

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Правове забезпечення інформаційної безпеки
в умовах сталого розвитку»

Рівень вищої освіти	Магістр
Ступінь вищої освіти	Магістр
Освітньо-професійна програма	Право
Заняття:	II семестр
Лекції	3, 4 чверті - 1 година на тиждень
Семінарські	1 година на тиждень
Кількість кредитів	3
Мова викладання	Українська



Інформація про викладача

Прізвище, ім'я, по батькові	Блінова Ганна Олександрівна
Науковий ступінь	доктор юридичних наук
Наукове звання	професор
Посада	професор кафедри цивільного, господарського та екологічного права НТУ «Дніпровська політехніка»
Контакти	Роб.тел. 0562-756-09-91; моб: 0967917242
E-mail	blinovahanna@i.ua Blinova.G.O@nmu.one
Профайл	http://cgp.nmu.org.ua/ua/vykl.php
Персональна сторінка	https://scholar.google.com.ua/citations?user=ySm66L0AAAAJ&hl=ru
Сторінка курсу в СДО НТУ «ДП»	https://do.nmu.org.ua/course/view.php?id=6829
Консультації	ауд.10/314, 1 година на тиждень (згідно графіку індивідуальних консультацій, що розміщений на інформаційному стенді кафедри)
Місце	Національний технічний університет «Дніпровська політехніка», 49005 м. Дніпро, пр. Дмитра Яворницького, 19; 10 корпус, 3 поверх, ауд. 314
Онлайн-консультації	електронна пошта (щоденно, окрім вихідних і святкових днів) Blinova.G.O@nmu.one

1. Анотація до курсу

Навчальна дисципліна призначена для студентів юридичних спеціальностей та всіх, хто цікавиться взаємозв'язком права та інформаційної безпеки фізичних, юридичних осіб, органів публічної влади та держави.

Дисципліна «Правове забезпечення інформаційної безпеки в умовах сталого розвитку» спрямована на : висвітлення актуальних питань правового регулювання засад інформаційної безпеки; характеристику повноважень органів, що утворюють систему суб'єктів забезпечення інформаційної безпеки держави; розкриття змісту положень національних та міжнародних нормативно-правових актів щодо засад обігу персональних даних фізичних осіб; визначення правових засад забезпечення кібербезпеки та порядку використання державних інформаційних ресурсів; аналіз актуальної судової практики у цій сфері та на виявлення недоліків правового регулювання інформаційної безпеки в Україні; спрямована на розкриття змісту основних прийомів і способів вирішення правозастосовних проблем у цій сфері; допомагає виробити навички щодо правового аналізу та наукового обґрунтування напрямів удосконалення чинного законодавства у сфері інформаційної безпеки в умовах сталого розвитку.

2. Мета та завдання навчальної дисципліни

Метою вивчення навчальної дисципліни «Правове забезпечення інформаційної безпеки в умовах сталого розвитку» є формування системи теоретичних знань здобувачів вищої освіти про основні положення права та засади правового регулювання суспільних відносин у сфері інформаційної безпеки; формування навичок використання правничої термінології в професійній діяльності; засвоєння здобувачами вищої освіти норм галузі інформаційного права; підвищення рівня правової культури і правосвідомості у здобувачів вищої освіти для забезпечення неухильного дотримання ними вимог закону та кваліфікованого його застосування під час своєї професійної діяльності.

Завдання курсу:

- розкрити зміст основних понять та концепцій, пов'язаних із забезпеченням інформаційної безпеки та кібербезпеки фізичних, юридичних осіб, органів публічної влади та держави;
- висвітлити діючу державну політику у сфері інформаційної безпеки держави, визначити основні стратегії та програми щодо її реалізації;
- розкрити існуючі підходи до правового регулювання діяльності суб'єктів забезпечення інформаційної безпеки в Україні;
- проаналізувати інтеграційні процеси в Європейському Союзі та їх вплив на регулювання діяльності суб'єктів забезпечення інформаційної безпеки в Україні;
- сформулювати у здобувачів знання та вміння здійснювати аналіз положень сучасного законодавства у сфері інформаційної безпеки та застосовувати їх;
- розвинути у здобувачів навички, що дозволять їм на основі теорії проаналізувати і знайти правове рішення спорів у сфері забезпечення інформаційної безпеки.

3. Результати навчання

Дисциплінарні результати навчання (ДРН)
Зміст
Проводити збір інформації про суб'єктний склад, зміст, особливості, правове регулювання та практику його застосування щодо суспільних відносин у сфері інформаційної безпеки, інтегрований аналіз цих відомостей та узагальнення матеріалів з різних джерел, включаючи наукову та професійну літературу, бази даних, цифрові, статистичні, тестові та інші, перевіряти їх на достовірність, використовуючи сучасні методи дослідження.
Використовувати у своїй діяльності алгоритми забезпечення інформаційної безпеки з урахуванням яких здійснювати презентацію свого дослідження з правової теми, застосовуючи першоджерела та прийоми правової інтерпретації складних комплексних проблем, що постають з цього дослідження, аргументувати висновки.
Оцінювати достовірність інформації та надійність її джерел з урахуванням положень нормативно-правових актів у сфері інформаційної безпеки, ефективно опрацьовувати та використовувати бази даних для проведення наукових досліджень та правозастосовної діяльності у тому числі у сфері інформаційної безпеки в умовах сталого розвитку України.

4. Структура курсу

Лекційні заняття
Тема 1. Інформаційне право та інформаційна безпека. Національні інтереси в інформаційній сфері та інформаційний суверенітет держави.
Тема 2. Система забезпечення інформаційної безпеки України в умовах сталого розвитку. Загрози інформаційній безпеці держави, суспільства, особи.
Тема 3. Правове регулювання обігу інформації та електронне урядування в умовах сталого розвитку України. Інформація з обмеженим доступом, її види та правові засади захисту.
Тема 4. Державна таємниця та організаційно-правовий механізм її захисту
Тема 5. Нормативно-правове регулювання захисту персональних даних в Україні
Тема 6. Міжнародні правові стандарти захисту даних.
Тема 7. Державні інформаційні ресурси в умовах реалізації цілей сталого розвитку України та правові засади забезпечення їх безпеки.
Тема 8. Кібербезпека як складова інформаційної безпеки держави. Проблеми та перспективи забезпечення кібербезпеки в умовах сталого розвитку України.
Тема 9. Боротьба з кіберзлочинністю. Відповідальність за порушення вимог інформаційної безпеки.
Семінарські заняття
Тема 1. Інформаційне право та інформаційна безпека. Національні інтереси в інформаційній сфері та інформаційний суверенітет держави.
Тема 2. Система забезпечення інформаційної безпеки України в умовах сталого розвитку. Загрози інформаційній безпеці держави, суспільства, особи.
Тема 3. Правове регулювання обігу інформації та електронне урядування в умовах сталого розвитку України. Інформація з обмеженим доступом, її види та правові засади захисту.
Тема 4. Державна таємниця та організаційно-правовий механізм її захисту
Тема 5. Нормативно-правове регулювання захисту персональних даних в Україні
Тема 6. Міжнародні правові стандарти захисту даних.

Тема 7. Державні інформаційні ресурси в умовах реалізації цілей сталого розвитку України та правові засади забезпечення їх безпеки.

Тема 8. Кібербезпека як складова інформаційної безпеки держави. Проблеми та перспективи забезпечення кібербезпеки в умовах сталого розвитку України.

Тема 9. Боротьба з кіберзлочинністю. Відповідальність за порушення вимог інформаційної безпеки.

5. Технічне обладнання та/або програмне забезпечення

Спеціально обладнана проектором аудиторія 10/307 або 10/310 для проведення лекційних та семінарських занять.

Технічні засоби навчання: 1) мультимедійне обладнання; 2) інформаційно-комунікаційні засоби; 3) персональні комп'ютери.

Студент повинен мати активований аккаунт університетської пошти (student.i.p@nmu.one) на Office 365 та бути зареєстрованим у СУДН «Moodle» 7 на дистанційний курс з навчальної дисципліни «Правове забезпечення інформаційної безпеки в умовах сталого розвитку».

6. Система оцінювання та вимоги

Оцінювання досягнень здобувачів здійснюється за допомогою прозорих процедур, що ґрунтуються на об'єктивних критеріях відповідно до Положення НТУ

«Дніпровська політехніка» «Про оцінювання результатів навчання здобувачів вищої освіти НТУ «Дніпровська політехніка»».

Досягнутий рівень компетентностей відносно очікуваних, що ідентифікований під час контрольних заходів, відображає реальний результат навчання здобувача вищої освіти за дисципліною.

6.1 Шкали

Оцінювання навчальних досягнень здобувачів вищої освіти НТУ «Дніпровська політехніка» здійснюється за рейтинговою (100-бальною) та інституційною шкалами. Остання необхідна (за офіційною відсутністю національної шкали) для конвертації (переведення) оцінок мобільних здобувачів.

Шкали оцінювання навчальних досягнень здобувачів вищої освіти НТУ «ДП»

Рейтингова	Інституційна
90 – 100	Відмінно
74 – 89	Добре
60 – 73	Задовільно
0 – 59	Незадовільно

Кредити ЄКТС навчальної дисципліни зараховується, якщо здобувач вищої освіти отримав підсумкову оцінку не менше 60-ти балів. Нижча оцінка вважається академічною заборгованістю, що підлягає ліквідації відповідно до Положення про організацію освітнього процесу НТУ «Дніпровська політехніка».

6.2 Засоби та процедури

Зміст засобів діагностики спрямовано на контроль рівня сформованості знань, умінь/навичок, комунікації, автономії та відповідальності здобувача вищої освіти за вимогами НРК до 7-го кваліфікаційного рівня під час демонстрації регламентованих робочою програмою результатів навчання.

Здобувач вищої освіти на контрольних заходах має виконувати завдання, орієнтовані виключно на демонстрацію дисциплінарних результатів навчання (розділ2).

Засоби діагностики, що надаються здобувачам вищої освіти на контрольних заходах у вигляді завдань для поточного та підсумкового контролю, формуються шляхом конкретизації вихідних даних та способу демонстрації дисциплінарних результатів навчання.

Засоби діагностики (контрольні завдання) для поточного та підсумкового контролю дисципліни затверджуються кафедрою.

Види засобів діагностики та процедур оцінювання для поточного та підсумкового контролю дисципліни подано нижче.

Під час поточного контролю лекційні заняття оцінюються шляхом тестування, усного опитування за кожною темою навчальної дисципліни. Семінарські заняття оцінюються якістю підготовки презентації та виступу на занятті за певною темою

За наявності рівня результатів поточних контролів з усіх видів навчальних занять не менше 60 балів, підсумковий контроль здійснюється без участі здобувача шляхом визначення середньозваженого значення поточних оцінок.

Засоби діагностики та процедури оцінювання

ПОТОЧНИЙ КОНТРОЛЬ			ПІДСУМКОВИЙ КОНТРОЛЬ	
Навчальне заняття	засоби діагностики	процедури	засоби діагностики	процедури
Лекції	контрольні завдання за кожною темою	методи евристичних питань, мозкового штурму, діалогового спілкування	комплексна контрольна робота (ККР)	визначення середньозваженого результату поточних контролів;
Семінарські заняття	контрольні завдання за кожною темою	усне опитування, тестування, виконання завдань під час семінарського заняття виступ-презентація, робота в малих групах, реферат/ ессе/ наукова доповідь		виконання ККР під час заліку за бажанням здобувача вищої освіти

Незалежно від результатів поточного контролю кожен здобувач вищої освіти під час заліку має право пройти підсумкове тестування, яке містить питання, що охоплюють ключові дисциплінарні результати навчання.

6.3 Реальні результати навчання здобувача вищої освіти ідентифікуються та вимірюються відносно очікуваних під час контрольних заходів за допомогою критеріїв, що описують дії здобувача для демонстрації досягнення результатів навчання.

Оцінювання з курсу навчальної дисципліни «Правове забезпечення інформаційної безпеки в умовах сталого розвитку» здійснюється з урахуванням розподілу отриманих балів за відповідний вид навчальної діяльності здобувача вищої освіти : 1) поточне тестування за кожною темою; 2) участь у форумі (дистанційно) або аудиторна робота на семінарських заняттях (очно); 3) виконання самостійної роботи; 4) виконання індивідуальних завдань.

Тестування – це метод ефективної перевірки рівня засвоєння знань, умінь і навичок із навчальної дисципліни. Тестування з навчальної дисципліни «Правове забезпечення інформаційної безпеки в умовах сталого розвитку» здійснюється за кожною темою.

Веб-форум або просто Форум – інтернет-ресурс, популярний різновид спілкування в інтернеті, для проведення дискусій, на якому користувачі обмінюються досвідом та ідеями з певної заданої теми. Оцінювання відповідей здійснюється автоматично.

З метою закріплення теоретичного матеріалу програмою дисципліни передбачено проведення семінарських занять. Семінарські заняття з курсу «Правове забезпечення інформаційної безпеки в умовах сталого розвитку» передбачають розгляд здобувачами теоретичних положень, засвоєних на лекціях та в процесі самостійної роботи, обговорення реферативних повідомлень, виконання практичних завдань. Рівень знань, підготовленості, ерудиції, активності здобувачів вищої освіти на семінарських заняттях оцінюється викладачем самостійно. В рамках навчальної дисципліни «Правове забезпечення інформаційної безпеки в умовах сталого розвитку» передбачено проведення семінарського заняття за більшістю тем та обговорення на семінарському занятті результатів виконаного здобувачами певного завдання, підготовленої презентації з використанням методів мозкового штурму, евристичних питань та діалогового спілкування. За умови очного навчання за кожною темою проводиться робота в малих групах.

Аудиторна робота здобувача на заняттях оцінюється безпосередньо викладачем при проведенні заняття. Участь в аудиторних заняттях передбачає активне включення здобувача в дискусії із викладачем та іншими здобувачами групи, ставлення питань, поширення власних думок, вражень та досвіду. Також оцінюється системність та активна участь у груповій діяльності.

Самостійна робота здобувача вищої освіти є основним засобом засвоєння навчального матеріалу у вільний від аудиторних занять час. Самостійна робота включає: попереднє опрацювання інформаційного забезпечення за всіма видами навчальних занять та розв'язання завдань самоконтролю опанування дисциплінарними результатами навчання відповідно до робочої програми дисципліни. Самостійна робота може здійснюватися у таких формах як підготовка до семінарських занять, самостійне вивчення додаткової літератури та додаткових питань, самостійне ознайомлення з нормативно-правовою базою, розв'язання завдань, робота з інформаційними ресурсами, підготовка до заліку.

Індивідуальні завдання здобувачів вищої освіти включають виконання есе, рефератів, презентацій, аналіз практичних ситуацій, підготовку реферативних

матеріалів із фахових публікацій, власні дослідження до конференцій тощо. Індивідуальні завдання сприяють більш поглибленому вивченню здобувачем вищої освіти теоретичного матеріалу, формуванню вмінь використання знань для вирішення відповідних практичних завдань, підвищення рівня підготовки і розкриття індивідуальних творчих здібностей.

Індивідуальними завданнями здобувачів вищої освіти в рамках вивчення навчальної дисципліни «Правове забезпечення інформаційної безпеки в умовах сталого розвитку» є підготовка презентації за завданням до запропонованої теми та виступ з нею на семінарському занятті.

У таблиці наведено розподіл максимальної кількості балів за певний вид навчальної роботи здобувача вищої освіти за темами навчальної дисципліни.

Розподіл балів за видами навчальної роботи здобувача вищої освіти

Теми	Тестування з теми	Участь у форумі, семінарському у занятті	Індивідуальні завдання	Самостійна робота	Підсумкова (тестова) роботи	Підсумкова оцінка
1.	3	3	2	2	20	
2.	3	3	2	2		
3.	3	3	2	2		
4.	3	3	2	2		
5.	3	3	2	2		
6.	3	3	2	2		
7.	2	2	2	2		
8.	2	2	1	1		
9	2	2	1	1		
Разом	24	24	16	16	20	100
	48		32			

Викладач, враховуючи досягнення здобувача вищої освіти з дисципліни, його системну та активну участь і роботу на платформі MOODLE, може додати **0-10 балів**.

Отримані бали на семінарських заняттях (максимально 48 балів) та бали за самостійну та індивідуальну роботу (максимально 32 бали) додаються до оцінки з підсумкової (тестової) роботи в кінці семестру (20 балів) та є підсумковою оцінкою за вивчення навчальною дисципліни. Максимально за поточною успішністю здобувач вищої освіти може набрати **100 балів**.

Загальна оцінка з навчальної дисципліни «Правове забезпечення інформаційної безпеки в умовах сталого розвитку» визначається за накопичувальною системою, тобто сума всіх балів, отриманих за виконання певного виду робіт здобувача вищої освіти.

Незалежно від результатів поточного контролю кожен здобувач має право скласти залік. Залік відбувається у письмовій формі або з використанням можливостей дистанційної платформи MOODLE.

7. Політика курсу

7.1 Політика щодо академічної доброчесності. Академічна доброчесність здобувачів вищої освіти є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів.

Політика щодо академічної доброчесності регламентується такими документами: «Положення про систему запобігання та виявлення плагіату в Національному технічному університеті «Дніпровська політехніка» та Кодекс академічної доброчесності НТУ «Дніпровська політехніка».

Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі).

У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

7.2 Комунікаційна політика.

Здобувачі вищої освіти повинні мати активовану університетську пошту.

Обов'язком здобувача вищої освіти є перевірка один раз на тиждень (щонеділі) поштової скриньки на Офіс365.

Протягом тижнів самостійної роботи обов'язком здобувача вищої освіти є робота з дистанційним курсом «Правове забезпечення інформаційної безпеки в умовах сталого розвитку» (<https://do.nmu.org.ua>)

Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту.

7.3 Політика щодо перескладання.

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку.

7.4 Відвідування занять.

Для здобувачів вищої освіти денної форми навчання відвідування занять є обов'язковим. Поважними причинами для неявки на заняття є хвороба, участь в університетських заходах, відрадження, які необхідно підтверджувати документами у разі тривалої (два тижні) відсутності. Про відсутність на занятті та причини відсутності здобувача вищої освіти має повідомити викладача або особисто, або через старосту. Якщо здобувач вищої освіти захворів, ми рекомендуємо залишатися вдома і навчатися за допомогою дистанційної платформи. Здобувачам вищої освіти, чий стан здоров'я є незадовільним і може вплинути на здоров'я інших здобувачів, буде пропонуватися залишити заняття (така відсутність вважатиметься пропуском з причини хвороби).

7.5 Бонуси. Здобувачі вищої освіти, які регулярно відвідували лекції (мають не більше двох пропусків без поважних причин) та мають написаний конспект лекцій отримують додатково 2 бали до результатів оцінювання до підсумкової оцінки.

7.6 Участь в анкетуванні. Наприкінці вивчення курсу навчальної дисципліни «Правове забезпечення інформаційної безпеки в умовах сталого розвитку» здобувачам пропонується заповнити анкету на платформі MOODLE, надавши відповідь на питання щодо їх враження стосовно курсу навчальної дисципліни. Заповнення анкети є важливою складовою навчальної активності здобувача, що дозволить оцінити дієвість застосованих методів викладання та врахувати пропозиції стосовно покращення змісту навчальної дисципліни «Правове забезпечення інформаційної безпеки в умовах сталого розвитку».

1. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1.1 Нормативно-правові акти:

1. Про публічні електронні реєстри: Закон України від 18 листопада 2021 року № 1907-IX. Відомості Верховної Ради. 2023. № 11. ст.27. URL: <https://zakon.rada.gov.ua/laws/show/1907-20#Text>

2. Про державну таємницю: Закон України від 21.01.1994 р. № 3855-XII. Відомості Верховної Ради. 1994. № 16. Стаття 93. URL: <https://zakon.rada.gov.ua/laws/show/3855-12#Text>

3. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Відомості Верховної Ради України. 1992. № 48. Стаття 650. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>

4. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. Відомості Верховної Ради України. 2010. № 34. Стор. 1188. Стаття 481. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

5. 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>

6. Про Державний реєстр виборців: Закон України від 22.02.2007 р. № 698-V. Відомості Верховної Ради України. 2007. № 20. Стор. 764. Стаття 282. URL: <https://zakon.rada.gov.ua/laws/show/698-16#Text>

7. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. Відомості Верховної Ради України (ВВР). 2011. № 32. Стаття 314. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>

8. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV. Відомості Верховної Ради України. 2003. № 36. Ст. 275. URL: <https://zakon.rada.gov.ua/laws/show/851-15#Text>

9. Про електронні комунікації: Закон України від 16 грудня 2020 року № 1089-IX. Офіційний вісник України від 26.01.2021. 2021 р., № 6, стор. 10, стаття 306, код акта 102665/2021. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text>

10. Про доступ до судових рішень: Закон України від 22.12.2005 р. № 3262-IV. Відомості Верховної Ради України. 2006. № 15. Ст. 128. URL: <https://zakon.rada.gov.ua/laws/show/3262-15#Text>

11. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII. Відомості Верховної Ради України. 2017. № 45. Стор. 5. Стаття 400. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>

12. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: Закон України від 20.11.2012 р. № 5492-VI. Відомості Верховної Ради України. 2013. № 51. Стор. 2733. Стаття 716. URL: <https://zakon.rada.gov.ua/laws/show/5492-17#Text>

13. Про Цілі сталого розвитку України на період до 2030 року. Указ Президента України від 30 вересня 2019 року № 722/2019. Урядовий кур'єр. 2019. № 188. URL: <https://zakon.rada.gov.ua/laws/show/722/2019#Text>

14. Про схвалення Концепції розвитку електронного урядування в Україні: Розпорядження Кабінету Міністрів України від 20.09.2017 р. № 649-р. Урядовий кур'єр. 2017. № 181. Урядовий кур'єр від 27.09.2017 № 181. URL: <https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text>

15. Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 08.11.2017 р. № 797-р. Урядовий кур'єр. 2017. № 217. URL: <https://zakon.rada.gov.ua/laws/show/797-2017-%D1%80#Text>

16. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». Указ Президента України від 26 серпня 2021 року № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>

17. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28 грудня 2021 року № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#n7>.

18. Про доступ до інформації, що знаходиться у розпорядженні державних органів: Рекомендація № R (81) 19 Комітету Міністрів Ради Європи 1981 р. URL: <http://cedem.org.ua/library/re81-19>.

19. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14 вересня 2020 року № 392/2020. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#Text>

1.2 Навчально-методичні та наукові джерела:

1. Мужанова Т.М. Інформаційна безпека держави. Навчальний посібник. Державний університет телекомунікацій. Київ. 2019. 131 с. https://nubip.edu.ua/sites/default/files/u34/posibnik_ibd_muzhanova_2019.pdf
2. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. 144 с.
3. Вишня В. Б. Основи інформаційної безпеки : навч. посіб. / В.Б. Вишня, О.С. Гавриш, Е.В. Рижков. Дніпро : ДДУВС, 2020. 128 с. URL: <https://er.dduvs.in.ua/handle/123456789/4206>
4. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. 166 с. : іл.
5. Блінова Г.О. Інформаційне забезпечення органів публічної адміністрації в Україні: адміністративно-правові засади : монографія. Запоріжжя: Видавничий дім «Гельветика», 2019. 503 с.
6. Blinova G.O., Demchuk A.M., Yatsyshyn M.M. Ukrainian legislation regulating information support of public administration bodies: history, present, perspectives. New and traditional approaches in modern legal research : collective monograph / H. O. Blinova, O. V. Dykyi, V. Dyntu, A. V. Khridochkin, etc. Lviv-Toruń: Liha-Pres, 2019. 284 p. pp. 1–26
7. Blinova A.A., Kelman M.S. Legal regulation of use of public electronic information resources by public administration bodies during development of of Ukraine as a digital country. Juridical sciences and their role in the formation of legal culture of a modern person : collective monograph. Lviv : Liha-Pres, 2019. 256 p. pp. 1–27.
8. Blinova A.A., Holovko K.V. International and foreign experience of legal regulation of the process of information support of public administration bodies in the conditions of digitization of public administration. Issues of the state of modern legal education and professional culture of lawyers : collective monograph / A. A. Blinova, K.V. Holovko, A.V. Khridochkin, O. Yu. Dubynskyi, etc. – Lviv- Toruń: Liha-Pres, 2019. – 252 p. pp. 1–30.
9. Блінова Г.О. Інформаційні бази даних поліції превентивної діяльності як складова інтегрованої системи управління ризиками у сфері публічної безпеки та цивільного захисту: науково-практичні рекомендації. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2021. 84 с.
10. Бочковий О.В., Блінова Г.О., Прокопов С.О., Мамедова Є.А. Інформаційне забезпечення діяльності патрульної поліції: науково-практичні рекомендації. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2021. 112 с.
11. Блінова Г.О., Прокопов С.О. Інформаційне забезпечення підрозділів ювенальної превенції Національної поліції України: науково-практичні рекомендації. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2021. 64 с.
12. Блінова Г.О. The mechanism of information support bodies public administration: concept, content, elements. Visegrad Journal on Human Rights. № 6. 2018 p. P. 44 – 48

13. Petro S. Korniienko, Oleh V. Plakhotnik, Hanna O. Blinova, Zhanna O. Dzeiko, Gennadii O. Dubov. Contemporary Challenges and the Rule of Law in the Digital Age. *Studies of Applied Economics*. DOI: 10.25115/eea.v39i9.5773. Volume 39-9, September 2021 // ISSN: 1133-3197
14. Мельник П., Костенко О., Блинова Х., Шинкаренко И. (2021). Опыт защиты персональных данных в Интернете и возможности их признания и защиты в Украине. *Ius Humani. Юридический журнал*, 10 (2), 87-100. URL: <https://doi.org/https://doi.org/10.31207/ih.v10i2.288>
15. Блінова Г.О., Потіп М.М. Судовий захист приватно-правових таємниць: вітчизняний та іноземний досвід. *Приватне та публічне право* № 4. 2021. С.27-34
16. Блінова Г.О., Потіп М.М. Процесуальні аспекти захисту таємниці про стан здоров'я. *Право і суспільство*. № 6. 2021. С. 28-36
17. Блінова Г.О., Потіп М.М. Таємниця особистого життя: зміст та захист. *Юридичний науковий електронний журнал* № 12. 2021. С. 113-116
18. Блінова Г.О. Правові засади використання електронних інформаційних ресурсів в концепції цифрової держави. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*, (2), 53–60. URL: <https://doi.org/10.54929/pmtl-issue2-2021-10>
19. Блінова Г.О. Становлення України як цифрової держави та удосконалення системи державних електронних інформаційних ресурсів. *Науковий журнал «Law. State. Technology»*. Вип. 1. 2021. С. 3-10. DOI: <https://doi.org/10.32782/LST/2021-2-1>
20. Блінова Г.О. Окремі аспекти правового регулювання інформаційних відносин у сфері будівництва. *Право та державне управління*. № 4. 2022. С. 35-41 DOI <https://doi.org/10.32840/pdu.2022.4.5>
21. Блінова Г.О. Сучасний стан та перспективи використання можливостей єдиної державної електронної системи у сфері будівництва для протидії корупції. *Актуальні проблеми вітчизняної юриспруденції*. №5. 2022. С. 67-72. DOI <https://doi.org/10.32782/39221355>
22. Блінова Г.О. Інформаційна система управління відходами : сучасний стан правового регулювання та перспективи. *Юридичний бюлетень*. №29. 2023. С. 45-54. DOI <https://doi.org/10.32850/LB2414-4207.2023.29.05>
23. Блінова Г.О. Інформаційно-правове забезпечення механізму поводження з відходами війни. *Юридичний науковий електронний журнал*. №7. 2023. С. 93-99. DOI <https://doi.org/10.32782/2524-0374/2023-7/20>
24. Блінова Г.О. Інформаційне забезпечення адміністрування місцевих податків і зборів: організаційно-правові аспекти. *Правова позиція*. 2023. № 2 (39). С. 110-116. DOI <https://doi.org/10.32782/2521-6473.2023-2.22>
25. Блінова Г.О., Чалик В.Р. Механізм адміністративно-правового регулювання використання інформаційних технологій у соціальній сфері. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. №3. 2023. С. 105-114. DOI: <https://doi.org/10.31733/2078-3566-2023-3-130-139>