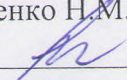


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
Чорноморський національний університет імені Петра Могили  
Інститут державного управління  
Кафедра місцевого самоврядування та регіонального розвитку

“ЗАТВЕРДЖУЮ”

Перший проректор

Іщенко Н.М.

  
“31” серпня 2021 року

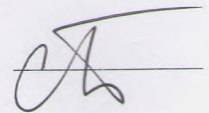
## РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

### Інформаційна політика і менеджмент

Спеціальність 281 «Публічне управління та адміністрування»

Розробник

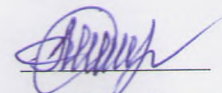
Бондар Г.Л.



Завідувач кафедри місцевого самоврядування

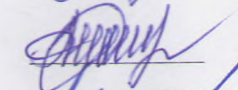
та регіонального розвитку

Штирьов О.М.



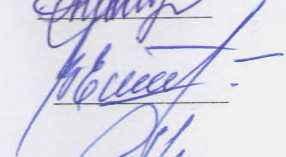
Гарант освітньої програми

Штирьов О. М.



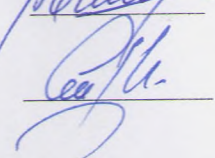
Директор ІДУ

Ємельянов В.М.



Начальник НМВ

Шкірчак С.І.



Миколаїв – 2021 рік

## 1. Опис навчальної дисципліни

Найменування показника	Характеристика дисципліни
Найменування дисципліни	Інформаційна політика і менеджмент
Галузь знань	28 «Публічне управління та адміністрування»
Спеціальність	281 «Публічне управління та адміністрування»
Спеціалізація (якщо є)	
Освітня програма	«Адміністративний менеджмент»
Рівень вищої освіти	перший (бакалаврський)
Статус дисципліни	нормативна
Курс навчання	2
Навчальний рік	2021/2022
Номер(и) семестрів (триместрів):	<b>Денна форма</b>
	<b>(IV семестр)</b>
Загальна кількість кредитів ЄКТС/годин	<b>3,5 кред./105 год.</b>
Структура курсу: – лекції – семінарські заняття (практичні, лабораторні, півгрупові) – годин самостійної роботи студентів	Лек. – 18 Сем. – 18  С/р - 69
Відсоток аудиторного навантаження	34%
Мова викладання	українська
Форма проміжного контролю (якщо є)	
Форма підсумкового контролю	іспит

## 2. Мета, завдання та результати вивчення дисципліни

### Значення навчальної дисципліни в реалізації освітньо-професійної програми підготовки магістрів державної служби:

Реалізація освітньо-професійної програми підготовки магістрів за спеціальністю „Публічне управління та адміністрування” пов’язана з наданням їм комплексу знань та умінь, які містяться у нормативній навчальній дисципліні „Інформаційна політика і менеджмент”.

Зазначене завдання актуальне з декількох причин.

По-перше, з розвитком демократичних процесів, побудовою громадянського та інформаційного суспільства система обміну інформації набуває принципово нових ознак і перетворюється в ефективну двосторонню комунікацію між владою та громадянським суспільством. Така тенденція спостерігатиметься на всіх рівнях відносин держави та інститутів громадянського суспільства на шляху до європейської інтеграції та розвитку України.

По-друге, інституалізація суспільних комунікацій є умовою розвитку демократичних процесів та становлення інформаційного та громадянського суспільства.

По-третє, інформаційна парадигма нині є основою державної інформаційної політики в Україні.

**Мета дисципліни** – дати майбутнім фахівцям систематизоване й емпірично аргументоване уявлення про функціонування інформаційної сфери у контексті переходу до інформаційного суспільства, зокрема державне управління нею, а також інформаційними процесами, які віддзеркалюють інтереси особистості, суспільства і держави.

**Завдання** – навчити студентів аналізувати національний інформаційний простір в контексті формування суспільної думки та забезпечення інформаційної безпеки особи, суспільства та держави; з’ясувати фактори, що визначають функціонування інформаційних потоків національного й іноземного походження; використовувати у практичній діяльності сукупність знань, професійних прийомів і методів, які впливають на формування національної інформаційної політики.

В результаті вивчення навчальної дисципліни студент повинен

#### **знати:**

- підходи до інформаційної політики та безпеки на сучасному етапі, особливості інформаційного менеджменту;

- наслідки впливу інформаційної революції на всі сфери життєдіяльності суспільства;

- результати впливу психологічних воєн на особу, суспільство та державу;

- основні положення концепції інформаційного суспільства, її засновників;

- внесок українських вчених у розвиток ідей інформаційного суспільства;

- актуальні концепції розвитку майбутнього;

- міжнародні програми розвитку інформаційного суспільства;

- національні особливості побудови інформаційного суспільства;

- принципи функціонування електронного уряду;

- моделі відносин держави з медіа структурами;

-сучасні інформаційні загрози та технології забезпечення захисту національного інформаційного простору.

- особливості психологічного впливу соціокультурних технологій на масову свідомість;

- функції ЗМІ, напрямки впливу мас медійної інформації на населення;

- технології управління інформацією та конструювання новин.

#### **уміти:**

- застосовувати теоретичні знання формування і розвитку інформаційного суспільства для підготовки пропозицій щодо вдосконалення інформаційного законодавства у відповідності до сучасних вимог;

- аналізувати інформаційну політику органів державної влади та місцевого самоврядування;

- подавати інформаційні запити в органи державної влади та місцевого самоврядування, відстоювати свої права у разі ненадання відповідей;

- своєю діяльністю сприяти проведенню відкритої інформаційної політики у публічному секторі;

- протидіяти інформаційним загрозам, як в особистому житті, так й у професійній діяльності.

Навчальна дисципліна має міждисциплінарний характер та інтегрує знання з інших освітніх і наукових галузей та виступає фундаментом для вивчення наступних навчальних дисциплін: «Державне управління», «Інформаційні технології», «Глобалізація та політика національної безпеки», «Взаємодія публічної влади з суспільством», «Управління конфліктами», «Історико-правові основи та інтеграційні процеси в ЄС».

**Місце дисципліни.** Навчальна дисципліна «Інформаційна політика і менеджмент» є складовою частиною циклу фундаментальної підготовки фахівців освітньо-кваліфікаційного рівня «бакалавр» зі спеціальності 281 «Публічне управління та адміністрування».

**Форми вивчення дисципліни:**

лекція, семінарські заняття, виконання індивідуальних завдань самостійної роботи, творчої роботи, контрольних заходів. Технічні засоби навчання використовуються під час проведення усіх форм занять згідно з рекомендаціями предметно-методичної комісії.

У процесі вивчення дисципліни використовується кредитно-модульна технологія - студенти опановують матеріал за змістовим модулем.

Під час проведення лекційних занять використовується проблемно-діяльнісний підхід, що сприяє глибокому засвоєнню знань і формуванню творчого професійного мислення у майбутніх фахівців.

Семінарські заняття носять проблемно-пошуковий і практично-творчий характер, студенти опрацьовують теоретичні і практичні завдання, розвивають мислення, поглиблюють і розширюють знання, обґрунтовують власну точку зору, роблять прогнози та пропонують шляхи вирішення поставлених завдань.

Виконуючи індивідуальні завдання, студенти, за допомогою викладача, розв'язують складні проблеми, уточнюють незрозумілі питання, обговорюють підходи практичного застосування отриманих знань під час професійної діяльності.

Виконуючи індивідуальні завдання, студенти, за допомогою викладача, розв'язують складні проблеми, уточнюють незрозумілі питання, обговорюють підходи практичного застосування отриманих знань під час професійної діяльності. Самостійна робота як форма організації навчального процесу, покликана забезпечити можливість студенту працювати з інформаційними ресурсами і базами даних та використовувати інформаційно-комунікаційні технології для пошуку, обробки, аналізу та використання інформації з різних джерел під час самостійного вивчення ним запропонованої літератури у пошуку відповідей на проблемні питання курсу, виконання практичних завдань з курсу. Самостійна робота студентів орієнтована на поглиблене вивчення окремих питань інформаційної політики та безпеки, а також формування вмінь і навичок підготовки документів, що регулюють інформаційну сферу.

Творча робота (презентація) за допомогою засобів Power Point.

Форми контролю – поточний, підсумковий семестровий контролі. Поточний контроль ґрунтується на системі оцінки успішності студентів і проводиться на семінарських заняттях: опитування, самостійна робота, творча робота, контрольна робота. Підсумковий контроль – іспит, наприкінці навчального курсу.

**Компетентності, яких набуває студент при вивченні дисципліни відповідно до освітньо-професійної програми**

<b>Загальні компетентності (ЗК)</b>	<b>Фахові компетентності спеціальності (ФК)</b>
ЗК05. Здатність до пошуку, оброблення, аналізу та захисту інформації з різних джерел.	ФК02. Здатність синтезувати управлінські рішення у сфері публічного адміністрування в умовах повної та неповної інформації.

**Програмні результати навчання**

Нормативні результати навчання, контрольні заходи та терміни виконання оголошуються студентам на першому занятті.

<b>№ з/п</b>	<b>Результати навчання (ПРН)</b>
1	ПРН 10. Уміти відшукувати та узагальнювати інформацію, робити висновки і формулювати рекомендації в межах своєї компетенції.
2	ПРН 19. Реалізовувати лідерські якості, проявляти здатність діяти соціально-відповідально та громадсько-свідомо на робочому місці.

### 3. Програма навчальної дисципліни

#### Денна форма II курс

№ п/п	Тема	Лекції	Практичні (семінарські, лабораторні, півгрупові)	Самостійна робота
<b>IV семестр</b>				
1.	<b>Тема 1.</b> Інформаційна політика та безпека в умовах формування інформаційного суспільства. Інформаційний менеджмент	2	2	9
2.	<b>Тема 2.</b> Інформаційна революція, концепції постіндустріального суспільства та постінформаційна ера	2	2	9
3.	<b>Тема 3.</b> Національні стратегії реалізації інформаційної політики	2	2	6
4	<b>Тема 4.</b> Електронний уряд: світовий досвід та впровадження в Україні	2	2	9
5	<b>Тема 5.</b> Цифровий розвиток України	2	2	9
6	<b>Тема 6.</b> Медіаполітика. Державна інформаційна політика та безпека	2	2	9
7	<b>Тема 7.</b> Кібербезпека та інформаційна безпека - складові інформаційної політики України.	2	2	6
8	<b>Тема 8.</b> Особливості та взаємозв'язок інформаційної безпеки та кібербезпеки	2	2	6
9	<b>Тема 9.</b> Захист аккаунту, антивірусні програми, захист персональних даних	2	2	6
	<b>Всього за курсом</b>	<b>18</b>	<b>18</b>	<b>69</b>

#### 4.Зміст навчальної дисципліни

##### 4.1. План лекцій

Денна форма

II курс

№	Тема заняття / план
<b>IV семестр</b>	
<b>Змістовий розділ 1. Теоретичне підґрунтя інформаційної політики</b>	
1	<b>Тема 1. Інформаційна політика та безпека в умовах формування інформаційного суспільства. Інформаційний менеджмент</b> 1. Інформаційна політика та безпека на сучасному етапі. 2. Визначення, об'єкт, предмет, мета інформаційної політики.
2	<b>Тема 2. Інформаційна революція, концепції постіндустріального суспільства та постінформаційна ера</b> 1. Інформаційна революція. 2. Постіндустріальне/інформаційне суспільство. 3. NETократія О. Барда і Я. Зодерквіста: умови перерозподілу влади.
3	<b>Тема 3. Національні стратегії реалізації інформаційної політики</b> 1. Загальна характеристика національних моделей інформаційного суспільства: європейська, англо-американська, азійська. 2. Політика розвитку інформаційного суспільства в Україні.
4	<b>Тема 4. Електронний уряд: світовий досвід та впровадження в Україні</b> 1. Сутність, мета і принципи організації електронного уряду. 2. Світовий досвід впровадження електронного уряду (США, Великобританія, Швейцарія, Естонія, Сінгапур, ПАР). 3. Процес формування електронного врядування в Україні.
5	<b>Тема 5. Цифровий розвиток України</b> 1. Подолання цифрового розриву шляхом розвитку цифрових інфраструктур. 2. Розвиток цифрових компетенцій громадян. 3. Реалізація проектів цифрових трансформацій
6	<b>Тема 6. Медіаполітика. Державна інформаційна політика та безпека</b> 1. Медіаполітика держави: механізми регулювання взаємовідносин держави зі ЗМІ. 2. Стратегії та технології державної інформаційної політики. 3. Структура державної інформаційної політики України. 4. Розуміння національної безпеки в інформаційному контексті.
<b>Змістовий розділ 2. Засади і принципи державної політики у сфері інформаційної безпеки та кібербезпеки</b>	
7	<b>Тема 7. Кібербезпека та інформаційна безпека - складові інформаційної політики України.</b> 1. Законодавче та нормативно-правове забезпечення національної безпеки, інформаційної безпеки та кібербезпеки в Україні. 2. Особливості і наслідки впливу кібернападів на критичну інфраструктуру України.
8	<b>Тема 8. Особливості та взаємозв'язок інформаційної безпеки та кібербезпеки</b> 1. Правила кібергігієни та захист персональних даних в мережі та поза нею. 2. Протидія методам соціальної інженерії: шахрайство, крадіжка, фішинг та підробні посилання. 3. Стеження за користувачами веб-браузерів та використання cookies: Chrome, Firefox, iExplorer, Safari, Opera, Edge, Mobile. 4. Безпека, зручність та загрози від сервісів для відеоконференції та навчання: Skype, Zoom, Cisco WebEx, Microsoft Team та Google+ Hangouts 5. Безпека та ризики використання соціальних мереж та месенджерів.
9	<b>Тема 9. Захист аккаунту, антивірусні програми, захист персональних даних</b> 1. Захист аккаунту від зламу: паролі та двоетапна аутентифікація. Небезпечні оновлення

та сайти.

2. Антивірусні програми: переваги та недоліки. Захищений доступ під час віддаленої роботи.

3. Сфера Дії GDPR (Загальний регламент захисту даних (захист персональних даних осіб в межах ЄС та ЄЕЗ, Regulation (EU) 2016/679)), ССРА та Закону України «Про захист персональних даних».

4. Відеоспостереження в публічних місцях: право на захист приватного життя і персональних даних.



## 4.2. План практичних (семінарських, лабораторних, півгрупових) занять

### Денна форма II курс

№ з/п	Назва теми
<b>IV семестр</b>	
1	<b>Тема 1. Інформаційна політика та безпека в умовах формування інформаційного суспільства</b> 1. Інформаційна політика та безпека на сучасному етапі. 2. Визначення, об'єкт, предмет, мета інформаційної політики.
2	<b>Тема 2. Інформаційна революція, концепції постіндустріального суспільства та постінформаційна ера</b> 1. Інформаційна революція. 2. Постіндустріальне/інформаційне суспільство. 3. NETократія О. Барда і Я. Зодерквіста: умови перерозподілу влади.
3	<b>Тема 3. Національні стратегії реалізації інформаційної політики</b> 1. Європейська модель побудови інформаційного суспільства (Фінляндія та Естонія). 2. Американський і азійський досвід побудови інформаційного суспільства: ➤ Модель Силіконової долини. ➤ Досвід «азійських тигрів» (Гонконг, Республіка Корея, Тайвань, Сінгапур). ➤ Інформаційні стратегії Китаю та Японії. ➤ Інформаційні стратегії Індії. 3. Політика розвитку інформаційного суспільства в Україні.
4	<b>Тема 4. Електронний уряд: світовий досвід та впровадження в Україні</b> 1. Сутність, мета і принципи організації електронного уряду. 2. Світовий досвід впровадження електронного уряду (США, Великобританія, Швейцарія, Естонія, Сінгапур, ПАР). 3. Процес формування електронного врядування в Україні.
5	<b>Тема 5. Цифровий розвиток України</b> 1. Подолання цифрового розриву шляхом розвитку цифрових інфраструктур. 2. Розвиток цифрових компетенцій громадян. 3. Реалізація проектів цифрових трансформацій
6	<b>Тема 6. Медіаполітика. Державна інформаційна політика та безпека</b> 1. Медіаполітика держави: механізми регулювання взаємовідносин держави зі ЗМІ. 2. Стратегії та технології державної інформаційної політики. 3. Структура державної інформаційної політики України. 4. Розуміння національної безпеки в інформаційному контексті.
7	<b>Тема 7. Кібербезпека та інформаційна безпека - складові інформаційної політики України.</b> 1. Законодавче та нормативно-правове забезпечення національної безпеки, інформаційної безпеки та кібербезпеки в Україні. 2. Особливості і наслідки впливу кібернападів на критичну інфраструктуру України.
8	<b>Тема 8. Особливості та взаємозв'язок інформаційної безпеки та кібербезпеки</b> 1. Правила кібергігієни та захист персональних даних в мережі та поза нею. 2. Протидія методам соціальної інженерії: шахрайство, крадіжка, фішинг та подрібні посилення. 3. Стеження за користувачами веб-браузерів та використання cookies: Chrome, Firefox, iExplorer, Safari, Opera, Edge, Mobile. 4. Безпека та ризики використання соціальних мереж та месенджерів.
9	<b>Тема 9. Захист аккаунту, антивірусні програми, захист персональних даних</b> 1. Захист аккаунту від зламу: паролі та двоетапна аутентифікація. Небезпечні оновлення та сайти.

	<p>2. Антивірусні програми: переваги та недоліки. Захищений доступ під час віддаленої роботи.</p> <p>3. Сфера Дії GDPR (Загальний регламент захисту даних (захист персональних даних осіб в межах ЄС та ЄЕЗ, Regulation (EU) 2016/679)), ССРА та Закону України «Про захист персональних даних».</p> <p>4. Відеоспостереження в публічних місцях: право на захист приватного життя і персональних даних</p>
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Семінарське заняття – форма навчального заняття, під час проведення якого викладач організує дискусію з попередньо визначених тем, до яких студенти готують тези виступів.

Завданнями семінарських занять є:

- поглиблення теоретичних знань, отриманих на лекціях;
- заохочення студентів до аналізу політичних подій, активної творчої роботи зі самостійного опрацювання рекомендованої літератури;
- вироблення у студентів умінь використовувати теоретичні політичні знання в практичній діяльності, на основі історико-правових знань вміти прогнозувати події та явища у суспільно-політичному житті України;
- стимулювання у студентів прагнення на основі знання політичних систем минулого та сучасності вдосконалювати політичну культуру, розуміти значення державних інститутів у житті суспільства;
- формування навички самостійної роботи з першоджерелами і довідковою літературою;
- формування навички діалогічного і критичного мислення.

На кожному семінарському занятті викладач оцінює підготовлені студентами доповіді, їх виступи, активність у дискусії, вміння формувати і обґрунтовувати свою позицію тощо. Підсумкові оцінки за кожне семінарське заняття вносяться у відповідний журнал. Отримані студентом оцінки за окремі семінарські заняття враховуються при виставленні підсумкової оцінки з даної навчальної дисципліни.

### 4.3. Завдання для самостійної роботи

#### Спеціальність 281 «Публічне управління та адміністрування»

##### Вимоги до підготовки завдань курсу:

Відповідь на семінарському занятті – це активна участь у обговоренні всіх питань, що виносяться на семінар, підкріплення доповіді цитатами та посиланнями на літературу. Вільне володіння матеріалом доповіді, що дозволяє задавати та відповідати на питання по темі.

Контрольна робота - це необхідна складова частина самостійного опанування студентами курсу „Інформаційна політика та менеджмент”. Завдання, яке виконується безпосередньо за темами лекційних занять і проводиться відповідно до кількості розділів. В ній мають бути розкриті основні аспекти одного з варіантів, дана характеристика різних складових даної теми згідно плану лекції. Контрольна робота складається із 5 питань.

Творча робота (презентація) за допомогою засобів Power Point. Це невелике за обсягом завдання, яке безпосередньо стосується теми поточного семінару виконується під час його проведення, підготоване заздалегідь самостійно. Передбачає підготовку та презентацію проекту до відповідної тематики семінарського заняття з використанням наочних засобів та використанням електронної техніки, висловлення обґрунтованої позиції щодо мети і результатів виконаного завдання.

Ситуативні завдання - практичне застосування знань, розвиток комунікативних здібностей з дотриманням ділової етики та етикету спілкування в публічному управлінні, висловлення обґрунтованої позиції щодо мети і результатів виконаного завдання.

#### ТВОРЧА РОБОТА (ПРЕЗЕНТАЦІЯ)

*Зробити презентацію за допомогою засобів Power Point.*

Надається можливість вибору одного з двох запропонованих варіантів завдань: промокампанія чи проект оптимізації політики державної установи.

Презентація має бути 7-10 слайдів, при підготовці можна об'єднуватися в групи.

#### СИТУАТИВНІ ЗАВДАННЯ

Мета: практичне застосування знань, розвиток комунікативних здібностей з дотриманням ділової етики та етикету спілкування в публічному управлінні.

Реалізація завдання: викладач пропонує студентам знайти, запропонувати власні шляхи вирішення отриманих завдань – проблемних ситуацій, з використанням опанованих під час навчання комунікативних технік та застосуванням норм ділової етики, етикету спілкування в управлінні.

## КОНТРОЛЬНА РОБОТА

Варіант обирається за номером прізвища студента у списку журналу.

Вимоги до написання КР:

1. Обсяг контрольної роботи становить 20-25 сторінок. У ній розкриваються питання з основних розділів курсу.
2. Контрольна робота виконується на окремих аркушах формату А4. На титульному листі наводиться її назва, дисципліна, курс, шифр групи, повністю прізвище, ім'я і по батькові. На другій сторінці вказується варіант завдання. Текст може бути написаний від руки, або надрукований через 1,5 інтервали (Times New Roman), розмір шрифту – 14.
3. Кожен пункт завдання викладається стисло, змістовно і відображає сутність сформульованого питання. Текст може містити схеми, малюнки, графіки.
4. У кінці наводиться список використаної літератури, оформлений за правилами. Ставиться дата і особистий підпис виконавця.
5. КР містить 5 завдань різної складності.

### Варіант 1

1. Які існують підходи до поняття «інформаційна політика»?
2. У чому полягають негативні наслідки глобалізації інформаційного простору?
3. Розкрийте значення концепції постіндустріального суспільства. Коли вона виникла і хто зробив вагомий внесок у її розвиток?
4. Що таке психологічна війна?

### Варіант 2

1. Які зміни, викликані інформаційною революцією, найчастіше обговорюються? Чому?
2. Визначте об'єкт та предмет інформаційної політики.
3. Охарактеризуйте класифікацію цивілізацій Е. Тоффлера.
4. Розкрийте суть ідеї «нетократичного» суспільства О. Барда і Я. Зодерквіста.

### Варіант 3

1. Назвіть сучасних дослідників суспільства майбутнього. Що їх об'єднує, а в чому їх погляди різні?
2. Чому автори «Нетократії» заперечують реалізацію ідеї мережевої демократії? Яка Ваша думка з цього приводу?
3. Інформаційні стратегії Китаю та Японії.
4. Чи можна подолати, за О. Бардом і Я. Зодерквістом, нерівність між класами в інформаційному суспільстві? Обґрунтуйте відповідь.
5. Безпека та ризики використання соціальних мереж.

### Варіант 4

1. Яка основна мета Окінавської хартії глобального інформаційного суспільства?
2. Внаслідок чого виникає цифрова нерівність? Запропонуйте заходи щодо подолання цифрової нерівності.
3. Охарактеризуйте китайський підхід до регулювання Інтернету.
4. Розкрийте особливості американської моделі розвитку інформаційного суспільства.
5. Безпека та ризики використання месенджерів.

### Варіант 5

1. Проаналізуйте правові засади побудови інформаційного суспільства в Україні.
2. Визначте основні завдання національної інформаційної політики.
3. Охарактеризуйте ієрархію нетократичної влади. Хто такі нетократи і консьюмтаріат?
4. Що таке колективний інтелект і колективний розум?
5. Антивірусні програми: переваги та недоліки.

### Варіант 6

1. Внесок українських вчених (В. Вернадського та В. Глушкова) у розвиток ідей інформаційного суспільства
2. Охарактеризуйте внесок японських дослідників у формування концепції інформаційного суспільства.
3. Дайте визначення поняття «електронний уряд».
4. Назвіть інститути державної влади України в галузі інформації.
5. Ваше ставлення до відеоспостереження в публічних місцях.

### Варіант 7

1. Назвіть напрями державної політики у сфері інформаційної безпеки України.
2. Чи існує в Україні цифрова нерівність? Якщо так, внаслідок чого вона виникає?
3. Охарактеризуйте інформаційні загрози, які виникають в українському суспільстві.
4. Які основні закони регулюють масмедійний простір України?
5. Фішинг як метод соціальної інженерії

#### **4.4. Забезпечення освітнього процесу**

Використання проектору; методичних матеріалів та посібників в електронній формі; використання платформи Moodle.

Використання можливостей Google meet під час проведення відеоконференцій (лекцій, семінарських занять, заліків) зі студентами в умовах карантину.

Методичне забезпечення навчальної дисципліни включає також:

- навчальні та робочі навчальні плани;
- робоча програма навчальної дисципліни;
- опорні конспекти лекцій;
- завдання для творчої роботи (презентації);
- завдання для проведення контрольної роботи;
- завдання для підсумкового контролю (питання до іспиту);
- законодавчі та методичні матеріали;
- підручники і навчальні посібники.

## 5. Підсумковий контроль

Контроль планується здійснювати шляхом оцінювання усних відповідей на семінарських заняттях, перевірки письмових робіт (самостійні і контрольні роботи), захист творчої роботи та проведення іспиту за результатами вивчення курсу.

### Питання до іспиту з курсу «Інформаційна політика та менеджмент»

1. Інформаційна політика на сучасному етапі: основні підходи, мета і завдання.
2. Інформаційна безпека в інформаційну добу.
3. Інформаційна революція.
4. Постіндустріальне/інформаційне суспільство.
5. Концепція «нетократичного» суспільства О. Барда і Я. Зодерквіста: основні положення.
6. Зміни влади та політичної структури в інформаційному суспільстві (за Е. Тоффлером).
7. Внесок українських вчених (В. Вернадський та В. Глушков) у розвиток ідей інформаційного суспільства.
8. Міжнародні програми розвитку інформаційного суспільства (Окінавська хартія глобального інформаційного суспільства, документи, затверджені у рамках Всесвітнього саміту з питань інформаційного суспільства (Женева, 2003 – Туніс, 2005) та ін.).
9. Політика розбудови інформаційного суспільства в Україні
10. Загальна характеристика національних моделей інформаційного суспільства: європейська, англо-американська, азійська.
11. Основні виміри цифрової нерівності та шляхи її подолання.
12. Сутність електронного уряду, мета та принципи його становлення.
13. Світовий досвід впровадження електронного уряду (на прикладі конкретної країни).
14. Проблеми формування електронного уряду в Україні.
15. Державна інформаційна політика України: фактори формування, головні напрями та пріоритетні завдання.
16. Інститути державної влади України в галузі інформації: структура та основні напрями діяльності (на прикладі конкретної установи).
17. Медіаполітика держави: моделі відносин держави з медіаструктурами.
18. Інформаційне законодавство України як підґрунтя державної інформаційної політики.
19. Розуміння національної безпеки в інформаційному контексті (Закон України «Про національну безпеку України»; «Стратегія національної безпеки України»).
20. Основні напрями формування державної інформаційної безпеки.
21. Технології забезпечення захисту національного інформаційного простору.
22. Глобалізація інформаційного простору.
23. Правові проблеми регулювання Інтернету.
24. Американська модель розвитку інформаційного суспільства.
25. Китайський підхід до регулювання Інтернету.
26. Законодавче та нормативно-правове забезпечення інформаційної безпеки та кібербезпеки в Україні.
27. Правила кібергігієни та захист персональних даних в мережі та поза нею.
28. Протидія методам соціальної інженерії: шахрайство, крадіжка, фішинг та підробні посилання.
29. Стеження за користувачами веб-браузерів та використання cookies.
30. Безпека, зручність та загрози від сервісів для відеоконференції та навчання.
31. Безпека та ризики використання соціальних мереж та месенджерів.
32. Захист аккаунту від зламу: паролі та двоетапна аутентифікація. Небезпечні оновлення та сайти.
33. Захищений доступ під час віддаленої роботи.
34. Закон України «Про захист персональних даних».
35. Відеоспостереження в публічних місцях: право на захист приватного життя і персональних даних.
36. Модель Силіконової долини.
37. Досвід «азійських тигрів» (Гонконг, Республіка Корея, Тайвань, Сінгапур).
38. Інформаційні стратегії Китаю та Японії.

39. Інформаційні стратегії Індії.
40. Європейська модель побудови інформаційного суспільства (Фінляндія та Естонія).
41. Світовий досвід впровадження електронного уряду США.
42. Світовий досвід впровадження електронного уряду Великобританії.
43. Світовий досвід впровадження електронного уряду Швейцарії
44. Світовий досвід впровадження електронного уряду Естонії
45. Світовий досвід впровадження електронного уряду Сінгапуру

**Приклад білету до іспиту  
(20 балів x 2 питання = 40 балів)**

**Чорноморський національний університет ім. Петра Могили**

Рівень вищої освіти – перший (бакалаврський)

Галузь знань: 28 – Публічне управління та адміністрування

Спеціальність: 281 «Публічне управління та адміністрування»

Навчальна дисципліна – **ІНФОРМАЦІЙНА ПОЛІТИКА ТА БЕЗПЕКА**

**ІСПИТОВИЙ БІЛЕТ**

1. Основні виміри цифрової нерівності та шляхи її подолання.
2. Глобалізація інформаційного простору.

*Затверджено на засіданні кафедри місцевого самоврядування та регіонального розвитку  
Протокол №2 від «31» серпня 2021 року*

Завідувач кафедри, доцент

Штиршов О.М.

Упорядник, доцент кафедри

Бондар Г. Л.

**6. Критерії оцінювання та засоби діагностики результатів навчання**  
**Система оцінювання роботи студентів з дисципліни.**  
**Денна форма, спеціальність 281«Публічне управління та адміністрування»**  
**Графік контрольних заходів та рейтингова шкала оцінювання**

**Оцінювання для денної форми (II курс):**

Форма контролю	Максимальна оцінка одиниці контролю	Кількість заходів	Сума балів
<b>4 семестр</b>			
Опитування на сем. заняттях	3	9	27
Виконання творча робота (презентація)	10	1	10
Виконання ситуативних завдань	13	4	13
Контрольна робота	10	1	10
<b>Загальна кількість балів</b>			<b>60</b>
<b>Іспит</b>			<b>40</b>
<b>Всього</b>			<b>100</b>

**Пояснення до умов визначення рейтингу**

Опитування на семінарах включає в себе: опитування з будь-якого питання, що винесене на семінарське заняття (за вибором викладача), відповідь на питання інших студентів, запитання студентів до інших студентів, відповідей інших студентів, відповідь на питання для повторення (з тем, що було вивчено раніше), вирішення ситуаційних завдань з необхідною аргументацією та посиланням на законодавство. Максимальна кількість балів може бути виставлена студентам, підготовленим до відповідей на усі питання теми. Оцінюючи відповідь, викладач керується такими критеріями, як: правильність відповідей на питання, повнота і конкретність відповіді, ступінь використання наукових і нормативних джерел, вміння пов'язати теорію з практикою, логіка і аргументованість викладу думок, культура мови.

Доповнення здійснюється студентом по темі семінару після основної відповіді по питанню винесеному на семінарське заняття. Метою доповнення є більш повне розкриття питання, винесеного на семінарське заняття, або висвітлення різноманітних наукових, практичних аспектів даного питання

Вирішення практичних ситуативних завдань здійснюється у вигляді розв'язання завдань з теми семінару, які надані викладачем студентам на попередньому семінарі. Студент самостійно, опрацювавши вдома матеріал до семінару, вирішує завдання з належним аргументуванням та доказовістю. На семінарі студент усно доповідає своє бачення вирішення завдання. Якщо відповідь студента є неповною, тоді долучаються інші студенти з відповідним оцінюванням їх відповідей або участю в обговоренні.

Творча робота (презентація) за допомогою засобів Power Point. Передбачає підготовку та презентацію проекту до відповідної тематики семінарського заняття з використанням наочних засобів та використанням електронної техніки, висловлення обґрунтованої позиції щодо мети і результатів виконаного завдання.



## Денна форма (II курс)

№ з/п	Види робіт. Критерії оцінювання знань студентів	Бали рейтингу	Максимальна кількість балів
<b>IV семестр</b>			
<b>1. Бали опитування на семінарських заняттях (3 бали x 9 занять)</b>			
<b>Критерії оцінювання</b>		<b>3 бали</b>	
<ul style="list-style-type: none"> <li>▪ студент в повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно вирішив усі тестові завдання</li> </ul>		<b>3</b>	
<ul style="list-style-type: none"> <li>▪ студент в цілому володіє навчальним матеріалом викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив половину тестових завдань</li> </ul>		<b>2</b>	
<ul style="list-style-type: none"> <li>▪ студент не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності, правильно вирішив меншість тестових завдань</li> </ul>		<b>1</b>	
<ul style="list-style-type: none"> <li>▪ студент частково володіє навчальним матеріалом не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив окремі тестові завдання</li> </ul>		<b>0</b>	
<b>2. Самостійна робота студентів (СРС) (Творча робота – презентація)</b>			
<b>Критерії оцінювання</b>		<b>10 балів</b>	
<ul style="list-style-type: none"> <li>• робота виконана та захищена згідно вимог та методичних рекомендацій у повному обсязі</li> </ul>		<b>10</b>	
<ul style="list-style-type: none"> <li>• робота виконана та захищена з незначними порушеннями вимог та методичних рекомендацій</li> </ul>		<b>8-9</b>	
<ul style="list-style-type: none"> <li>• робота виконана згідно вимог та методичних рекомендацій, але не захищена</li> </ul>		<b>5-7</b>	
<ul style="list-style-type: none"> <li>• робота не захищена або виконана частково, з порушенням вимог і методичних рекомендацій</li> </ul>		<b>2-4</b>	
<ul style="list-style-type: none"> <li>• робота не здана або виконана частково, із значними порушеннями вимог і методичних рекомендацій</li> </ul>		<b>0-1</b>	
<b>2. Самостійна робота студентів (СРС) (Ситуативні завдання)</b>			
<b>Критерії оцінювання</b>		<b>13 балів</b>	
<ul style="list-style-type: none"> <li>• робота виконана та захищена згідно вимог та методичних рекомендацій у повному обсязі</li> </ul>		<b>10-13</b>	
<ul style="list-style-type: none"> <li>• робота виконана та захищена з незначними порушеннями вимог та методичних рекомендацій</li> </ul>		<b>8-9</b>	
<ul style="list-style-type: none"> <li>• робота виконана згідно вимог та методичних рекомендацій, але не захищена</li> </ul>		<b>5-7</b>	

• робота не захищена або виконана частково, з порушенням вимог і методичних рекомендацій	2-4
• робота не здана або виконана частково, із значними порушеннями вимог і методичних рекомендацій	0-1
<b>3. Самостійна робота студентів (СРС) (Контрольна робота)</b>	
<b>Критерії оцінювання</b>	<b>10 балів</b>
• робота виконана та захищена згідно вимог та методичних рекомендацій у повному обсязі	10
• робота виконана та захищена з незначними порушеннями вимог та методичних рекомендацій	8-9
• робота виконана згідно вимог та методичних рекомендацій, але не захищена	5-7
• робота не захищена або виконана частково, з порушенням вимог і методичних рекомендацій	2-4
• робота не здана або виконана частково, із значними порушеннями вимог і методичних рекомендацій	0-1
<b>5. Іспит з дисципліни</b>	
<b>Критерії оцінювання</b>	<b>40 балів</b>
Іспит з дисципліни містить питання згідно навчальної програми. Студент відповідає на питання різного ступеня складності.	

## 7. Рекомендовані джерела інформації

### Основна:

1. An Intelligent Multi-Stage Model for Countering the Impact of Disinformation on the Cybersecurity System / M.Kryshchanovych, N. Lyubomudrova, H. Bondar, V. Motornyy, V. Kuchmenko // *Ingénierie des Systèmes d'Information* Vol. 28, No. 1, February, 2023, pp. 41-47  
Journal homepage: <http://iieta.org/journals/isi>. DOI: <https://doi.org/10.18280/isi.280105>
2. . Бондар Г. Л., Гаркуша А.М. Інформаційна політика та етика в добу діджиталізації // *Публічне управління та митне адміністрування*. - №4 (23). -2019. – С.23-33.
3. Бондар Г. Л., Ракутіна Л. О. Інформаційна політика та інформаційна безпека // *Публічне управління та митне адміністрування*. - №4 (23). – С. 42-49 [Електронний ресурс]. – Режим доступу: <http://customs-admin.umsf.in.ua/archive/2019/4/6.pdf>.
4. Бондар Г.Л. Цифрова трансформація уряду України, відкриті дані (open data) та електронні послуги // *Public Administration and Regional Development*. – 11, 2021. – С.97-123. DOI: 10.34132/pard2021.11.05
5. Бондар Г.Л. Загальноєвропейська система цифрової ідентифікації для громадян країн-членів ЄС та захист персональних даних // *Могилянські читання – 2020 : Досвід та тенденції розвитку суспільства в Україні : глобальний, національний та регіональний аспекти : XXIII Всеукр. наук.-практ. конф. : тези доп. Публічне управління в Україні в умовах децентралізації влади та наближення її до європейських стандартів, Миколаїв, 16–20 листоп. 2020 р. / ЧНУ ім. Петра Могили. – Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2020. – 136 с. - С.47-49.*
6. Бондар Г.Л. Публічна інформація органів влади у формі відкритих даних (open data Ukraine) та громадянське суспільство // *Міжнародна науково-практична конференція на тему «Державне управління в Україні: виклики та перспективи» / Класичний приватний університет, Запоріжжя, 7–8 травня 2021 р., С. 31-35.*
7. Бондар Г.Л. Взаємодія і комунікація між державою та громадянами за допомогою відкритих даних (громадські послуги, інтерактивні карти, веб-сайти та державні проекти) / «Ольвійський форум - 2021: стратегії країн Причорноморського регіону в геополітичному просторі» : XV Міжнар. наук.-практ. конф. 10-13 червня 2021 р., Миколаїв, С. 78-81.
8. Смельянов В. М., Бондар Г. Л. Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури України // *Public Administration and Regional Development*. – 5, 2019. – С. 493-523 [Електронний ресурс]. – Режим доступу: <https://pard.mk.ua/index.php/journal/article/view/141/106><https://pard.mk.ua/index.php/journal/article/view/141/106>.
9. Кіберзагроза BlackEnergy2/3. Історія атак на критичну ІТ інфраструктуру України : Відділ реагування на інциденти CyS Centrum (CyS-CERT). 6 січня 2016 р. [Електронний ресурс]. – Режим доступу: [https://cys-centrum.com/ru/news/black\\_energy\\_2\\_3](https://cys-centrum.com/ru/news/black_energy_2_3).
10. Кіберполіція попереджає про активізацію хакерів в період карантину. 06.04.2020 : Офіційний сайт Національної поліції [Електронний ресурс]. – Режим доступу: <https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-poperedzhaje-pro-aktivizacziyu-xakeriv-u-period-karantinu/>.
11. Ляковський І. Каліфорнійський GDPR: 5 Must have Політики конфіденційності [Електронний ресурс]. – Режим доступу : <https://legalitgroup.com/kalifornijskij-gdpr-5-must-have-politiki-konfidentsijnosti/>.
12. Основні правила кібергігієни: Офіційний сайт CERT-UA [Електронний ресурс]. – Режим доступу: <https://cert.gov.ua/recommendations/21>.
13. Почепцов Г. Г. Інформаційна політика : навч. посіб. / Почепцов Георгій Георгійович, Чукут Світлана Анатоліївна. - К. : Знання, 2006. – 663 с.
14. Рекомендації щодо підвищення рівня захищеності інформаційно-телекомунікаційних систем та інформаційних ресурсів державних органів і установ Основні

правила кібергігієни: Офіційний сайт CERT-UA [Електронний ресурс]. – Режим доступу: <https://cert.gov.ua/recommendations/20>.

15. Башук А.І. Інформаційна політика : [навч. посіб.] / Алла Іванівна Башук. – Ч.1. – К.: Вид-во ІЖ КНУ ім. Т. Шевченка, 2007. – 90 с.

16. Карпенко В.О. Інформаційна політика та безпека : підручник / Віталій Опанасович Карпенко. — К. : Нора-Друк, 2006. — 320с.

17. Міжнародна інформаційна безпека: сучасні виклики та загрози. – К.: Центр вільної преси, 2006. – 916 с.

18. Почепцов Г.Г. Інформаційна політика : навч. посіб. / Почепцов Георгій Георгійович, Чукут Світлана Анатоліївна. — К. : Знання, 2006. — 663с.

19. Бард А., Зодерквист Я. Нетократия. Новая правящая элита и жизнь после капитализма: Пер. с англ. – СПб.: Стокгольмская школа экономики в Санкт-Петербурге, 2004. – 252 с. // <http://www.avatargroup.ru/booksreader.aspx?dbid=304>

20. Белл Д. Прихід постіндустріального суспільства // Сучасна зарубіжна соціальна філософія. Хрестоматія: Навч. посіб. / Упоряд. В. Лях. – К.: Либідь, 1996. – С. 194-251.

21. Белл Д. Социальные рамки информационного общества // Новая технократическая волна на Западе. – М., 1986 // <http://www.nethistory.ru/biblio/1043172230.html>

22. Башук А.І. Підходи до інформаційної політики у контексті переходу до інформаційного суспільства / А.І. Башук // Наукові записки Інституту журналістики : наук. збірник / за ред. В.В. Різуна ; КНУ імені Тараса Шевченка. – К., 2010. – Т.38 (січень-березень). – С. 152-157.

23. Вернадський В.І. Вибрані праці. – К.: Наукова думка, 2005. – 302 с.

24. Всесвітній саміт з питань інформаційного суспільства (Женева 2003 – Туніс 2005) : підсумкові документи [переклад, упорядкування, укладання Словника термінів Ю.Пероганич] / К.: Державне підприємство «Державне видавничо-інформаційне агенство «ЗВ`ЯЗОК», 2006. – 131 с.

25. Інформаційна політика України: європейський контекст : моногр. / [Губерський Леонід Васильович, Камінський Євген Євменович, Макаренко Євгенія Анатоліївна та ін.]. — К. : Либідь, 2007. — 360с.

26. Інформаційне Суспільство. Шлях України. – К.: Бібліотека інформаційного суспільства, 2004. – 289 с.

27. Йенсен Ролф. Общество мечты. Как грядущий сдвиг от информации к воображению преобразит ваш бизнес: Пер. с англ. – СПб.: Стокгольмская школа экономики в Санкт-Петербурге, 2002. – 271 с. // <http://ntsaphil.univ.kiev.ua>

28. Кастельс М. Информационная эра: экономика, общество, культура / М. Кастельс ; [Б.Э.Верпаховский (пер.)]. – М.: Госуд. ун-т. Высшая школа экономики, 2000. – 607 с.

29. Литвиненко О.В. Інформаційний простір як чинник забезпечення національних інтересів України : монографія / Литвиненко О.В., Бінько І.Ф., Потіха В.М. – К.: ІМВ КУ імені Тараса Шевченка, 1998. – 87 с.

30. Мей Кр. Інформаційне суспільство. Скептичний погляд: Пер. з англ. – К.: «К.І.С.», 2004. – 220 с.

31. Тоффлер Е. Третья Хвиля – К.: Видавничий дім «Всесвіт», 2000. – 480 с.

### **Законодавча та нормативно-правова база:**

1. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 №3475-IV [Електронний ресурс]. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/3475-15>.

2. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV [Електронний ресурс]. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/851-15>.

3. Про затвердження Положення про інтегровану систему електронної ідентифікації: Постанова Кабінету Міністрів України від 19.06.2019 №546. – [Електронний ресурс]. – Режим доступу : <https://www.kmu.gov.ua/npas/pro-zatverdzhennya-polozhennya-pro-integrovanu-sistemu-elektronnoyi-identifikaciyi-i190619>.

4. Про захист інформації в автоматизованих системах: Закон України від 31.05.2005 № 2594-IV [Електронний ресурс]. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/2594-15>.
5. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 №80/94-ВР. – [Електронний ресурс]. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>.
6. Про Концепцію Національної програми інформатизації : Закон України від 04.02.1998 № 75/98-ВР [Електронний ресурс]. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80>.
7. Про Національну систему конфіденційного зв'язку: Закон України від 10.01.2002 №2919-III [Електронний ресурс]. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/2919-14>.
8. Про обмін правовою інформацією: Угода, Перелік, Міжнародний документ від 21.10.1994. – [Електронний ресурс]. – Режим доступу : [https://zakon.rada.gov.ua/laws/show/997\\_699](https://zakon.rada.gov.ua/laws/show/997_699)
9. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 №2163-VIII. – [Електронний ресурс]. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/2163-19>.
10. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 №2824-IV. – [Електронний ресурс]. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/2824-15>.
11. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» Указ Президента України; Стратегія від 15.03.2016 № 96/2016. – [Електронний ресурс]. – Режим доступу : <https://zakon5.rada.gov.ua/laws/show/96/2016>.
12. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України; Доктрина від 25.02.2017 №47/2017. – [Електронний ресурс]. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/47/2017>.
13. Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 8.11.2017 №797-р. – [Електронний ресурс]. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/797-2017-%D1%80>.
14. Про схвалення Концепції розвитку системи електронних послуг в Україні: Розпорядження Кабінету Міністрів України від 16.11.2016 №918-р. – [Електронний ресурс]. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/918-2016-%D1%80>.
15. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 17.01.2018 №67-р. – [Електронний ресурс]. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/en/67-2018-%D1%80>.
16. Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних: Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 р. – [Електронний ресурс]. – Режим доступу : <https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf>.
17. Про інформацію: Закон України від 02.10.1992 №2657-XII [Електронний ресурс]. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/2657-12>.
18. Про захист персональних даних: Закон України від 01.06.2010 №2297-VI [Електронний ресурс]. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/2297-17>.
19. Про електронні довірчі послуги: Закон України від 05.10.2017 №2155-VII [Електронний ресурс]. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/2155-19#n534>.
20. Про національну безпеку України: Закон України від 21.06.2018 №2496-VIII [Електронний ресурс]. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/2496-19>.
21. Про Національну програму інформатизації: Закон України від 04.02.1998 №74/98-ВР [Електронний ресурс]. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80>.