

Міністерство освіти і науки України
Національний університет водного господарства та
природокористування
Навчально–науковий інститут економіки та менеджменту
Кафедра менеджменту та публічного управління

07-06-155М

МЕТОДИЧНІ ВКАЗІВКИ

до виконання практичних завдань і самостійного вивчення
навчальної дисципліни «Цифровізація документообороту та
електронний офіс» для здобувачів вищої освіти першого
(бакалаврського) рівня за освітньо-професійною програмою
«Фінанси, банківська справа та страхування», спеціальності D2
«Фінанси, банківська справа, страхування та фондовий ринок»
денної та заочної форм навчання

Рекомендовано науково-
методичною радою з якості ННІ
економіки та менеджменту
Протокол № 1 від 24.09.2024 р.

Рівне – 2024

Методичні вказівки до виконання практичних завдань і самостійного вивчення навчальної дисципліни «Цифровізація документообороту та електронний офіс» для здобувачів вищої освіти першого (бакалаврського) рівня за освітньо-професійною програмою «Фінанси, банківська справа та страхування», спеціальності D2 «Фінанси, банківська справа, страхування та фондовий ринок» денної та заочної форм навчання [Електронне видання] / Маланчук Л. О. – Рівне : НУВГП, 2024. – 18 с.

Укладачі: Маланчук Л. О., к.е.н., доцент кафедри менедженту та публічного врядування.

Відповідальний за випуск: Тихончук Л. Х, д.держ.упр., професор, завідувач кафедри менедженту та публічного врядування.

Керівник групи забезпечення спеціальності:
Кондрацька Н. М., к.е.н., доцент кафедри фінансів та економічної безпеки.

© Л. О. Маланчук, 2024
© НУВГП, 2024

1. ЗАГАЛЬНІ ВКАЗІВКИ

1.1. Загальні рекомендації до вивчення дисципліни

Мета навчальної дисципліни «Цифровізація документообороту та електронний офіс»

Метою вивчення дисципліни є формування у студентів системних знань щодо сучасних підходів до організації електронного документообігу, управління інформаційними потоками та впровадження цифрових технологій в офісній діяльності, а також набуття практичних навичок роботи з електронними системами управління документами.

Завданням навчальної дисципліни є:

- опанування базових понять, термінів і категорій у сфері електронного документообігу та цифрової трансформації;
- засвоєння принципів організації електронного офісу та правил роботи з електронними документами;
- вивчення нормативно-правового забезпечення цифрового документообігу, включаючи використання електронного підпису, печатки та електронної ідентифікації;
- оволодіння методами безпечного збереження, архівації та передачі електронних документів;
- набуття практичних умінь роботи з сучасними платформами та програмними продуктами для електронного документообігу;
- розвиток здатності аналізувати та застосовувати інноваційні цифрові рішення для оптимізації управлінських процесів;
- формування навичок організації віддаленої командної роботи та управління електронним офісом в умовах цифрової економіки.

Після вивчення даної дисципліни здобувачі вищої освіти повинні отримати *компетентності*:

ЗК02. Здатність застосовувати знання у практичних ситуаціях.

ЗК05. Навички використання інформаційних та комунікаційних технологій.

ЗК08. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК12. Здатність працювати автономно.

СК06. Здатність застосовувати сучасне інформаційне та програмне забезпечення для отримання та обробки даних у сфері фінансів, банківської справи, страхування та фондового ринку.

СК09. Здатність здійснювати ефективні комунікації

У процесі викладання курсу передбачено формування таких *програмних результатів* навчання:

ПР08. Застосовувати спеціалізовані інформаційні системи, сучасні фінансові технології та програмні продукти.

ПР16. Застосовувати набуті теоретичні знання для розв'язання практичних завдань та змістовно інтерпретувати отримані результати.

ПР 25. Застосовувати сучасні методи управління для забезпечення ефективного функціонування економічних систем з дотриманням принципу неприпустимості корупції та недоброчесності.

1.2. Навчально-методичні матеріали дисципліни

Базова література:

1. Маланчук Л. О., Гонгадзе Я. В. Основи електронного документообігу та електронного урядування: навч. посібник. Рівне : НУВГП, 2025, 243 с.

2. Алексенцев А. І. Автоматизація діловодства. М. : ЗАТ Бізнес-школа «Інтел-синтез», 2004 р. 240 с.

3. Асеев Г. Управління сучасним документообігом: теорія, структура, методи. *Вісник Книжкової палати*, 2004. № 5. С. 32–36.

4. Матвієнко О., Цивін М. Основи організації електронного документообігу : навчальний посібник. К. : Центр навчальної літератури, 2008. 112с.

Допоміжна література:

1. Електронне урядування в публічному управлінні: словник основних термінів і понять . Львів : Растр-7, 2024. 128 с.

2. Електронне урядування : навч. посіб. / Семенченко А. І. та ін. ; за ред. А. І. Семенченка; Кабінет Міністрів України, Нац. ун-т

біоресурсів і природокористування України, Навч.-наук. ін-т післядиплом. освіти. Херсон : Грінь Д. С., 2014. 391 с.

3. . Ковбасюк Ю. В. Державне управління : підручник. Дніпропетровськ : НАДУ, 2013. 324 с.

4. Матвієнко О. В. Основи організації електронного документообігу : навч. посіб. К. : Центр учбової літератури, 2008. 112 с.

5. Семенченка А. І., Дрешпака В. М. Електронне урядування та електронна демократія : навчальний посібник. Частина 2. Київ : ФОП Москаленко О. М., 2017. 72 с.

6. Скібіцька Л. І. Діловодство : навч. посіб. для студ. ВНЗ 2–ге вид. Київ : Кондор, 2012. 219 с.

7. Тітенко Л. А. Діловодство з використанням комп'ютерної техніки : навч. посіб. Держ. вищ. навч. закл. «Київ. нац. екон. ун–т ім. Вадима Гетьмана». Київ : КНЕУ, 2014. 345 с.

8. Федусенко О. В., Доманецька І. М., Красовська Г. М. Проектування систем електронного документообігу : навч. посіб. для студ., які навч. за напрямом підгот. 6.050101 «Комп'ютерні науки». Київ. нац. ун–т буд–ва і архітектури. Київ : КНУБА, 2017. 287 с.

9. Чукут С. А., Загвойська О. В., Цимбаленко Я. Ю. Основи електронного урядування : навч. посібник. Електронне мережне навчальне видання. Київ : КПП ім. Ігоря Сікорського. 2022. 248 с.

1.3. Структура дисципліни

№	Назви змістових модулів і тем	Кількість годин							
		денна форма				заочна форма			
		усьо го	в т.ч.			усьо го	в т.ч.		
			л	пр	ср		л	пр	ср
Модуль 1									
Змістовий модуль 1.									
1	ВИЗНАЧЕННЯ ОСНОВНИХ ТЕРМІНІВ	14	4	2	8	12	1	-	11
2	ЕЛЕКТРОННИЙ ДОКУМЕНТ	12	2	2	8	12	1	-	11
3	ЕЛЕКТРОННИЙ	12	2	2	8	12	1	-	11

	ДОКУМЕНТООБІГ								
	Разом за змістовим модулем 1	38	8	6	24	36	3	-	33
Змістовий модуль 2									
4	ЕЛЕКТРОННЕ ВРЯДУВАННЯ	12	2	2	8	12	1	1	10
5	ЦИФРОВА ГРАМОТНІСТЬ	12	2	2	8	12	-	1	11
6	ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС	12	2	2	8	12	1	1	10
7	ДІЯ	12	2	2	8	12	-	1	11
	Разом за змістовим модулем 2	82	14	14	54	84	3	6	75
	Всього годин	120	2	20	78	120	6	6	108

2. ПЛАНИ ПРАКТИЧНИХ ЗАНЯТЬ ЗАВДАННЯ ДЛЯ ПРАКТИЧНИХ ЗАНЯТЬ

1. Створіть електронний документ у форматі PDF і підпишіть його за допомогою електронного підпису. Поясніть процес підписання та надайте зразок підписаного документа.

2. Дослідіть різні формати електронного підпису (XAdES, PAdES, CAdES) і створіть приклад підпису в кожному з них.

3. Ознайомтесь із платформою для петицій, що використовуються в Україні і створіть петицію щодо актуальної проблеми.

4. Зареєструйтесь в електронній системі документообігу або державних послуг (наприклад, у системі «Дія»), створіть профіль користувача та збережіть дані.

5. Створіть налаштування для введення в систему електронного документообігу (наприклад, налаштування прав доступу користувачів, створення шаблонів документів).

6. Порівняйте процеси обробки документа в традиційному паперовому вигляді та в електронній формі. Створіть таблицю з порівнянням плюсів і мінусів.

7. Використовуючи статистику, проаналізуйте рівень цифрової грамотності населення України. Оцініть необхідні навички для використання електронного врядування.

8. Напишіть електронне звернення через державний портал (наприклад, портал «Дія») і описати процес обробки такого звернення в системі електронного врядування.

9. Створіть модель електронного документообігу для умов малих організацій, враховуючи специфіку роботи з документами в електронному форматі.

10. Оцініть безпеку електронного документообігу в організації, досліджуючи існуючі вразливості в програмному забезпеченні.

11. Створіть план для розробки електронного архіву документів, враховуючи вимоги до безпеки та збереження даних.

12. Побудуйте схему процесу затвердження електронного документа (від його створення до підписання), вказуючи етапи та ролі користувачів.

13. Оцініть, як забезпечується захист персональних даних у системах електронного документообігу, і розробіть план заходів для підвищення безпеки.

14. Досліджуйте, як електронний документообіг може бути інтегрований із іншими інформаційними системами організації, такими як CRM, ERP тощо.

15. Створіть політику доступу для користувачів системи електронного документообігу в організації, включаючи різні рівні доступу до документів та їх обробки.

16. Ознайомтесь з актуальними законодавчими ініціативами щодо електронного документообігу в Україні (наприклад, закони про електронний підпис) та оцініть їх вплив на організації.

17. Проведіть тестування системи електронного документообігу в організації, оцініть її ефективність, швидкість обробки документів і надайте рекомендації для покращення.

18. Розробіть концепцію та алгоритм роботи електронного журналу для реєстрації вхідних та вихідних документів, а також для їх подальшої обробки.

19. Створіть детальний план впровадження електронного врядування в невеликій громадській організації, включаючи вибір програмного забезпечення, налаштування доступу, підготовку співробітників до роботи з новими технологіями.

20. Проведіть порівняльний аналіз популярних платформ для електронного документообігу оцініть їх переваги та недоліки для різних типів організацій.

21. Створіть реальний документ і застосуйте до нього електронний підпис, використовуючи систему електронного підпису. Поясніть, як цей процес підвищує довіру до електронного документа.

ПАКЕТ СИТУАЦІЙНИХ ВПРАВ

Ситуаційне завдання №1

Уявіть, що ви працюєте в департаменті ІТ компанії, яка впроваджує електронний документообіг. Ваша задача – допомогти керівництву вибрати та впровадити систему для організації електронного документообігу в компанії, яка відповідатиме вимогам сучасного інформаційного суспільства і забезпечить безпеку обміну інформацією.

Вибір системи повинен базуватися на таких критеріях:

- інтеграція з існуючими корпоративними системами;
- можливість автоматизації обробки документів;
- забезпечення конфіденційності та безпеки через електронні підписи та контроль доступу;
- легкість використання для співробітників і підвищення ефективності внутрішнього документообігу.

Ваше завдання – розробити рекомендації для керівництва компанії щодо вибору системи електронного документообігу та зазначити основні кроки для її впровадження.

Ситуативне завдання №2

Ваша компанія розпочала перехід до використання електронних документів для внутрішнього документообігу. Всі документи будуть створюватися, підписуватися та зберігатися в електронному форматі. Однак, перед впровадженням цієї системи потрібно забезпечити юридичну силу електронних документів і відповідність нормативним вимогам. Тому вам потрібно організувати процес створення, обробки та збереження електронних документів у компанії.

Запитання до завдання:

1. Яким чином ви забезпечите юридичну силу електронних документів у відповідності до вимог українського законодавства?
2. Які заходи слід вжити для збереження і архівації електронних документів?

3. Як ви будете використовувати електронний підпис для забезпечення автентичності та цілісності електронних документів?

4. Які законодавчі акти та нормативні документи слід врахувати при реалізації електронного документообігу?

Ситуаційне завдання №3

Ви працюєте в управлінні електронного документообігу великої державної установи. Нещодавно ваша організація вирішила перейти до повного впровадження електронного документообігу з використанням кваліфікованих електронних підписів (КЕП). Вашим завданням є організація процесу підписання важливих адміністративних актів і договорів, а також налаштування процедури автентифікації підписувачів.

Під час запуску проекту виявлено, що деякі працівники організації не володіють необхідними знаннями щодо роботи з електронними підписами та методами їх зберігання. Крім того, є зацікавлені сторони, які вимагають гарантії щодо безпеки та юридичної сили підписаних документів.

Завдання:

1. Проаналізуйте ситуацію з точки зору правової значимості електронного підпису. Які форми електронного підпису повинні використовуватись для різних видів документів в організації? Які критерії визначають вибір підпису (простий, удосконалений, кваліфікований)?

2. Розробіть план навчання для працівників організації щодо використання кваліфікованих електронних підписів (КЕП) та організації процесу автентифікації.

3. Яким чином організація може забезпечити безпеку зберігання електронних підписів та документів на різних етапах їхнього життєвого циклу?

4. Оцініть правові та практичні ризики, які можуть виникнути при використанні електронних підписів і як можна знизити ці ризики за допомогою законодавчих норм або технічних засобів.

5. Опишіть можливі наслідки для організації, якщо буде виявлено підробку електронного підпису або порушення цілісності електронного документа.

Додаткове завдання:

Підготуйте презентацію для керівництва організації, яка міститиме огляд всіх необхідних процедур для забезпечення ефективного та безпечного використання електронних підписів в установі.

Ситуаційне завдання №4

Ви працюєте в команді, яка відповідає за впровадження системи електронного документообігу (СЕД) у великій державній організації. Ваша організація має понад 1000 співробітників, і вже зараз зіштовхується з проблемами в управлінні великими обсягами документів, високими витратами на зберігання паперових документів та повільною обробкою даних. Більш того, документообіг часто відбувається вручну, що веде до неефективності та збоїв у роботі.

Ваша задача – вибрати та впровадити систему електронного документообігу, яка б оптимізувала робочі процеси, підвищила ефективність роботи співробітників, і водночас забезпечила б надійну безпеку та конфіденційність документів.

Завдання:

1. Аналіз і вибір системи:

- ознайомтесь з переліком систем електронного документообігу (Microsoft SharePoint, DOCS.UA, АСКОД, FossDoc, e-Docs, Megapolis.DocNet);

- визначте, яка з цих систем найкраще відповідає потребам вашої організації. Розгляньте різні аспекти, такі як інтеграція з іншими системами, безпека, зручність користування та можливості масштабування.

2. Опишіть, які методи безпеки будуть використовуватися для забезпечення конфіденційності та захисту інформації в новій системі (контроль доступу, шифрування даних, аутентифікація користувачів, аудит дій з документами).

3. Після впровадження системи, запропонуйте метрики для оцінки її ефективності. Як ви будете вимірювати покращення у роботі організації, скорочення часу на обробку документів, зниження кількості помилок чи витрат на зберігання документів?

Додаткове завдання:

Підготуйте презентацію для керівництва організації, в якій пояснить обрану систему, її переваги та етапи впровадження. Вкажіть, як нова система дозволить організації зекономити час і гроші та поліпшити взаємодію між співробітниками.

Ситуаційне завдання №5

Ви працюєте в команді, яка розробляє стратегію цифрової трансформації для однієї з державних установ України (наприклад, Міністерство охорони здоров'я, Пенсійний фонд України або Державна фіскальна служба). Ця організація стикається з проблемами, пов'язаними з повільним документообігом, великим обсягом паперової документації, високим рівнем адміністративних витрат та ризиками несанкціонованого доступу до конфіденційних даних.

Ваша задача – розробити концепцію впровадження технологій блокчейн та штучного інтелекту в процеси електронного документообігу у державному органі. Враховуючи виклики, з якими стикаються державні установи (повільний документообіг, безпека даних, бюрократія), вам потрібно:

1. Оцініть, як існуюча система електронного документообігу може бути покращена за допомогою нових технологій.
2. Поясніть, як блокчейн та AI можуть вирішити ці проблеми. Обґрунтуйте, яку з технологій доцільніше впроваджувати в першу чергу.
3. Як впровадження цих технологій змінить процеси в установі? Як це вплине на час обробки документів і рівень безпеки?

Ситуаційне завдання №6

Ви – консультант для державного органу, який намагається впровадити електронне врядування в своїй діяльності. Вашим завданням є розробити план для покращення комунікації та підвищення ефективності роботи органу через цифрові технології. Ви повинні вивчити переваги електронного урядування та запропонувати конкретні кроки для їх впровадження.

Завдання:

1. Оцініть існуючі проблеми в управлінні, які можна вирішити за допомогою електронного врядування (наприклад, складність доступу до послуг, корупційні ризики, затримки в процесах).

Як ці проблеми впливають на ефективність і довіру громадян до органу?

2. Ви повинні вибрати три ключові переваги електронного урядування (наприклад, прозорість і підзвітність, зручність для громадян, зменшення бюрократії) та обґрунтувати їх важливість для обраної установи.

Як ці переваги можуть покращити взаємодію з громадянами і підприємствами?

3. Окресліть етапи впровадження електронного урядування, починаючи з вивчення потреб і до впровадження першої електронної платформи для надання послуг.

Як ви плануєте залучити громадян до використання електронних послуг та забезпечити їхній доступ до цієї платформи?

Ситуаційне завдання №7

Ваш університет отримав грант на створення системи електронного врядування для одного з регіонів країни. Ваша команда відповідальна за розробку та впровадження цього проєкту, який включає:

- реєстрацію та управління заявами на отримання адміністративних послуг (податкова реєстрація, реєстрація бізнесу, отримання довідок);
- створення електронних платформ для участі громадян у державних процесах, таких як голосування на місцевих виборах, петиції та опитування;

– впровадження нових цифрових інструментів для зручного доступу до інформації та послуг.

Однак, під час тестування системи, виявлено серйозні уразливості, які можуть призвести до витоку персональних даних користувачів.

Завдання:

1. Як би ви описали основні загрози безпеці цієї електронної платформи? Визначте ключові уразливості системи, на які потрібно звернути увагу. Оцініть, якими можуть бути наслідки для державного управління та довіри громадян у разі таких порушень безпеки.

2. Як ви розробили б стратегію для забезпечення безпеки цієї системи? Які технічні рішення, такі як шифрування, багатофакторна аутентифікація або використання протоколів безпеки, ви б рекомендували впровадити? Які кроки ви б вжили для захисту персональних даних громадян, щоб уникнути витоків та атак?

3. Вивчіть приклади країн, які успішно запровадили систему електронного врядування. Які рішення вони застосували для захисту даних громадян і протидії кіберзагрозам?

Ситуаційне завдання №8

Вашій команді доручено створення стратегії для подальшого розвитку електронного врядування в Україні. Вам потрібно взаємодіяти з Міністерством цифрової трансформації для підготовки проекту з удосконалення цифрових сервісів для громадян та бізнесу. Одним із завдань є інтеграція послуг, таких як податкові та соціальні пільги, в єдину систему для зручності користувачів.

Завдання:

1. Опишіть, які послуги повинні бути включені до системи, щоб забезпечити зручність та доступність для громадян України. Як Міністерство цифрової трансформації може забезпечити надійний доступ до цих послуг?

2. Як можна заохотити громадян активно користуватися новими цифровими послугами? Які кроки повинно вжити Міністерство для того, щоб мінімізувати бар'єри у використанні цифрових платформ?

2.1. Вимоги до оформлення

ІНДЗ оформляють на стандартних аркушах паперу формату А 4 (210 x 297 мм).

Поля: ліве, верхнє, нижнє – 20 мм, праве – 10 мм, абзац – 10 мм.

Міжстроковий інтервал – 1,5. Нумерація аркушів, крім титульного, справа, зверху. Шрифт 14, Times New Roman. Обсяг роботи до 15 аркушів.

Список літератури – не менше 10 джерел.

2.2. Перелік тем ІНДЗ

Підвищення цифрової грамотності є ключовим аспектом для успішного функціонування електронного врядування. Ваша команда отримала завдання створити план підвищення цифрової грамотності серед певної групи населення (наприклад, пенсіонери, малозабезпечені верстви, сільське населення).

Завдання для студентів:

1. Опишіть особливості цільової групи. Які фактори впливають на низький рівень цифрової грамотності цієї групи? Як це може вплинути на доступ до електронних послуг?

2. Розробіть програму навчання, яка включає як теоретичну частину (пояснення основ цифрових технологій), так і практичну частину (навчання на реальних прикладах через онлайн–курси або майстер–класи).

3. Як можна залучити місцеві органи влади та бізнес до процесу підвищення цифрової грамотності населення? Розробіть рекомендації для взаємодії з партнерами.

Серії освітнього серіалу на платформі «Дія. Освіта» з
кібергігієни для молоді

Серія №	Назва серії	Опис	Тривалість
1	2	3	4
1.	Що таке кібергігієна?	Розповідь про реальні випадки зламу акаунтів відомих людей через недостатній захист. Основи кібергігієни.	3 хв

2.	Хто такі хакери?	Визначення хакерів, відмінність етичних хакерів від кіберзлочинців. Приклади атак, як це сталося з Київстаром.	3 хв
3.	Хто захищає нас від кіберзлочинців?	Огляд кіберзахисту в Україні, роль СБУ, Кіберполіції та Держспецзв'язку. Як реагувати на кіберінциденти.	4 хв
4.	Злам. Як діють кіберзлочинці	Методи зламу, включаючи технічні і соціальну інженерію, приклади атак, такі як DDoS на Telegram.	4 хв
5.	Безпека гаджетів	Як захистити свої гаджети від крадіжки або втрати, важливість паролів, шифрування, блокування.	3 хв
6.	Як софт забезпечує кібергігієну	Вплив програмного забезпечення на безпеку, важливість оновлення і використання перевірених додатків.	4 хв
7.	(Анти) Віруси	Різні види вірусів і їх вплив на пристрої. Як антивіруси допомагають захистити дані.	4 хв
8.	Зберігайся. Резервні копії	Важливість резервних копій, метод 3-2-1, автоматичне резервування та шифрування для захисту файлів.	4 хв
9.	Все про паролі	Як створювати надійні паролі, використання менеджерів паролів і загрози, пов'язані з простими паролями.	4 хв
10.	Подвійний захист	Як двофакторна аутентифікація забезпечує додатковий рівень захисту акаунтів. Різні види аутентифікації.	3 хв
11.	Безпека мережі	Захист від загроз в публічних Wi-Fi мережах, шифрування, використання VPN, налаштування DNS-серверів.	5 хв
12.	Фішинг: як хакери крадуть ваші дані	Різновиди фішингу та методи захисту від них: електронний, смс-фішинг, вебфішинг, дїпфейк-фішинг.	7 хв
13.	Захисти свій e-mail	Як захистити свою пошту від фішингових атак, використання резервних скриньок, плюс-адресація.	3 хв

14.	Не давай свій номер хакеру	Як захистити номер телефону від шахраїв, важливість PIN-коду для SIM-карти, заходи захисту.	3 хв
15.	Безпека банківських карток	Як захистити картки від шахраїв під час онлайн-покупок, важливість CVV-коду, використання 3-D Secure.	3 хв
16.	Контент під твоїм контролем	Як налаштувати приватність в інтернеті, контролювати геолокацію, захищати особисту інформацію.	5 хв
17.	FOMO – небезпека знати все	Як обирати надійні новинні джерела, перевіряти інформацію і уникати інформаційного перевантаження.	3 хв

Цей серіал допомагає молоді засвоїти основи кібербезпеки, навчаючи їх захищати свої персональні дані та уникати загроз в інтернеті. Навчання на освітньому серіалі «Кібергігієна для молоді» завершується фінальним тестом, який допомагає перевірити засвоєні знання та навички. Тест охоплює основні теми серіалів, дозволяючи учасникам оцінити рівень розуміння матеріалу та перевірити, як добре вони засвоїли правила кібербезпеки та захисту особистих даних. Після успішного проходження тесту учасники отримують сертифікат, який підтверджує їхню кваліфікацію в галузі кібергігієни.

Для отримання сертифікату необхідно виконати наступні кроки. Спочатку потрібно переглянути всі серії освітнього серіалу. Під кожною серією розміщено міні-тест, який слід пройти. По завершенню навчання буде доступне фінальне тестування. Для отримання сертифікату необхідно успішно пройти це тестування.

Отже, портал «Дія» став важливим інструментом для підвищення цифрової грамотності населення в Україні, забезпечуючи доступ до різноманітних освітніх ресурсів та сервісів, спрямованих на розвиток навичок користування цифровими технологіями. Через платформу «Дія. Освіта» громадяни можуть отримати знання у сферах кібербезпеки, цифрової грамотності, особистої безпеки в інтернеті та багатьох інших актуальних темах. Платформа також пропонує курси, що орієнтовані на конкретні професії, дозволяючи користувачам удосконалювати професійні

навички, покращувати кар’єрні перспективи та інтегруватися в цифровий простір.

Завдяки зручному формату навчання, що включає освітні серіали, тести та інтерактивні завдання, платформа дозволяє досягати високих результатів навіть тим, хто тільки починає свій шлях у світі цифрових технологій. Зокрема, серіали з кібергігієни є важливим етапом у боротьбі з кіберзлочинністю та шахрайством, допомагаючи молоді і дорослим краще розуміти загрози в інтернеті і як захистити свої дані.

У зв’язку з глобальними викликами цифровізації та швидкими змінами в інформаційних технологіях, платформа «Дія» є не лише інструментом для підвищення цифрової грамотності, а й важливим ресурсом для розвитку суспільства, що здатне ефективно взаємодіяти з новітніми технологіями та адаптуватися до умов цифрового світу. Вона робить освіту доступною для кожного громадянина, підтримуючи принципи інклюзивності та рівного доступу до знань.

2.3. Вимоги до оформлення

ІНДЗ оформляють на стандартних аркушах паперу формату А 4 (210 x 297 мм).

Поля: ліве, верхнє, нижнє – 20 мм, праве – 10 мм, абзац – 10 мм.

Міжстроковий інтервал – 1,5. Нумерація аркушів, крім титульного, справа, зверху. Шрифт 14, Times New Roman. Обсяг роботи до 15 аркушів.

Список літератури – не менше 10 джерел.

2.4. Оцінювання ІНДЗ

Контроль виконання ІНДЗ включає поточний контроль за виконанням та його захист. Оцінка виконання та захист ІНДЗ проводиться за 40 – бальною шкалою.

Теоретична частина	Презентація результатів ІНДЗ	Сума
15	15	30