

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

МЕТОДИЧНІ ВКАЗІВКИ
з організації самостійної роботи
до вивчення курсу
«Інформаційна політика та безпека»
для студентів 1 курсу магістратури
денної та заочної форми навчання
спеціальності С7 «Журналістика»
освітньої програми «Журналістика»

Методичні вказівки з організації самостійної роботи до вивчення курсу «Інформаційна політика та безпека» для студентів I курсу магістратури денної та заочної форм навчання спеціальності С7 «Журналістика» освітньої програми «Журналістика» / Укл.: В. Л. Погребна. Запоріжжя: НУ «Запорізька політехніка», 2026. 49 с.

Укладач: В. Л. Погребна, професор, д. філол. н.

Рецензент: С. А. Панченко, доцент, к. філол. н.

Відповідальний
за випуск: Н. В. Островська, доцент, к. н. із соц. ком.

Затверджено
на засіданні кафедри
журналістики
Протокол № 10
від 13 травня 2026 р.

Рекомендовано до видання
НМК факультету
соціальних наук
Протокол № 3
від 13 травня 2026 р.

ЗМІСТ

Вступ.....	4
Зміст курсу.....	7
Форми контролю та критерії оцінювання знань.....	11
Практичні заняття.....	17
Індивідуальні завдання та методичні рекомендації до їх виконання.....	26
Зразки тестових завдань контрольної роботи для студентів денної форми навчання.....	28
Контрольна робота для студентів заочної форми навчання.....	39
Питання, що виносяться на екзамен.....	40
Перелік джерел посилання.....	43
Політики курсу.....	48

ВСТУП

Майбутні працівники у медіасфері повинні знати особливості правового забезпечення державної інформаційної політики, зовнішні та внутрішні чинники ескалації загроз інформаційній безпеці України, правила безпечного споживання інформації.

Засвоєні знання з курсу «Інформаційна політика та безпека» сприятимуть успішній реалізації студентів у професії та житті, а набуті у процесі вивчення цієї дисципліни компетентності – оволодінню таких навчальних дисциплін, як «Прикладні соціально-комунікаційні технології», «Спічрайтинг» та ін.

Мета вивчення дисципліни: ознайомлення студентів з сутністю та основними складовими сучасної державної інформаційної політики, розгляд сучасних інформаційних загроз та методів протидії їм в інформаційній сфері.

Основними **завданнями** вивчення дисципліни є:

- розглянути закони, тенденції, закономірності розвитку інформаційно-комунікаційної сфери, а також інформаційні процеси, які віддзеркалюють інтереси особистості, суспільства і держави.
- окреслити вітчизняний досвід правового регулювання інформаційної сфери;
- проаналізувати основні напрями здійснення державної інформаційної політики в Україні й забезпечення інформаційної безпеки;
- порівняти законодавчу базу окремих медіаінституцій України та країн Європейського Союзу;
- виявити особливості безпечного споживання та розповсюдження інформації.

Згідно з вимогами освітньо-професійної програми студенти повинні у результаті вивчення навчальної дисципліни отримати такі компетентності:

Загальні компетентності:

ЗК01. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК04. Здатність спілкуватися іноземною мовою як усно, так і письмово.

ЗК05. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

Фахові компетентності:

СК02. Здатність критично осмислювати проблеми у сфері журналістики та дотичні до них міждисциплінарні проблеми.

СК05. Здатність зрозуміло і недвозначно доносити власні висновки з питань журналістики, а також знання та пояснення, що їх обґрунтовують, до фахівців і нефахівців, зокрема до осіб, які навчаються.

СК06. Здатність інтегрувати знання та розв'язувати складні задачі журналістики у широких та/або мультидисциплінарних контекстах, за умов неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності.

Результати навчання, формування яких забезпечує вивчення дисципліни. Студент повинен уміти:

ПРН02. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан та розвиток журналістики.

ПРН03. Проводити збір, інтегрований аналіз та узагальнення матеріалів з різних джерел, включаючи наукову та професійну літературу, бази даних, та перевіряти їх на достовірність, використовуючи сучасні методи дослідження.

ПРН06. Оцінювати достовірність інформації та надійність джерел, ефективно опрацьовувати та використовувати інформацію для проведення наукових досліджень та практичної діяльності.

ПРН09. Проводити порівняльний аналіз законодавчої бази та діяльності окремих медіаінституцій України та країн Європейського Союзу.

ПРН14. Здійснювати професійну діяльність у межах етичних і професійних стандартів, керуватися принципами інформаційної безпеки, вміти застосовувати критичне мислення й технології медіааналізу в умовах інформаційних війн.

Опис навчальної дисципліни подано у табл. 1, яка наведена нижче.

Таблиця 1 – Опис навчальної дисципліни

Обов'язковий освітній компонент	
Рівень вищої освіти	другий (магістерський) рівень
Ступінь вищої освіти	магістр
Галузь знань	С «Соціальні науки, журналістика та інформація»
Спеціальність	С7 «Журналістика»
Обмеження щодо форм навчання	Без обмежень

Найменування показників	Характеристика навчальної дисципліни	
	денна форма навчання	заочна форма навчання
Кількість кредитів	5	
Модулів	1	1
Змістових модулів	2	2
Семестр	1	1
Загальна кількість годин	150	
з них аудиторних:	60	10
<i>лекції</i>	24	6
<i>практичні</i>	-	4
<i>лабораторні</i>	-	-
<i>семінарські</i>	36	-
з них самостійної роботи:	90	140
Занять на тиждень	5 год.	-
Індивідуальні завдання	20	
Форма контролю	екзамен	
Курсова робота (проект) (загальний обсяг)	-	

ЗМІСТ КУРСУ

Змістовий модуль 1. Національний інформаційний простір: сучасний стан та проблеми

Тема 1. Державна інформаційна політика, її основні напрями Державна інформаційна політика як сукупність основних напрямів і способів діяльності держави по одержанню, використанню, поширенню та зберіганню інформації.

Головні напрями державної інформаційної політики: забезпечення доступу громадян до інформації; створення національних систем і мереж інформації; зміцнення матеріально-технічних, фінансових, організаційних, правових і наукових основ інформаційної діяльності; забезпечення ефективного використання інформації; сприяння постійному оновленню, збагаченню та зберіганню національних інформаційних ресурсів; створення загальної системи охорони інформації; сприяння міжнародному співробітництву в галузі інформації і гарантування інформаційного суверенітету України.

[3, 4, 6, 10, 11, 16, 22].

Тема 2. Основні функції Міністерства культури та стратегічних комунікацій України

Особливості діяльності. Підпорядковані органи. Попередні відомства. Стратегічні комунікації та інформаційна безпека. Захист культурної спадщини та національної пам'яті. Державна мовна політика. Безбар'єрність у культурі.

[36].

Тема 3. Стратегія формування та розвитку єдиного інформаційного простору України

Національний інформаційний простір: сучасний стан та проблеми. Державне управління національними інформаційними ресурсами. Інформаційна політика зарубіжних країн щодо побудови інформаційного суспільства.

[3, 4, 6, 10, 11, 16, 22, 44, 45].

Тема 4. Засади державної інформаційної політики

Історичні умови, які впливають на нинішню інформаційну політику. Ідеологічні та політичні аспекти держінформполітики. Структурні установи, через які держава проводить свою інформаційну політику. Шляхи і форми реалізації інформаційної стратегії і тактики. Аномалії інформаційної політики. Чужоземна експансія в українське медіа-поле: мета і реальні та можливі наслідки. Виклики і перспективи державної інформаційної політики.

[3, 4, 6, 10, 11, 16, 22, 44, 45].

Тема 5. Медіа та державна інформаційна політика

Характеристика сучасного інформаційного простору України: передісторія, формування, структура, особливості. Особливості сучасної інформаційної політики. Інформаційна політика щодо національного радіо- та телерадіоєфіру. Інтернет як важлива галузь державної інформаційної політики. Українська присутність в Інтернеті.

Журналістика та державна ідеологія. Влада і журналістика.

[3, 4, 6, 10, 11, 16, 18, 22, 30, 37, 44, 45].

Тема 6. Правове забезпечення державної інформаційної політики. Законодавство в галузі інформації

Законодавчі акти, які регулюють взаємини засобів масової комунікації та суспільства. Закони: «Про інформацію» (1992 р.), «Про медіа» (2022) та ін.

Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»

Указ Президента України Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»

Закон України Про національну безпеку України (Відомості Верховної Ради (ВВР), 2018, № 31, ст.241).

Указ Президента України №348/2021 від 11 серпня 2021 року «Стратегія комунікації з питань євроатлантичної інтеграції України на період до 2025 року»

Міжнародно-правові акти у сфері інформаційної політики. Законодавчі новації в медіаіндустрії як відповідь на безпекові виклики та виконання вимог щодо членства України в ЄС.

Рекомендації CM/Rec(2022)16 Комітету Міністрів Ради Європи державам-членам щодо боротьби з мовою ворожнечі, ухвалені 20 травня 2022 року; Рекомендації CM/Rec(2022)4 Комітету Міністрів державам-членам щодо просування сприятливого середовища для якісної журналістики у цифрову еру, ухвалені 17 березня 2022 року; Рекомендації CM/Rec(2022)13 Комітету Міністрів державам-членам щодо впливу цифрових технологій на свободу вираження, ухвалені 6 квітня 2022 року.

Порівняльний аналіз офіційних документів: Закону України «Про доступ до публічної інформації» та Конвенції Ради Європи про доступ до офіційних документів.

[4, 10, 11, 16, 23, 35, 37, 46-50, 59, 60].

Змістовий модуль 2.

Визначення і характеристика чинників інформаційної безпеки медіапростору України

Теми 7-8. Інформаційна безпека держави, суспільства, особи

Шляхи вирішення проблеми інформаційної безпеки. Об'єкти деструктивного інформаційного впливу. Види інформаційної зброї. Форми проведення пропаганди. Форми диверсифікації громадської думки. Основні загрози національній безпеці України в інформаційній сфері.

[1, 2, 5, 6-9, 12, 13, 15, 25-29].

Тема 9. Поняття інформаційної війни

Історія походження термінів: психологічна війна, інформаційні/психологічні операції, пропаганда. Визначення понять: психологічні війни (операції), інформаційні війни, пропаганда. Підходи до визначення пропаганди. Теоретичні аспекти психологічних операцій. Асиметрична інформаційна дія.

[1, 2, 5, 9, 12, 13, 18, 19, 24, 28, 29, 31-34, 40, 51-56].

Тема 10. Сучасні інформаційні війни

Сучасні інформаційні війни всередині країни: причини, приводи, практика. Зовнішні інформаційні війни – форми і види інформаційної експансії.

[1, 2, 5, 9, 12, 13, 18, 19, 24, 28, 29, 31-34, 40, 51-56].

Тема 11. Внутрішні та зовнішні чинники ескалації загроз інформаційній безпеці України

Внутрішні чинники ескалації загроз інформаційній безпеці України (впровадження політичної цензури; створення негативного іміджу України на міжнародній арені внаслідок неефективної інформаційної політики; руйнування моральних цінностей людини й суспільства внаслідок інформаційного впливу негативного характеру; тиск на ЗМІ з метою зміни їх політичного курсу (економічні та законодавчі санкції); прояви політичного екстремізму стосовно журналістів; монополізація окремих видів інформаційних послуг; обмеженість рекламного ринку та іноземних інвестицій).

Зовнішні чинники ескалації загроз інформаційній безпеці України (діяльність іноземних розвідок; міжнародна комп'ютерна злочинність; високий рівень присутності зарубіжних держав в інформаційному просторі України; спрямований інформаційний вплив на Україну з боку іноземних держав або конкуруючих компаній).

[1, 2, 5, 9, 12, 13, 14, 18, 19, 24, 28, 29, 31-34, 40, 51-56].

Тема 12. Медіаграмотність як вимога сучасного інформаційного суспільства, особливості протидії загрозам інформаційної безпеки.

Загрози у сучасному інформаційному просторі. Необхідність формування медіаінформаційної грамотності у сучасних умовах. Розвиток критичного мислення як протидія політичним маніпуляціям. Правила безпечного споживання інформації. Особливості безпечного споживання радіо- та телевізійної інформації. Особливості безпечного споживання інформації в друкованих та онлайн-медіа. Шляхи мінімізації впливів маніпуляторів в YouTube. Особливості маніпуляцій в Viber та Telegram-каналах.

[1, 5, 17, 20, 21, 37, 38, 42, 43, 57, 58].

ФОРМИ КОНТРОЛЮ ТА КРИТЕРІЇ ОЦІНЮВАННЯ ЗНАНЬ

Згідно з діючою в університеті системою комплексної діагностики знань студентів, з метою стимулювання планомірної та систематичної навчальної роботи, оцінка знань студентів здійснюється за 100-бальною системою. Позитивною вважається оцінка від 60 до 100 балів.

Форми контролю знань студентів:

- поточний;
- рубіжний;
- підсумковий (екзамен).

Методами контролю є: усний контроль (усне опитування), письмовий, тестовий, а також методи самоконтролю і самооцінки.

Поточний контроль знань студентів протягом одного семестру включає оцінку за роботу на лекційних, семінарських заняттях та самостійну роботу.

Критерії поточної оцінки знань студентів

Під час занять студенти усно доповідають на питання, виконують індивідуальні завдання, аналізують виступи одногрупників. Активна робота студента на занятті оцінюється в 2 бали.

Критерії оцінки на семінарському занятті наведені нижче у табл. 2, розподіл балів з дисципліни «Інформаційна політика та безпека» у табл. 3.

Таблиця 2 – Критерії оцінки на практичному занятті

Бали	Критерії оцінки
2	Студент(ка) в повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів або письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та завдань, активний, часто виступає і часто задає питання
1	Студент(ка) володіє більшою частиною навчального матеріалу, виконує більшість завдань і домашньої/самостійної роботи, іноді виступає і ставить питання

Таблиця 3 – Розподіл балів з дисципліни

	Поточна навчальна діяльність	Кількість балів			Разом
		Семінарські заняття			
		Опитування	контрольна робота	індивідуальні творчі завдання	
1	Змістовий модуль 1 (6 лекц., 9 практ. зан.)	18	6	11	35
	Тема 1.	2			2
	Тема 2.	2+2			6
	Тема 3.	2			4
	Тема 4.	2+2		3	4
	Тема 5.	2		3	2
	Тема 6.	2+2		5	4
	Контрольна робота		6		5
2	Змістовий модуль 2 (6 лекц., 9 практ. зан.)	18	6	11	35
	Тема 7.	2			4
	Тема 8.	2+2			6
	Тема 9.	2		3	4
	Тема 10.	2+2			4
	Тема 11.	2		3	2
	Тема 12.	2+2		5	4
	Контрольна робота		6		5
	Разом	36	12	22	70

За певні види роботи студенту надаються бали:

«2» бали – вища оцінка за відповідь на семінарському занятті;
 «5» балів – вища оцінка за виконання творчого індивідуального завдання (написання студентами есеїв, анотацій, складання конспектів).

«6» балів – аудиторна контрольна робота (рубіжний контроль).
 Студент має змогу отримати додаткові бали за:

а) доповнення виступу:

2 бали – отримують студенти, які глибоко володіють матеріалом, чітко визначили його зміст; зробили глибокий системний аналіз змісту виступу, виявили нові ідеї та положення, що не були розглянуті, але суттєво впливають на зміст доповіді, надали власні аргументи щодо основних положень даної теми.

1 бал отримують студенти, які виклали матеріал з обговорюваної теми, що доповнює зміст виступу, поглиблює знання з цієї теми та висловили власну думку.

б) суттєві запитання до доповідачів:

2 бали отримують студенти, які своїм запитанням до виступаючого суттєво і конструктивно можуть доповнити хід обговорення теми.

1 бал отримують студенти, які у своєму запитанні до того, хто виступає вимагають додаткової інформації з ключових проблем теми, що розглядається.

Максимальна кількість балів, яку може набрати студент за кожен змістовий модуль у ході аудиторних занять, а також в системі дистанційної освіти moodle – 70.

Максимальна кількість балів, які може отримати студент під час екзамену – 30.

Рубіжний контроль знань студентів здійснюється через проведення письмових контрольних робіт (тестів), які проводяться на окремому тижні під час заняття. Здобувач має змогу отримати 7 балів у першому змістовому модулі, 8 – у другому змістовому модулі за виконання індивідуальних завдань та підвищити загальну суму балів.

Якщо здобувач виконав успішно всі наведені до рубіжного контролю завдання – він може не виконувати контрольну роботу/тести.

В структурі навчання виділяють 2 змістових модулі. Тобто студенти двічі за семестр складають рубіжний контроль.

Підсумковий модульний контроль

Семестровий підсумковий контроль з дисципліни є обов'язковою формою контролю навчальних досягнень здобувача вищої освіти. Підсумковий модульний контроль знань студентів означає поступове накопичення балів від одного поточного контролю до іншого в кінцевому рахунку отримання загального підсумкового балу.

Критерії оцінки на екзамені

Три питання потребують змістовної відповіді, кожна з них розкриває сутність того чи іншого поняття або теоретичного положення (оцінюється від 0 до 10 балів за кожне питання). Максимальна кількість складає **30 балів**. При дистанційному навчанні використовуються тестові завдання або усна співбесіда. Тест складається з питань, які в сумі дають також **30 балів**.

30 балів отримують студенти, які повністю розкрили сутність питань, дали чітке визначення понять.

25-20 балів отримують студенти, які правильно, але не повно розкрили сутність питань, дали чітке визначення понять.

15-10 балів отримують студенти, які правильно, але лише частково розкрили сутність питань, дали визначення понять.

10-5 балів отримують студенти, які поверхово розкрили сутність питань, дали не зовсім чітке визначення понять.

0 балів отримують студенти, які недопущені або не з'явилися на залік.

Замість виконання завдань (вивчення тем) можуть додатково враховуватись такі види активностей здобувача (неформальна освіта) за умов підтвердження результатів (сертифікат з зазначення обсягу кредитів, сертифікат участі, грамота учасника конференції, сертифікат за призове місце у конкурсі тощо):

– проходження тренінг-курсів чи дистанційних курсів з використання сучасних освітніх технологій на платформах Coursera, Prometheus тощо (за наявності відповідного документу про їх закінчення, надання копії викладачу);

– участь в майстер-класах, форумах, конференціях, семінарах, зустрічах з проблем у галузі публічних виступів (з підготовкою промови, спічу, презентації, імпровізації, самоаналізу після дискусії, інформаційного повідомлення тощо, що підтверджено навчальною програмою заходу чи відповідним сертифікатом; збірником тез тощо).

Кожен здобувач заочної форми навчання виконує контрольну роботу за варіантом. Вибір варіанту здійснюється за порядковим номером П.І.Б. студента у списку академічної групи або журналу обліку відвідування занять. В кожному варіанті необхідно розглянути певні питання (які можуть бути розділені на два-три підпункти).

Кожен варіант контрольної роботи оцінюється в 70 балів максимум. Після перевірки викладачем письмової контрольної роботи та її захисту в усному вигляді викладач допускає здобувача до екзамену. Критерії оцінки відповідей на екзамені той самий, що і у денної форми. Завдання екзамену складають 30 балів.

Таблиця 4 – Критерії оцінки контрольної роботи для студентів заочної форми навчання

Контрольна робота (захист)	Критерії оцінки
61-70	Студент(ка) у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних відповідей і обговорення, глибоко та всебічно розкриває зміст теоретичних питань й завдань, використовуючи при цьому обов'язкову й додаткову літературу. Демонструє набуття загальних та фахових компетентностей. Робота відповідає стандартам оформлення
51-60	Студент(ка) достатньо повно володіє навчальним матеріалом, обгрунтовано викладає його під час усного виступу, відповідей. Розкриває зміст теоретичних питань та завдань, використовуючи при цьому обов'язкову літературу. Здобувач(ка) має власну думку щодо тематики. При викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Робота відповідає стандартам оформлення
41-50	Студент(ка) в цілому, володіє навчальним матеріалом, викладає його основний зміст під час усного виступу та відповідей на запитання, але без глибокого всебічного аналізу, обгрунтування, без використання необхідної літератури, допускаючи при цьому окремі неточності та помилки. Робота має відхилення від стандартів оформлення та помилки

31-40	Студент(ка) не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час усного виступу. Відповіді на запитання загальні, короткі, студент(ка) недостатньо розкриває зміст теоретичних питань, допускаючи при цьому суттєві неточності
21-30	Студент(ка) частково володіє навчальним матеріалом, не в змозі викласти зміст більшості питань під час доповіді. Допускаються суттєві помилки. Зміст тексту роботи не розкриває тему
11-20	Студент(ка) майже не володіє навчальним матеріалом та не в змозі його викласти, слабко розуміє зміст теоретичних питань та практичних завдань
0-10	Студент(ка) не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань

Продовження табл. 4

ПРАКТИЧНІ ЗАНЯТТЯ

Семінарські заняття дають змогу студентам застосувати теоретичні знання у реальному або змодельованому медійному середовищі. Це стимулює критичне мислення, аналітичні навички та глибше розуміння комунікативних процесів. Колективне обговорення кейсів, моделювання комунікативних ситуацій, аналіз маніпулятивних прийомів навчає не лише розпізнавати вплив, а й будувати ефективні етичні комунікації. Заняття допомагають студентам формувати навички для майбутньої кар'єри у сфері журналістики, PR, реклами, соціальних комунікацій, медіаменеджменту та аналітики.

Методичні рекомендації студентам для виконання практичних занять:

- ознайомтесь з темою (табл. 5) та питаннями, що винесені на обговорення на семінарському занятті;
- ретельно опрацюйте запропоновані теоретичні джерела;
- виконайте письмове завдання (за наявності) та здайте у файловому форматі для перевірки у системі мудл;
- застосуйте опрацьований матеріал під час обговорення дискусійних питань з теми та реалізації практичних кейсів.

Таблиця 5 – Тематика практичних занять

№ з/п	Назва теми	Кількість годин
1	Основні напрями державної інформаційної політики	2
2	Основні функції Міністерства культури та стратегічних комунікацій України	2
3	Інформаційна політика зарубіжних країн щодо побудови інформаційного суспільства	2
4	Національний інформаційний простір: сучасний стан та проблеми	2
5	Засади державної інформаційної політики	2
6	Аномалії інформаційної політики	2
7	Медіа та державна інформаційна політика	2

Продовження табл. 5

8	Правове забезпечення державної інформаційної політики	2
9	Законодавчі новації в медіаіндустрії як відповідь на безпекові виклики та виконання вимог щодо членства України в ЄС. Міжнародні правові акти у сфері інформаційної політики	2
10-11	Інформаційна безпека держави, суспільства, особи	4
12	Інформаційний суверенітет і національна безпека	2
13	Поняття інформаційної війни	2
14	Інформаційна безпека телевізійного простору України	2
15	Інформаційна безпека в мережі Інтернет	2
16	Внутрішні та зовнішні чинники ескалації загроз інформаційній безпеці України	2
17	Медіаграмотність як вимога сучасного інформаційного суспільства	2
18	Правила безпечного споживання інформації	2

Плани практичних занять

Практичне заняття № 1

Основні напрями державної інформаційної політики

Питання для обговорення:

1. Державна інформаційна політика як сукупність основних напрямів і способів діяльності держави по одержанню, використанню, поширенню та зберіганню інформації.
2. Головні напрями державної інформаційної політики:
 - забезпечення доступу громадян до інформації; створення національних систем і мереж інформації;
 - зміцнення матеріально-технічних, фінансових, організаційних, правових і наукових основ інформаційної діяльності;

- забезпечення ефективного використання інформації; сприяння постійному оновленню, збагаченню та зберіганню національних інформаційних ресурсів;
 - створення загальної системи охорони інформації;
 - сприяння міжнародному співробітництву в галузі інформації і гарантування інформаційного суверенітету України.
3. Завдання державної інформаційної політики.
 4. Законодавчі акти, які регулюють взаємини медіа та суспільства.

Практичне заняття № 2

Основні функції Міністерства культури та стратегічних комунікацій України

Питання для обговорення:

1. Особливості діяльності Міністерства культури та стратегічних комунікацій України.
2. Підпорядковані органи.
3. Попередні відомства Міністерства культури та стратегічних комунікацій України.
4. Стратегічні комунікації та інформаційна безпека.
5. Захист культурної спадщини та національної пам'яті.
6. Державна мовна політика.
7. Безбар'єрність у культурі.

Виконайте завдання: ознайомтесь зі структурою та наповненням сайту Міністерства культури та стратегічних комунікацій України (URL : [Головна | Міністерства культури та стратегічних комунікацій](#))

Практичне заняття № 3

Інформаційна політика зарубіжних країн щодо побудови інформаційного суспільства

Питання для обговорення:

1. Загальні аспекти зарубіжного досвіду регулювання інформаційної сфери
2. Американський досвід розвитку національної інформаційної інфраструктури
3. Канадський досвід побудови інформаційної магістралі

4. Інформаційна політика Європейського Союзу щодо побудови інформаційного суспільства
5. Правове регулювання інформаційної сфери в Україні та світі

Практичне заняття № 4

Національний інформаційний простір: сучасний стан та проблеми

Питання для обговорення:

1. Характеристика сучасного інформаційного простору України: передісторія, формування, структура, особливості.
2. Особливості сучасної інформаційної політики.
3. Інформаційна політика щодо національного радіо- та телерадіоєфіру.
4. Інтернет як важлива галузь державної інформаційної політики. Українська присутність в Інтернеті.

Практичне заняття №5

Засади державної інформаційної політики

Питання для обговорення:

1. Історичні умови, які впливають на нинішню інформаційну політику.
2. Ідеологічні та політичні аспекти держінформполітики.
3. Законодавчі акти, які регулюють взаємини засобів масової комунікації та суспільства.
4. Структурні установи, через які держава проводить свою інформаційну політику.
5. Шляхи і форми реалізації інформаційної стратегії і тактики.

Практичне заняття №6

Аномалії інформаційної політики

Питання для обговорення:

1. Визначення цензури. Історія, зміст, форми і суть цензурного нагляду. Цензурний контроль як антидемократичний складник інформаційної політики.
2. Економічна залежність медіа – могилиниця їхньої незалежності.
3. Тиск на медіа через структури виконавчої влади.

4. Чужоземна експансія в українське медіа-поле: мета і реальні та можливі наслідки. Інформаційний тиск через телебачення та Інтернет.

5. Терор проти журналістів.

6. Боротьба журналістів за свободу слова.

Виконайте завдання: наведіть приклади прояву політичного екстремізму стосовно журналістів.

Практичне заняття № 7.

Медіа та державна інформаційна політика

Питання для обговорення:

1. Журналістика та державна ідеологія.
2. Влада і журналістика: колізії і конфлікти.
3. Свобода слова – підмурівок інформаційної політики.
4. Основні загрози національній безпеці України в інформаційній сфері.

Виконайте завдання: Змодельуйте ситуацію законного та незаконного обмеження свободи слова.

Практичні заняття № 8.

Правове забезпечення державної інформаційної політики

Питання для обговорення:

1. Законодавство у сфері медіа.
2. Доктрина інформаційної безпеки України.
3. Стратегія інформаційної безпеки.
4. Закон України «Про національну безпеку України».

Практичне заняття № 9.

Законодавчі новації в медіаіндустрії як відповідь на безпекові виклики та виконання вимог щодо членства України в ЄС. Міжнародні правові акти у сфері інформаційної політики

Питання для обговорення:

1. Указ Президента України №348/2021 від 11 серпня 2021 року «Стратегія комунікації з питань євроатлантичної інтеграції України на період до 2025 року».

2. Порівняльний аналіз офіційних документів Закону України «Про доступ до публічної інформації» та Конвенції Ради Європи про доступ до офіційних документів.

3. Міжнародні правові акти у сфері інформаційної політики:

Рекомендації CM/Rec(2022)16 Комітету Міністрів Ради Європи державам-членам щодо боротьби з мовою ворожнечі, ухваленої 20 травня 2022 року.

Рекомендації CM/Rec(2022)4 Комітету Міністрів державам-членам щодо просування сприятливого середовища для якісної журналістики у цифрову еру, ухваленої 17 березня 2022 року.

Рекомендації CM/Rec(2022)13 Комітету Міністрів державам-членам щодо впливу цифрових технологій на свободу вираження, ухваленої 6 квітня 2022 року.

Практичні заняття № 10-11.

Інформаційна безпека держави, суспільства, особи

Питання для обговорення:

1. Визначення понять «інформаційна безпека», «інформаційна безпека держави», «інформаційна безпека суспільства», «інформаційна безпека особи».
2. Шляхи вирішення проблем інформаційної безпеки.
3. Об'єкти деструктивного інформаційного впливу.
4. Види інформаційної зброї.
5. Форми проведення пропаганди.
6. Форми диверсифікації громадської думки.

Практичне заняття № 12.

Інформаційний суверенітет і національна безпека

Питання для обговорення:

1. Інформація в сучасному світі, її роль і значення в політичних протистояннях.
2. Поняття інформаційного суверенітету та інформаційної безпеки країни.
3. Захист національного медіа-простору – вимога часу
4. Технічні аспекти інформаційної безпеки.

Практичне заняття № 13.

Поняття інформаційної війни

Питання для обговорення:

1. Історія походження термінів: психологічна війна, інформаційні/психологічні операції, пропаганда.

2. Визначення понять: психологічні війни (операції), інформаційні війни, пропаганда.
3. Підходи до визначення пропаганди.
4. Теоретичні аспекти психологічних операцій.
5. Асиметрична інформаційна дія.
6. Сучасні інформаційні війни всередині країни: причини, приводи, практика.
7. Зовнішні інформаційні війни – форми і види інформаційної експансії.

Виконайте завдання: прореферуйте видання:

Почепцов Г. Сучасні інформаційні війни. Київ : Києво-Могилянська академія, 2016. 502 с.

Почепцов Г. Інформаційні операції та ментальні війни. Київ : Вид. дім «Києво-Могилянська академія», 2024. 320 с.

Практичне заняття № 14.

Інформаційна безпека телевізійного простору України

Питання для обговорення:

1. Чинники інформаційної безпеки телевізійного простору:
 - державна складова формування телепростору;
 - суспільний чинник телевізійної інфраструктури;
 - особистість у телевізійному просторі країни
2. Політико-правові аспекти безпеки телевізійного простору.
3. Мовний чинник інформаційної безпеки

Виконайте завдання:

прореферуйте видання: Сашук Г. Безпекові виміри телепростору: Монографія. Київ : Грамота, 2007. 136 с.

Практичне заняття № 15.

Інформаційна безпека в мережі Інтернет

Питання для обговорення:

1. Інтернет як значущий фактор соціалізації.
2. Основні джерела небезпек у Інтернеті. Типи загроз. Загрози соціальних мереж.
3. Рекомендації для нейтралізації факторів ризику.
4. 9 лютого – День безпечного Інтернету (Safer Internet Day).
5. Основні правила безпечної роботи (поведінки) в інтернеті.

6. Правила збереження персональної інформації.

Виконайте завдання: наведіть 2-3 приклади небезпек у Інтернеті.

Практичне заняття № 16.

Внутрішні та зовнішні чинники ескалації загроз інформаційній безпеці України

Питання для обговорення:

Внутрішні чинники

1. Впровадження політичної цензури.
2. Створення негативного іміджу України на міжнародній арені внаслідок неефективної інформаційної політики.
3. Руїнування моральних цінностей людини й суспільства внаслідок інформаційного впливу негативного характеру.
4. Тиск на медіа з метою зміни їх політичного курсу (економічні та законодавчі санкції).
5. Прояви політичного екстремізму стосовно журналістів.
6. Монополізація окремих видів інформаційних послуг.
7. Обмеженість рекламного ринку та іноземних інвестицій.

Зовнішні чинники

1. Діяльність іноземних розвідок.
2. Міжнародна комп'ютерна злочинність.
3. Високий рівень присутності зарубіжних держав в інформаційному просторі України.
4. Спрямований інформаційний вплив на Україну з боку іноземних держав або конкуруючих компаній.

Виконайте завдання: Назвіть форми і види зовнішніх та внутрішніх інформаційних війн

Практичне заняття № 17.

Медіаграмотність як вимога сучасного інформаційного суспільства

Питання для обговорення:

1. Загрози у сучасному інформаційному просторі.
2. Необхідність формування медіаінформаційної грамотності у сучасних умовах.
3. Розвиток критичного мислення як протидія політичним маніпуляціям.

Виконайте завдання:

Напишіть есей «Важливість медійної та інформаційної грамотності в наш час»

Практичне заняття № 18.**Правила безпечного споживання інформації****Питання для обговорення:**

1. Особливості безпечного споживання радіо- та телевізійної інформації.
2. Особливості безпечного споживання інформації в друкованих та онлайн-медіа.
3. Шляхи мінімізації впливів маніпуляторів в YouTube.
4. Особливості маніпуляцій в Viber та Telegram-каналах.

Виконайте завдання:

Знайдіть 4-5 прикладів маніпулювання аудиторією через порушення стандартів в засобах масової комунікації (результати подати у вигляді аналізу цих прикладів).

ІНДИВІДУАЛЬНІ ЗАВДАННЯ ТА МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДО ЇХ ВИКОНАННЯ

Під час вивчення дисципліни «Інформаційна політика та безпека» виокремлено такі види самостійного навчання студента:

- підготовка до семінарських занять;
- відпрацювання пропущених тем лекцій і семінарських занять;
- виконання індивідуальних завдань;
- підготовка до рубіжного контролю та підсумкового контролю (екзамен);
- робота з інформаційними джерелами;
- отримання навичок в системі неформальної освіти.

З метою самостійного опрацювання частини програмного матеріалу з курсу, поглиблення знань, отриманих у процесі лекційних та семінарських занять, студенти мають виконувати індивідуальні завдання. Із зазначеного курсу заплановано: для студентів заочної форми навчання – контрольна робота, для студентів денної форми навчання – творчі індивідуальні завдання.

Індивідуальні завдання до першого змістового модуля (треба виконати до 7-го тижня):

1. Назвіть форми і види зовнішніх інформаційних війн.
2. Змоделюйте ситуацію законного та незаконного обмеження свободи слова.

3. Складіть анотацію до статті Георгія Почепцова «Інформаційні війни: нові тенденції». URL: http://osvita.mediasapiens.ua/trends/1411978127/informatsionnye_voyny_novye_tendentsii/

Індивідуальні завдання до другого змістового модуля (треба виконати до 12-го тижня)

1. Назвіть форми і види внутрішніх інформаційних війн.
2. Наведіть приклади прояву політичного екстремізму стосовно журналістів.

3. Складіть конспект за статтею Георгія Почепцова «Перші дослідження в галузі інформаційних війн: від минулого до сучасності». URL: <http://osvita.mediasapiens.ua/trends>

Студенти мають змогу завантажити свої напрацювання в

систему дистанційного навчання (moodle) НУ «Запорізька політехніка» (<https://moodle.zp.edu.ua/>).

Отримання навичок Soft Skills.

Рівень успіху вже давно перестав залежати тільки від того, наскільки добре фахівець виконує свої безпосередні обов'язки. Сьогодні не менш важливі й Soft Skills («м'які навички») – універсальні непрофесійні якості, які допомагають нам взаємодіяти між собою в команді, спільноті, громаді незалежно від сфери діяльності. Рекомендовані матеріали щодо отримання:

1. Медіаграмотність: як не піддаватися маніпуляціям. Курс. URL: <https://courses.prometheus.org.ua/courses/course-v1:Prometheus+MEDIA+L101+2022+T3/course/>

2. Думай інакше: зламай перешкоди на шляху до навчання та відкрий свій прихований потенціал. Курс. URL: <https://courses.prometheus.org.ua/courses/course-v1:Prometheus+MINDSHIFT101+2021+T2/course/>

3. Культура толерантності: як побудувати суспільство, комфортне для всіх. Курс. URL: <https://courses.prometheus.org.ua/courses/course-v1:Prometheus+TOL101+2020+T3/course/>

В умовах дії обставин непоборної сили рекомендовані такі курси з онлайн-освіти:

1. Життєстійкість молоді в умовах криз. URL: [https://courses.prometheus.org.ua/courses/course-v1:Prometheus+RESILIENCE101+2022+T3/about](https://courses.prometheus.org.ua/courses/course-v1:Prometheus+RESILIENCE101+2022+T3/about;);

2. Інформаційна безпека URL: https://courses.prometheus.org.ua/courses/course-v1:Internews+INFOS101+UA_2021+T3/about.

ЗРАЗКИ ТЕСТОВИХ ЗАВДАНЬ КОНТРОЛЬНОЇ РОБОТИ ДЛЯ СТУДЕНТІВ ДЕННОЇ ФОРМИ НАВЧАННЯ

До змістового модуля №1.

1. Виберіть правильну відповідь:

Інформаційна політика в державі залежить від:

- а) від суспільно-політичного ладу і типу державного утворення;
- б) від політичних партій;
- в) від суспільства;
- г) від впливу країн сусідів.

2. Виберіть правильну відповідь:

Інформаційні матеріали – це:

- а) сукупність джерел та систем, що містять інформацію, призначену для передачі;
- б) ресурси, які розкривають духовні, культурні, історичні, національні цінності, традиції, надбання держави, нації в різних сферах життя суспільства;
- в) інформаційна інфраструктура, тобто абсолютно всі проміжні ланки між інформацією та людиною;
- г) друковані наукові і художні видання.

3. Виберіть правильну відповідь:

У статті 34 якого закону зазначається: «Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб і на свій вибір»:

- а) Конвенція про захист прав людини і основних свобод;
- б) Загальна декларація прав людини;
- в) Конституція України;
- г) Кодекс етики журналіста.

4. Виберіть правильну відповідь: Цензура як перешкоджання свободі думки і слова, вільному вираженню думок та переконань, в Україні заборонена:

- а) Конституцією України ст. 24;
- б) Конституцією України ст. 15 та рядом інших законів;
- в) Цивільним кодексом України ст. 206;
- г) Конституцією України (ст. 24) та Цивільним кодексом України (ст. 206).

5. Виберіть правильну відповідь:

Структура, що забезпечує виконання конституційних повноважень Президента в інформаційній сфері, опрацьовує законодавчі акти інформаційної політики, проводить моніторинг та аналіз інформаційного простору, забезпечує аналітичними матеріалами Президента.

а) головна інформаційна служба секретаріату президента України;

б) національна рада України з питань телебачення та радіомовлення;

в) комітет у справах свободи слова та інформації верховної ради України;

г) державні засоби масової інформації.

6. Виберіть правильну відповідь:

Різновид державної політики, що охоплює весь спектр міжнародних відносин:

а) міжнародна державна політика;

б) всесвітня державна політика;

в) загальна державна політика;

г) зовнішня державна політика.

7. Виберіть правильну відповідь:

За тоталітарного режиму державна інформаційна політика характеризується:

а) свободою слова і преси; свободою громадянина; верховенством права;

б) встановленням повного контролю над усіма сферами життя;

в) мілітаризацією державного апарату, посиленням впливу гіпертрофованого військово-промислового комплексу на формування і проведення внутрішньої і зовнішньої політики;

г) високою політичною свободою людини, реальним здійсненням її прав, що дозволяє йому робити вплив на державне управління суспільством, можливістю громадян приймати участь у формуванні внутрішньої та зовнішньої політики.

8. Виберіть правильну відповідь:

Термін «політика» з грецької мови перекладається як ...

а) відносини країн;

б) державна діяльність;

в) закон;

г) партія.

9. Виберіть правильну відповідь:

Державна інформаційна політика – це:

- а) міжнародне співробітництво в галузі інформації;
- б) гарантування інформаційного суверенітету України;
- в) створення національних систем і мереж інформації;
- г) сукупність основних напрямів і способів діяльності держави по одержанню, використанню, поширенню та зберіганню інформації.

10. Виберіть правильну відповідь:

Журналісти вбачають основні загрози для свободи слова та медіа в Україні:

- а) в економічній залежності ЗМІ, відсутності відповідальності за порушення їхніх прав і в перешкодженні професійній діяльності;
- б) у відсутності відповідальності за порушення їхніх прав;
- в) у перешкодженні професійній діяльності;
- г) усі варіанти відповідей правильні.

11. Виберіть правильну відповідь:

Стаття Конституції України, в якій проголошується свобода слова і думки:

- а) 44;
- б) 21;
- в) 34;
- г) 68.

12. Виберіть правильну відповідь:

Типи цензури:

- а) позитивна та негативна;
- б) відкрита та прихована;
- в) інформаційна та аналітична;
- г) внутрішня та зовнішня.

13. Виберіть правильну відповідь: Головним органом у системі центральних органів виконавчої влади у сфері забезпечення інформаційного суверенітету України, зокрема, з питань поширення суспільно важливої інформації в Україні та за її межами, а також забезпечення функціонування державних інформаційних ресурсів є:

- а) Адміністрація Президента України;
- б) Голова Ради національної безпеки і оборони України;
- в) Міністерство культури та стратегічних комунікацій України;

г) Верховна Рада України.

14. Виберіть правильну відповідь:

Стаття Конституції України, в якій проголошується заборона цензури:

а) 37; б) 69; в) 21; г) 15.

15. Виберіть правильну відповідь:

Свобода слова – це:

а) небезпечні діяння з інформаційного впливу на соціальні групи осіб, державні органи влади та управління, пов'язані з поширенням інформації, яка містить погрози переслідуванням, розправою, вбивствами;

б) право людини вільно висловлювати свої думки – розглядається прихильниками лібералізму як одна з найважливіших громадянських свобод. охоплює свободу вираження поглядів як в усній, так і в письмовій формі (свобода преси і змі); в меншій мірі стосується до політичної і соціальної реклами (пропаганди). ідеологія лібералізму ставить державну цензуру, або будь-яку іншу форму державного примусу до висловлення поглядів або відмови від них, поза законом;

в) стан захищеності психіки та здоров'я людини від деструктивного інформаційного впливу;

г) вплив на психіку людини шляхом залякування, погроз із метою спонукання до певної запланованої моделі поведінки.

16. Цензура – це:

а) програмна закладка, яка завчасно впроваджується в інформаційні системи й мережі, що забезпечують управління об'єктами військової та цивільної інфраструктури;

б) легальні та (або) протиправні акції, реалізація яких може мати негативний вплив на безпеку інформаційного простору держави;

в) контроль влади за змістом і розповсюдженням інформації, друкованої продукції, музичних і сценічних творів, творів образотворчого мистецтва, кіно-, фотоматеріалів, передач радіо і телебачення, веб-ресурсів, у деяких випадках — також приватного листування, з метою обмеження або недопущення поширення ідей і відомостей, визнаних владою шкідливими, небажаними для неї або суспільства в цілому;

г) організоване цілеспрямоване застосування спеціальних інформаційних засобів і технологій для внесення змін у свідомість особи чи населення.

17. Виберіть правильну відповідь:

Виберіть правильну відповідь:

Державна політика поділяється на:

- а) відкрити і закрити;
- б) повну і часткову;
- в) внутрішню і зовнішню;
- г) державну і не державну.

18. Виберіть правильну відповідь:

Загальне керівництво у сферах національної безпеки та оборони України здійснюють:

- а) Президент України;
- б) Голова Ради національної безпеки і оборони України;
- в) Президент України, Верховний Головнокомандувач Збройних Сил України і Голова Ради національної безпеки і оборони України;
- г) Верховний Головнокомандувач Збройних Сил України.

До змістового модуля №2.

1. Виберіть правильну відповідь: Акти зовнішньої інформаційної агресії – це:

- а) легальні або протиправні акції, реалізація яких може мати негативний вплив на безпеку інформаційного простору держави;
- б) сплановані дії, спрямовані на ворожу, дружню або нейтральну аудиторію, які передбачають вплив на її свідомість і поведінку за допомогою використання організованої інформації та інформаційних технологій для досягнення певної мети;
- в) небезпечні діяння з інформаційного впливу на соціальні групи осіб, державні органи влади та управління, пов'язані з поширенням інформації, яка містить погрози переслідуванням, розпорою, вбивствами, а також викривлення об'єктивної інформації, що спричиняє виникнення кризових ситуацій у державі, нагнітання страху і напруги в суспільстві;
- г) протиправні діяння у сфері використання електронних обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж.

2. Виберіть правильну відповідь:

Інформаційний тероризм – це:

а) легальні або протиправні акції, реалізація яких може мати негативний вплив на безпеку інформаційного простору держави;

б) сплановані дії, спрямовані на ворожу, дружню або нейтральну аудиторію, які передбачають вплив на її свідомість і поведінку за допомогою використання організованої інформації та інформаційних технологій для досягнення певної мети;

в) небезпечні діяння з інформаційного впливу на соціальні групи осіб, державні органи влади та управління, пов'язані з поширенням інформації, яка містить погрози переслідуванням, розпорою, вбивствами, а також викривлення об'єктивної інформації, що спричиняє виникнення кризових ситуацій у державі, нагнітання страху і напруги в суспільстві;

г) протиправні діяння у сфері використання електронних обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж.

3. Виберіть правильну відповідь: Комп'ютерна злочинність – це:

а) легальні або протиправні акції, реалізація яких може мати негативний вплив на безпеку інформаційного простору держави;

б) сплановані дії, спрямовані на ворожу, дружню або нейтральну аудиторію, які передбачають вплив на її свідомість і поведінку за допомогою використання організованої інформації та інформаційних технологій для досягнення певної мети;

в) небезпечні діяння з інформаційного впливу на соціальні групи осіб, державні органи влади та управління, пов'язані з поширенням інформації, яка містить погрози переслідуванням, розпорою, вбивствами, а також викривлення об'єктивної інформації, що спричиняє виникнення кризових ситуацій у державі, нагнітання страху і напруги в суспільстві;

г) протиправні діяння у сфері використання електронних обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж, за які чинним Кримінальним кодексом України передбачено відповідальність.

4. Виберіть правильну відповідь: Об'єктами забезпечення інформаційної безпеки держави є:

а) інформаційно-телекомунікаційна інфраструктура (суб'єкти та засоби створення, поширення інформації і передачі даних);

б) інформація (особиста, конфіденційна, власність держави, з обмеженим доступом);

в) свідомість (особи, групи осіб, суспільства);

г) усі варіанти відповідей правильні.

5. Виберіть правильну відповідь:

Яких чуток не існує?

а) недостовірні з елементами правдоподібності;

б) абсолютно недостовірні;

в) достовірні;

г) правдоподібні.

6. Виберіть правильну відповідь:

Види інформаційного протиборства

а) інформаційно-технічне та інформаційно-психологічне;

б) інформаційно-суспільне та інформаційно-державне;

в) інформаційно-особистісне та інформаційно-групове;

г) видів інформаційного протиборства не існує.

7. Виберіть правильну відповідь:

Не є основними методами спеціальних інформаційних операцій та актів зовнішньої інформаційної агресії

а) дезінформування;

б) пропаганда;

в) поширення чуток;

г) правдиве висвітлення інформації.

8. Виберіть правильну відповідь:

Сплановані дії, спрямовані на аудиторію, які передбачають вплив на її свідомість і поведінку за допомогою використання інформаційних технологій.

а) спеціальні інформаційні операції;

б) акти зовнішньої інформаційної агресії;

в) інформаційна атака;

г) спеціальні інформаційні технології.

9. Виберіть правильну відповідь:

Диверсифікація громадської думки – це:

а) розпорошення уваги правлячої еліти держави на різні штучно акцентовані проблеми і відволікання тим самим від вирішення нагальних першочергових завдань;

б) вплив на психіку людини шляхом залякування, погроз із метою спонукання до певної запланованої моделі поведінки;

в) діяльність щодо поширення різної інформації (переважно неправдивої) серед широких верств населення;

г) комплекс специфічних програмно-інформаційних засобів, створених для ураження інформаційного ресурсу противника.

10. Виберіть правильну відповідь:

Різновиди інформаційної безпеки:

а) держави, особи, суспільства;

б) інформаційно-технічна, інформаційно-психологічна;

в) особиста, конфіденційна, з обмеженим доступом;

г) первинна, вторинна.

11. Виберіть правильну відповідь:

Протиправні діяння у сфері використання електронних обчислювальних машин автоматизованих систем та комп'ютерних мереж – це:

а) комп'ютерний тероризм;

б) комп'ютерна атака;

в) комп'ютерна злочинність;

г) мережева злочинність.

12. Виберіть правильну відповідь:

Інформаційна безпека держави – це :

а) стан її захищеності, при якій спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації та ін., за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдає суттєвої шкоди національним інтересам;

б) небезпечні діяння з інформаційного впливу на соціальні групи осіб, державні органи влади та управління, пов'язані з поширенням інформації, яка містить погрози переслідуванням, розправою, вбивствами;

в) засоби подолання систем захисту, засоби дезорганізації роботи технічних засобів та комп'ютерних систем;

г) поширення різних політичних, філософських, наукових, художніх, інших мистецьких ідей з метою їх упровадження у громадську думку та активізацію, тим самим використання цих ідей у масовій практичній діяльності населення.

13. Виберіть правильну відповідь:

Комп'ютерний вірус – це :

а) голосові синтезатори, що дозволяють формувати провокаційні повідомлення та передавати їх голосами лідерів країни та поширювати їх через засоби масової інформації;

б) програмна закладка, яка завчасно впроваджується в інформаційні системи й мережі, що забезпечують управління об'єктами військової та цивільної інфраструктури;

в) спеціальна програма, яка здатна до саморозповсюдження без відома користувача і всупереч його бажанню. вона заражає програмне забезпечення шляхом свого об'єктного коду до коду зараженої програми;

г) вплив на психіку людини шляхом залякування, погроз із метою спонукання до певної запланованої моделі поведінки.

14. Виберіть правильну відповідь:

Інформаційна війна – це:

а) форма ведення інформаційного протиборства між різними суб'єктами (державами, неурядовими, економічними або іншими структурами), який передбачає проведення комплексу заходів з нанесення шкоди інформаційній сфері конфронтуючої сторони і захисту власної інформаційної безпеки;

б) стан незахищеності особи, суспільства і держави, при якому не досягається інформаційний розвиток;

в) підриг морального духу населення і, як наслідок, зниження обороноздатності та бойового потенціалу;

г) дестабілізація політичних відносин між партіями, об'єднаннями та рухами з метою розпалення конфліктів, стимулювання недовіри, підозри, загострення ворожнечі, боротьби за владу.

15. Виберіть правильну відповідь: Спеціальні інформаційні операції – це:

а) легальні або протиправні акції, реалізація яких може мати негативний вплив на безпеку інформаційного простору держави;

б) сплановані дії, спрямовані на ворожу, дружню або нейтральну аудиторію, які передбачають вплив на її свідомість і поведінку за допомогою використання організованої інформації та інформаційних технологій для досягнення певної мети;

в) небезпечні діяння з інформаційного впливу на соціальні групи осіб, державні органи влади та управління, пов'язані з поширенням інформації, яка містить погрози переслідуванням,

розправою, вбивствами, а також викривлення об'єктивної інформації, що спричиняє виникнення кризових ситуацій у державі, нагнітання страху і напруги в суспільстві;

г) протиправні діяння у сфері використання електронних обчислювальних машин (комп'ютерів), автоматизованих систем.

16. Виберіть правильну відповідь:

Інформаційний вплив – це:

а) це стан захищеності психіки та здоров'я людини від деструктивного інформаційного впливу, який призводить до неадекватного сприйняття;

б) організоване цілеспрямоване застосування спеціальних інформаційних засобів і технологій для внесення змін у свідомість особи чи населення;

в) протиправні діяння у сфері використання електронних обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж;

г) проведення спецслужбами, передусім іноземних держав, таємних операцій та акцій негативного чи навіть деструктивного ідеологічного, ідейно-політичного та соціального впливу на особу.

17. Інформаційна безпека особи – це :

а) стан захищеності, при якій спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації та ін., за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдає суттєвої шкоди національним інтересам;

б) стан захищеності психіки та здоров'я людини від деструктивного інформаційного впливу, який призводить до неадекватного сприйняття нею дійсності та (або) погіршення її фізичного стану

в) можливість безперешкодної реалізації суспільством та окремими його членами своїх конституційних прав, пов'язаних з можливістю вільного одержання, створення й поширення інформації, а також ступінь їхнього захисту від деструктивного інформаційного впливу;

г) небезпечні діяння з інформаційного впливу на соціальні групи осіб, державні органи влади та управління, пов'язані з поширенням

інформації, яка містить погрози переслідуванням, розправою, вбивствами.

18. Інформаційна безпека суспільства – це:

а) можливість безперешкодної реалізації суспільством та окремими його членами своїх конституційних прав, пов'язаних з можливістю вільного одержання, створення й поширення інформації, а також ступінь їхнього захисту від деструктивного інформаційного впливу.

б) стан захищеності психіки та здоров'я людини від деструктивного інформаційного впливу, який призводить до неадекватного сприйняття нею дійсності та (або) погіршення її фізичного стану

в) стан захищеності, при якій спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації та ін., за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдає суттєвої шкоди національним інтересам;

г) небезпечні діяння з інформаційного впливу на соціальні групи осіб, державні органи влади та управління, пов'язані з поширенням інформації, яка містить погрози переслідуванням, розправою, вбивствами.

КОНТРОЛЬНА РОБОТА ДЛЯ СТУДЕНТІВ ЗАОЧНОЇ ФОРМИ НАВЧАННЯ

1. Назвіть форми і види зовнішніх інформаційних війн.
2. Назвіть форми і види внутрішніх інформаційних війн.
3. Змодельуйте ситуацію законного та незаконного обмеження свободи слова.
4. Визначте поняття «загроза інформаційній безпеці».
5. Наведіть приклади прояву політичного екстремізму стосовно журналістів.
6. Пройдіть тести (див. варіанти тестів для студентів денної форми навчання).

ПИТАННЯ, ЩО ВІНОСЯТЬСЯ НА ЕКЗАМЕН

1. Національний інформаційний простір: сучасний стан та проблеми.
2. Державна інформаційна політика. Основні напрями.
3. Засади державної інформаційної політики.
4. Державна ідеологія та інформаційна політика.
5. Правові основи інформаційної політики.
6. Засоби масової інформації і державна інформаційна політика.
7. Інформація в сучасному світі, її роль і значення в політичних протистояннях.
8. Сучасна структура медіа-сфери в Україні.
9. Особливості сучасної інформаційної політики.
10. Інформаційна політика щодо національного телерадіофіру.
11. Інтернет як важлива галузь державної інформаційної політики. Українська присутність в Інтернеті.
12. Інформаційна безпека України: поняття, сутність та загрози в інформаційній сфері.
13. Інформаційні війни (психологічні операції) і національна безпека.
14. Сучасні інформаційні війни всередині країни: причини, приводи, практика.
15. Зовнішні інформаційні війни – форми і види інформаційної експансії.
16. Механізми забезпечення конституційного права громадян на інформацію та механізми інформаційної безпеки.
17. Чужоземна експансія в українське медіаполе: мета і реальні та можливі наслідки.
18. Технічні аспекти інформаційної безпеки.
19. Поняття інформаційного суверенітету та інформаційної безпеки країни.
20. Проблеми інформаційної безпеки України.
21. Джерела загроз інформаційній безпеці.
22. Методи запобігання та ліквідації загроз інформаційній безпеці.
23. Сутність інформаційної безпеки держави, суспільства та особи.
24. Пострадянський простір як об'єкт інформаційного впливу.
25. Інформаційна безпека телевізійного простору.

26. Основні напрямки інформаційної політики України.

27. Визначення поняття «загроза інформаційній безпеці».

28. Інформаційна безпека як складова національної безпеки України.

29. Основні принципи забезпечення інформаційної безпеки України.

30. Внутрішні чинники ескалації загроз інформаційній безпеці України: впровадження політичної цензури.

31. Внутрішні чинники ескалації загроз інформаційній безпеці України: створення негативного іміджу України на міжнародній арені внаслідок неефективної інформаційної політики.

32. Внутрішні чинники ескалації загроз інформаційній безпеці України: руйнування моральних цінностей людини й суспільства внаслідок інформаційного впливу негативного характеру.

33. Внутрішні чинники ескалації загроз інформаційній безпеці України: тиск на ЗМІ з метою зміни їх політичного курсу (економічні та законодавчі санкції).

34. Внутрішні чинники ескалації загроз інформаційній безпеці України: прояви політичного екстремізму стосовно журналістів.

35. Внутрішні чинники ескалації загроз інформаційній безпеці України: монополізація окремих видів інформаційних послуг.

36. Внутрішні чинники ескалації загроз інформаційній безпеці України: обмеженість рекламного ринку та іноземних інвестицій.

37. Зовнішні чинники ескалації загроз інформаційній безпеці України: діяльність іноземних розвідок.

38. Зовнішні чинники ескалації загроз інформаційній безпеці України: міжнародна комп'ютерна злочинність.

39. Зовнішні чинники ескалації загроз інформаційній безпеці України: високий рівень присутності зарубіжних держав в інформаційному просторі України.

40. Зовнішні чинники ескалації загроз інформаційній безпеці України: спрямований інформаційний вплив на Україну з боку іноземних держав або конкуруючих компаній.

41. Функції та діяльність Національної Ради з питань телебачення й радіомовлення.

42. Поняття інформаційних воєн у сучасній теорії національної безпеки.

43. Проблема інформаційно-психологічної безпеки особистості в інформаційному просторі України.

44. Інформаційне поле запорізького регіону: тенденції особливості розвитку.

45. Різноманітні підходи до тлумачення поняття «інформаційне суспільство».

46. Указ Президента України Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»

47. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»

48. Закон України «Про національну безпеку України».

49. Особливості діяльності Міністерства культури та стратегічних комунікацій України.

50. Загрози у сучасному інформаційному просторі.

51. Необхідність формування медіаінформаційної грамотності у сучасних умовах. Розвиток критичного мислення як протидія політичним маніпуляціям.

52. Особливості безпечного споживання радіо- та телевізійної інформації.

53. Особливості споживання інформації в онлайн-медіа.

54. Шляхи мінімізації впливів маніпуляторів в YouTube.

55. Особливості маніпуляцій в Viber та Telegram-каналах.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

Базові джерела

1. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. Київ : Інтертехнологія, 2009. 164 с.
2. Горбулін В. Світова гібридна війна: український фронт: монографія. Київ: НІСД, 2017. 496 с.
3. Дубас О. П. Інформаційно-комунікаційний простір: культурно-політичні детермінанти : монографія. Київ : Генеза, 2011. 256 с.
4. Інформаційна політика України: європейський контекст: монографія. Ред. С. В. Головка. Київ : Либідь, 2007. 360 с.
5. Захарченко А. Наративи масового ураження. Тактики і стратегії інформаційної війни. Київ : Наш формат, 2026. 240 с.
6. Карпенко В. Інформаційна політика та безпека. Підручник. Київ : Нора-Друк, 2006. 320 с.
7. Кіслов Д. В. Політична безпека масових комунікацій: Монографія. Київ : «МП Леся», 2010. 208 с.
8. Кормич Б. А. Інформаційна безпека: організаційно-правові основи. Навчальний посібник. Київ : Кондор, 2008. 384 с.
9. Курбан О.В. Інформаційні війни у соціальних он-лайн-мережах : монографія. Київ : Київ, ун-т ім. Б. Грінченка, 2017. 392 с.
10. Нестеряк Ю. В. Державна інформаційна політика України. Теоретико-методологічні засади : монографія. Київ : НАДУ, Саміт-книга, , 2014. 292 с.
11. Почепцов Г. Г., Чукут С. А. Інформаційна політика: Навчальний посібник. Київ : Знання, 2008. 663 с.
12. Почепцов Г. Сучасні інформаційні війни. Київ : Києво-Могилянська академія, 2016. 502 с.
13. Почепцов Г. Інформаційні операції та ментальні війни. Київ : Вид. дім «Києво-Могилянська академія», 2024. 320 с.
14. Сащук Г. Безпекові виміри телепростору: Монографія. Київ : Грамота, 2007. 136 с.

Допоміжні джерела

15. Андреева О. М. Національна безпека України в контексті національної ідентичності і взаємовідносин з Росією. Київ : Парламентське вид-во, 2009. 360 с.

16. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти. За ред. О. М. Бандурки. Монографія. Харків : Вид-во університету внутрішніх справ, 2000. 368 с.

17. Бабіч О. Особливості маніпуляції масовою свідомістю в друкованих ЗМІ під час висвітлення воєнних подій. *Вісник Київ. нац. ун-ту ім. Т. Шевченка: військово-спеціальні науки*. 2007. Вип. 14-15. С. 89-92.

18. Гібридна війна і журналістика. Проблеми інформаційної безпеки : навчальний посібник. За заг. ред. В. О. Жадька. Київ : Вид-во НПУ імені М. П. Драгоманова, 2018. 356 с.

19. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення. *Вісник НАДУ*. 2015. № 1. С. 136-141.

20. Джолос О.В. Індекс медіаграмотності українців: споживання та користування медіа. *Держава та регіони. Серія: Соціальні комунікації*. 2023. № 4 (56). С. 138-145.

21. Джолос О.В. Інформаційна та медійна грамотність як запорука демократичного розвитку України. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Філологія. Соціальні комунікації*. 2019. Т. 30 (69). № 4. Ч. 2. С. 173-177.

22. Джолос О. В. Мікромедіа як домінуючі джерела інформації під час російсько-української війни. *Інформаційний спротив ворожим наративам засобами мікромедіа в умовах російсько-української війни: матеріали Міжнародної науково-практичної конференції (27-28 листопада 2023 р.)*. Запоріжжя : Запорізький національний університет, 2023. С. 37-40.

23. Джолос О.В. Україна удосконалює правове регулювання медіа у відповідь на безпекові загрози і вимоги як до країни-кандидата в члени ЄС. *Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи : тези доп. учасників міжн. наук.-практ. конф.* (Анн-Арбор - Харків, 12-13 груд. 2023 р.). Харків: НДІ ППСН, 2023. С. 76-79.

24. Жарков Я. Інформаційно-психологічне протиборство в сучасному світі: проблемно-історичний аналіз. *Вісник Київського нац. ун-ту ім. Т. Шевченка*. 2007. Вип. 14-15. С. 101-104.

25. Жарков Я.М., Дзюба М.Т., Замаруєва І.В. Інформаційна безпека особистості, суспільства, держави. Київ: Видавничо-поліграфічний центр «Київський університет», 2008. 274 с.

26. Зубок М.І. Інформаційна безпека. Навчальний посібник. Київ : Київський національний торговельно-економічний університет, 2009. 133 с.

27. Інформаційна безпека (соціально-правові аспекти): Підручник. За заг. ред. Є. Д. Скулиша. Київ : КНТ, 2010. 776 с.

28. Інформаційні виклики гібридної війни: контент, канали, механізми протидії : аналіт. доп. За заг. ред. А. Баровської. Київ : НІСД, 2016. 109 с.

29. Історія інформаційно-психологічного протиборства : підруч. За заг. ред. Є.Д. Скулиша. Київ : Наук.-вид. відділ НА СБ України, 2012. 212 с.

30. Карпенко В. Преса і незалежність України: практика медіа-політики 1988-1998 рр. Київ : Нора-Друк, 2003. 355 с.

31. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі: навчальний посібник. Київ: ВІКНУ, 2016. 286 с.

32. Литвиненко О.В. Інформаційний вплив та операції: теоретико-аналітичні нариси : монографія. Київ : НІСД, 2003. 240 с.

33. Магда Є. Гібридна війна. Вижити і перемогти. Київ : Віват, 2015. 304 с.

34. Магда Є.В. Гібридна віна – вижити і перемогти. Харків : Віват, 2015. 604 с.

35. Марущак А. І. Інформаційне право: Регулювання інформаційної діяльності. Київ : Видавничий дім «Скіф», 2008. 344 с.

36. Міністерство культури та стратегічних комунікацій України. URL : [Головна | Міністерства культури та стратегічних комунікацій](#)

37. Никоненко Л. Медіа як регулятор взаємодії суб'єктів політико-правового процесу. *Від медіаграмотності до медіакультури: стратегії, проблеми, перспективи: тези доповідей Міжнародної науково-практичної Інтернет-конференції* (м. Миколаїв, 27 квітня 2016 року). Миколаїв : ОШПО, 2016. С. 62-64.

38. Островська Н. В., Мірошніченко П. В. Проблеми та виклики українського фактчекінгу під час російсько-української війни. *Вісник Національного університету «Львівська політехніка» : журналістика*. 2026. Вип. 2, № 12. С. 109–118.

39.Почепцов Г. Комунікаційні технології : підручник. Київ : Видавничий дім «Киево-Могилянська академія», 2020. 512 с.

40.Прибутько П. С. Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах. Київ : Вид. ПАЛИВОДА А.В., 2007. 252 с.

41.Соціальні мережі як чинник розвитку громадянського суспільства : монографія [О. С. Онищенко, В. М. Горовий, В. І. Попик та ін.]; НАН України, Нац. б-ка України ім. В. І. Вернадського. Київ, 2013. 220 с.

42.Черних О. О. Аналіз класифікацій загроз в Інтернеті. *Вісник ЛНУ імені Тараса Шевченка*. 2015. № 1 (290). С. 281-289.

Інформаційні ресурси

43. Безпека молоді в Інтернеті: Дослідження ЮНІСЕФ в Україні, Росії та Туреччині. URL : https://www.unicef.org/ukraine/ukr/media_18561.html.

44.Бурлаков С. В. Роль засобів масової інформації у розвитку національної інформаційної політики. *Юридична наука*. 2020. № 7 (109). С. 45-51. <https://doi.org/10.32844/10.32844/2222-5374-2020-109-7.06>

45.Декларація принципів «Побудова інформаційного суспільства – глобальне завдання в новому тисячолітті» від 12.12.2015 р. URL: http://gska2.rada.gov.ua/pls/zweb_n/webproc4_1?id=&pf3511=13798

46. Закон України «Про інформацію». URL : <https://zakon.rada.gov.ua/laws/show/2657-12#Text>

47. Закон України «Про медіа» URL : <https://zakon.rada.gov.ua/laws/show/2849-20#Text>

48. Закон України «Про національну безпеку України». *Відомості Верховної Ради (ВВР)*. 2018. № 31 ст. 241. URL : <https://zakon.rada.gov.ua/laws/show/2469-19#Text>

49.Карпенко В. Інформаційна політика та безпека. Підручник. Київ: Нора-Друк, 2006. URL : <http://ukrlife.org/main/karp/bezpeka.htm>

50. Конституція України. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>

51.Магда Є. Гібридна війна: питання і відповіді. *MediaSapiens*. 2015. URL :

http://osvita.mediasapiens.ua/trends/1411978127/gibridna_viyna_pitannya_i_vidpovidi/undefined/?media=print.

52. Мельникова-Курганова О. Маргінальний пропагандистський світ в окупації. URL: <https://detector.media/infospace/article/221975/2024-01-21-marginalnyy-propagandystskyy-svit-v-okupatsii/>

53. Почепцов Г. Війна та пропаганда крокують у ногу. URL : <https://detector.media/infospace/article/244128/2025-09-15-viyna-ta-propaganda-krokyut-u-nogu/>

54. Почепцов Г. Інформаційні війни: нові тенденції. URL : http://osvita.mediasapiens.ua/trends/1411978127/informatsionnye_voyny_novye_tendentsii/

55. Почепцов Г. Інформаційні війни: тенденції та шляхи розвитку. URL : https://ms.detector.media/ethics/manipulation/informatsiyne_viyni_tendentsii_ta_shlyakhi_rozvitku/

56. Почепцов Г. Перші дослідження в галузі інформаційних війн: від минулого до сучасності. URL: <http://osvita.mediasapiens.ua/trends>

57. Рябоконт О. Міжнародний досвід сучасної цензури і фільтрації контенту в мережі Інтернет. URL : <http://nbuviap.gov.ua/images/konferenciya/Ryabokon.pdf>

58. Середюк-Буз В. Міжнародно-правове регулювання свободи вираження поглядів в мережі Інтернет. *Форум права*. 2012. №3. С. 659–664. URL: <http://www.nbu.gov.ua/e-journals/FP/2012-3/12svvvvmi.pdf>

59. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України». URL : <https://zakon.rada.gov.ua>

60. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». URL : <https://www.president.gov.ua/documents/472017-21374>

ПОЛІТИКИ КУРСУ

Політика щодо відвідування. Відвідування та відпрацювання пропущених занять є обов'язковим. Допускається пропуски занять з поважних причин, які підтверджується документально. За таких умов навчання може відбуватися в режимі онлайн за погодженням із викладачем. Відпрацювання пропущених занять проводиться згідно з графіком консультацій викладача. За об'єктивних причин (наприклад, лікарняні, стажування, мобільність, індивідуальний графік) аудиторні види занять і завдань також можуть бути трансформовані в систему дистанційного навчання (сервіс moodle).

Політика дедлайнів. Студент зобов'язаний дотримуватись крайніх термінів (дата для аудиторних видів робіт або час в системі дистанційного навчання), до яких має бути виконано певне завдання. За наявності поважних причин (відповідно до інформації, яку надано деканатом) студент має право на складання індивідуального графіку вивчення окремих тем дисципліни.

Політика щодо проведення аудиторних занять. Під час проведення аудиторних занять слід дотримуватись встановленого порядку, брати активну участь в обговоренні запропонованих питань, висловлюючи та відстоюючи власну думку, виказуючи повагу та толерантність до чужої думки. Мобільні пристрої можна використовувати під час проведення аудиторних занять лише з дозволу викладача. За «гострої» потреби дозволяється залишати аудиторію на короткий час.

Політика щодо академічної доброчесності. При вивченні курсу «Інформаційна політика та безпека» політика дотримання академічної доброчесності визначається Кодексом академічної доброчесності Національного університету «Запорізька політехніка» https://zp.edu.ua/uploads/dept_nm/Nakaz_N253_vid_29.06.21.pdf

Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Виявлення ознак академічної недоброчесності в письмовій роботі студента (відсутність посилань на використані джерела, фабрикування джерел, списування тощо) є підставою для її незарахування викладачем, незалежно від масштабів плагіату.

Під час виконання письмових контрольних видів робіт а також здійснені різних видів контролю успішності заборонено

користуватися допоміжними паперовими матеріалами («шпаргалками») та мобільними пристроями.

Політика дотримання прав та обов'язків студентів. Права і обов'язки студентів відображено у п.7.5 Положення про організацію освітнього процесу в НУ «Запорізька політехніка» (https://zp.edu.ua/uploads/dept_nm/Polozhennia_pro_organizatsiyu_osvitnoho_protsesu.pdf).

Політика конфіденційності та захисту персональних даних. Обмін персональними даними між викладачем і студентом в межах вивчення дисципліни, їх використання відбувається на основі закону України «Про захист персональних даних». У статті 10, п. 3 цього документу зазначається: «Використання персональних даних працівниками суб'єктів відносин, пов'язаних з персональними даними, повинно здійснюватися лише відповідно до їхніх професійних чи службових або трудових обов'язків. Ці працівники зобов'язані не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, крім випадків, передбачених законом. Таке зобов'язання чинне після припинення ними діяльності, пов'язаної з персональними даними, крім випадків, установлених законом» (<https://zakon.rada.gov.ua/laws/show/2297-17#Text>).

Політика трансферу кредитів. Замість виконання завдань (вивчення тем) можуть додатково враховуватись інші види активності здобувача (неформальна освіта) за умов підтвердження результатів (сертифікат з зазначенням обсягу кредитів, грамота учасника, призера, лауреата тощо).