

Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра **Права** (№ 702)

ЗАТВЕРДЖУЮ


(підпис)

Гарант освітньої програми
Голубов А.Є.
(ініціали та прізвище)

« 31 » серпня 2022 р.

**СИЛАБУС ВИБІРКОВОЇ
НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

**ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В
УКРАЇНІ**

(назва навчальної дисципліни)

Галузь знань: 08 Право
(шифр і найменування галузі знань)

Спеціальність: 081 Право
(код і найменування спеціальності)

Освітня програма: Право
(найменування освітньої програми)

Рівень вищої освіти:
перший (бакалаврський)

Силабус введено в дію з 01.09.2022 року

Харків – 2022 р.

Розробник: Філіпенко Наталія Євгенівна, доктор юридичних наук,
доцент, доцент кафедри права гуманітарно-правового
факультету

(прізвище та ініціали, посада, науковий ступінь і вчене звання)

(підпис)

Силабус навчальної дисципліни розглянуто на засіданні кафедри Права

(назва кафедри)

Протокол № 1 від « 26» серпня 2022 р.

Завідувач кафедри Д.Ю.Н. доцент
(Науковий ступінь і вчене звання)

(підпис)

Спіцина Г.О.
(ініціали та прізвище)

1. Загальна інформація про викладача

Філіпенко Наталія Євгенівна, доктор юридичних наук, доцент, доцент кафедри права п. filipenko@khai.edu

Сферу наукових інтересів становлять проблеми судової експертизи у кримінальному та адміністративному провадженнях за фактами втручань у діяльність об'єктів критичної інфраструктури та повітряного транспорту; кримінологія; правове регулювання інформаційної безпеки в Україні; актуальні проблеми правового регулювання та організації безпеки суб'єктів господарювання критичної інфраструктури та повітряного транспорту; актуальні проблеми запобігання корупції.

2. Опис навчальної дисципліни

Семестр, в якому викладається дисципліна 7

Обсяг дисципліни: 6 кредитів ЄКТС/150 годин, у тому числі аудиторних – 64 год., самостійної роботи здобувачів – 116 год.

Форма здобуття освіти – *денна*

Дисципліна *обов'язкова*

Види навчальної діяльності – *лекції, семінарські та практичні заняття*

Види контролю – *модульний контроль, іспит*

Мова викладання – *українська*

Пререквізити: теорія держави та права; кримінальне право; міжнародне право; кримінально-процесуальне право; адміністративне право; криміналістика; соціологія тощо.

Кореквізити навчальної дисципліни: захист інформації в інформаційних системах; сучасні проблеми доказування у кримінальному провадженні; використання кримінального аналізу щодо протидії кримінальним правопорушенням на об'єктах критичної інфраструктури та повітряного транспорту; актуальні проблеми правового регулювання та організації безпеки суб'єктів господарювання критичної інфраструктури та повітряного транспорту; судові експертизи у кримінальному та адміністративному провадженнях за фактами втручань у діяльність об'єктів критичної інфраструктури та повітряного транспорту. тощо.

3. Мета та завдання навчальної дисципліни

Мета курсу – формування юриста з освітньо-кваліфікаційним рівнем бакалавр, вироблення у нього почуття інноваційного характеру, високих навичок професійної діяльності та набуття вмінь, необхідних для застосування спеціалізованих заходів у сферах інформаційної та комп'ютерної безпеки, які забезпечують захист сучасних інформаційних систем у професійній діяльності, пов'язаній з отриманням, обробкою, накопиченням і

захистом особистої та юридичної інформації.

Предметом навчальної дисципліни є основи нормативно-правового забезпечення інформаційної безпеки в Україні.

Основними завданнями вивчення дисципліни є забезпечення ознайомлення з новітніми науковими та практичними досягненнями у сфері протидії злочинності; вироблення навичок та вмінь комплексного аналізу загроз інформаційній безпеці, прогнозуванням та програмуванням антикризових заходів тощо.

Компетентності, які набуваються:

Інтегральна компетентність. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі професійної правничої діяльності або у процесі навчання, що передбачає застосування правових доктрин, принципів і правових інститутів і характеризується комплексністю та невизначеністю умов.

Загальні компетентності (ЗК).

ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК2. Здатність застосовувати знання у практичних ситуаціях.

ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК7. Здатність вчитися і оволодівати сучасними знаннями.

ЗК9. Здатність працювати в команді.

ЗК10. Здатність діяти на основі етичних міркувань (мотивів).

ЗК11. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

Спеціальні (фахові, предметні) компетентності спеціальності (СК).

СК1. Здатність застосовувати знання з основ теорії та філософії права, знання і розуміння структури правничої професії та її ролі у суспільстві.

СК2. Знання і розуміння ретроспективи формування правових та державних інститутів.

– СК3. Повага до честі і гідності людини як найвищої соціальної цінності, розуміння їх правової природи.

СК4. Знання і розуміння міжнародних стандартів прав людини, положень Конвенції про захист прав людини та основоположних свобод, а також практики Європейського суду з прав людини.

СК 7. Здатність застосовувати знання завдань, принципів і доктрин національного права, а також змісту правових інститутів, щонайменше з таких галузей права як: конституційне право, адміністративне право і адміністративне процесуальне право, цивільне і цивільне процесуальне право, кримінальне і кримінальне процесуальне право.

СК 8. Знання і розуміння особливостей реалізації та застосування норм матеріального і процесуального права.

СК 11. Здатність визначати належні та прийнятні для юридичного аналізу факти.

СК 12. Здатність аналізувати правові проблеми, формувати та обґрунтовувати правові позиції.

СК 13. Здатність до критичного та системного аналізу правових явищ і застосування набутих знань у професійній діяльності.

СК 14. Здатність до консультування з правових питань, зокрема, можливих способів захисту прав та інтересів клієнтів, відповідно до вимог професійної етики, належного дотримання норм щодо нерозголошення персональних даних та конфіденційної інформації.

СК 16. Здатність до логічного, критичного і системного аналізу документів, розуміння їх правового характеру і значення.

Програмні результати навчання:

ПРН 1. Визначати переконливість аргументів у процесі оцінки заздалегідь невідомих умов та обставин.

ПРН 2. Здійснювати аналіз суспільних процесів у контексті аналізованої проблеми і демонструвати власне бачення шляхів її розв'язання.

ПРН 3. Проводити збір і інтегрований аналіз матеріалів з різних джерел.

ПРН 4. Формулювати власні обґрунтовані судження на основі аналізу відомої проблеми.

ПРН 5. Давати короткий висновок щодо окремих фактичних обставин (даних) з достатньою обґрунтованістю.

ПРН 6. Оцінювати недоліки і переваги аргументів, аналізуючи відому проблему.

ПРН 7. Складати та узгоджувати план власного дослідження і самостійно збирати матеріали за визначеними джерелами.

ПРН 8. Використовувати різноманітні інформаційні джерела для повного та всебічного встановлення певних обставин.

ПРН 9. Самостійно визначати ті обставини, у з'ясуванні яких потрібна допомога, і діяти відповідно до отриманих рекомендацій.

ПРН 10. Вільно спілкуватися державною та іноземною мовами як усно, так і письмово, правильно вживаючи правничу термінологію.

ПРН 11. Володіти базовими навичками риторики.

ПРН 12. Доносити до респондента матеріал з певної проблематики доступно і зрозуміло.

ПРН 13. Пояснювати характер певних подій та процесів з розумінням професійного та суспільного контексту.

ПРН 17. Працювати в групі, формуючи власний внесок у виконання завдань групи.

ПРН 18. Виявляти знання і розуміння основних сучасних правових доктрин, цінностей та принципів функціонування національної правової системи.

ПРН 19. Демонструвати необхідні знання та розуміння сутності та змісту основних правових інститутів і норм фундаментальних галузей права.

ПРН 20. Пояснювати природу та зміст основних правових явищ і процесів.

ПРН 21. Застосовувати набуті знання у різних правових ситуаціях, виокремлювати юридично значущі факти і формувати обґрунтовані правові висновки.

ПРН 22. Готувати проекти необхідних актів застосування права відповідно до правового висновку зробленого у різних правових ситуаціях.

ПРН 23. Надавати консультації щодо можливих способів захисту прав та інтересів клієнтів у різних правових ситуаціях.

4. Зміст навчальної дисципліни

МОДУЛЬ 1

Змістовний модуль 1. Загальна частина

Тема 1.

Базові терміни та визначення. Основні задачі забезпечення інформаційної безпеки. Джерела загроз інформаційній безпеці.

Мета і завдання курсу. Базові терміни та визначення. Нормативно-правові джерела інформаційної безпеки України. Про концепцію інформаційної безпеки України. Основні задачі інформаційної безпеки. Методи запобігання та ліквідації загроз інформаційній безпеці. Організаційні основи захисту інформації. Організаційно-технічні заходи захисту інформації.

Тема 2.

Правове регулювання інформаційної безпеки в Україні як наука та навчальна дисципліна, її предмет, метод і система.

Загальна характеристика правового регулювання інформаційної безпеки в Україні як юридичної науки, її предмет та метод. Сучасний стан та перспективи розвитку правового регулювання інформаційної безпеки в Україні, окремих її напрямків в сучасній Україні.

Місце правового регулювання інформаційної безпеки в Україні в системі юридичних дисциплін. Роль правового регулювання інформаційної безпеки в Україні у формуванні професійних якостей юриста, його юридичного світогляду, мислення, правової культури.

Тема 3.

Організаційно-правові й тактико-технічні заходи захисту державної таємниці.

Суб'єкти інформаційного простору. Види інформації за змістом (інформація про фізичну особу; інформація довідково-енциклопедичного характеру; інформація про стан довкілля (екологічна інформація); інформація про товар (роботу, послугу); науково-технічна інформація; податкова інформація; правова інформація; статистична інформація; соціологічна інформація; інші види інформації). Поняття й механізм віднесення відомостей до державної таємниці. Основні організаційно-правові заходи щодо охорони державної таємниці.

Тема 4.

Організаційно-правові й тактико-технічні заходи захисту комерційної таємниці.

Поняття й механізм віднесення відомостей до комерційної таємниці. Перелік відомостей, що не становлять комерційної таємниці. Правовий захист комерційної таємниці. Зовнішні та внутрішні заходи захисту комерційної

таємниці. Нормативно-правові засади створення служби безпеки підприємства (фірми). Структура, функції, завдання служби безпеки підприємства (фірми). Організаційно-технічні заходи захисту комерційної таємниці.

Тема 5.

Організаційно-правові й тактико-технічні заходи захисту банківської таємниці.

Поняття і сутність банківської таємниці. Умови ефективного функціонування банківської системи України. Перелік відомостей, що становлять банківську таємницю. Правовий захист банківської таємниці. Структура, функції та завдання служби безпеки банків. Організаційно-технічні заходи захисту банківської таємниці.

Тема 6.

Основи криптографічного захисту інформації

Поняття криптографічного захисту інформації. Історія виникнення та розвиток сучасних криптографічних методів захисту інформації. Нормативно-правове регулювання криптографічного захисту інформації («Положення про порядок здійснення криптографічного захисту інформації в Україні»). Діяльність Державної служби спеціального зв'язку та захисту інформації України.

Тема 7.

Оперативно-розшукові заходи забезпечення інформаційної безпеки

Поняття оперативно-розшукової діяльності. Повноваження органів і підрозділів, які здійснюють оперативно-розшукову діяльність у сфері забезпечення інформаційної безпеки. Повноваження оперативних підрозділів правоохоронних органів щодо отримання банківської та комерційної інформації.

Тема 8.

Протидія кібертерористичним атакам на об'єкти критичної інфраструктури та авіаційного транспорту

Поняття кіберзагроз та кібертерористичних атак. Основні заходи протидії кіберзагрозам на об'єктах критичної інфраструктури та авіаційного транспорту.

Тема 9.

Міжнародний стандарт безпеки ISO/IEC 17799:2005 із захисту інформації.

Загальні відомості про Міжнародний стандарт безпеки ISO/IEC 17799:2005 із захисту інформації. Його основні положення: Політика безпеки. Організаційні заходи щодо забезпечення безпеки. Класифікація і управління ресурсами. Безпека персоналу. Фізична безпека. Управління комунікаціями і

процесами. Контроль доступу. Розробка і технічна підтримка обчислювальних систем. Управління інцидентами інформаційної безпеки. Управління неперервністю бізнесу. Відповідність системи основним вимогам.

Змістовний модуль 2. Особлива частина

Тема 10.

Міжнародно-правові засади інформаційної безпеки.

Міжнародна інформація та її джерела. Поняття міжнародного інформаційного права. Обмеження у міжнародному інформаційному праві. Відповідальність держави за інформаційні міжнародно-правові діяння.

Тема 11.

Принципи, джерела та суб'єкти міжнародної системи інформаційної безпеки.

Основні принципи регулювання правовідносин щодо міжнародної інформаційної діяльності. Конвенційні засади міжнародного інформаційного права. Міжнародні договори, їх роль у регулювання транскордонної інформаційної діяльності. Джерела міжнародного інформаційного права: поняття та види. ООН як провідна глобальна організація забезпечення міжнародної безпеки. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України.

Тема 12.

Концептуальні засади правового забезпечення інформаційної безпеки України в умовах євроінтеграції.

Місце України в системі міжнародної та регіональної безпеки. Еволюція співробітництва Україна – НАТО у формуванні системи інформаційної безпеки. Співробітництво України та ЄС в сфері інформаційної безпеки: досягнення та перспективи.

Модульний контроль.

5. Індивідуальні завдання

Навчальним планом не передбачено

6. Методи навчання

Лекції, семінарські заняття, практична робота

7. Методи контролю

Модульний контроль, іспит

8. Критерії оцінювання та розподіл балів, які отримують здобувачі

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			

Робота на лекціях	0...1	5	0...5
Виконання і захист лабораторних (практичних) робіт	0...4	4	0...16
Модульний контроль	0...10	1	0...10
Змістовний модуль 2			
Робота на лекціях	0...1	11	0...11
Виконання і захист лабораторних (практичних) робіт	0...4	8	0...32
Модульний контроль	0...26	1	0...26
Усього за семестр			0...100

Білет для іспиту складається з 2 теоретичних питань, і 1 практичного завдання (30 б + 30 б + 40 б) = 100 балів...

Під час складання семестрового іспиту здобувач має можливість отримати максимум 100 балів.

Критерії оцінювання роботи здобувача протягом семестру

Відповідно до п. 3.2. Положення про рейтингове оцінювання досягнень студентів у Національному аерокосмічному університеті ім. М.Є. Жуковського «Харківський авіаційний інститут» студенту можуть призначатися бали за інші активності, пов'язані з навчальною дисципліною, які нараховуються та можуть бути враховані у загальній оцінці за семестр. Бали зокрема можуть призначатися за такі активності, пов'язані з навчальною дисципліною, як:

- участь у науковому комунікативному заході (конференції, семінарі, круглому столі тощо) із написанням тез наукової доповіді за предметом навчальної дисципліни (20 балів);
- участь у другому турі Всеукраїнської олімпіади відповідного напрямку (20 балів);
- участь (прослуховування) не менше у 5 вебінарах, пов'язаних з навчальною дисципліною (3-15 балів);
- участь у тренінгу, пов'язаному з навчальною дисципліною (15 балів);
- проходження он-лайн курсу, пов'язаного з навчальною дисципліною (20 балів);
- участь та отриманні рейтингового місця у тематично пов'язаному із предметом навчальної дисципліни студентському конкурсі (30 балів);
- розробка та створення дидактичного матеріалу за тематикою предмету навчальної дисципліни (15 балів) (підтвердження - дидактичний матеріал);
- проведення правоосвітнього заходу із учнями шкіл та інших навчальних закладів за тематикою навчальної дисципліни (20 балів);
- написання реферату /презентації, доповіді (5 балів) з обов'язковою перевіркою на антиплагіат через систему Unicheck (оригінальність тексту не менше 80 %);

- участь у не менше заходах, що проводяться студентськими професійними об'єднаннями за спеціальністю (5-15 балів);
- інші активності, пов'язані з навчальною дисципліною, за попереднім погодженням із науково-педагогічним працівником, який викладає навчальну дисципліну.

Семестровий контроль (іспит/залік) проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до іспиту/заліку. Під час складання семестрового іспиту/заліку студент має можливість отримати максимум 100 балів.

Білет для іспиту складається з двох теоретичних питань (60 балів) і одного практичного (40 балів)

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

9. Політика навчального курсу

Відвідування занять. Регуляція пропусків. Інтерактивний характер курсу передбачає обов'язкове відвідування практичних занять. Студенти, які за певних обставин не можуть відвідувати практичні заняття регулярно, мусять впродовж тижня узгодити із викладачем графік індивідуального відпрацювання пропущених занять. Окремі пропущені завдання мають бути відпрацьовані на найближчій консультації впродовж тижня після пропуску. Відпрацювання занять здійснюється усно у формі співбесіди за питаннями, визначеними планом заняття. В окремих випадках дозволяється письмове відпрацювання шляхом виконання індивідуального письмового завдання. Студенти, які станом на початок екзаменаційної сесії мають понад 70% невідпрацьованих пропущених занять, до відпрацювання не допускаються.

Дотримання вимог академічної доброчесності студентами під час вивчення навчальної дисципліни. Під час вивчення навчальної дисципліни студенти мають дотримуватися загальноприйнятих морально-етичних норм і правил поведінки, вимог академічної доброчесності, передбачених «Положенням про академічну доброчесність Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» (<https://khai.edu/assets/files/polozhennya/polozhennya-pro-akademichnu-dobrochesnist.pdf>). Очікується, що роботи студентів будуть їх оригінальними

дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману. При виконанні індивідуальної самостійної роботи до захисту допускаються реферати, які містять не менше 60 % оригінального тексту при перевірці на плагіат, есе – 70 %

Вирішення конфліктів. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, а також правила етичної поведінки регламентуються «Кодексом етичної поведінки в Національному аерокосмічному університеті ім. М. Є. Жуковського «Харківський авіаційний інститут» (<https://khai.edu.ua/university/normativna-baza/ustanovchi-dokumenti/kodeks-etichnoi-povedinki/>).

10. Методичне забезпечення

1. Опорний конспект лекцій.
2. Навчально-методичне забезпечення дисципліни (НМКД); <https://mentor.khai.edu/course/>

11. Рекомендована література

Законодавство

1. Конституція України від 28 червня 1996 р. ВВР. 1996. № 30. Ст. 141.
2. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних, ратифікована згідно із Законом України № 2438–VI від 06.07.2010 р. URL: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_326.
3. Конвенція про кіберзлочинність ратифікована Законом України від 07.09.2005 р. № 2824–IV URL: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_575.
4. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних, ратифікований згідно із Законом України № 2438–VI від 06.07.2010р. URL: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_363.
5. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, ратифікований Законом України від 21.07.2006 р. № 23–V URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_687.
6. Доклад рабочей группы по управлению Интернетом. Шато де Босси, 2005. URL: <http://www.wgig.org/WGIG-Report.html>.
7. Документи Всесвітнього Самміту з Інформаційного Суспільства (BCIC): Декларація принципів та План Дій. Женева, 2003; Зобов'язання та Програма для інформаційного суспільства. Туніс, 2005 URL: <http://www.itu.int/wsis/outcome/booklet/indexru.html>.

8. Про міжнародне приватне право. Закон України від 23.06.2005 р. № 2709– IV // ВВР. 2005ю. N 32. ст.422.
9. Про міжнародні договори України. Закон України від 29.06.2004 р. 1906– IV // ВВР. 2004. N 50. ст.540.
10. Про державну таємницю. Закон України від 21. 01.1994 р. № 3856-XII. URL: <https://zakon.rada.gov.ua/laws/show/3855-12#Text>.
11. Про інформацію. Закон України № 2658-XII від 02.10.92. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.
12. Про оперативно-розшукову діяльність. Закон України № 2136-XII від 18.02.92. URL: <https://zakon.rada.gov.ua/laws/show/2135-12#Text>.
13. Про банки і банківську діяльність. Закон України № 2121-III від 07.12.2000. URL: <https://zakon.rada.gov.ua/laws/show/2121-14#Text/>
14. Окинавская Хартия глобального информационного общества (Окинава, 22 июля 2000 года) // Дипломатический вестник. 2000. N 8. С. 51 – 56. URL: zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=998_163.
15. Резолюция Международного Союза Электросвязи № 133 «Роль администраций Государств–Членов в управлении интернационализированными (многоязычными) наименованиями доменов» / МСЭ, Анталия, 2006. URL: http://www.ifapcom.ru/files/Documents/resolution_133.pdf.
16. Рекомендация о развитии и использовании многоязычия и всеобщем доступе к киберпространству (32-я Генеральная конференция ЮНЕСКО, Париж, 2003. URL: <http://www.unesco.org>.
17. Рекомендації щодо забезпечення правомірності використання комп'ютерних програм вільного користування, Державна служба інтелектуальної власності України. URL: <http://www.sdip.gov.ua/ua/rozcompprogfree.html>.
18. Рекомендації щодо застосування вільних публічних ліцензій на використання об'єктів авторського права і суміжних прав. Державна служба інтелектуальної власності України. URL: <http://www.sdip.gov.ua/ua/recvilnuxpublits.html>.
19. Рекомендації щодо онлайн-ліцензування. Державна служба інтелектуальної власності України. URL: <http://www.sdip.gov.ua/ua/reconlinelits.html>.
20. Статут Організації Об'єднаних Націй від 26 червня 1945 р.
21. Статут Організації Об'єднаних Націй з питань освіти, науки і культури (ЮНЕСКО) від 16.11.1945 р.
22. Угода про торговельні аспекти прав інтелектуальної власності (ТРИПС). URL: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=981_018.
23. Affirmation of Commitments by the United States Department of Commerce and the Internet Corporation for Assigned Names and Numbersюю , 30.09.2009. URL: <http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm>.
24. Council of Europe: Declaration CM(2005)56 of the Committee of Ministers on human rights and the rule of law in the Information Society. URL: <https://wcd.coe.int/wcd/ViewDoc.jsp?id=849061>.
25. Declaration by the Committee of Ministers on Internet governance principles, adopted on 21 September 2011. URL: http://www.coe.int/t/dghl/standardsetting/media/Doc/CM_en.asp.
26. Declaration by the Committee of Ministers on the protection of freedom of expression and information and freedom of assembly and association with regard to Internet domain names and name strings, adopted on 21 September 2011. URL: http://www.coe.int/t/dghl/standardsetting/media/Doc/CM_en.asp.
27. Declaration of Principles. Building the Information Society: a global challenge in the new Millennium / Document WSIS–03/GENEVA/DOC/4–E. – 12 December 2003. URL: <http://www.itu.int/wsis/docs/geneva/official/dop.html>.

28. Declaration of the Committee of Ministers on network neutrality, adopted on 29 September 2010. URL: http://www.coe.int/t/dghl/standardsetting/media/Doc/CM_en.asp.
29. Declaration of the Committee of Ministers on the Digital Agenda for Europe, adopted 29 September 2010 . URL: http://www.coe.int/t/dghl/standardsetting/media/Doc/CM_en.asp
30. Declaration of the Committee of Ministers on the management of the Internet protocol address resources in the public interest, adopted on 29 September 2010 . – Режим доступа: http://www.coe.int/t/dghl/standardsetting/media/Doc/CM_en.asp.
31. E–Justice: a Tool for Citizens, Practitioners and Business (Forum on Judicial Cooperation in Civil Matters: Debate with National Parliaments, 2 December 2008). URL: http://www.ccbe.org/fileadmin/user_upload/NTCdocument/Study_EJustice_2_De1_1246866101.pdf
32. European Commission Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI). – 2001. URL: www.cryptome.org/echelon-ep-fin.htm.
33. Illegal and Harmful Content on the Internet (European Commission Communication to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions, COM(96) 487, Brussels–Luxembourg, 16 October 1996). URL: <http://www2.echo.lu/legal/en/internet/communic.html>.
34. Recommendation CM/Rec (2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet. URL: <https://coe.int/>.
35. Report by the Council Working Party on Legal Data Processing (e–Justice). Brussels, 2007.
36. Resolution of The European Parliament of 19 February 2001 on the organisation and management of the internet – international and European policy issues 1998–2000 // OJ. 2001. C 343. P. 286.
37. The Macbride report Communication and Society Today and Tomorrow, Many Voices One World, Towards a new more just and more efficient world information and communication order , Kogan Page, London/Uniput, New York/Unesco, Paris. Unesco, 1980. URL: <http://unesdoc.unesco.org/images/0004/000400/040066eb.pdf>.
38. The Uniform Domain Name Dispute Resolution Policy and WIPO (INTA Conference Paper), WIPO, 2011. URL: <http://www.wipo.int/amc/en/docs/wipointaudrp.pdf>.
39. The WIPO Copyright Treaty (WCT). 1996. URL: <http://www.wipo.int/clea/docs/en/wo/wo033en.htm>.
40. The WIPO Performances and Phonograms Treaty (WPPT). 1996. URL: <http://www.wipo.int/clea/docs/en/wo/wo034en.htm>.
41. Towards Knowledge Societies: UNESCO World Report.
42. Understanding Cybercrime: A Guide for Developing Countries ITU, 2009. URL: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf>.

Основна (базова) література:

43. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти / За загальною редакцією д-ра юрид. наук, проф. Бандурки О.М. : Монографія. Харків: Вид-во Ун-ту внутр. Справ, 2000. 368 с.
44. Баранов А. А. Информационная инфраструктура: проблемы регулирования деятельности. К. : ТОВ «Видавничий дім Дмитра Бураго», 2012. 352 с.
45. Дзюбань О.П. Філософія інформаційного права: світоглядні й загальнотеоретичні засади: Монографія. Харків: Майдан, 2013. — 360 с.
46. Довгань О. Д. Забезпечення інформаційної безпеки в контексті глобалізації: теоретико - правові та організаційні аспекти : монографія. НАПрН України, НДПП, НАН України, Нац. б-ка України ім. В. І. Вернадського. Київ, 2015. 388 с.
47. Довгань О.Д. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. К.: Вид-во «Артек». 2017. – 113с.
48. Довгань О.Д. Право власності на інформацію і правовий захист баз даних /О.Д.Довгань// Наукові праці Національної бібліотеки України імені В. І. Вернадського /редкол. В.Попик, Г.Боряк, В.Горовий [та ін..] ; відп. ред. В.Горовий ; НАН України, Нац. б-ка України ім. В. І. Вернадського, Асоц. б-к України К., 2017. Вип.43. С. 42-53.
49. Довгань О.Д. Система інформаційної безпеки України: онтологічні виміри / О.Д. Довгань, Т.Ю.Ткачук // Інформація і право № 1 (24). 2018 . С. 89-104.
50. Довгань О.Д. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс / О.Д. Довгань, Т.Ю.Ткачук // Інформація і право № 2 (25). 2018 . С. 73-85.
51. Доступ до інформації та електронне урядування / Автори-упорядники М.С. Демкова, М.В. Фігель. К.: Факт, 2004. 336 с.
52. Електронна комерція і право / Уклад. А.А. Маєвська Х., 2010. 256 с. URL: http://tempus-khai.org.ua/download_file.php?id=83
53. Задорожний А.В., Пазюк А.В. Международное информационное право. Т. 1: Учебное пособие, К. : Феникс, 2013.
54. Захаров Є. Правові засади моніторингу телекомунікацій (доповідь на громадських слуханнях 14.12.2003 г.). URL: http://www.khpg.org.ua/ru/index.php?id=1071399822#_ftnref1
55. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія / О.О.Золотар. К. : ТОВ “Видавничий дім “АртЕк”, 2018. 446 с.
56. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посібник / Б.А. Кормич. К.: Кондор, 2004 . 384 с.
57. Кормич БА. Організаційно-правові основи політики інформаційної безпеки України: Автореф. дис... докт. юрид. наук: 12.00.07 / Національний університет внутрішніх справ МВС України. Харків, 2004. 41с.
58. Кохановська О.В.Правове регулювання у сфері інформаційних відносин / О.В.Кохановська. К., 2001. 212с.
59. Кохановська О. В. Форми захисту інформаційних прав у доктрині і законодавстві України // Бюлетень Мін'юсту України.К., 2006. №3. с. 70-77.
60. Макаренко Є.А. Міжнародні інформаційні відносини: Монографія. К.: Наша культура і наука, 2002. 452 с.
61. Марущак А.І. Правові основи захисту інформації з обмеженим доступом: Курс лекцій / А.І. Марущак. К.: КНТ, 2007. 208 с
62. Марущак А.І. Інформаційне право: Доступ до інформації: навч. посіб. / А.І. Марущак. К.: КНТ, 2007. 532 с.
63. Марущак А.І. Інформаційне право: регулювання інформаційної діяльності: навч. посіб. / А.І. Марущак. К.: Скіф, 2008. 334 с.
64. Марущак А.І. Пріоритети розвитку інформаційного права України / А.І.Марущак // Інформація і право. 2011. № 1(1). С. 20-25.

65. Міжнародна інформація. / Кудрявцева С.П., Колос В.В. Навчальний посібник. К.: Видавничий Дім «Слово», 2005. 400с.
66. Новицький А.М. Правове регулювання інституціоналізації інформаційного суспільства в Україні: Монографія / А.М. Новицький. Ірпінь: НУДПС України, 2011. 444 с.
67. Організація захисту інформації з обмеженим доступом: підручник / А.М. Гуз, О.Д. Довгань, А.І. Марущак та ін.; за заг. ред. Є.Д. Скулиша. К.: Наук.-вид. відділ НА СБ України, 2011. 378 с.
68. Пазюк А. Права людини та Інтернет. К.: МГО Прайвесі Юкрейн, 2002. 150 с.
69. Пазюк А.В. Захист прав людини стосовно обробки персональних даних: міжнародні стандарти. К.: МГО Прайвесі Юкрейн, 2000. 88 с.
70. Право на приватність: *conditio sine qua non* / Харківська правозахисна група. Харків: Фоліо, 2003. 216 с.
71. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: Монографія / Т.Ю. Ткачук. К. : ТОВ «Видавничий дім «АртЕк», 2018. 411 с.
72. Україна на шляху до суспільства знань: освіта, наука, культура / за ред. А.В. Пазюк. К., 2005. 69 с.
73. Шахбазян К.С. Міжнародно-правові основи регулювання відносин в мережі Інтернет: Дис. ... канд. юрид. наук: 12.00.11 / Київський національний ун-т ім. Тараса Шевченка. К., 2009.
74. Шевчук О., Голобубцький О. Інформаційне суспільство. URL: <http://www.e-ukraine.biz/ukraine1.html>.
- Довідкові джерела:**
112. Документи Ради Європи та діяльність в рамках проекту боротьби з кіберзлочинністю. URL: www.coe.int/cybercrime
113. Международный Союз Электросвязи (МСЭ): Верен идеи соединить мир. URL: <http://www.itu.int/ru/about/Pages/default.aspx>
114. Перелік організацій, призначених ICANN для вирішення спорів. Режим доступу: www.icann.org/en/dndr/udrp/approved-providers.htm.
115. Проект 'Creative Commons' в Україні. URL: <http://creativecommons.org.ua/>.
116. Список міжнародно-правових документів у галузі інтелектуальної власності / Wikipedia. URL: <http://uk.wikipedia.org/wiki/>.
117. Співробітництво України з Міжнародним союзом електрозв'язку (МСЕ) . URL: <http://www.stc.gov.ua/uk/publish/article/86659>.
118. Український Форум з управління Інтернетом IGF-UA . URL: <http://igf-ua.org/>.
119. Хронологія Інтернет: Robert H'obbes' Zakon. Hobbes' Internet Timeline 10.1 URL: <http://www.zakon.org/robert/internet/timeline/>.
120. Communication theory / Wikipedia. URL: http://en.wikipedia.org/wiki/Communication_theory.
121. Council of Europe: Information society and Media. URL: <http://www.coe.int/t/dghl/standardsetting/media/>.
122. Creative Commons . URL <http://creativecommons.org/about>.
123. Creative Commons licenses. URL: http://en.wikipedia.org/wiki/Creative_Commons_licenses.
124. Diagram of ICANN's multi-stakeholder model. URL: <http://www.icann.org/en/structure/>.
125. History of the Internet / Wikipedia. URL: http://en.wikipedia.org/wiki/History_of_the_Internet.
126. Internet Architecture Board . URL: www.iab.org/.
127. Internet Assigned Numbers Authority (IANA). URL: <http://www.iana.org/>.
128. Internet Corporation for Assigned Names and Numbers. URL: <http://www.icann.org/>.
129. Internet Engineering Steering Group . URL: <http://www.ietf.org/iesg/>.

130. Internet Engineering Task Force . URL: <http://www.ietf.org/>.
131. Internet Governance / Wikipedia. URL: http://en.wikipedia.org/wiki/Internet_governance.
132. Internet Governance Forum. URL: <http://www.intgovforum.org/cms/aboutigf>.
133. Internet Governance Forum / Wikipedia. URL: http://en.wikipedia.org/wiki/Internet_Governance_Forum.
134. Internet Library of Law and Court Decisions. URL: <http://www.internetlibrary.com/>.
135. Internet Society (ISOC) . URL: <http://www.isoc.org/>.
136. UNESCO and WSIS. URL: <http://www.unesco.org/new/en/communication-and-information/flagship-project-activities/unesco-and-wsis/resources/official-statements-and-documents/>.

17. Інформаційні ресурси

1. Офіційний портал Верховної Ради України. URL: <http://rada.gov.ua/>
2. Урядовий портал органів виконавчої влади України. URL: <http://www.kmu.gov.ua/>
3. Єдиний державний реєстр судових рішень. URL: reyestr.court.gov.ua/
4. Інформаційна правова система ЛІГА:ЗАКОН. URL: <http://lz.ligazakon.ua/ua/>
5. Юридична бібліотека Національної бібліотеки України імені В. І. Вернадського. URL: http://irbis-nbuv.gov.ua/info_law.html.