

ДОНЕЦЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ФАКУЛЬТЕТ № 3

**КАФЕДРА ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ ТА
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЦИФРОВА ПОЛІТИКА ТА ЕЛЕКТРОННЕ ВРЯДУВАННЯ

Галузь знань 28 Публічне управління та адміністрування
Спеціальність 281 Публічне управління та адміністрування
Освітній ступінь другий (магістерський)
Освітньо-професійна програма «Публічне управління та адміністрування»
Шифр за ОПП: ОК 8

Мова навчання: українська

Кропивницький – 2024

Розробники:

ЗЕЛЕНСЬКИЙ Сергій,

доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету № 3 ДонДУВС, кандидат юридичних наук, доцент

Робочу програму розглянуто та затверджено на засіданні кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету № 3 ДонДУВС
Протокол № 7 від «12» листопада 2024 року

Завідувач кафедри



Артур ВОЛОБОЄВ

Робочу програму погоджено з гарантом освітньо-професійної програми
«Публічне управління та адміністрування»
«12» листопада 2024 року

Гарант ОПП



Олена БУЛГАКОВА

**Лист оновлення та перезатвердження
робочої програми навчальної дисципліни**

| Навчальний рік | Дата засідання кафедри – розробника РПНД | Номер протоколу | Підпис завідувача |
|----------------|--|-----------------|-------------------|
| | | | |
| | | | |
| | | | |

1. ВСТУП

1.1. Опис навчальної дисципліни

| Найменування показників | Характеристика навчальної дисципліни | |
|---|--------------------------------------|-----------------------|
| | денна форма навчання | заочна форма навчання |
| Статус навчальної дисципліни: | обов'язкова | |
| Мова викладання, навчання та оцінювання | українська | |
| Рік підготовки | 1-й | |
| Семестр | 2-й | |
| Кількість кредитів ЄКТС / годин | 4 / 120 | |
| Модулів: | 1 | |
| Змістових модулів: | 1 | |
| Лекції: | 20 годин | 6 годин |
| Семінарські: | 20 годин | 6 годин |
| Практичні: | | |
| Самостійна робота: | 80 годин | 108 годин |
| Індивідуальні завдання (курсова робота): | не передбачено | |
| Підсумковий семестровий контроль: | залік | |
| Співвідношення кількості годин аудиторних занять до самостійної роботи становить: | 1:2 | 1:9 |

1.2. Мета та завдання навчальної дисципліни

Мета: підготовка висококваліфікованих, конкурентоспроможних, інтегрованих у світовий науково-освітній простір фахівців магістерського ступеня, які в умовах сучасних суспільних трансформацій і викликів, здатні формулювати і розв'язувати завдання практичного змісту системи публічного управління та адміністрування на міжнародному, національному, регіональному та місцевому рівнях, а також здійснювати дослідницьку та викладацьку діяльність через формування комплексу професійних та ІТ-компетентностей щодо цифрової політики та електронного врядування як

механізму політичної взаємодії, з використанням новітніх інформаційних і комунікаційних технологій.

Завдання: формування сучасних теоретичних та практичних знань, умінь та навичок з цифрового розвитку та електронної демократії; налагодження ефективних комунікацій з метою кращої підготовки до співробітництва та взаємодії в інформаційному суспільстві та суспільстві знань; формування навичок самостійної роботи з традиційною літературою та джерелами в Інтернеті; розвиток логічного, аналітичного та критичного мислення; вироблення вміння застосовувати у професійній діяльності основні методи і принципи цифрової політики та електронного врядування.

1.3. Передумови для вивчення навчальної дисципліни

Пререквізити навчальної дисципліни: «Інформатика для управлінців», «Теорія і практика публічного управління», «Публічне управління».

Постреквізити навчальної дисципліни: «Публічне управління регіональним розвитком», «Проектний менеджмент», «Публічне управління інвестиціями в умовах ревіталізації».

2. РЕЗУЛЬТАТИ НАВЧАННЯ ЗА ДИСЦИПЛІНОЮ

| | ПРН 2 | ПРН 03 | ПРН 7 | ПРН 8 | ПРН 10 |
|---|-------|--------|-------|-------|--------|
| Знати та розуміти організацію групових форм внутрішньо організаційної комунікації, категорійно-понятий апарат інформаційного суспільства, е-врядування та е-демократії | + | | | + | + |
| Знати загальні принципи, методи і моделі е-врядування та е-демократії, класифікацію, ієрархію та систему надання адміністративних послуг | + | + | + | | + |
| Вміти оцінювати та аналізувати поточний стан е-демократії, ведення органами державної влади та місцевого самоврядування своїх електронних інформаційних ресурсів | + | | + | + | + |
| Вміти організувати обробку документації, підготовку, прийняття та впровадження управлінських рішень засобами сучасних інформаційно-комунікаційних технологій задля інформаційного забезпечення органів державної влади та місцевого самоврядування | + | | + | + | + |
| Вміти користуватися програмно-технічним забезпеченням; розуміти заходи, пов'язані з протидією загрозам інформаційній безпеці та політики безпеки в системах е-врядування; з основами кібергігієни, соціальної інженерії та кібербезпеки в умовах воєнного стану | + | + | + | | + |

3. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

| Назви змістовних модулів та тем | Кількість годин | | | | | | | | | |
|---|-----------------|--------------|---------------------|-------------------|-------------------|--------------|--------------|---------------------|-------------------|-------------------|
| | денна форма | | | | | заочна форма | | | | |
| | Усього | у тому числі | | | Самостійна робота | Усього | у тому числі | | | Самостійна робота |
| | | лекції | семінарські заняття | практичні заняття | | | лекції | семінарські заняття | практичні заняття | |
| Модуль 1 | | | | | | | | | | |
| Змістовий модуль 1. Цифрова політика та електронне врядування | | | | | | | | | | |
| Тема 1. Цифрова політика та електронне врядування: сутність та основні підходи | 16 | 2 | 2 | | 12 | 16 | 2 | | | 14 |
| Тема 2. Впровадження електронного врядування в Україні | 20 | 4 | 4 | | 12 | 20 | 2 | | | 18 |
| Тема 3. Електронна демократія: сутність та стратегії реалізації | 20 | 4 | 4 | | 12 | 20 | | 2 | | 18 |
| Тема 4. Електронні послуги | 24 | 4 | 4 | | 16 | 24 | 2 | | | 22 |
| Тема 5. Технології розвитку цифрової політики та електронного врядування | 18 | 2 | 2 | | 14 | 18 | | 2 | | 16 |
| Тема 6. Захист інформації в системах електронного врядування | 22 | 4 | 4 | | 14 | 22 | | 2 | | 20 |
| Усього годин | 120 | 20 | 20 | | 80 | 120 | 6 | 6 | | 108 |

4. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Змістовий модуль 1. ЦИФРОВА ПОЛІТИКА ТА ЕЛЕКТРОННЕ ВРЯДУВАННЯ

Тема 1. ЦИФРОВА ПОЛІТИКА ТА ЕЛЕКТРОННЕ ВРЯДУВАННЯ: СУТНІСТЬ ТА ОСНОВНІ ПІДХОДИ.

Сутність цифрової політики та електронного врядування. Загальносвітові тенденції розвитку ІКТ як фактор впливу на електронне врядування: глобалізація, розвиток світового інформаційного суспільства. Моделі електронного врядування. Очікування та наслідки впровадження електронного

врядування. Проблеми та загрози при впровадженні електронного врядування. Історія звітів ООН з розвитку електронного врядування. Індекс розвитку електронного врядування, індекс онлайн послуг, індекс людського капіталу, індекс електронної участі, індекс локальних онлайн-сервісів. Сектори міжсуб'єктної взаємодії в системі електронного врядування.

Тема 2. ВПРОВАДЖЕННЯ ЕЛЕКТРОННОГО ВРЯДУВАННЯ В УКРАЇНІ.

Основні етапи розвитку електронного врядування в Україні. Діяльність Міністерства цифрової трансформації України. Розвиток електронного врядування на регіональному та місцевому рівнях в Україні. Поняття «розумне місто», «електронне місто», «електронний регіон». Досвід упровадження електронного врядування в містах України. Кращі зарубіжні практики електронного врядування на місцевому та регіональному рівнях (Австралія, Франція, Швейцарія, Об'єднані Арабські Емірати).

Тема 3. ЕЛЕКТРОННА ДЕМОКРАТІЯ: СУТНІСТЬ ТА СТРАТЕГІЇ РЕАЛІЗАЦІЇ.

Сутність електронної демократії. Довідник з електронної демократії Ради Європи. Основні етапи розвитку електронної демократії. Електронні звернення та електронні петиції в Україні. Електронний парламент. Електронне голосування: сутність та регулювання. Стандарти електронного голосування Ради Європи. Досвід електронного голосування США та Естонії. Ризики та загрози впровадження електронного голосування.

Тема 4. ЕЛЕКТРОННІ ПОСЛУГИ.

Сутність е-послуг та фактори, які впливають на їх ефективність. Сутність електронних адміністративних послуг. Організація надання електронних адміністративних послуг. Фази зрілості електронних послуг. Досвід Європейського союзу щодо сумісності. Модель ООН розвитку онлайн-послуг. Досвід надання електронних послуг за кордоном. Електронні публічні послуги в країнах Європи. Електронні публічні послуги в країнах Азії. Електронні послуги в Україні. Перспективні напрями розвитку послуг електронного уряду. Портал Дія. Доступ до публічної інформації: теоретичні та правові основи. Публічна інформація у формі відкритих даних. Зарубіжний та український досвід використання відкритих даних.

Тема 5. ТЕХНОЛОГІЇ РОЗВИТКУ ЦИФРОВОЇ ПОЛІТИКИ ТА ЕЛЕКТРОННОГО ВРЯДУВАННЯ.

Базові аспекти організації електронної взаємодії органів публічної влади. Стан та тенденції розвитку електронної взаємодії в Україні. Реалізація електронної взаємодії в європейських країнах: інтероперабельність та моделі електронної взаємодії. Програмне забезпечення електронної взаємодії публічних службовців. Інформаційно-комунікаційні технології розвитку

цифрової політики та електронного врядування. Організаційні технології розвитку електронного врядування. Громадські проекти мобілізації людських ресурсів за допомогою інформаційно-комунікаційних технологій.

Тема 6. ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО ВРЯДУВАННЯ.

Основні визначення та поняття інформаційної безпеки й захисту інформації. Сутність захисту інформації. Завдання у сфері захисту інформації. Основні проблеми безпечного функціонування систем електронного врядування. Поняття та види загроз інформаційній безпеці в системах електронного врядування. Канали витоку інформації. Законодавчий рівень забезпечення протидії загрозам інформаційній безпеці. Адміністративний та процедурний рівні забезпечення протидії загрозам інформаційній безпеці. Програмно-технічний рівень протидії загрозам інформаційній безпеці та політика безпеки в системах е-врядування. Рівні системи електронного врядування з точки зору протидії загрозам інформаційній безпеці. Сутність мережевої війни. Загрози електронному врядуванню у мережевій війні. Поняття кібербезпеки. Правові основи та принципи забезпечення кібербезпеки. Кібербезпека та інформаційна війна. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA. Основи кібергігієни. Методи соціальної інженерії. Кібербезпека в умовах воєнного стану.

5. ПОРЯДОК ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

5.1. Методи навчання

Під час проведення навчальних занять можуть застосовуватися такі методи:

- словесні методи навчання;
- наочні методи навчання;
- практичні методи навчання;
- проблемно-пошукові методи навчання;
- активні методи навчання, у тому числі з використанням поліцейських квестів.

5.2. Порядок оцінювання результатів навчання

Оцінювання роботи здобувачів та здобувачок вищої освіти здійснюється відповідно до загальноуніверситетської системи оцінювання знань.

Система передбачає:

для денної форми навчання

| | Поточний контроль | | Підсумковий контроль |
|---------------------------------------|---------------------|-------------------|----------------------|
| | Семінарські заняття | Самостійна робота | Залік |
| | 40 | 20 | 40 |
| Всього за навчальну дисципліну | 100 | | |

Для переведу оцінок у бали необхідно користуватися формулою:

$$AP = \frac{\text{сума всіх отриманих оцінок за аудиторну роботу}}{\text{кількість аудиторних занять за семестр за аудиторну роботу}} * 8 =$$

для заочної форми навчання

| | Поточний контроль | | Підсумковий контроль |
|---------------------------------------|---------------------|-------------------|----------------------|
| | Семінарські заняття | Самостійна робота | Залік |
| | 20 | 40 | 40 |
| Всього за навчальну дисципліну | 100 | | |

Для переведу оцінок у бали необхідно користуватися формулою:

$$AP = \frac{\text{сума всіх отриманих оцінок за аудиторну роботу}}{\text{кількість аудиторних занять за семестр за аудиторну роботу}} * 4 =$$

При оцінюванні заліку застосовуються такі критерії:

– 36-40 балів – здобувач/здобувачка вищої освіти вільно володіє навчальним матеріалом, надав/надала повну, вичерпну відповідь на поставлене запитання, з посиланням на чинні нормативно-правові акти (або правильно відповів/відповіла на 90-100 % тестових завдань). Максимальна кількість балів може бути знижена, якщо під час відповіді здобувач/здобувачка вищої освіти не зробив/зробила посилання на чинні нормативно-правові акти чи допустив/допустила незначні помилки.

– 28-35 балів – здобувач/здобувачка вищої освіти володіє достатнім обсягом навчального матеріалу, надав/надала відповідь на питання але

допустив/допустила помилки, що впливають на загальний висновок (або правильно відповів/відповіла на 70-89 % тестових завдань);

– 20-27 балів – здобувач/здобувачка вищої освіти володіє навчальним матеріалом поверхово і фрагментарно на репродуктивному рівні або володіє частиною навчального матеріалу чи допускає значні помилки, які приводять до викривлення інформації (або правильно відповів/відповіла на 50-69% тестових завдань);

– 0-19 балів – здобувач/здобувачка вищої освіти не може виконати завдання, не володіє навчальним матеріалом, відмовляється відповідати на запитання або робить принципові помилки, які викривлюють усе рішення (або правильно відповів/відповіла менше ніж на 50 % тестових завдань).

Для визначення ступеня засвоєння навчального матеріалу та подальшого його оцінювання на семінарському занятті слід врахувати певні рівні знань:

1. Теоретична відповідь

– оцінка «5» високий рівень – здобувач/здобувачка вищої освіти вільно володіє навчальним матеріалом, опрацювавши основну та додаткову літературу, аргументовано висловлює свої думки, проявляє творчий підхід до виконання індивідуальних та колективних завдань у самостійній роботі;

– оцінка «4» добрий рівень – здобувач/здобувачка вищої освіти володіє певним обсягом навчального матеріалу, здатний/здатна його аналізувати, але не має достатніх знань для формулювання висновків, поєднання теоретичних знань із практичними прикладами;

– оцінка «3» задовільний рівень – здобувач/здобувачка вищої освіти володіє навчальним матеріалом поверхово і фрагментарно на репродуктивному рівні або володіє частиною навчального матеріалу;

– оцінка «0» незадовільний рівень – здобувач/здобувачка вищої освіти не володіє навчальним матеріалом, відмовляється відповідати на запитання.

2. Тест: правильне вирішення тесту оцінюється в 1 бал.

3. Завдання: у письмовій або усній формі вважається вирішеним і оцінюється:

– оцінка «5» високий рівень – повністю правильно вирішено завдання, надано відповіді на всі поставлені в умовах питання, з посиланням на чинні нормативно-правові акти;

– оцінка «4» добрий рівень – повністю правильно вирішено завдання, надано відповіді на всі поставлені в умовах питання, але не зроблено посилання на чинні нормативно-правові акти чи допущено незначні помилки;

– оцінка «3» задовільний рівень – надано відповіді не на всі поставлені в умовах питання, чи не зроблено посилання на чинні нормативно-правові акти, чи допущено значні помилки;

– оцінка «0» незадовільний рівень – не правильно вирішено завдання.

4. Реферативне повідомлення в письмовій формі – оцінюється в 5 балів:

– 1 бал – належне оформлення реферативного повідомлення;

- 1 бал – глибока проробка теми (наявність достатньої кількості літературних джерел, наявність ґрунтовних висновків);
 - 1 бал – теоретична обґрунтованість теми, визначення її актуальності, мети, завдань, чітко розроблений науковий апарат;
 - 2 бали – грамотна і аргументована презентація реферату.
- Кожну оцінку викладач/викладачка мають аргументовано мотивувати.

Шкала оцінювання: національна та ECTS

| Сума балів | Оцінка за національною шкалою | Оцінка за шкалою ECTS | Пояснення |
|------------|-------------------------------|-----------------------|--|
| 90-100 | Відмінно | A | Кредит зараховано. Контрольні заходи виконані лише з незначною кількістю помилок. |
| 82-89 | Добре | B | Кредит зараховано. Контрольні заходи виконані вище середнього рівня з кількома помилками. |
| 75-81 | | C | Кредит зараховано. Контрольні заходи виконані вірно з певною кількістю суттєвих помилок |
| 67-74 | Задовільно | D | Кредит зараховано. Контрольні заходи виконані непогано, але зі значною кількістю недоліків |
| 60-66 | | E | Кредит зараховано. Виконання контрольних заходів задовольняє мінімальним критеріям |
| 35-59 | Незадовільно | FX | Кредит не зараховано. Здобувачу/здобувачці вищої освіти надається можливість скласти оговорені контрольні заходи для поліпшення підсумкової оцінки |
| 1-34 | | F | Кредит не зараховано. Здобувач/здобувачка вищої освіти мають повторно освоювати навчальний матеріал дисципліни (модуля). |

6. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. Вишня В. Б., Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки : навч. посіб. Дніпро: ДДУВС, 2020. 128 с.
2. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою : навчальний посібник. Дніпро: ДДУВС, 2020. 144 с.
3. Електронне урядування та електронна демократія: навч. посіб. / за заг. ред. А. І. Семенченка, В. М. Дрешпака. К., 2017. 86 с.
4. Інформаційні технології : підруч. / В. Б. Вишня, К. Ю. Ісмаїлов, І. В. Краснобрижий, С. О. Прокопов, Е. В. Рижков. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2021. 492 с.
5. Когут Ю.І. Кібервійни, кібертероризм, кіберзлочинність: практичний посібник. Київ, Консалтінгова компанія Сідкон, Дакор. 2022. 284 с.
6. Чукут С. А., Загвойська О. В., Цимбаленко Я. Ю. Основи електронного урядування. К.: КПІ ім. Ігоря Сікорського. 2022. 268 с.

Додаткові

1. Antonova L., Mokhova J. Improvement of e-governance mechanisms in Ukraine in the conditions of digital transformations. *Public Administration and Regional Development*, (15), 2023. 10-29. <https://doi.org/10.34132/pard2022.15.01>
2. Бутенко Т. А., Сирий В. М. Інформаційні системи та технології: навчальний посібник. Харків: ХНАУ ім. В. В. Докучаєва, 2020. 207 с.
3. Вовкодав О. В. Сучасні інформаційні технології: навчальний посібник. Тернопіль: ТНЕУ, 2017. 550 с.
4. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою : навчальний посібник. Дніпро: ДДУВС, 2020. 144 с.
5. Імплементация принципів електронного врядування як основа реформування системи публічного управління / А. О. Касич, І. В. Пономаренко, С. В. Бреус, Б. В. Десятник // Державне управління: удосконалення та розвиток. 2021. № 2. Режим доступу: <http://www.dy.nayka.com.ua/?op=1&z=1974>.
6. Когут Ю.І. Кібервійни, кібертероризм, кіберзлочинність (концепції, стратегії, технології): практичний посібник / Ю.І. Когут. Київ: Консалтінгова компанія «Сідкон»; ВД «Дакор» 2022. 284 с.
7. Корчак Н., Рачинський А., Ларіна Н. Цифрова трансформація та електронне врядування: наукові підходи дослідження в сфері публічного управління та адміністрування. *Аспекти публічного управління*. 2023. 11(3). С. 43-49.
8. Кужда Т. І. Стан та перспективи розвитку електронного урядування в Україні та в світі / Кужда Т. І. // Актуальні проблеми публічного управління та адміністрування: Колективна монографія. Т. : ФОП Паляниця В. А. 2020. С. 71–86.
9. Миргород-Карпова В. В., Шевцов Я. А. Електронне урядування в Україні: поточні досягнення, проблеми реформування та діяльність

міністерства цифрової трансформації України. *Правові горизонти / Legal horizons*. 2020. С. 35–42.

10. Міхровська М. Цифрове урядування – електронне урядування 2.0. *Collection of scientific papers «ΛΟΓΟΣ»*, (November 11, 2022; Paris, France), 2022. С. 38-40.

11. Мохова Ю. Л. Державні механізми розвитку електронного урядування в умовах цифрових трансформацій України : дис. докт. наук з держ. упр. 2021. 490 с.

12. Хаустова М. Г. Державна політика в умовах цифровізації суспільства. *Міжнародний досвід реалізації програм та стратегії цифровізації. Аналітично-порівняльне правознавство*, (2), 2022. С. 209-216.

13. Шевченко О. О., Бочко, Н. Є. Модернізація моделі розвитку е-урядування в умовах цифрових трансформацій. *Дніпровський науковий часопис публічного управління, психології, права*, 2022. (4). С. 45-50.

Нормативно-правові акти

1. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 № 2163-VIII. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.

2. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану. Постанова Кабінету Міністрів України від 12.03.2022 № 263. *Урядовий портал. Єдиний веб-портал органів виконавчої влади*. URL: <https://www.kmu.gov.ua/npas/deyaki-pitannya-zabezpechennya-funkcionuvannya-informacijno-komunikacijnih-sistem-elektronnih-komunikacijnih-sistem-publichnih-elektronnih-reyestriv-v-umovah-voennogo-stanu-263>.

3. Про внесення змін до деяких законів України щодо заборони виготовлення та поширення інформаційної продукції, спрямованої на пропагування дій держави-агресора. Закон України від 03.03.2022 № 2109-IX. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/2109-20#Text>.

4. Про внесення змін до Кримінального кодексу України щодо підвищення боротьби з кіберзлочинністю в умовах дії воєнного стану. Закон України від 24.03.2022 № 2149-IX. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/2149-20#Text>.

5. Про електронні довірчі послуги. Закон України від 05.10.2017 № 2155-VII. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>.

6. Про електронні документи та електронний документообіг. Закон України від 22.05.2003 № 851-IV. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/851-15#Text>.

7. Про електронні комунікації. Закон України від 16.12.2020 № 1089-IX. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text>.

8. Про захист інформації в інформаційно-комунікаційних системах. Закон України від 05.07.2014 № 80/94-ВР. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>.

9. Про інформацію. Закон України від 02.10.1992 № 2657-XII. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.

10. Про Національну програму інформатизації. Закон України від 01.12.2022 № 2807-IX. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/2807-20#Text>.

Інформаційні ресурси

1. Державна служба спеціального зв'язку та захисту інформації України. URL: <https://cip.gov.ua/ua>.

2. Дія, цифрова освіта. Освітній курс «Електронний підпис». URL: <https://osvita.diia.gov.ua/courses/digital-signature>.

3. Дія, цифрова освіта. Освітній курс «Персональні дані». URL: <https://osvita.diia.gov.ua/courses/personaldata>.

4. Дія: Державні послуги онлайн. URL: <https://diia.gov.ua>.

5. Міністерство цифрової трансформації України. URL: <https://thedigital.gov.ua>.

6. Освітня платформа «МІА: Освіта». URL: <https://osvita.dnuvs.ukr.education/md/course/view.php?id=755>.