



## МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

# НАКАЗ

19 10 20 18 р.

м. Київ

№ 1140

Деякі питання Національного  
репозитарію академічних текстів

З метою забезпечення реалізації розпорядження Кабінету Міністрів України від 22 липня 2016 року № 504-р «Про створення Національного репозитарію академічних текстів», постанови Кабінету Міністрів України від 19 липня 2017 року № 541 «Положення про Національний репозитарій академічних текстів», наказів Міністерства освіти і науки України від 07.12.2016 № 1466 «Про затвердження плану заходів щодо створення та введення в експлуатацію Національного репозитарію академічних текстів», від 25.10.2017 № 1421 «Про розпорядника Національного репозитарію академічних текстів», від 04.07.2018 № 707 «Про затвердження Регламенту роботи Національного репозитарію академічних текстів», зареєстрованим в Міністерстві юстиції України 23 липня 2018 р. за № 858/32310, з урахуванням Порядку формування тематики наукових досліджень і науково-технічних (експериментальних) розробок, що фінансуються за рахунок коштів державного бюджету (далі – Порядок), затвердженого постановою Кабінету Міністрів України від 11 січня 2018 року № 13,

НАКАЗУЮ:

1. Затвердити як рекомендаційні Примірні технічні характеристики Національного репозитарію академічних текстів, що додаються.

2. Державній науковій установі «Український інститут науково-технічної експертизи та інформації» (Камишин В. В.):

забезпечити розроблення, затвердження та погодження з МОН Технічного завдання на виконання науково-дослідної роботи «Створення та забезпечення функціонування тестової експлуатації першої черги Національного репозитарію академічних текстів» з урахуванням пункту 9 Порядку та Примірних технічних характеристик Національного репозитарію академічних текстів, затверджених пунктом 1 цього наказу;

внести зміну до пункту 2 тематичного плану наукових досліджень та розробок, які виконує Державна наукова установа «Український інститут науково-технічної експертизи та інформації» за рахунок коштів державного бюджету у 2018 році, шляхом приведення назви науково-дослідної роботи до редакції, визначеної абзацом другим пункту 2 цього наказу, та подати тематичний план до департаменту науково-технічного розвитку (Хименко О. А.) на погодження.

3. Контроль за виконанням цього наказу покласти на заступника Міністра Стріху М. В.

Міністр



Л. М. Гриневич

ЗАТВЕРДЖЕНО

Наказ Міністерства освіти і  
науки України

від 19.10.2018 № 1140

## **ПРИМІРНІ ТЕХНІЧНІ ХАРАКТЕРИСТИКИ Національного репозитарію академічних текстів**

### **Загальна частина**

1. Примірні технічні характеристики Національного репозитарію академічних текстів встановлюють рекомендаційні вимоги, на основі яких розпорядник Національного репозитарію здійснює створення та забезпечення тестової експлуатації та функціонування Національного репозитарію академічних текстів (далі – Вимоги) як визначеної послідовності черг та модулів.

Терміни у цих Вимогах вживаються у значенні наведеному у Положенні про Національний репозитарій академічних текстів (далі – Положення), затвердженому постановою Кабінету Міністрів України від 19 липня 2017 р. № 541, та Регламенті роботи Національного репозитарію академічних текстів (далі – Регламент), затвердженому наказом Міністерства освіти і науки України від 04.07.2018 № 707, зареєстрованим в Міністерстві юстиції України 23 липня 2018 р. за № 858/32310.

2. Національний репозитарій як загальнодержавна розподілена електронна база даних, в якій накопичуються, зберігаються і систематизуються академічні тексти, повинен забезпечувати:

можливість отримання від інституціональних учасників бібліографічних відомостей, описів академічних текстів та інших пов'язаних з ними даних (включаючи анотації та списки літератури, що містяться в академічних текстах, з прив'язкою до основного тексту), представлених у центральному та локальних репозитаріях, а також оприлюднених в електронній або паперовій формі;

можливість розміщення інституціональними учасниками на безоплатній основі академічних текстів;

можливість розміщення публікацій, розташованих на Інтернет-платформах та інформаційної інтеграції з іншими базами даних, як це передбачено Положенням;

авторизацію та автентифікацію користувачів;

безоплатний і вільний доступ через мережу Інтернет з будь-якого місця у будь-який час без будь-яких обмежень за рівнем освіти, фахом, спеціалізацією тощо відвідувачів та користувачів Національного репозитарію до інформації,

що міститься в Національному репозитарії, відповідно до обсягів прав, зазначених у розділі IV Регламенту.

Хронологічні обмеження для академічних текстів та інших пов'язаних з ними даних, що зберігаються у Національному репозитарії, не встановлюються. До Національного репозитарію включаються академічні тексти незалежно від дати їх створення та оприлюднення.

3. Офіційний веб-портал Національного репозитарію має доменне ім'я «nrat.gov.ua».

4. Технічні вимоги щодо формату представлення академічних текстів, які включаються до Національного репозитарію, та їх верифікації відповідно до пункту 4 розділу III Регламенту визначаються Розпорядником.

5. Національний репозитарій є Комплексною системою з отримання, оброблення, збереження інформації та надання її для ознайомлення на вимогу користувача (далі – Система).

6. Система має бути побудована за ієрархічно-модульним принципом з описом призначення і функціональної поведінки кожної підсистеми та кожного її модуля, з можливістю розширення її функціональних складових та перманентного контролю цілісності. Структурна взаємодія підсистем та модулів системи має бути орієнтована на вертикально-ієрархічні зв'язки, не допускаючи горизонтальних.

Інформаційна взаємодія між функціональними підсистемами має бути адаптивною та підтримувати розподілену між апаратними одиницями роботу. Взаємодія підсистем має здійснюватися через адаптивний функціонал передачі інформації (процедурний, загальна пам'ять, системні сокети, мережевий зв'язок).

Центральний банк даних Системи має бути апаратно відокремленим від функціоналу головної системи. В Системі для зберігання інформації має бути передбачено формування кластерного середовища та визначені засоби взаємодії з центральним банком даних.

7. Система має забезпечувати можливості:

надійного збереження інформації – реєстру академічних текстів, їх електронних версій та інших пов'язаних з ними даних, розміщених у Національному репозитарії;

комплексного аналізу запитів користувачів щодо академічних текстів за тематикою, авторством, належністю до закладу вищої освіти та наукових установ, впровадженням, міжнародною співпрацею тощо;

комплексного оцінювання використання академічних текстів (у тому числі використання у дисертаціях на здобуття наукових ступенів та кваліфікаційних випускних роботах здобувачів вищої освіти) щодо читання, скачування, цитування, врахування рекомендацій користувачів, зокрема за

видами, тематикою, категоріями, у розрізі окремих академічних текстів чи їх сукупності, у прив'язці до авторів, наукових установ, закладів вищої освіти тощо, результати якого можуть використовуватись МОН, іншими заінтересованими суб'єктами під час оцінювання діяльності закладів вищої освіти, наукових установ, бібліотек, наукових видавництв, організацій;

побудови наукометричної бази даних;

аналізу цитованості академічних текстів;

системного аналізу наукового простору та моніторингу його трансформації;

перевірки академічних текстів на наявність збігів текстових (літерних і цифрових символів) та графічних фрагментів;

складання рейтингів, що характеризують стан і динаміку розвитку наукової, освітньої, інноваційної діяльності в Україні та відповідної інфраструктури;

відстеження на вимогу авторів або правовласників академічних текстів нових надходжень до Національного репозитарію на наявність збігів текстових (літерних і цифрових символів) та графічних фрагментів;

доступу до ресурсів Національного репозитарію, зокрема до реєстру академічних текстів та їх електронних версій, спеціальних програмних комплексів (роботів) з метою індексації та аналізу метаданих цих текстів й поширення відповідної інформації (з урахуванням обмежень, визначених пунктом 5 розділу IV Регламенту) із обов'язковим посиланням на її джерело – офіційний веб-портал Національного репозитарію.

8. Система створюється та вводиться в експлуатацію по чергово:

першу чергу складають роботи зі створення моделі програмно-апаратного комплексу центрального репозитарію;

другу чергу складають організаційно-методичні роботи та заходи зі створення програмно-технічних умов для підключення локальних репозитаріїв інституціональних учасників та користувачів;

третю чергу складають організаційно-методичні роботи та заходи зі створення програмних умов для побудови комплексної аналітичної підсистеми Національного репозитарію та удосконалення інструментів роботи з локальними репозитаріями та користувачами.

Виконання кожної черги передбачає здійснення повного комплексу робіт зі створення, тестової, дослідної та промислової експлуатації Системи.

Обсяг і зміст робіт кожної черги визначається Розпорядником Національного репозитарію за погодженням із МОН.

### **Особливості об'єкта автоматизації Національного репозитарію**

9. Об'єктом автоматизації Національного репозитарію є сукупність процесів проектування, розробки та функціонування Національного репозитарію академічних текстів як універсальної за змістом

загальнодержавної електронної бази даних, де накопичуються, зберігаються, систематизуються, піддаються комплексному аналізу вітчизняні академічні тексти (наукового, науково-технічного та освітнього характеру) і до якої забезпечується безперешкодний віддалений доступ відвідувачів, користувачів та інституціональних учасників (далі – Об'єкт автоматизації).

10. Об'єкт автоматизації має містити підсистему центрального репозитарію, що підтримується Розпорядником Національного репозитарію, та підсистеми локальних репозитаріїв, що підтримуються інституціональними учасниками Національного репозитарію.

11. Реєстр академічних текстів як частина Національного репозитарію розміщується в підсистемі центрального репозитарію, формується і підтримується Розпорядником.

Реєстр академічних текстів є відкритим та містить бібліографічні відомості про академічні тексти, що включені до центрального та локальних репозитаріїв, а також оприлюднені в електронній або паперовій формі.

12. Підсистема локального репозитарію є самостійною інформаційною структурною одиницею об'єкта автоматизації, яка в кожному окремому випадку реалізується інституціональним учасником Національного репозитарію самостійно, з урахуванням вимог до вмісту (визначених Положенням та Регламентом), інформаційної безпеки та ефективної взаємодії з центральним репозитарієм.

13. Підсистема локального репозитарію повинна забезпечувати обмін даними з підсистемою центрального репозитарію щодо бібліографічних відомостей, передбачених законодавством, описів академічних текстів, включаючи анотації та списки літератури, що містяться в академічних текстах, з прив'язкою до основного тексту, згідно переліку, що визначається Розпорядником.

14. Підсистема центрального репозитарію повинна забезпечувати прийом і обробку даних, що надходять від підсистем локальних репозитаріїв, з метою систематизації та формування реєстру академічних текстів, їх електронних версій та інших пов'язаних з ними даних, розміщених у Національному репозитарії, реалізації можливостей пошуку інформації в Національному репозитарію, проведення аналітичної роботи.

15. Об'єкт автоматизації щодо академічного тексту повинен забезпечувати можливість:

систематизації академічних текстів на основі бібліографічних відомостей та описів, передбачених законодавством;

фіксації дати введення академічного тексту до Національного репозитарію та відомостей про джерело інформації академічного тексту;

зміни змісту академічного тексту шляхом доповнення додатковою інформацією (відомостями щодо виявлених друкарських помилок, неточностей, заявами та роз'ясненнями методичного характеру, базами даних досліджень тощо);

відкликання академічного тексту з Національного репозитарію;

обмеження доступу до електронної версії академічного тексту або їх частини на постійній або тимчасовій основі відповідно до чинного законодавства щодо авторських прав на вимогу видавців та (або) правовласників академічного тексту;

використання електронних версій академічних текстів або їх частин, доступ до яких обмежено в установленому порядку, виключно Розпорядником в аналітичних цілях та у спосіб відповідно до Закону України «Про авторське право і суміжні права»;

структурування академічних тестів за видами, як це передбачено Положенням:

- дисертації на здобуття наукових ступенів та автореферати дисертацій;
- кваліфікаційні випускні роботи здобувачів вищої освіти;
- статті у наукових виданнях, у тому числі всі статті (сукупність статей), на підставі захисту яких присуджено науковий ступінь;
- монографії, у тому числі ті, на підставі захисту яких присуджено науковий ступінь;
- наукові видання;
- звіти у сфері наукової і науково-технічної діяльності;
- депоновані наукові роботи;
- підручники, навчальні посібники та інші науково- та навчально-методичні праці;

структурування академічних тестів за ознаками: авторства, афіліації авторів, мови публікації, року публікації, ключових слів, галузей знань, УДК тощо;

авторизації та автентифікації користувачів;

безоплатного і вільного доступу: відвідувачів – до реєстру академічних текстів; користувачів – до інформації, що в ньому міститься, включаючи реєстр академічних текстів, їх електронні версії та інші пов'язані з ними дані, через офіційний веб-портал Національного репозитарію;

інформаційної інтеграції з іншими базами даних, зокрема ресурсами відкритих даних України та інших держав, базами центральних органів виконавчої влади.

16. Розпорядник Національного репозитарію забезпечує:

функціонування Національного репозитарію;

накопичення, збереження, систематизацію, відтворення, оприлюднення та поширення в електронному форматі передбачених Положенням та Регламентом академічних текстів та інших пов'язаних з ними даних, які опубліковані в Україні або походять з України;

моніторинг надходження академічних текстів до Національного репозитарію та надання інформації про використання його ресурсів;  
 формування та надання у відкритий доступ реєстру академічних текстів;  
 програмний інтерфейс доступу до центрального репозитарію інституціональних учасників;  
 інформаційну безпеку та технічну підтримку центрального репозитарію;  
 умови для організації перевірки академічних текстів на наявність збігів текстових (літерних і цифрових символів) та графічних фрагментів;  
 аналітичну обробку інформації;  
 інформаційне забезпечення розвитку освіти, науки та інновацій через відкритий доступ до відкритих даних, що містяться у Національному репозитарії;  
 максимально повне представлення академічних текстів, наданих інституціональними учасниками, у світовому науково-освітньому просторі;  
 інформаційну інтеграцію з іншими базами даних, зокрема ресурсами відкритих даних України та інших держав, базами центральних органів виконавчої влади;  
 підтримку політики відкритої науки і відкритого доступу та необхідні умови для стимулювання видавців і правовласників до передачі електронних версій академічних текстів та інших пов'язаних з ними даних і зняття (частково чи повністю) обмежень доступу до них користувачів Національного репозитарію.

17. Розпорядник Національного репозитарію відповідає за збереження описової, бібліографічної інформації, електронних версій академічних текстів та інших пов'язаних з ними даних, переданих до центрального репозитарію, а також за забезпечення доступу до них користувачам згідно з режимом, визначеним інституціональним учасником до локального репозитарію.

### **Базові принципи та функціональні особливості Системи**

18. Будь-який елемент (модуль, підсистема, документ тощо) Національного репозитарію має розглядатися як окремий об'єкт зі своїми властивостями та історією (успадкуванням).

Побудова та проектування ієрархії підсистем та модулів, а також чіткий контроль за шляхами надходження інформації мають забезпечуватись дотриманням класичних принципів об'єктно-орієнтованого програмування.

19. Система відповідно до структурного розподілу функцій інформаційного забезпечення має містити в собі такі складові верхнього рівня:

- підсистема імпорту даних;
- підсистема обробки змісту;
- підсистема взаємодії з користувачами (зовнішніми та внутрішніми);
- пошукова підсистема;



аналітична підсистема;  
підсистема підтримки банку даних.

20. Взаємодія із зовнішніми користувачами має забезпечуватися через зовнішні інтерфейси таких базових категорій: інтерфейс користувача (відвідувача, авторизованого користувача) та інтерфейс інституціонального учасника.

21. Зовнішні інтерфейси реалізуються через веб-портал доступу до Національного репозитарію та забезпечують реалізацію:

відображення інформаційних блоків, що містять нормативні документи, новини, відомості про останні надходження до Національного репозитарію, аналітичні матеріали, огляди, кращі практики та будь які інші змістовні елементи, які можуть бути корисними для освітян, науковців та інноваторів з огляду на реалізацію мети, призначення та завдань Національного репозитарію;

можливості реєстрації для отримання доступу до розширеного функціоналу у межах Національного репозитарію;

автентифікації зареєстрованих користувачів та визначення їх статусу згідно Реєстру користувачів та послуг Національного репозитарію академічних текстів;

простого пошукового механізму отримання даних реєстру академічних текстів Національного репозитарію;

розширеного пошукового механізму для роботи з вмістом Національного репозитарію;

додаткові можливості (збереження пошукових запитів, повідомлення про нові надходження) в рамках персонального електронного кабінету;

сервіси та функції, передбачені Регламентом та спрямовані на взаємодію з користувачами тощо.

Реєстр користувачів та послуг Національного репозитарію академічних текстів розробляється та затверджується Розробником за погодженням з МОН.

22. Підсистема підтримки користувачів має:

містити кабінети користувачів – як їх власні профілі із загальними відомостями про них (перелік даних, які надає користувач у свій кабінет, визначається адміністративною підсистемою);

зберігати пошукові запити та результати пошуку користувачів як під час, так і після користування Національним репозитарієм;

забезпечувати формування власної бібліотеки користувача як окремого модуля підсистеми підтримки користувачів;

забезпечувати інформування відповідно до індивідуально оформленої підписки;

забезпечувати можливості використання додаткових аналітичних інструментів роботи з академічними текстами та пов'язаними з ними даними;

можливість використання інструменту перевірки на наявність текстових

(літерних і цифрових символів) та графічних фрагментів.

Власна бібліотека користувача має складатися з двох незалежних частин.

Перша частина формується через звичайний механізм закладок, за допомогою якого користувач може зберігати пошукові запити та їх результати, а також електронні версії академічних текстів, власні примітки, коментарі, рецензії, оформлювати та накопичувати необхідні посилання на академічні тексти тощо.

Друга частина являє собою кабінет автора академічних текстів, який формується відповідно до індивідуального профілю напівавтоматично на основі документів Національного репозитарію, автором яких є користувач, а також тих академічних текстів, де містяться посилання на роботи користувача як автора.

Власна бібліотека користувача має забезпечувати виявлення будь-яких посилань на користувача та представляти користувачеві його науковий профіль, надавати показник цитування, хронологію публікацій та будь-які аналітичні матеріали щодо кожної роботи окремо та публікацій користувача в цілому.

23. Інтерфейс інституціональних учасників має бути системою програмної взаємодії, орієнтованою на підключення вже існуючих локальних репозитаріїв та автоматизовану передачу інформації центральному репозитарію.

Статус інституціонального учасника та відповідні дозволи мають визначатися адміністраторами Системи.

Автентифікація та обмін інформацією між локальними репозитаріями та центральним репозитарієм має відбуватися в автоматизованому режимі на програмному рівні за стандартизованими протоколами взаємообміну між електронними репозитаріями OAI-PMH та SWORD.

24. Внутрішня взаємодія з користувачами має реалізовуватися через низку адміністративних функцій, які дозволяють контролювати як процеси функціонування Системи в цілому та її підсистем, так і змінювати її параметри та конфігурації.

Відповідно до функцій окремих підсистем, адміністратори та оператори центрального репозитарію повинні мати можливість:

додавання нового типу документів до Національного репозитарію, зміни структури вже створених типів документів;

контролювати механізми перевірки коректності кожної складової даних, що надходять до Національного репозитарію;

керувати зареєстрованими користувачами та інституціональними учасниками на загальному рівні;

отримати детальний звіт щодо активності кожного користувача (як фізичної особи, так і інституціонального учасника);

отримувати гнучку статистику щодо наповнення Національного репозитарію за розділами, типами документів тощо;

формування інформаційне наповнення веб-порталу Національного

репозитарію;

формувати та корегувати шаблони відображення змістовної частини Національного репозитарію (окрім безпосередньо змістовних сторінок збережених повних текстів);

формувати звітні складні пошукові запити та статистичні зрізи.

25. Підсистема імпорту має відповідати її функціональному навантаженню, яке залежить від кількості визначених шляхів наповнення центрального репозитарію. Підсистема імпорту має працювати під жорстким керуванням відповідного менеджера. Кожна підсистема імпорту має мати власного програмного менеджера, до функціоналу якого повинна бути віднесена, у тому числі, адміністративна частина налаштувань. Менеджер має оперувати даними відносно режимів, часових та інших параметрів, які впливають на функціонування того чи іншого модуля імпорту.

Кожен модуль імпорту має бути окремою мікропрограмою, логіка роботи якої залежить від призначення. Виходячи з варіантів розташування документів, а також з того, що фактична робота полягає в опрацюванні кожного окремого документа, модулі імпорту мають розглядатися як нащадки визначеного заздалегідь класу. При цьому, базовий клас визначається за найбільш запитуваними методами (отримання сторінки з мережі Інтернет за посиланням; отримання переліку файлів у каталозі; трансформація WinWord документа у текстовий XML формат тощо), а також за найважливішими методами заповнення пустого об'єкту документа.

Нащадки базового класу імпорту повинні мати персоналізований функціонал, відтворений розробниками саме для кожного окремого джерела документів.

Фактично кожен модуль імпорту має виконувати три завдання:

отримання тим чи іншим шляхом пакету документів;

трансформацію кожного документа до формату, який легко опрацьовувати (наприклад, XML формат);

заповнення даними примірника класу внутрішнього формату документів Національного репозитарію.

Головним модулем імпорту має бути модуль підтримки взаємодії за протоколами OAI-PMH та SWORD. Решта шляхів наповнення та відповідних програмних модулів визначається Розробником у процесі розробки.

26. Результатом роботи модулів імпорту мають бути заповнені (повністю або частіше частково) об'єкти, які містять у собі новий документ, що має бути розташованим у банку даних. При цьому, робота Національного репозитарію не повинна передбачати виключно просте збереження даних.

1) Структура документа є складним ієрархічним об'єктом, який має бути пов'язаним своїми властивостями з іншими об'єктами системи (документами, авторами, джерелами тощо). Формування програмної системи за принципами об'єктно-орієнтованого програмування має забезпечувати можливість реалізувати властивості документа таким чином, що побудова зв'язків між

поточними даними та даними банку даних буде виконуватись автоматично, оскільки методи пошуку, наприклад, інформації за автором та побудовою посилань на інші його роботи, притаманна до самої властивості «Автор», а точніше - до об'єкта, який містить у собі властивість документа.

Таким чином, після того як підсистема імпорту сформує новий документ та надішле його до підсистеми обробки, мають бути ініційовані механізми побудови внутрішніх зв'язків для кожної властивості. Результатом роботи всіх методів побудови зв'язків має стати розміщення документа відповідно до його картки у загальній структурі Національного репозитарію – тематичних розділах, авторських добірках, журнальних випусках тощо.

2) Найголовнішою функцією підготовки документа до розташування в Національному репозитарії має бути аналіз змістовної частини документа для досягнення наступних цілей:

- побудови повнотекстового індексу для безпосереднього пошуку за ключовими словами;

- мовного аналізу, який має дати можливість проведення пошуку з урахуванням відмінювання слів;

- формування термінологічних графів, що визначають словосполучення та частотні показники;

- виявлення цитування змістовних частин та інших перетинів між існуючими в Національному репозитарії документами;

- формування посилань на інші документи Національного репозитарію, виходячи з назви, авторства, афіліації та інших відомостей для побудови зв'язків.

Часові параметри обробки змістовної частини у поточному режимі можуть бути некритичними.

Механізми морфологічного аналізу та інших завдань під час обробки документа можуть визначатися системою зберігання даних та математичним апаратом, який використовується розробниками для вирішення поточного завдання.

27. Пошукова підсистема має забезпечувати такі базові функції, як формування запитів до банку даних у відповідності з отриманими від інших підсистем критеріями.

Простими пошуковими запитам є зазвичай ті запити, що надійшли від користувачів (або інших підсистем), коли критеріями пошуку стають властивості документів та/або деяка множина ключових слів чи словосполучень. Такі запити мають оброблятися швидко, оскільки відповідні властивості документів є змістом пошукових індексів банку даних.

Результатом обробки простих запитів має бути перелік об'єктів, що містять посилання на відповідні документи Національного репозитарію та які задовольняють критерії пошуку, інформаційну картку кожного документа, а також (у випадку повнотекстового пошуку) частину тексту, яка містить запитані слова. Весь перелік об'єктів має повернутися, найчастіше, до підсистеми взаємодії з користувачами та відобразитися у них відповідно до

розроблених шаблонів виводу інформації.

Складними пошуковими запитами виступають, найчастіше, запити від підсистеми імпорту, коли необхідно провести контекстний аналіз змістовної частини документу для побудови зв'язків взаємоцитовування, а також взаємопосилань. Для такого складного пошуку має використовуватися побудовані під час імпорту даних морфологічні графи. Складний пошук може тривати деякий час, тому зазвичай може не надаватися користувачам (окрім пошуків відповідності невеликих об'ємів тексту).

Проведення подібного складного пошуку, ініційованого підсистемою імпорту, має проходити на основі вхідного нового документу, який підлягає аналізу, при цьому результатом обробки мають стати два інформаційні масиви.

Перший масив має містити результат обробки вхідного документу, його параметри цитування, а також можливі посилання з наданого документу до інших інформаційних одиниць, що містяться у Національному репозитарію. Наприклад, використання цитат з інших документів або наведення повної назви у переліку використаної літератури має бути автоматично оброблено та трансформовано у гіперпосилання на першоджерело.

Другий масив має містити відповідні модифікації інших документів, які мають бути проведені виходячи з появи нової інформаційної одиниці (посилання на новий поточний документ, які вже існували в банку даних, зміни у даних цитування тощо).

Таким чином, додавання нового документу до банку даних має модифікувати існуючу систему взаємозв'язків між складовими банку даних, підтримуючи актуальність та інформаційну повноту.

28. Підсистема підтримки банку даних має виконувати функцію реалізації інтерфейсу (API) взаємодії решти підсистем та системи керування базами даних. Такий інтерфейс має бути розроблено з урахуванням наступних функціональних вимог:

механізми взаємодії мають бути незалежні від фактично обраної системи керування базами даних (СКБД) (у випадку зміни базової СКБД чи розподілення даних між принципово різними СКБД). Решта підсистем не повинна вимагати ніяких програмних змін;

інтерфейс має передбачати одночасну взаємодію з декількома СКБД, які конфігуруються за допомогою адміністративного режиму підсистеми із визначенням типів СКБД та змісту, відповідного кожній.

Таким чином інші підсистеми у процесі функціонування не повинні навіть «знати», де і яким чином зберігаються дані. Запит на отримання (поновлення, видалення) даних має проводитися типовими розробленими функціями, а фактичну взаємодію - реалізовувати розроблений API. Крім того, до функцій підсистеми підтримки банку даних мають бути віднесені функції періодичної перевірки цілісності банків даних, формування резервних копій тощо.

29. Базовою одиницею інформації, яка зберігається у Національному

репозитарії, є документ. Незалежно від фактичного змісту будь-який документ має бути представлений у вигляді змістовної частини (чи декількох) та набору супроводжувальних властивостей (картки документа), починаючи від переліку авторів і завершуючи датою останньої зміни.

Відповідно до звичайної схеми формування складного об'єкта, кожна властивість може представляти собою окремих інший об'єкт. Наприклад, властивість «Картка документа» – це об'єкт, що містить властивість «Автор», яка у свою чергу є переліком відповідних об'єктів, з яких можливо отримати повну наявну інформацію щодо особи автора. Ураховуючи викладене, в Національному репозитарії, наприклад, об'єкт «Автор» має містити не лише інформацію конкретного документа, але і поєднувати усю наявну в банку даних інформацію відносно обраної особи.

Поєднані таким чином структури, які зберігаються не в якості звичайних довідників-переліків, а як незалежні та динамічні сутності, мають автоматично відтворювати зв'язки між опрацьованими документами та їх властивостями і надають споживачам можливість гнучкого пошуку та максимум змістовної інформації.

Базовий перелік властивостей загального «максимального» документа має формуватися на етапі програмування системи, виходячи з аналізу джерел наповнення банку даних, які будуть складати стартовий зміст Національного репозитарію, наприклад, НДДКР.

Поява нових властивостей має бути передбачена як окрема конфігураційна адміністративна підсистема і, в загальному випадку, не повинна вимагати залучення програмістів для реалізації відповідного коду. Тому під час реалізації системи необхідно відтворити максимально повний набір властивостей, кожна з яких має власну поведінку та власний тип змісту. У такому випадку, у разі необхідності додавання нової властивості до документів з банку даних буде достатньо лише поповнити структуру документів, які зберігаються, заздалегідь розробленим елементом, функції, зміст та поведінка якого вже визначені.

Інформаційними об'єктами, які зберігаються у банку даних, можуть бути екземпляри класів «Автор», «Джерело», «Видавництво», «Організація» тощо. Цей перелік є динамічним та може розширюватися внаслідок аналізу інформації, яка надходитиме до Національного репозитарію.

30. Інтерфейс користувача має задовольняти таким вимогам:
- бути зручним, прийнятним та зрозумілим для роботи із системою;
  - забезпечувати максимальну швидкість обробки запитів незалежно від складності запитів;
  - мати зручну форму представлення отриманих даних;
  - надавати можливість взаємодії зі споживачами на низькошвидкісних каналах зв'язку (наприклад, з мобільних пристроїв), використовуючи технологічні засоби для зменшення об'ємів інформації, що передається;
  - представляти усі URL-посилання в рамках Національного репозитарію у вигляді стійких посилань, без параметричних розширень.

Інтерфейс Системи як для споживачів, так і в адміністративній частині, має бути реалізовано українською мовою. Система індексації змісту документів має зберігати дані у форматі UTF8, що забезпечує багатомовну підтримку.

31. Надійність Системи повинна забезпечуватися шляхом використання в якості апаратних платформ засобів з підвищеною надійністю, при цьому перевага має надаватися серверним рішенням на базі модульних серверів із запасом надійності основних компонентів: блоків живлення, мережних інтерфейсів, дискових масивів тощо.

Цілісність даних у разі збоїв має бути забезпечена незалежно від симптоматики прояву – чи то збоїв живлення, чи то апаратна або програмна складові тощо. Кластерна організація банку даних та наявність резервних копій є необхідними вимогами.

Захист онлайн-ресурсу від цілеспрямованих атак має здійснюватися як шляхами інформаційних ін'єкцій, так і безпосередньо технічними (наприклад, DDOS).

Для забезпечення контролю, зберігання, оновлення, відновлення даних у системі необхідно передбачити наступні можливості:

- контроль цілісності даних — як на логічному рівні, так і на фізичному;
- періодичне тестування структури документів та організації банку даних;
- збереження резервних копій (повних чи інкрементальних);
- протоколювання процесів у системі.

32. Вимоги до захисту інформації в Національній репозитарії повинні відповідати вимогам щодо технічного захисту інформації, викладеним у законах України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», постанові Кабінету Міністрів України від 26 березня 2006 р. № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», у нормативних документах «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» (НД ТЗІ 2.5-004-99) та «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу» (НД ТЗІ 2.5-010-03) та в інших нормативно-правових актах і нормативних документах у сфері технічного захисту інформації в Україні.

Інформаційна безпека повинна відповідати наступним вимогам:

захист має забезпечуватися комплексом програмно-технічних засобів та підтримуючих їх організаційних заходів на всіх технологічних етапах обробки інформації та у всіх режимах функціонування, у тому числі при проведенні ремонтних і регламентних робіт;

програмно-технічні засоби захисту не повинні погіршувати основні функціональні показники системи, у першу чергу - надійність та швидкодію;

розмежування прав доступу користувачів і адміністраторів повинне будуватися за принципом «що не дозволено, те заборонено».

Для захисту Національного репозитарію від створення несанкціонованих повних копій його програмне забезпечення має унеможливити несанкціоноване зовнішнє копіювання повного змісту Національного репозитарію або його масштабних частин. Захист інформації у локальних репозитаріях має здійснюватися інституціональними учасниками відповідно до законодавства.

Захист інформації повинен забезпечуватися впродовж усього періоду її існування. З моменту створення об'єкта у Національному репозитарії і аж до його знищення (якщо така необхідність виникне) усі запити на доступ до об'єкта та об'єкта на доступ до інших об'єктів мають контролюватися комплексами засобів захисту.

Система захисту інформації повинна відповідати вимогам чинного законодавства у сфері захисту інформації.

З метою реалізації шифрування інформації, автентифікації повідомлень і підтвердження їх походження при передачі каналами зв'язку необхідні модулі повинні включати до свого складу засоби криптографічного захисту інформації, допущені до експлуатації у встановленому законодавством порядку.

33. Програмні засоби захисту інформації повинні забезпечувати контроль доступу, безпеку й цілісність даних і захист самої системи захисту.

Система захисту інформації повинна забезпечити:  
захист інформації від несанкціонованого доступу;  
ідентифікацію та автентифікацію користувачів;  
розмежування доступу користувачів до модулів, інформаційних об'єктів і довідників, що дозволить організувати одночасну сумісну роботу декількох користувачів, які виконують різні службові обов'язки та мають різні права доступу;

налаштування інтерфейсу користувача має здійснюватися таким чином, щоб він містив лише об'єкти та функції, надані користувачеві в доступ;

безперервну реєстрацію критичних для безпеки подій (входу користувачів, спроб несанкціонованого доступу, імпорту / експорту тощо) у спеціальних протоколах аудиту.

Компоненти програмних комплексів захисту повинні мати експертні висновки Державної служби спеціального зв'язку та захисту інформації України щодо відповідності вимогам нормативних документів системи криптографічного захисту інформації.

Засоби антивірусного захисту повинні бути встановлені на робочих місцях адміністраторів та бути інтегрованими у підсистему імпорту зовнішніх документів для контролю та захисту банку даних від наповнення потенційно небажаним змістом.

### **Програмно-апаратне оточення Системи та доступ до мережі Інтернет**



34. У якості базової операційної системи роботи серверної частини Національного репозитарію може бути обрана система сімейства Linux/Unix (наприклад, у тому числі з використанням кластерної структури).

Клієнтська частина програмного забезпечення має бути розроблена як веб-сервіс, доступ до якого проводиться штатними переглядачами операційних систем, у тому числі - мобільних, із підтримкою HTML5.

Взаємодія між віддаленими споживачами та НРАТ має проводитись на базі шифрованого протоколу HTTPS із використанням персоналізованого сертифікату.

Для ефективного розміщення та зручності обслуговування усе серверне обладнання, обладнання зберігання даних, обладнання безперебійного електроживлення, активне мережеве обладнання повинно бути сумісним для встановлення в стандартну комутаційну стійку.

У якості накопичувачів для збереження змісту Національного репозитарію має бути використано дисковий масив (RAID-5 або вище), який забезпечить зберігання даних навіть у випадку апаратного збою одного (чи декількох) складових. Відповідно до наповнення складових середовища збереження документів та баз даних, а також резервних копій, виходячи з підвищених вимог швидкості роботи баз даних, мають бути розділені.

Усі обчислювальні одиниці, на яких функціонує серверна частина Національного репозитарію, мають бути поєднані у відокремлену мережеву інфраструктуру на швидкості не нижче 1 Gb. Взаємодія із «зовнішнім» середовищем має проводитись шляхом організації проміжного маршрутизатора-брандмауера, який забезпечить комунікаційний доступ до Національного репозитарію лише декларованими засобами.

35. Для забезпечення доступу користувачів до Національного репозитарію має бути налагоджений канал передачі даних до мережі Інтернет із швидкістю приймання-передавання не нижче гарантованих 100 МБіт/с із необмеженим обсягом трафіку. Безперервність доступу до мережі Інтернет необхідно забезпечити наявністю резервного каналу доступу до мережі Інтернет.

### **Нормативно-правове забезпечення створення та функціонування системи**

36. При побудові Національного репозитарію мають бути дотримані вимоги таких актів:

Конституція України;

Закони України:

«Про інформацію», «Про доступ до публічної інформації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про електронний цифровий підпис», «Про захист персональних даних»;

Укази Президента України:

від 20 жовтня 2005 року № 1497 «Про першочергові завдання щодо впровадження новітніх інформаційних технологій», від 01 серпня 2002 року № 683 «Про додаткові заходи щодо забезпечення відкритості у діяльності органів державної влади», від 27 вересня 1999 року № 1229 «Про затвердження Положення про технічний захист інформації в Україні»;

постанови Кабінету Міністрів України:

від 29 серпня 2002 р. № 1302 «Про заходи щодо подальшого забезпечення відкритості у діяльності органів виконавчої влади», від 04 лютого 1998 р. № 121 «Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних», від 12 квітня 2002 р. № 522 «Про затвердження Порядку підключення до глобальних мереж передачі даних», від 04 лютого 2002 р. № 3 «Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади», від 10 вересня 2003 р. № 1433 «Про затвердження Порядку використання комп'ютерних програм в органах виконавчої влади», від 28 жовтня 2004 р. № 1452 «Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності», від 12 вересня 2009 р. № 869 «Про затвердження загальних вимог до програмних продуктів, які закупаються та створюються на замовлення державних органів», від 29.03.2006 №373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»;

ДК 010-98 «Державний класифікатор управлінської документації»;

ДСТУ 3396.0-96 «Захист інформації»;

ДСТУ 3396 0-96 «Захист інформації. Технічний захист інформації. Основні положення»;

ДСТУ 3396 1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт»;

ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення»;

ДСТУ 3973-2000 «Система розроблення та поставлення продукції на виробництво. Правила виконання науково-дослідних робіт. Загальні положення»;

ДСТУ 3974-2000 «Система розроблення та поставлення продукції на виробництво. Правила виконання дослідно-конструкторських робіт. Загальні положення»;

ДСТУ 3582:2013 «Інформація та документація. Бібліографічний опис. Скорочення слів і словосполучень в українській мові. Загальні вимоги та правила»;

ДСТУ ГОСТ 7.1:2006 «Система стандартів з інформації, бібліотечної та видавничої справи. Бібліографічний опис. Загальні вимоги та правила складання 7.1-2003»;

ДСТУ 3278-95 «Система розроблення та поставлення продукції на виробництво. Основні терміни та визначення»;

ДСТУ ISO/IEC 33001:2016(ISO/IEC 33001:2015, IDT) «Інформаційні технології. Оцінювання процесу. Поняття та термінологія»;

ДСТУ ISO/IEC 10745:2017 (ISO/IEC 10745:1995, IDT) «Інформаційні технології. Взаємозв'язок відкритих систем. Модель безпеки верхніх рівнів»;

ДСТУ ISO/IEC 2382:2017 (ISO/IEC 2382:2015, IDT) «Інформаційні технології. Словник термінів»;

ДСТУ ISO/IEC 27036-1:2017 (ISO/IEC 27036-1:2014, IDT) «Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах з постачальниками. Частина 1. Огляд і поняття»;

ДСТУ ISO/IEC 27036-2:2017 (ISO/IEC 27036-2:2014, IDT) «Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах з постачальниками. Частина 2. Вимоги»;

ДСТУ ISO/IEC 27036-3:2017 (ISO/IEC 27036-3:2013, IDT) «Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах з постачальниками. Частина 3. Настанови щодо безпеки ланцюга постачання інформаційних та комунікаційних технологій»;

ДСТУ ISO/IEC 27039:2017 (ISO/IEC 27039:2015, IDT) «Інформаційні технології. Методи захисту. Вибірання, розгортання та експлуатування систем виявлення та запобігання вторгненням (СВЗВ)»;

ДСТУ ISO/IEC 29182-3:2017 (ISO/IEC 29182-3:2014, IDT) «Інформаційні технології. Сенсорні мережі. Еталонна архітектура сенсорних мереж. Частина 3. Огляд еталонної архітектури»;

ДСТУ ISO/IEC 27013:2017(ISO/IEC 27013:2015, IDT) «Інформаційні технології. Методи захисту. Настанови для інтегрованого впровадження ISO/IEC 27001 та ISO/IEC 20000-1»;

ДСТУ ISO/IEC 14709-1:2017 (ISO/IEC 14709-1:1997; Amd 1:2004, IDT) «Інформаційні технології. Конфігурація кабельної мережі приміщень користувачів для застосунків. Частина 1. Базовий доступ до цифрової мережі з інтеграцією послуг (ISDN)»;

ДСТУ ISO/IEC 14709-2:2017 (ISO/IEC 14709-2:1998; Amd 1:2005, IDT) «Інформаційні технології. Конфігурація кабельної мережі приміщень користувачів для застосунків. Частина 2. Первинний доступ для цифрової мережі з інтеграцією послуг (ISDN)»;

ДСТУ ISO/IEC 29155-3:2017 (ISO/IEC 29155-3:2015; IDT) «Інженерія систем і програмного забезпечення. Структура порівняльного аналізу ефективності проектів інформаційних технологій. Частина 3. Настанова щодо звітності»;

ДСТУ ISO/IEC 28361:2017 (ISO/IEC 28361:2007, IDT) «Інформаційні технології. Телекомунікації та обмін інформацією між системами. Проводовий інтерфейс (NFC-WI) у мережах обміну даними ближнього поля»;

ДСТУ ISO/IEC 29182-1:2017 (ISO/IEC 29182-1:2013, IDT) «Інформаційні технології. Сенсорні мережі. Еталонна архітектура сенсорних мереж. Частина 1. Загальний огляд та вимоги»;

ДСТУ ISO/IEC TR 18053:2017 (ISO/IEC TR 18053:2000, IDT) «Інформаційні технології. Телекомунікації та обмін інформацією між

системами. Словник термінів у сфері телекомунікаційних застосунків із комп'ютерною підтримкою, стадія III»;

ДСТУ ISO/IEC 29155-1:2017 (ISO/IEC 29155-1:2011; IDT) «Інженерія систем і програмного забезпечення. Структура порівняльного аналізу ефективності проектів інформаційних технологій. Частина 1. Поняття та визначення»;

ДСТУ ISO/IEC 29155-2:2017 (ISO/IEC 29155-2:2013; IDT) «Інженерія систем і програмного забезпечення. Структура порівняльного аналізу ефективності проектів інформаційних технологій. Частина 2. Вимоги до порівняльного аналізу»;

ДСТУ ISO 9001-2015 «Системи управління якістю. Вимоги»;

НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації у комп'ютерних системах від несанкціонованого доступу»;

НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації у комп'ютерних системах від несанкціонованого доступу»;

НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі»;

НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу»;

НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»;

НД ТЗІ 3.6-001-2000 «Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу»;

НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі»;

НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»;

РД 50-34.698-90 «Руководящий документ по стандартизации. Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов»;

ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;

ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы стадии создания»;

ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;

ГОСТ 34.603.-92 «Информационная технология. Виды испытаний автоматизированных систем».

37. При створенні програмних продуктів Національного репозитарію мають бути дотримані вимоги таких актів:

Конституція України;

Закони України:

«Про інформацію», «Про доступ до публічної інформації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про електронний цифровий підпис», «Про захист персональних даних»;

Укази Президента України:

від 20 жовтня 2005 року № 1497 «Про першочергові завдання щодо впровадження новітніх інформаційних технологій», від 01 серпня 2002 року № 683 «Про додаткові заходи щодо забезпечення відкритості у діяльності органів державної влади», від 27 вересня 1999 року № 1229 «Про затвердження Положення про технічний захист інформації в Україні»;

постанови Кабінету Міністрів України:

від 29 серпня 2002 р. № 1302 «Про заходи щодо подальшого забезпечення відкритості у діяльності органів виконавчої влади», від 04 лютого 1998 р. № 121 «Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних», від 12 квітня 2002 р. № 522 «Про затвердження Порядку підключення до глобальних мереж передачі даних», від 04 лютого 2002 р. № 3 «Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади», від 10 вересня 2003 р. № 1433 «Про затвердження Порядку використання комп'ютерних програм в органах виконавчої влади», від 28 жовтня 2004 р. № 1452 «Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності», від 12 вересня 2009 р. № 869 «Про затвердження загальних вимог до програмних продуктів, які закуповуються та створюються на замовлення державних органів», від 29 березня 2006 р. № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»;

ДК 010-98 «Державний класифікатор управлінської документації»;

ДСТУ 4163–2003 «Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлювання документів»;

ДСТУ 3396 0-96 «Захист інформації. Технічний захист інформації. Основні положення»;

ДСТУ 3396 1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт»;

ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення»;

ДСТУ 3973-2000 «Система розроблення та поставлення продукції на виробництво. Правила виконання науково-дослідних робіт. Загальні положення»;

ДСТУ 3974-2000 «Система розроблення та поставлення продукції на

виробництво. Правила виконання дослідно-конструкторських робіт. Загальні положення»;

ДСТУ 3582:2013 «Інформація та документація. Бібліографічний опис. Скорочення слів і словосполучень в українській мові. Загальні вимоги та правила»;

ДСТУ ГОСТ 7.1:2006 «Система стандартів з інформації, бібліотечної та видавничої справи. Бібліографічний опис. Загальні вимоги та правила складання 7.1-2003»;

ДСТУ 3278-95 «Система розроблення та поставлення продукції на виробництво. Основні терміни та визначення»;

ДСТУ ISO/IEC 15026-1:2017 (ISO/IEC 15026-1:2013, IDT) «Інженерія систем і програмних засобів. Гарантії стосовно систем і програмних засобів. Частина 1. Поняття та основні терміни»;

ДСТУ ISO/IEC 17788:2017 (ISO/IEC 17788:2014, IDT) «Інформаційні технології. Хмарні обчислення. Огляд та основні терміни»;

ДСТУ ISO/IEC 17825:2017 (ISO/IEC 17825:2016, IDT) «Інформаційні технології. Методи захисту. Методи тестування протидії класам неінвазивних атак на криптографічні модулі»;

ДСТУ ISO/IEC 19510:2015 «Інформаційні технології. Модель і нотація бізнес-процесу групою управління об'єктами (OMG) (ISO/IEC 19510:2013, IDT)»;

ДСТУ ISO/IEC 24760-2:2017 (ISO/IEC 24760-2:2015, IDT) «Інформаційні технології. Методи захисту. Структура керування ідентифікаційною інформацією. Частина 2. Еталонна архітектура та вимоги»;

ДСТУ ISO/IEC 27017:2017 (ISO/IEC 27017:2015, IDT) «Інформаційні технології. Методи захисту. Звід практик стосовно заходів інформаційної безпеки, що ґрунтуються на ISO/IEC 27002, для хмарних послуг»;

ДСТУ ISO/IEC 27034-1:2017 (ISO/IEC 27034-1:2011; Cor 1:2014, IDT) «Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 1. Огляд і загальні поняття»;

ДСТУ ISO/IEC 27034-2:2017 (ISO/IEC 27034-2:2015, IDT) «Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 2. Нормативна структура організації»;

ДСТУ ISO/IEC/IEEE 29119-1:2017 (ISO/IEC/IEEE 29119-1:2013, IDT) «Інженерія систем і програмних засобів. Тестування програмних засобів. Частина 1. Поняття та визначення»;

ДСТУ ISO/IEC/IEEE 29119-2:2017 (ISO/IEC/IEEE 29119-2:2013, IDT) «Інженерія систем і програмних засобів. Тестування програмних засобів. Частина 2. Процеси тестування»;

ДСТУ ISO/IEC/IEEE 29119-3:2017 (ISO/IEC/IEEE 29119-3:2013, IDT) «Інженерія систем і програмних засобів. Тестування програмних засобів. Частина 3. Документація тестування»;

ДСТУ ISO/IEC/IEEE 29119-4:2017 (ISO/IEC/IEEE 29119-4:2015, IDT) «Інженерія систем і програмних засобів. Тестування програмних засобів. Частина 4. Методики тестування»;

ДСТУ ISO/IEC TR 14143-4:2017 (ISO/IEC TR 14143-4:2002, IDT) «Інформаційні технології. Вимірювання програмного забезпечення. Вимірювання функційного розміру. Частина 4. Еталонна модель»;

ДСТУ ISO/IEC 14143-6:2017 (ISO/IEC 14143-6:2012, IDT) «Інформаційні технології. Вимірювання програмного забезпечення. Вимірювання функційного розміру. Частина 6. Настанова щодо застосування стандартів серії ISO/IEC 14143 та пов'язаних з ними міжнародних стандартів»;

ДСТУ ISO/IEC TR 14143-5:2017 (ISO/IEC TR 14143-5:2004, IDT) «Інформаційні технології. Вимірювання програмного забезпечення. Вимірювання функційного розміру. Частина 5. Визначення функційних доменів для застосування під час вимірювання функційного розміру»;

ДСТУ ISO/IEC TR 20004:2017 (ISO/IEC TR 20004:2015, IDT) «Інформаційні технології. Методи захисту. Уточнений аналіз вразливості програмного забезпечення згідно з ISO/IEC 15408 та ISO/IEC 18045»;

ДСТУ ISO/IEC TR 19566-1:2017 (ISO/IEC TR 19566-1:2016, IDT) «Інформаційні технології. Системи JPEG. Частина 1. Пакування інформації з використанням кодових потоків і форматів файлів»;

ДСТУ ISO/IEC TR 19566-2:2017 (ISO/IEC TR 19566-2:2016, IDT) «Інформаційні технології. Системи JPEG. Частина 2. Транспортні механізми та пакування»;

ДСТУ 2844-94 «Програмні засоби ЕОМ. Забезпечення якості. Терміни та визначення»;

ДСТУ ISO/IEC 9126-1:2001:2013 «Програмна інженерія. Якість продукту. Частина 1. Модель якості»;

ДСТУ 34.602-89 «Техническое задание на создание автоматизированной системы»;

ДСТУ ISO/IEC 25010:2016 «Інженерія систем і програмних засобів. Вимоги до якості систем і програмних засобів та її оцінювання (SQuaRE). Моделі якості системи та програмних засобів»;

ДСТУ ISO 9001-2015 «Системи управління якістю. Вимоги»;

НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації у комп'ютерних системах від несанкціонованого доступу»;

НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації у комп'ютерних системах від несанкціонованого доступу»;

НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі»;

НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу»;

НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»;

НД ТЗІ 3.6-001-2000 «Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу»;

НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного

завдання на створення комплексної системи захисту інформації в автоматизованій системі»;

НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»;

ГОСТ 19.005-85 «ЕСПД. Р-схеми алгоритмов и программ. Обозначения условные графические и правила выполнения»;

ГОСТ 19.104-78 «ЕСПД. Основные надписи»;

ГОСТ 19.403-79 «Ведомость держателей подлинников»;

РД 50-34.698-90 «Руководящий документ по стандартизации. Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов».

### **Порядок контролю та приймання робіт**

38. Контроль за процесом створення Національного репозитарію забезпечується Замовником шляхом створення робочої групи, в складі і з повноваженнями, необхідними для успішної реалізації Системи.

Після здачі Національного репозитарію в експлуатацію робоча група розформовується.

Для приймання робіт зі створення Національного репозитарію утворюється приймальна комісія.

Порядок виконання робіт визначається затвердженими Календарними планами робіт.

Тестування Системи має забезпечити:

повну перевірку функцій системи;

перевірку взаємодії центрального репозитарію з локальними репозитаріями;

перевірку взаємодії Національного репозитарію в цілому із користувачами для отримання необхідної інформації;

перевірку надійності та стійкості функціонування програмних і технічних засобів.

### **Вимоги до документування**

39. Для Системи на різних стадіях її створення повинні бути випущені такі документи з числа передбачених у ГОСТ 34.201-89 «Комплекс стандартів на автоматизовані системи. Види, комплектність і позначення документів при створенні автоматизованих систем»:

Пояснювальна записка;

Схема організаційної структури Національного репозитарію;

Інструкція відвідувача, користувача та інституціонального учасника;

Кошторисна документація.



## Перспективи розвитку модернізації Системи

40. Перспективним розвитком отриманої Системи має стати взаємодія з відповідними міжнародними ресурсами, що сприятиме розвитку та популяризації Національного репозитарію, а також формуватиме представлення рівня національної науки для світової спільноти.

Модернізація процесів Національного репозитарію має надавати велику кількість аналітичної та статистичної інформації. Поява нових джерел повнотекстових наукових документів буде ініціювати створення нових модулів імпорту, а зростання змісту банку даних дасть можливість вдосконалювати підсистеми побудови взаємозв'язків між документами, побудови глосаріїв та онтологічних словників.

Виконуючий обов'язки директора  
департаменту науково-технічного розвитку



О. А. Хименко