**СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**
**«ІНФОРМАЦІЙНА БЕЗПЕКА В ЦИФРОВОМУ ВРЯДУВАННІ»**

| | |
|---|---|
| **Рівень освіти** | другий (магістерський) |
| **Спеціальність** | 281 Публічне управління та адміністрування |
| **Освітньо-професійна програма** | Публічне управління та адміністрування |
| **Тривалість викладання** | 4-та чверть |
| **Кількість кредитів** | 4 кредити ЄКТС (120 годин) |
| **Заняття:** | |
| лекції: | 2 години на тиждень |
| практичні: | 4 години на тиждень |
| **Мова викладання** | Українська |

**Сторінка курсу в СДО НТУ «ДП»:** https://do.nmu.org.ua/course/view.php?id=5366

**Кафедра, що викладає:** Державного управління і місцевого самоврядування (ДУМС)

**Викладач:**

**Кравцов Олег Валентинович**
к.х.н., доцент

**Персональна сторінка**
https://palsg.nmu.org.ua/ua/kafedra/teachers/Kravtsov/Kravtsov.php

**E-mail:** kravtsov.ol.v@nmu.one

## 1. Анотація до курсу

Сучасний стан розвитку інформаційного простору характеризується новими потребами у створенні умов для безпечного функціонування його суб'єктів, коли особливо важливими стають проблеми протидії інформаційним війнам та захист власного кіберпростору. В даний час для захисту цих ресурсів потрібна не просто розробка приватних механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів тощо). Головною метою будь-якої системи забезпечення інформаційної безпеки є створення умов функціонування органів публічного управління, запобігання загроз його безпеки, захист законних інтересів власників інформації від протиправних посягань, недопущення розкрадання фінансових засобів, розголошення, втрати, витоку, спотворення і знищення службової інформації, забезпечення в рамках виробничої діяльності всіх підрозділів. Під час вивчення цієї дисципліни Ви отримаєте необхідні знання щодо основних понять, сутності та завдань в сфері інформаційної безпеки і захисту інформації та відповідні вміння щодо побудови системи управління інформаційною безпекою.

## 2. Мета та завдання курсу

**Мета дисципліни** – формування у здобувачів вищої освіти комплексу теоретичних знань у сфері інформаційної безпеки, розвиток професійних компетентностей щодо забезпечення

належного рівня інформаційної безпеки та протидії кіберзагрозам в органах публічного управління в умовах цифрової трансформації суспільства та держави.

**Завдання курсу:**

- **знати і розуміти:** принципи інформаційної та кібербезпеки, структуру та основні вимоги нормативно-правових документів України у сфері інформаційної та кібербезпеки, основні загрози інформаційної безпеки, методи і критерії оцінки ефективності заходів по захисту інформації, правових, організаційних і технічних заходів щодо забезпечення захисту інформації, мети та етапів робіт щодо розбудови ІБ в умовах цифрової трансформації;
- **вміти:** виявляти і класифікувати загрози інформаційної безпеки, виявляти джерела, ризики і форми атак на інформацію, практично застосовувати настанови міжнародних та національних стандартів інформаційної та кібербезпеки, планувати заходи по захисту інформації, виходячи з відомих загроз і фінансових можливостей організації, розраховувати ефективність заходів по захисту інформації, розробляти практичні рекомендації щодо реалізації системи управління інформаційною безпекою.

## 3. Результати навчання

Дисциплінарні результати навчання:

- продемонструвати знання: предмету і завдань дисципліни; термінології; основних понять та принципів в сфері інформаційної безпеки;
- продемонструвати розуміння: головних характеристик інформації як об’єкту захисту; правових, організаційних і технічних заходів щодо захисту інформації; проблематики і специфіки загроз ІБ;
- продемонструвати розуміння: системного підходу до опису ІБ, мети та етапів робіт щодо розбудови ІБ в умовах цифрової трансформації;
- продемонструвати вміння аналізувати та оцінювати інформаційні ризики;
- продемонструвати здатність практично застосовувати настанови міжнародних та національних стандартів інформаційної та кібербезпеки;
- продемонструвати здатність розробляти практичні рекомендації щодо реалізації системи управління інформаційною безпекою;
- продемонструвати практичні навички щодо розроблення політик безпеки;
- продемонструвати знання: предмету і завдань дисципліни; термінології; основних понять та принципів в сфері інформаційної безпеки.

## 4. Структура курсу

| Тижні | Тематика занять | Вид занять | Ресурси | Оцінка |
|---|---|---|---|---|
| 1 | Вступ до курсу<br>Мета, завдання, результати<br>Політика курсу<br>Навчальні матеріали<br>Система та критерії оцінювання | Лекція | Силабус<br>Презентація курсу<br>Методичні рекомендації<br>Рекомендовані джерела<br>ККР для проведення заліку | – |
| | Тема 1**. Загальні основи інформаційної безпеки**. | | Презентація за темою<br>Рекомендовані джерела | 0-2 |
| | Практичне заняття «Опис системи. Ідентифікація загроз». | Практичне заняття | Методичні рекомендації | - |

| Тижні | Тематика занять | Вид занять | Ресурси | Оцінка |
|---|---|---|---|---|
| 2 | Тема 1. **Загальні основи інформаційної безпеки**. | Лекція | Презентація за темою<br>Рекомендовані джерела | 0-2 |
| | Практичне заняття «Опис системи. Ідентифікація загроз». | Практичне заняття | Методичні рекомендації | - |
| 3 | Тема 2. **Характеристика інформаційної безпеки.** | Лекція | Презентація за темою<br>Рекомендовані джерела | 0-2 |
| | Практичне заняття «Опис системи. Ідентифікація загроз». | Практичне заняття | Методичні рекомендації | 0-10 |
| 4 | Тема 2**. Характеристика інформаційної безпеки.** | Лекція | Презентація за темою<br>Рекомендовані джерела | 0-2 |
| | Практичне заняття «Ідентифікація вразливостей. Визначення вірогідності реалізації вразливостей». | Практичне заняття | Методичні рекомендації | - |
| 5 | Тема 3. **Стандарти інформаційної безпеки.** | Лекція | Презентація за темою<br>Рекомендовані джерела | 0-2 |
| | Практичне заняття «Ідентифікація вразливостей. Визначення вірогідності реалізації вразливостей». | Практичне заняття | Методичні рекомендації | 0-10 |
| 6 | Тема 3. **Стандарти інформаційної безпеки.** | Лекція | Презентація за темою<br>Рекомендовані джерела | 0-2 |
| | Практичне заняття «Аналіз дій. Розрахунок ризику». | Практичне заняття | Методичні рекомендації | - |
| 7 | Тема 4. **Забезпечення систем захисту інформації** | Лекція | Презентація за темою<br>Рекомендовані джерела | 0-2 |
| | Практичне заняття «Аналіз дій. Розрахунок ризику». | Практичне заняття | Методичні рекомендації | 0-10 |
| 8 | Тема 4. **Забезпечення систем захисту інформації** | Лекція | Презентація за темою<br>Рекомендовані джерела | 0-2 |
| | Практичне заняття «Рекомендації з управління ризиками. Розробка політик інформаційної безпеки». | Практичне заняття | Методичні рекомендації | - |
| 9 | Тема 5. **Управління інформаційною безпекою** | Лекція | Презентація за темою<br>Рекомендовані джерела | 0-2 |
| | Практичне заняття «Рекомендації з управління ризиками. Розробка політик інформаційної безпеки». | Практичне заняття | Презентації здобувачів | 0-10 |
| 10 | Тема 5. **Управління інформаційною безпекою** | Лекція | Презентація за темою<br>Рекомендовані джерела | 0-2- |
| | Презентація результатів виконання командного / індивідуального завдання щодо розробки програми розвитку закладу охорони здоров’я»<br>Підведення підсумків вивчення дисципліни | Практичне заняття | Методичні рекомендації<br>Силабус<br>ККР для проведення заліку | 0-40 |

Командне / індивідуальне завдання «**Розроблення програми розвитку системи управління інформаційною та кібербезпекою»** полягає у розробленні, презентації результатів та захисті

здобувачами вищої освіти концепції програми розвитку закладу охорони здоров'я. (***Мета*** індивідуального завдання **–** розвинути здатність практично застосовувати відповідні методи та інструменти управління у сфері розроблення системи управління інформаційною та кібербезпекою). Вітається робота в команді.

***Форма проведення:*** розроблення, презентація та захист (відповіді на запитання, дискусія) командного / індивідуального завдання перед аудиторією (бажано використовувати MS PowerPoint).

***Зміст індивідуального завдання:*** На прикладі окремої організації, пов'язаної з вашим життям та / або професійною діяльністю, розробити концепцію політики інформаційної безпеки, результатом реалізації якої буде позитивний ефект для певної території / галузі / громади.

Для представлення результатів виконання завдання необхідно заповнити відповідний шаблон, який розміщено у застосунку Teams MS Office та на дистанційній платформі Moodle.

## 5. Технічне обладнання та/або програмне забезпечення

Комп'ютерне та мультимедійне обладнання.
Активований корпоративний акаунт НТУ «ДП» (student.i.p@nmu.one).
Microsoft Office 365. Застосунки Microsoft Office: Teams, Forms, Whiteboard, OneNote.
Платформа дистанційного навчання НТУ «ДП» Moodle.
Підключення до Internet.

## 6. Система оцінювання та вимоги

**6.1. Навчальні досягнення здобувачів вищої освіти** за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

| Рейтингова шкала | Інституційна шкала |
|---|---|
| 90 – 100 | відмінно |
| 74-89 | добре |
| 60-73 | задовільно |
| 0-59 | Незадовільно |

Загальні критерії досягнення результатів навчання відповідають описам 7-го кваліфікаційного рівня НРК.

**6.2**. Здобувачі вищої освіти можуть отримати **підсумкову оцінку** з навчальної дисципліни **на підставі поточного оцінювання знань** за умови, якщо набрана кількість балів з поточного тестування та виконання і захисту практичних робіт складатиме не менше 60 балів. Максимально за поточною успішністю здобувач вищої освіти може набрати 100 балів.

**Теоретична частина** оцінюється за результатами *участі у дискусіях* під час інтерактивних лекцій, виконанню та *презентації результатів індивідуального завдання*, зміст якого описано у розділі 4 (участь у дискусіях та презентація результатів окремих завдань оцінюється в межах 100 балів відповідно до Загальних критеріїв досягнення результатів навчання для 7-го кваліфікаційного рівня за НРК (магістр)» (див. «Положення про оцінювання результатів навчання здобувачів вищої освіти Національного технічного університету «Дніпровська політехніка» https://cutt.ly/1ORACPD) із подальшим перерахунком відповідно до розподілу балів за окремими темами та завданнями, див. у табл. розділу 4). Загалом за участь у дискусіях і захист результатів виконання індивідуального завдання отримується **максимум 60 балів**.

**Практичні роботи** (індивідуальні і командні завдання, розподіл балів див. у табл. розділу 4) виконуються під час практичних занять (презентація результатів окремих завдань оцінюється в межах 100 балів відповідно до Загальних критеріїв досягнення результатів навчання для 7-го кваліфікаційного рівня за НРК (магістр)» (див. «Положення про оцінювання результатів

навчання здобувачів вищої освіти Національного технічного університету «Дніпровська політехніка» https://cutt.ly/1ORACPD) із подальшим перерахунком відповідно до розподілу балів за окремими темами та завданнями, див. у табл. розділу 4). При несвоєчасному здаванні практичної роботи оцінка знижується вдвічі. У сумі за практичну частину курсу при поточному оцінюванні отримується **максимум 40 балів**.

Отримані бали за теоретичну частину та практичні роботи додаються і є підсумковою оцінкою за вивчення навчальної дисципліни. Максимально за поточною успішністю здобувач вищої освіти може набрати 100 балів.

Розподіл максимальної кількості балів за складовими поточного контролю:

| Теоретична частина | Практична частина | **Разом** |
|---|---|---|
| 60 | 40 | **100** |

**6.3. Критерії оцінювання підсумкової роботи.** У випадку якщо здобувач вищої освіти за поточною успішністю отримав менше 60 балів та/або прагне поліпшити оцінку проводиться **підсумкове оцінювання (залік)** під час сесії. Якщо здобувач не здав у письмовій формі виконаних індивідуальних завдань (дві практичні роботи), він отримує незадовільну підсумкову оцінку з дисципліни.

**Залік** проводиться у вигляді комплексної контрольної роботи, яка включає запитання з теоретичної та практичної частини курсу. Білет складається з **60 тестових завдань і**з чотирма варіантами відповідей, одна правильна відповідь оцінюється в 1 бал **(разом 60 балів)** та **10 тестових завдань** з практичної частини, кожне з запитань оцінюється максимум у 4 бали **(разом 40 балів**), причому:

- 4 бали – відповідність еталону;
- 3 бали – відповідність еталону з незначними помилками;
- 2 бали – часткова відповідність еталону, питання повністю не розкрите;
- 1 бал – невідповідність еталону, але відповідність темі запитання;
- 0 балів – відповідь не наведена або не відноситься до теми запитання.

Отримані бали за відкриті та закриті тести додаються і є підсумковою оцінкою за вивчення навчальної дисципліни. Максимально за підсумковою роботою здобувач вищої освіти може набрати 100 балів.

## 7. Політика курсу

**7.1. Політика щодо академічної доброчесності.** Академічна доброчесність здобувачів вищої освіти є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів) що можуть використовуватися в освітньому процесі. Політика щодо академічної доброчесності регламентується положенням «Положення про систему запобігання та виявлення плагіату у Національному технічному університеті «Дніпровська політехніка»: http://www.nmu.org.ua/ua/content/activity/us_documents/System_of_prevention_and_detection_of_plagiarism.pdf.

У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

**7.2. Комунікаційна політика.**

Здобувачі вищої освіти повинні мати активовану університетську пошту.

Обов’язком здобувача вищої освіти є перевірка один раз на тиждень (щонеділі) поштової скриньки на НТУ Microsoft Office та відвідування групи дисципліни у Microsoft Teams.

Рекомендуємо створити профілі та підписатися на сторінку кафедри державного управління і місцевого самоврядування у Facebook: https://www.facebook.com/kafedra.publicmanagement/.

Протягом тижнів самостійної роботи обов’язком здобувача вищої освіти є робота у рамках дисципліни дистанційно у застосунку Microsoft Teams та на корпоративній платформі Moodle (www.do.nmu.org.ua ).

Усі письмові запитання до викладача стосовно дисципліни мають надсилатися на університетську електронну пошту або до групи у Microsoft Teams.

**7.3. Політика щодо перескладання.**

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

**7.4. Відвідування занять.**

З 24.02.2022 реалізація освітньої діяльності відбувається в умовах правового режиму воєнного стану. Наявна низка небезпек: повітряні тривоги, ризики припинення енергозабезпечення, мобільного та Інтернет-зв'язку. Згідно з наказами по університету у 2024-2025 навчальному році освітня діяльність здобувачів другого (магістерського) рівня вищої освіти всіх форм навчання здійснюється з використанням дистанційних технологій через синхронні та асинхронні комунікації.

Відвідування онлайн лекцій та практичних занять реалізується через приєднання до «наради» в «команді» Microsoft Teams. Під час повітряної тривоги заняття перериваються і продовжуються лише за умов перебування учасників освітнього процесу у захищених приміщеннях. Викладачем (за технічної та безпекової можливості) здійснюється запис заняття для підтримки асинхронного формату навчання.

У випадках відсутності енергозабезпечення, мобільного та Інтернет-зв'язку викладачем забезпечується асинхронний формат навчання та комунікація зі здобувачами за допомогою каналів зв’язку, що функціонують.

Про причини неможливості взяти участь в онлайн заняттях, ускладненні доступу до матеріалів на дистанційних платформах НТУ «ДП» тощо здобувач вищої освіти має повідомити викладача в особистих повідомленнях чатів Microsoft Teams, або листом на корпоративну е-пошту НТУ «ДП», або через старосту чи представника адміністрації інституту.**7.5. Політика щодо оскарження оцінювання**. Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може оскаржити виставлену викладачем оцінку у встановленому порядку.

**7.6. Зарахування результатів навчання, які отримані у неформальній освіті.** Здобувачі вищої освіти має право на зарахування результатів навчання, які отримані у неформальній освіті, за окремими темами або видами навчальної активності із попереднім погодженням з викладачем дисципліни та гарантом освітньої програми. Визнання результатів здійснюється за наявності відповідних сертифікатів.

**7.7. Участь в анкетуванні.** Наприкінці вивчення курсу та перед початком сесії здобувачам вищої освіти буде запропоновано анонімно заповнити електронні анкети (MS Forms). Посилання на форму буде розміщено у Teams курсу. Заповнення анкет є важливою складовою вашої навчальної активності, що дозволить оцінити дієвість застосованих методів викладання та врахувати ваші пропозиції стосовно покращення змісту навчальної дисципліни.

## 8. Рекомендовані джерела інформації

### Основні

1. Захист інформації в публічному управлінні та адмініструванні : конспект лекцій / уклад. О.В. Кравцов. Дніпро : ДРІДУ НАДУ, 2019. 62 с. 1 електрон. опт. диск (CD-ROM).

2. Методичні вказівки до виконання практичних завдань з дисципліни «Захист інформації в публічному управлінні та адмініструванні». Створення системи менеджменту інформаційної безпеки / уклад. О.В. Кравцов. Дніпро : ДРІДУ НАДУ, 2019. 28 с. 1 електрон. опт. диск (CD-ROM).

### Нормативні документи

1. Конституція України : прийнята на п'ятій сесії Верховної Ради України 28.06.1996 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

2. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.

3. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.

4. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

5. Про державну таємницю : Закон України від 21.01.1994 р. № 3855-XII URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text.

6. Про електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

7. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

8. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 14.05.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

9. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 15.10.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

10. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text.

11. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. № 423.

12. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. Затверджено наказом Держстандарту України від 19.12.96 р. № 511.

13. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р. № 200.

14. ДСТУ ISO/IEC 27000:2017 Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Огляд і словник термінів (ISO/IEC 27000:2016, IDT).

15. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

16. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).

17. ДСТУ ISO/IEC 27003:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова (ISO/IEC 27003:2017, IDT).

18. ДСТУ ISO/IEC 27004:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання (ISO/IEC 27004:2016, IDT)

19. ДСТУ ISO/IEC 27005:2015 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT).

**Додаткові**

1. Азарова А. О., Ткачук Л. М., Нікіфорова Л. О. та ін. Публічне управління та адміністрування в контексті захисту його інформаційного простору. *Вісник ЖДТУ. Серія «Економіка, управління та адміністрування».* 2019. № 2. С. 149–155.

2. Антонюк А.О. Основи захисту інформації в автоматизованих системах : навч. посіб. Київ: КМ Академія, 2003. 244 с.

3. Герасимюк К. Х. Механізми державного управління кібер- та інформаційною безпекою: проблеми та шляхи вирішення. *Економіка, управління та адміністрування*. 2021, № 3 (97), С. 36–40. URL: https://doi.org/10.26642/ema-2021-3(97)-36-40.

4. Домарев В. В. Безопасность информационных технологий. Системный подход. Київ: ТИД ДС, 2004. 992 с.

5. Дорошев В. В., Домарев В. В. Рекомендации по обеспечению безопасности конфиденциальной информации согласно «Критериев оценки надежных компьютерных систем TCSEC (Trusted Computer Systems Evaluation Criteria)». *«Оранжевая книга». Бизнес и безопасность*, 1998, № 1, США, С. 19–21.

6. Дячек О., Рябченко К., Доценко, А. Безпека даних в інформаційно-комунікаційному середовищі та її складність для нових бізнес-моделей. *Економіка та суспільство*. 2022, 38. URL: https://doi.org/10.32782/2524-0072/2022-38-16.

7. Защита информации и безопасность компьютерных систем/ В.В. Домарёв. Київ: Диа Софт», 1999. 480 с.

8. Інформаційна безпека держави : підручник / В. М. Петрик, М. М. Присяжнюк, Д. С. Мельник та ін.; в 2 т. Т.1. / за заг. ред.. В. В. Остроухова. Київ : ДНУ «Книжкова палата Україна», 2016. 264 с.

9. Марущак А., Скіцько О. Вплив тіньових інформаційних технологій на інформаційну безпеку суб'єкта господарювання. *Безпека інформації*. 2018. Т. 24, № 1. С. 69–74.

10. Науменко Н. Ю., Дубницький В. І. Методологічне забезпечення формування інформаційної безпеки в сфері економічної безпеки регіону. *Вісник економічної науки України*. 2019. № 1 (36). С. 35–39.

11. Публічне управління та адміністрування в умовах інформаційного суспільства: вітчизняний і зарубіжний досвід : монографія / ред. С. Чернов, В. Воронкова, В. Банах, та ін. ; ЗДІА. Запоріжжя : ЗДІА, 2017. 603 с.

12. Савченко О. С. Проблеми запровадження цифровізації у систему публічного управління. *Таврійський науковий вісник. Серія: Публічне управління та адміністрування*. 2022, № 3, 102–108. URL: https://doi.org/ 10.32851/tnv-pub.2022.3.14.

13. Термінологічний словник з питань технічного захисту інформації / за ред. В. О. Хорошка ; 3-тє вид. Київ : Поліграф Колсалтинг, 2003. 268 с.

14. Хох В. Д., Мелешко Є. В., Смірнов О. А. Дослідження методів аудиту систем управління інформаційною. *Системи управління, навігації та зв'язку : зб. наук. пр.* Полтава : ПНТУ, 2017. Т 1 (41). С. 38–42.

**Інформаційні ресурси**

1. CERT-UA. Команда реагування на комп’ютерні надзвичайні події України. URL: https://cert.gov.ua
2. Державна служба спеціального зв’язку та захисту інформації України. URL: http://www.dsszzi.gov.ua
3. ТОВ «ТЗІ». URL: http://tzi.com.ua
4. Всеукраїнська асоціація «Інформаційна безпека та інформаційні технології».

URL: https://vaibit.org.ua
5. Інфобезпека. URL: http://www.infobezpeka.com
6. ЕПОС. URL: http://www.epos.ua
7. Міністерство цифрової трансформації України. Центральний засвідчувальний орган. URL: http://czo.gov.ua
8. ISO/IEC 27001. URL: https://www.iso27001security.com