислення і вміння самостійно аналізувати обставини правової реальності та давати їм оцінку в контексті положень чинного законодавства України і норм міжнародного права.

Відвідування лекційних і лабораторних занять здобувачем освіти покликане забезпечити отримання ним концентрованих знань, що досягається у тому числі безпосередньою участю в обговоренні відповідної тематики, а також зверненням до викладача із запитаннями з метою конкретизації тих чи інших аспектів предмету розгляду. Разом із цим для забезпечення освітнього компонента викладач використовує сучасні технології, зокрема хмарні сервіси і освітні платформи чим створює можливості для самостійного ефективного засвоєння здобувачем освіти пропонованого матеріалу у межах елементів структури освітнього компонента. У зв'язку з цим, якщо інше не встановлено положеннями нормативно-правових документів Університету, здобувач освіти, який пропустив лекційне або лабораторне заняття, може самостійно опрацювати відповідний матеріал і пройти контроль знань з використанням відповідних електронних сервісів або ж пройти контроль знань на одному з практичних аудиторних занять. Також у разі необхідності здобувач освіти може відвідати консультацію з конкретної теми для заповнення прогалин у знаннях.

Політика щодо академічної доброчесності

Дотримання академічної доброчесності педагогічними, науково-педагогічними та науковими працівниками передбачає:

- посилення на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про методики і результати досліджень, джерела використаної інформації та власну педагогічну (науково-педагогічну, творчу) діяльність;
- контроль за дотриманням академічної доброчесності здобувачами освіти;
- об'єктивне оцінювання результатів навчання.

Дотримання академічної доброчесності здобувачами освіти передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);
- посилення на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

Порушенням академічної доброчесності вважається:

академічний плагіат - оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів власного дослідження (творчості) та/або відтворення опублікованих текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;

самоплагіат - оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів;

фабрикація - вигадкування даних чи фактів, що використовуються в освітньому процесі або наукових дослідженнях;

фальсифікація - свідомо зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень;

списування - виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання, зокрема під час оцінювання результатів навчання;

обман - надання завідомо неправдивої інформації щодо власної освітньої (наукової, творчої) діяльності чи організації освітнього процесу; формами обману є, зокрема, академічний плагіат, самоплагіат, фабрикація, фальсифікація та списування;

хабарництво - надання (отримання) учасником освітнього процесу чи пропозиція щодо надання (отримання) коштів, майна, послуг, пільг чи будь-яких інших благ матеріального або нематеріального характеру з метою отримання неправомірної переваги в освітньому процесі;

необ'єктивне оцінювання - свідоме завищення або заниження оцінки результатів навчання здобувачів освіти;

надання здобувачам освіти під час проходження ними оцінювання результатів навчання допомоги чи створення перешкод, не передбачених умовами та/або процедурами проходження такого оцінювання;

вплив у будь-якій формі (прохання, умовляння, вказівка, погроза, примушування тощо) на педагогічного (науково-педагогічного) працівника з метою здійснення ним необ'єктивного оцінювання результатів навчання.

Політика щодо дедлайнів та перескладання

Поточний контроль за темами освітнього компонента здійснюється в рамках практичних занять, що проводяться згідно з розкладом.

Здобувач освіти має право повторно скласти поточний контроль за темою лише один раз.

Якщо тема передбачає надання здобувачем освіти усної відповіді щодо питань плану теми, а також вирішення юридичної задачі, здобувач освіти має право повторно скласти ту частину (ті частини) завдань, за які ним одержані бали нижче максимальних.

Зараховується найбільший результат, одержаний здобувачем освіти за результатами складання відповідної частини завдань або їх повторного складання.

Ліквідація академічної заборгованості здійснюється централізовано для всіх здобувачів освіти у визначений викладачем час до дати, встановленої для повторного проведення іспиту («перша, друга та третя відомості»).

V. Підсумковий контроль

Підсумковий контроль здійснюється у формі заліку, що полягає в оцінці засвоєння здобувачем освіти навчального матеріалу з освітнього компонента на підставі результатів виконання всіх видів запланованої навчальної роботи протягом семестру: аудиторної роботи під час лекційних, практичних (семінарських, індивідуальних), практичних занять (тощо) самостійної роботи, виконання ІНДЗ, модульних робіт тощо.

Підсумковий модульний контроль здійснюється після завершення вивчення тем змістового модуля у формі виконання здобувачем освіти модульного контрольного завдання.

Підсумкова модульна оцінка визначається в балах як сума поточної та контрольної модульних оцінок. Модуль зараховується здобувачеві, якщо він успішно виконав всі види навчальної роботи, передбачені силабусом освітнього компонента.

Перескладання будь-яких видів робіт, передбачених силабусом освітнього компонента, з метою підвищення підсумкової модульної оцінки не дозволяється. Заборгованість із модуля повинна бути ліквідована здобувачем у позааудиторний час до початку підсумкового контролю з наступного модуля. Кінцевий термін ліквідації заборгованості з модульного контролю обмежується початком заліково-екзаменаційної сесії.

Залік викладач виставляє за результатами поточної роботи за умови, що здобувач освіти виконав ті види навчальної роботи, які визначено силабусом (програмою) освітнього компонента. Мінімальна позитивна кількість балів – 60.

У випадку, якщо здобувач освіти не відвідував окремі аудиторні заняття (з поважних причин), на консультаціях він має право відпрацювати пропущені заняття та добрати ту кількість балів, яку було визначено на пропущені теми. У дату складання заліку викладач записує у відомість суму поточних балів, які здобувач освіти набрав під час поточної роботи (шкала від 0 до 100 балів).

У випадку, якщо здобувач освіти набрав менше ніж 60 балів, він складає залік під час ліквідації академічної заборгованості шляхом виконання комплексного контрольного завдання у формі тестів. У цьому випадку бали, набрані під час поточного оцінювання, анулюються. Максимальна кількість балів під час ліквідації академічної заборгованості з заліку – 100.

Повторне складання заліку з освітнього компоненту допускається не більше як два рази: один раз – викладачеві, другий – комісії, яку створює декан (директор) факультету (інституту).

Залік відбувається в період заліково-екзаменаційної сесії, передбаченої навчальним планом, згідно із затвердженим графіком освітнього процесу і розкладом.

Перелік питань для підготовки до заліку

1. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України.
2. Національний кіберпростір: сучасні виклики та кіберзагрози.
3. Основні напрямки розбудови національної системи кібербезпеки.
4. Державна політика у сфері кібербезпеки в Україні.
5. Правові основи забезпечення кібербезпеки України.
6. Принципи застосування законодавства у сфері кібербезпеки.
7. Основні положення Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447/2021.
8. Принципи забезпечення кібербезпеки.
9. Кіберзагроза: поняття та правовий зміст.
10. Класифікація кіберзагроз та їх зміст.
11. Захист прав, свобод і законних інтересів громадян України у кіберпросторі.
12. Об'єкти кібербезпеки.
13. Об'єкти кіберзахисту.
14. Правові та організаційні засади створення та функціонування національної системи захисту критичної інфраструктури.

15. Суб'єкти забезпечення кібербезпеки: поняття та види.
16. Правовий статус основних суб'єктів національної системи кібербезпеки: Державної служби спеціального зв'язку та захисту інформації України, Національної поліції України, Служби безпеки України, Міністерства оборони України та Генерального штабу Збройних Сил України, розвідувальних органів, Національного банку України.
17. Державна служба спеціального зв'язку та захисту інформації України як один із основних суб'єктів забезпечення кібербезпеки України.
18. Нормативно-правові акти Державної служби спеціального зв'язку та захисту інформації України.
19. Інформаційна безпека та її місце в системі національної безпеки України.
20. Нормативно-правове регулювання відносин щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.
21. Нормативно-правове забезпечення інформаційної безпеки в Україні.
22. Основні положення Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28 грудня 2021 року № 685/2021.
23. Забезпечення захисту прав і свобод людини в інформаційній сфері.
24. Технологія blockchain як складова інформаційної безпеки.
25. Кібербезпека та захист персональних даних.
26. Правове регулювання відносин, пов'язаних із захистом і обробкою персональних даних.
27. Захист персональних даних: міжнародні стандарти та законодавство України.
28. Правовий статус суб'єктів відносин, пов'язаних із персональними даними.
29. Кібербезпека та інтернет речей: правове регулювання.
30. Правове регулювання відносин, пов'язаних із забезпеченням доступу до публічної інформації.
31. Інформаційна безпека у системі електронного урядування.
32. Захист інформації в системах електронного документообігу.
33. Захист інформації та кіберзахист у платіжних системах.
34. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.
35. Правові аспекти регулювання відносин у соціальних мережах.
36. Відповідальність за порушення законодавства у сфері кібербезпеки.
37. Поняття та види кіберзлочинів.
38. Кримінальна відповідальність за кіберзлочини.
39. Поняття та види форм адміністративно-правової протидії кіберзлочинності в Україні.
40. Фінансове забезпечення заходів кібербезпеки.
41. Контроль за законністю заходів із забезпечення кібербезпеки України.
42. Напрями зовнішньополітичної діяльності України у сфері кібербезпеки.
43. Міжнародне співробітництво у сфері кібербезпеки.

VI. Шкала оцінювання

Оцінка в балах	Лінгвістична оцінка
90–100	Зараховано
82–89	
75–81	
67–74	

60–66	
1–59	Незараховано (необхідне перекладання)

VII. Рекомендована література та інтернет-ресурси

Законодавство

1. Конституція України. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>
2. Конвенція про кіберзлочинність: ратифікована із застереженнями і заявами Законом №2824-IV від 07.09.2005. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
3. Загальна декларація прав людини. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text
4. Конвенція про захист прав людини і основоположних свобод. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text
5. Кодекс України про адміністративні правопорушення від 7 грудня 1984 року №8073-X. URL: <https://zakon.rada.gov.ua/laws/show/80731-10#Text>
6. Кримінальний кодекс України від 5 квітня 2001 року №2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>
7. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23 лютого 2006 року №3475-IV. URL: <https://zakon.rada.gov.ua/laws/show/3475-15#Text>
8. Про доступ до публічної інформації: Закон України від 13 січня 2011 року №2939-VI. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#top>
9. Про електронні довірчі послуги: Закон України від 5 жовтня 2017 року №2155-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>
10. Про електронні документи та електронний документообіг: закон України від 22 травня 2003 року №851-IV URL: <https://zakon.rada.gov.ua/laws/show/851-15#Text>
11. Про електронні комунікації: Закон України від 16 грудня 2020 року №1089-IX. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text>
12. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: Закон України від 6 грудня 2019 року №361-IX URL: <https://zakon.rada.gov.ua/laws/show/361-20#Text>
13. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 5 липня 1994 року №80/94-BP. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>
14. Про захист персональних даних: Закон України від 1 червня 2010 року №2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
15. Про інформацію: закон України від 2 жовтня 1992 року №2657-XII URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
16. Про критичну інфраструктуру: Закон України від 16 листопада 2021 року №1882-IX. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text> (введення в дію, відбудеться 15.06.2022)
17. Про національну безпеку України: Закон України 21 червня 2018 року №2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
18. Про оборону України: Закон України від 6 грудня 1991 року №1932-XII. URL: <https://zakon.rada.gov.ua/laws/show/1932-12#n168>
19. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року №2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
20. Про науково-технічну інформацію: Закон України від 25 червня 1993 року №3322-XII. URL: <https://zakon.rada.gov.ua/laws/show/3322-12#top>

21. Про особливості надання публічних (електронних публічних) послуг: Закон України від 15 липня 2021 року №1689-IX. URL: <https://zakon.rada.gov.ua/laws/show/1689-20#Text>
22. Про державну таємницю. Закон України від 21 січня 1994 року № 3855-XII. URL: <https://zakon.rada.gov.ua/laws/show/3855-12#Text>
23. Стратегія інформаційної безпеки: затв. Указом Президента України від 28 грудня 2021 року №685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#n7>
24. Стратегія кібербезпеки України: затв. Указом Президента України від 26 серпня 2021 року №447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#n12>
25. Стратегія національної безпеки України: затв. Указом Президента України від 14 вересня 2020 року № 392/2020. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#n12>
26. Положення про Національний координаційний центр кібербезпеки: затв. Указом Президента України від 7 червня 2016 року №242/2016. URL: <https://zakon.rada.gov.ua/laws/show/242/2016#Text>
27. Деякі питання електронної взаємодії електронних інформаційних ресурсів: постанова Кабінету Міністрів України від 8 вересня 2016 р. №606. URL: <https://zakon.rada.gov.ua/laws/show/606-2016-%D0%BF#Text>
28. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури: затв. постановою Кабінету Міністрів України від 19 червня 2019 р. №518. URL: <https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text>
29. Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних: затв. постановою Кабінету міністрів України від 21 жовтня 2015 р. №835. URL: <https://zakon.rada.gov.ua/laws/show/835-2015-%D0%BF#Text>
30. Порядок проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом: затв. постановою Кабінету Міністрів України від 11 листопада 2020 р. №1176. URL: <https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#n8>
31. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: затв. постановою Кабінету Міністрів України від 29 березня 2006 р. №373. URL: <https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text>
32. Про утворення територіального органу Національної поліції: постанова Кабінету Міністрів України від 13 жовтня 2015 р. №831. URL: <https://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF#Text>
33. Положення про захист інформації та кіберзахист у платіжних системах: затв. Постановою Правління Національного банку України 19.05.2021 №43. URL: <https://zakon.rada.gov.ua/laws/show/v0043500-21#Text>
34. Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та просертифікацію кібербезпеки інформаційно-комунікаційних технологій». URL: https://zakon.rada.gov.ua/laws/show/984_024-19#Text

Література

1. Біленчук П. Д., Обіход Т. В. Кібербезпека і засоби запобігання та протидії кіберзлочинності й кібертероризму. *Часопис Київського університету права*. 2018. №3. С. 235–239. URL: http://nbuv.gov.ua/UJRN/Chkup_2018_3_54
2. Білявська Ю., Микитенко Н, Шестак Я. Кібербезпека та захист інформації під час пандемії COVID-19. *Товари і ринки*. 2021. №1. С. 34–46. URL: http://nbuv.gov.ua/UJRN/tovary_2021_1_5

3. Бойко В. Д., Василенко М. Д., Кухаренко С. В. Кібербезпека в ЄС та країнах-членах: генезис та проблеми її підвищення. *Інформаційна безпека людини, суспільства, держави*. 2019. №3. С. 57–69. URL: http://nbuv.gov.ua/UJRN/iblsd_2019_3_8
4. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект. Львів : Магнолія – 2006, 2018. 320 с.
5. Бутузов В. Співвідношення понять «комп'ютерна злочинність» та «кіберзлочинність». *Інформаційна безпека людини, суспільства, держави*. 2010. №1 (3). С. 16–18.
6. Войціховський А. В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. *Журнал східноєвропейського права*. 2018. №53. С. 26–37. URL: http://nbuv.gov.ua/UJRN/jousepr_2018_53_6
7. Горлинський В., Горлинський Б. Кібербезпека як складова інформаційної безпеки України. *Information Technology and Security*. 2019. Vol. 7, Iss. 2. С. 136–148. URL: http://nbuv.gov.ua/UJRN/inftech_2019_7_2_5
8. Гуцалюк М. В. Напрями посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю. *Інформація і право*. 2021. № 4. С. 141–147. URL: http://nbuv.gov.ua/UJRN/Infpr_2021_4_16
9. Гуцалюк М. В. Шляхи посилення спроможностей правоохоронних та інших державних органів у сфері боротьби з кіберзлочинністю. *Інформація і право*. 2020. №3. С. 75–87. URL: http://nbuv.gov.ua/UJRN/Infpr_2020_3_11
10. Даник Ю. Г. Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібероборони : підручник. Вид. 2-ге, перероб. та доп. Одеса.: ОНАЗ ім. О. С. Попова, 2019. 320 с.
11. Дзюндзюк В. Б., Котух Є. В. Кібербезпека як один з пріоритетів національної політики. *Державне будівництво*. 2020. № 2. URL: http://nbuv.gov.ua/UJRN/DeBu_2020_2_4
12. Діденко А. С. Мета, завдання та принципи державної політики у сфері протидії кіберзлочинності. *Право і Безпека*. 2020. №1. С. 53–59. URL: http://nbuv.gov.ua/UJRN/Pib_2020_1_9
13. Ємельянов В. М. Бондар Г. Л. Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури України. *Публічне управління та регіональний розвиток*. 2019. №5. С. 493–523. URL: http://nbuv.gov.ua/UJRN/purr_2019_5_4
14. Жеребець О. М. Реалізація державної політики у сфері протидії кіберзлочинності: законодавчий аспект. *Інформація і право*. 2021. №4. С. 129–134. URL: http://nbuv.gov.ua/UJRN/Infpr_2021_4_14
15. Звоздецька О. Я. Кібербезпека ЄС в умовах посилення кіберзагроз в сучасному глобалізованому світі. *Медіафорум: аналітика, прогнози, інформаційний менеджмент*. 2019. Т. 7. С. 27–46. URL: http://nbuv.gov.ua/UJRN/mfapim_2019_7_4
16. Кіберняні. *Дія. Цифрова освіта*. URL: <https://osvita.diia.gov.ua/courses/cybernanny>
17. Кіндзерський Ю. В. Кібербезпека та становлення цифрової економіки: проблеми взаємозв'язку. *Економічний вісник Дніпровської політехніки*. 2020. №3. С. 18–26. URL: http://nbuv.gov.ua/UJRN/evngu_2020_3_4
18. Ковалів М. В., Єсімов С. С., Ярема О. Г. Інформаційне право України : навч. посіб. Львів : Львівський державний університет внутрішніх справ, 2022. 416 с. URL: <https://dspace.lvduvs.edu.ua/bitstream/1234567890/4844/1/InformPravoUKR.pdf>
19. Кормич Б. А., Міщенко І. В. Інформаційне право України : навч.-метод. посіб. (для студ. ден. та заоч. форми навч.). Одеса : НУ «Одеська юридична академія» 2021. 45 с. URL: <http://dspace.onua.edu.ua/handle/11300/16014>
20. Маковець О. П., Дрозд І. К. Кібербезпека як фактор фінансової безпеки підприємства. *Економіка. Фінанси. Право*. 2020. №5 (3). С. 31–35.
21. Малишева Н. Р. Кібербезпека космічної діяльності та можливості її забезпечення засобами міжнародного права. *Правова держава*. 2021. Вип. 32. С. 245–257. URL: http://nbuv.gov.ua/UJRN/PrDe_2021_32_28

22. Манжай О. В., Манжай І. А. Правові засади захисту інформації : підручник. Харків : Панов, 2020. 162 с.
23. Муляр Г. В., Ховпун О. С. Особливості доказування кіберзлочинів. *Право. Людина. Довкілля*. 2019. Vol. 10, № 3. С. 132–138. URL: http://nbuv.gov.ua/UJRN/IHE_2019_10_3_19
24. Основи кібергігієни. *Дія. Цифрова освіта*. URL: <https://osvita.diia.gov.ua/courses/cyber-hygiene>
25. Попередній аналітичний звіт комітету Верховної ради України з питань цифрової трансформації про контроль за виконанням Закону України «Про основні засади кібербезпеки в Україні». Березень 2020 року. URL: https://www.ua.undp.org/content/dam/ukraine/img/demgov/Rada%20for%20Europe/Report_on_Cybersecurity_02.pdf
26. Савчук М. М. Захист інформаційних технологій та кібербезпека (стенограма наукової доповіді на засіданні Президії НАН України 25 верес. 2019 р.). *Вісник Національної академії наук України*. 2019. №11. С. 23–28. URL: http://nbuv.gov.ua/UJRN/vnanu_2019_11_6
27. Саєнко М. І., Савела Є. А., Тополянський Ю. Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Наук. вісн. Ужгород. нац. ун-ту. Серія : Право*. 2021. Вип. 64. С. 386–391. URL: http://nbuv.gov.ua/UJRN/nvuzhpr_2021_64_74
28. Скибун О. Ж. Кібербезпека систем електронних комунікацій органів державної влади України. *Вісн. Нац. акад. держ. управління при Президентові України. Серія : Державне управління*. 2021. № 1. С. 30–39. URL: http://nbuv.gov.ua/UJRN/vnaddy_2021_1_6
29. Сліпченко Т. О. Кібербезпека як складова системи захисту національної безпеки: європейський досвід. *Актуальні проблеми правознавства*. 2020. Вип. 1. С. 128–133. URL: http://nbuv.gov.ua/UJRN/aprpr_2020_1_22
30. Сопілко І. М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Юридичний вісник. Повітряне і космічне право*. 2021. №2. С. 110–115. URL: http://nbuv.gov.ua/UJRN/Npnau_2021_2_16
31. Стежко С. М., Фица В. М. Кібербезпека як важливий фактор забезпечення життєдіяльності вітчизняної енергетичної галузі. *Інформація і право*. 2021. №4. С. 113–120. URL: http://nbuv.gov.ua/UJRN/Infpr_2021_4_12
32. Філінович В. В. Кібербезпека та Інтернет речей: правовий аспект. *Юридичний вісник. Повітряне і космічне право*. 2020. №4. С. 122–127. URL: http://nbuv.gov.ua/UJRN/Npnau_2020_4_19
33. Форос Г. В., Жогов В. С. Особливості трактування поняття «кібербезпека» в сучасній юридичній науці. *Правова держава*. 2019. №33. С. 128–134. URL: http://nbuv.gov.ua/UJRN/Prav_2019_33_20