отеки» [у громадянина Люкшина вилучено 7 010 кн., 2113 журн.] (ф. Р-5861, оп. 1, д. 7).

Також виявлено документи, записки, довідки, листування з питання будівництва Бібліотеки, в т. ч. копію листа директора книгозбірні О. Чекушина М. Хрущову.

Значну пошукову роботу у фондах ДОДА провели співробітники краєзнавчого відділу – хранитель Музею історії ДОУНБ З. Рижкова, М. Пушкар. Ними переглянуто регіональні періодичні видання 20–40-х років XX століття, що збереглися у фондах архіву. На основі цих розвідок підготовлено бібліографічний покажчик "Духовна скарбниця краю: Історія і сучасність Дніпропетровської обласної державної наукової бібліотеки" (Д., 1999. – 133 с.).

З. Рижкова систематизувала зібрані матеріали, здійснила літературну обробку розрізнених рукописних документів, спогадів ветеранів бібліотеки.

Сьогодні ми – творці історії ДОУНБ, і всі події, пов'язані з нею, здобутки з плином часу стануть хвилюючим минулим. Від забуття їх врятують фотолітописи, аматорські кінострічки, краєзнавчі, бібліографічні, аналітичні інформаційні видання, серед яких: щорічник "Моє Придніпров'я. Календар пам'ятних дат Дніпропетровської області на... рік"; серія ювілейних видань до 170-річчя установи; "Дніпропетровська обласна універсальна наукова бібліотека: Сторінки історії" (2004 р.); спогади ветеранів "Люди. Роки. Бібліотечне життя" та ін.

Історія нашої Бібліотеки – це самовіддане служіння своїй справі, неспокій, втрати і перемоги багатьох поколінь її працівників. Це частка історії рідної України.

ПРОБЛЕМИ ЗБЕРІГАННЯ І ЗАХИСТУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ: ДОСВІД ФРН

ЗАРУБІЖНИЙ ДОСВІД

На базі вивчення німецьких професійних джерел автор розкриває систему понять та технологічних процесів, які забезпечують захист електронних документів. Стаття дає уявлення про основні вимоги, що висуваються до згаданої технології, про діючі міжнародні акти і протоколи. Також у ній йдеться про недосконалості сучасних механізмів захисту електронних документів. Серед існуючих засобів зберігання розглядаються такі, як електронна архівація, технології кодування та електронного підпису

В. Рудюк

До електронно-документаційних послуг висуваються такі самі вимоги стосовно збереження і захисту інформації, що й до традиційних форм ділових документних ресурсів: ідеться про гарантоване зберігання документа протягом певного часу та надійний його захист. Окрім того, у рамках електронного документообігу постають специфічні питання: як захистити документи від знищення або пошкодження внаслідок втрати фізичних властивостей носіїв інформації, зміни програмних і технічних компонентів; як запобігти некоректному поводженню з документами через низьку комп'ютерну грамотність персоналу або користувачів та ін.

Електронна архівація. Окрім технічних проблем – нетривкості магнітних та оптичних носіїв інформації, термін придатності яких звичайно становить від 3 до 30 років, нестабільності та обмеженої конвертованості форматів даних тощо, потребує вирішення питання організації даних. Для повноцінного представлення суті справи, з приводу котрої укладено електронний документ, повинен бути зрозумілим контекст і його зв'язок з іншими документами. Ізольовані дані й файли не відповідають таким вимогам, тому електронні архіви мають зберігати, наприклад, нарівні з окремими документами контекстну інформацію[1].

На даний час не вирішено, які носії інформації і пристрої для зчитування слід використовувати для електронної архівації документів, з яких процесів вона повинна складатися тощо[2].

Проведене у ФРН 2000 року в рамках дискусії щодо зберігання управлінських електронних документів опитування засвідчило, що фахівці не мають чіткого уявлення про зміст поняття "тривала архівація електронних документів" і про рекомендовані методи. Під тривалою архівацією часто розуміли не перебування електронних документів в архіві, а їхнє зберігання протягом певного часу в обчислювальних центрах, що насправді визначається як електронна (цифрова) реєстрація. Накопичення електронних документів на місцях створює загрозу для архівів, котрим згодом доведеться зіткнутися з масованим напливом переданих на зберігання об'єктів[3].

Нині у ФРН поняття електронної архівації складається з двох поданих нижче визначень.

Електронна тривала архівація (*elektronische Langzeitarchivierung*). Про такі технології йдеться, якщо інформація повинна зберігатись і залишатися придатною для використання протягом щонайменше десяти років[4].

Німецькі фахівці вважають це визначення алогізмом, оскільки сама архівація передбачає тривалість. Основні проблеми у цьому контексті – менший термін придатності електронних носіїв інформації (у порівняні з паперовими), швидка змінюваність форматів даних, версій програмних і технічних компонентів[5].

[1] Bischof: Archivierung digitaler Unterlagen, Kap. 2.

[2] Пріоритетного значення у роботі з електронної архівації нині набула розробка програмних засобів, що гарантуватимуть незмінність документів під час їхнього зберігання, забезпечуватимуть швидкий доступ та ефективне управління величезними масивами даних незалежно від носіїв інформації. Така світова тенденція була сформульована у 2003 р. і дістала назву Information Lifecycle Management (ILM), мета-програмне керування повним циклом існування електронної інформації замість використання звичайних накопичувачів. Див.: PK-DML.

[3] Bischof: Ende der Aktenzeit?

[4] Ведучи мову про технології електронної тривалої архівації, німецькі фахівці мають на увазі не лише зберігання інформації, але також технології обробки її в архіві. Див.: NESTOR.

[5] Bischof: Archivierung digitaler Unterlagen.

Контрольована електронна архівація (*revisionssichere elektronische Archi-vierung*). Визначення постало з фахових дискусій стосовно поводження з електронними податковими документами; у ФРН визнано обов'язковим застосування контрольованих архівних систем і накопичувачів інформації (*revisionssichere Archiv- und Speichersysteme*)[6] – таких, що забезпечують зберігання документів від шести до десяти років і відповідають десяти вимогам:

1) зберігання кожного документа у незмінному вигляді;

2) неприпустимість втрати документів під час передачі в архів або знаходження в архіві;

3) неприпустимість пошкоджень документів протягом передбаченого строку придатності носія;

4) можливість знайдення будь-якого документа за допомогою пошукових технологій;

5) можливість знайдення будь-якого документа у найкоротший термін;

6) знайдення у результаті пошуку потрібного документа, а не будь-якого іншого;

7) придатність документа до візуалізації і роздрукування у тій самій формі, у котрій його було створено;

8) протоколювання всіх процесів в архіві, котрі можуть спричинити зміни його організації, та відновлюваність вихідного стану;

9) готовність електронного архіву до міграції на нові платформи, носії, програмні засоби (ПЗ) і технічні компоненти без втрати інформації;

10) доступність користувачеві інформації про законодавчі норми і галузеві вимоги, що регулюють діяльність архіву у частині захисту даних та інформації, протягом всього часу існування архіву[7].

Задовольнити всі вимоги повністю за нинішнього стану обладнання і технологій неможливо. Функціональні вимоги до нині використовуваних у ФРН електронних архівних систем, зокрема, такі:

- прямий доступ до інформаційних об'єктів (електронних документів) або інформаційних колекцій (списків, контейнерних електронних документів тощо);
- управління інформаційними об'єктами, з використанням баз даних (БД), завдяки метаданим та/або індексуванню змісту прийнятих на зберігання об'єктів;
- підтримка різних пошукових технологій для забезпечення прямого доступу до інформації;
- уніфіковане спільне зберігання будь-яких інформаційних об'єктів – від відсканованого рукопису і файлів *Word* до вмісту БД тощо;
- управління архівними системами з неперезаписуваними носіями, включаючи можливість доступу до носіїв, що більше не входять безпосередньо до системи;
- гарантування можливості візуалізації документів протягом усього періоду їхнього зберігання в архіві незалежно від походження (типу комп'ютера і ПЗ); з цією метою передбачено наявність програм-конвертерів для створення стабільних архівних форматів і представлення інформаційних об'єктів, чиї «рідні» ПЗ вже недоступні[8]. Ведучи мову про технології електронної архівації, слід мати на увазі, з одного боку, призначені для управління архівними документами ПЗ, з іншого – носії, використовувані для зберігання електронних архівів. Магнітні носії нині вважають непридатними для цього, оскільки електронні дані, що зберігаються на них, можуть бути змінені або знищені будь-коли (особливо ці побоювання справедливі для жорстких дисків, котрі перебувають у динамічному використанні); магнітні плівки, окрім того, швидко зношуються, магнітний шар руйнується. Оптимальним наразі вважається застосування оптично-цифрових носіїв, запис на які можна здійснити за допомогою лазера лише один раз[9]. Вони захищені – завдяки своїм фізичним властивостям – від внесення змін і мають значно більший термін придатності у порівнянні з магнітними носіями. Втім, європейські закони і норми не регламентують прямо використання саме таких носіїв інформації, оскільки тривала архівація даних повинна передбачати зміну технологій у майбутньому.

Окрім класичних архівних фондів, що складаються із змінних носіїв інформації (наприклад, оптично-цифрових), використовуються інші технології: 1) *CAS Content Adressed Storage:* система жорстких дисків, що за допомогою спеціального ПЗ наділені однаковими властивостями, перезапис або зміна інформації неможливі через її кодування під час архівації та особливу форму адресації[10]; 2) *WORM-Tapes* – виготовлені за спеціальною технологією магнітні носії (касети, дискети та ін.), наділені властивостями *WORM*[11].

Гарантувати збереженість і доступність архівної електронної інформації можна комбінуванням різних стратегій.

1. *Стандартизація* – одна з основних передумов доступності електронної інформації протягом тривалого часу; стандартизації підлягають файлові формати, метадані інформаційного об'єкта, типи і властивості носіїв інформації тощо. Можливість тривалого зберігання електронного документа повинна враховуватись уже на стадії створення файла, зокрема, рекомендовано використовувати так звані стабільні формати, що характеризуються значним поширенням, відкритою специфікацією (нормуванням) або їх створювали для тривалого зберігання даних (наприклад, *XML, TIFF, PDF, JPEG, PNG*).[12]

2. *Міграція* – це збереження доступності інформації протягом необмеженого часу шляхом регулярного перенесення даних із застарілого у нове системне оточення (технічні компоненти, призначені для зберігання даних та управління ними). Оригінальніст ь та автентичність інформації, авторські права і заборона копіювання можуть бу-

[6] Netlexikon: Elektronische Archivierung.

[7] Ці критерії мають узагальнений фаховий характер і в умовах запровадження технічних систем підлягають конкретизації або інтерпретації. Див.: Handelsgesetzbuch, §§ 239, 257; Abgabenordnung, §§ 146, 147; Grundsatze ordnungsma?iger DV-gestutzter Buchfuhrungssysteme; Kampffmeier/Rogalla.

[8] Повний перелік вимог див.: Netlexikon: Elektronische Archivierung; Henstorf/Kampffmeier/Prochnow.

[9] Технологія має назву WORM: Write Once, Read Multiple Times. Типи використовуваних носіїв такі: CD-WORM (неперезаписуваний компакт-диск з обсягом пам'яті до 800 Кб), DVD-WORM (обсяг від 4 до 17 Гб), 5 ?"-WORM (створений спеціально для електронної архівації, обсяг пам'яті понад 50 Гб).

[10] У цьому випадку йдеться звичайно про замкнені архівні підсистеми, котрі можуть бути інтегровані – подібно до традиційних жорстких дисків – в інформаційно-комунікаційні системи і мережі.

[11] Такі носії у ФРН особливо поширені в адміністративних установах і на підприємствах (здебільшого великих, що мають власні обчислювальні центри), де віддавна застосовують машини та бібліотечні системи з магнітними носіями і де WORM-плівки можна використовувати для тривалого зберігання інформації, причому для автоматизації процесів запису і захисту таких архівів не потрібна модернізація наявного ПЗ.

[12] Borghoff/Rodig/Scheffszyk.

ти порушені у процесі міграції; так само сумнівна можливість повноцінного пошуку у перенесених даних, якщо під час міграції вони, контекстна інформація або метадані зазнали змін. Тому ще на стадії організації архіву потрібно передбачити можливість вчасної міграції, що відбуватиметься без порушення прав, без змін і втрат інформації; для цього, наприклад, може знадобитися створення оригінального ПЗ для міграції форматів даних[13].

3. *Емуляція* передбачає створення нових комп'ютерних систем і ПЗ, здатних симулювати власні старі версії і в такий спосіб працювати з даними, генерованими у старих комп'ютерах та операційних системах (ОС). Ця стратегія поки що рідко використовується у контексті тривалої архівації; причина полягає у непередбачуваності витрат і труднощів при майбутній емуляції, котра за певних обставин може виявитися неможливою.

4. *Інкапсуляція* – процес, котрий німецькі фахівці вважають особливо важливим як підготовчий до емуляції; сутність полягає у зберіганні разом з інформаційними об'єктами ПЗ, за допомогою котрого вони можуть бути відтворені, а також відповідних метаданих. Недоліками стратегії є занадто великий розмір об'єкта («капсули»), що зберігається, а також відсутність гарантії, що архівовані ПЗ можуть бути використані у майбутньому.

5. *Конвертація* у процесі використання – стратегія, що передбачає постійну наявність у системі програм – конверторів та оглядачів, здатних при відкриванні файла у застарілому форматі перевести його у більш актуальний. Відмінність від емуляції полягає у тому, що в умовах конвертації інформаційний об'єкт пристосовується до наявного системного оточення, а при емуляції навпаки – нове оточення симулює те, у котрому було створено об'єкт. Недоліками такої конвертації є проблематичність збереження структури документів, цілісності електронного підпису тощо[14].

На доволі гостре запитання, які електронні документи підлягають зберіганню в архіві, німецькі колеги пропонують таку відповідь: 1) підлягають архівації електронні документи, що не мають паперових версій (електронні версії документів, котрі було роздруковано і підшито до справ, підлягають знищенню); 2) не підлягають архівації електронні документи, які не містять важливої інформації щодо суті справи або вказівок стосовно свого походження та здійснених процесів обробки[15].

Проблеми безпеки даних. Захист даних, котрі становлять сутність та зміст електронного документа, ґрунтується на врахуванні загальних і специфічних факторів ризику. Цілковита їхня нейтралізація на даний час проблематична.

Загальні фактори ризику. Дія цих факторів зумовлена природою електронних даних. Вжиття відповідних контрзаходів є неодмінною умовою при запровадженні електронної форми ділових документальних комунікацій.

- «Віртуальні» електронні дані не можна прочитати без відповідних технічних і програмних засобів; відсутність або невідповідність цих засобів (застаріле обладнання, дефектні носії, некоректні версії ПЗ та ін.) можуть ускладнити відтворення, зберігання, кодування даних тощо.
- Електронні дані нетривкі: завжди є ризик втрати даних без видимих причин, наприклад, внаслідок розмагнічування носіїв у зв'язку із закінченням терміну їхньої придатності, в результаті перезапису даних, відмови обладнання та ін.
- Електронні дані відкриті: розміщення їх в глобальних електронних мережах уможливлює доступ до даних з будь-якого місця й дає змогу як постачальникам, так і користувачам документаційних послуг ігнорувати галузеві та національні закони та норми.
- Контроль за використанням електронних даних ненадійний: найважливішим засобом такого контролю є протоколи, що ведуться в електронному вигляді та уразливі щодо дії наведених вище факторів – так само, як і дані, користування котрими підлягає протоколюванню.

Специфічні фактори ризику. Вони зумовлені, наприклад, змістом та особливостями використання накопичуваних даних.

- Накопичення відомостей про особу. Комунікаційні системи і мережі акумулюють протоколи з фіксацією часу, тривалості контакту та обсягу переданих даних, відомості про місцезнаходження електронних пристроїв відправника та отримувача повідомлень тощо; після належної систематизації та аналізу вказані дані можуть дати широке уявлення про особу, що становить потенційну загрозу втручання в її приватну і соціальну сферу. Доступ до цих відомостей відкритий з огляду на загальні фактори ризику.
- Централізація даних. У процесі надання електронно-документаційних послуг часто створюються централізовані фонди документів; це логічне рішення для надання різноманітних послуг через один «електронний офіс» або в одному комунікаційному акті, проте таким чином ускладнюються систематизація фондів і контроль доступу до них, створюються вигідні умови для блокування низки електронно-документаційних послуг.
- Автоматизація процесів прийняття рішень. Постійне зростання кількості електронних документів і поява відповідного ПЗ зумовлює тенденцію до прийняття рішень за результатами машинного опрацювання документів; у багатьох випадках – насамперед у нестандартних ситуаціях – це може зашкодити інтересам користувача електронно-документаційної послуги.

Фактори ризику при наданні електронно-документаційних послуг. Дія цих факторів ґрунтується на тому, що такі послуги передбачають електронну комунікацію між сторонніми особами та власними комп'ютерними системами; це створює загрозу завдання шкоди документам або коректності роботи систем.

- Несанкціоноване втручання у процес надання електронно-документаційної послуги. У більшості випадків доступні електронні документи розташовують поза власною мережею; це вигідний спосіб уникнути несанкціонованого доступу до внутрішніх БД, проте за межами корпоративної мережі специфічні захисні механізми не діють.
- Ризики при використанні робочих програм. Недостатньо чітке розмежування прав роботи з БД або окремими категоріями документів може призвести до несан-кціонованого доступу: наприклад, якщо кілька користувачів мають один код доступу або з базою працюють люди, службові повноваження котрих не передбачають цього.
- Невідповідність систем безпеки. Нерегулярне оновлення призначених для захисту даних алгоритмів, обладнання і ПЗ, несистематична перевірка протоколів корис-

[13] Фахівці висловлюють сподівання, що результатом досліджень, здійснюваних у рамках ILM, стане цілковита автоматизованість або навіть непотрібність процесів міграції.

[14] Очікується, що впровадження системи електронного управління правами (Digitales Rechtemanage-ment, DRM) загострить проблему авторських прав в умовах періодичного копіювання або перенесення електронних даних при їхньому тривалому зберіганні. Див.: NESTOR.

[15] Bischoff: Ende der Aktenzeit? S. 1-2.

тування даними тощо становлять загрозу при наданні електронно-документаційних послуг.

Фактори ризику при пересиланні та використанні електронних документів. Відправнику та отримувачу електронних даних звичайно невідомі і непідвладні характеристики комунікаційних каналів, наприклад, якість кабельних мереж або кількість і розташування комп'ютерів-посередників; відтак постає ймовірність несанкціонованої зміни даних при передачі внаслідок навмисних дій або технічних помилок. Також через неправильну інсталяцію ПЗ, використання застарілих версій, вірусне ураження, фізичні або розумові вади людини та ін. можуть виникати проблеми при роботі з належним чином переданими та отриманими електронними документами.

Вимоги щодо надійності комунікаційних і документаційних систем.

Конфіденційність. Ця вимога передбачає захищеність документа від ознайомлення з ним сторонніх осіб – перш за все, під час пересилання. Механізм протидії – кодування електронних документів перед їхнім пересиланням адресату або на сервер для зберігання. Хоча ця технологія передбачає різні ступені захисту, звичайно використовують один алгоритм кодування – той, що забезпечує захист найважливіших документів. Гарантування конфіденційності значною мірою залежить від надійності призначеного для кодування ПЗ і комп'ютерного обладнання, електронних ключів тощо.

Цілісність. Відповідно до цієї вимоги, дані та інформація повинні надійти до зазначеного адресата неушкодженими і без змін[16]. Незалежно від природи несанкціонованих змін запропоновано два механізми протидії: електронний підпис, коди аутентифікації повідомлення (*Message Authentication Codes, MAC*). За їхньою допомогою на основі даних, що захищаються, можна утворювати кодовані додатки, що містять відомості про оригінальний документ та у разі його зміни засвідчать цей факт, проте не дадуть змоги ні визначити зміни, які відбулися, ні відновити документ.

Ідентифікація. Ця вимога передбачає ідентифікацію даних і комуніканта. 1. Ідентифікація даних покликана підтвердити, що документ складено або відправлено саме потрібною особою. 2. Ідентифікація комуніканта підтверджує, що партнер у комунікативному акті – дійсно особа, чиї реквізити наведено. Механізми ідентифікації – перевірка електронного підпису і *MAC*.

Незаперечність. Ця вимога так само, як і попередня, має дві складові: 1) незаперечність походження означає, що відправник електронного документа не зможе заперечити цей факт. Виконання цієї вимоги можливе завдяки електронному підпису; *MAC* у цьому випадку звичайно не застосовують, оскільки перевірка відповідності цих кодів складніша за перевірку підпису; 2) незаперечність отримання полягає у тому, що адресат не зможе заперечити цей факт після надходження документа. Технології електронного підпису дають змогу засвідчувати такий факт фіксацією часу надходження документа.

Є ще низка вимог щодо надійності комунікаційних і документаційних систем (для виконання котрих криптографічні методи непридатні або придатні частково): доступність (можливість повсякчасного використання технічних компонентів, наприклад, веб-серверу, що містить документи), підтримка форм і форматів документів, алгоритмів засвідчення та перевірки документів, знищення або блокування відомостей про користувачів у разі потрапляння цих даних до документальних фондів загального доступу, неможливість зберігання документів у таких фондах або в інших "тимчасових депозитаріях" понад визначений термін тощо.

Технології кодування та електронного підпису. У сфері електронного документообігу передбачено два види кодування: 1) перетворення тексту електронного документа на шифр (кодування файла); 2) захист електронних комунікацій на момент передавання даних (кодування каналу). Таємність кодування забезпечується не секретністю алгоритмів, а секретністю створюваних ними ключів – комбінацій електронних даних. Якщо для кодування і розкодування використовують один ключ, йдеться про симетричний метод, якщо різні (переважно це відбувається при використанні електронного підпису) – про асиметричний. Найвідоміші алгоритми симетричного кодування, що використовуються для захисту електронних документів, – *DES (Data Encryption Standard)*, *Triple-DES*, *AES (Advanced Encryption Standard)*, асиметричні – *RSA, ElGamal*. Найчастіше в умовах електронного документообігу вдаються до комбінованих алгоритмів кодування, користуючись перевагами обох методів.

Електронний підпис, згідно з європейськими законами, – це «дані в електронній формі, що додаються до інших електронних даних або логічно пов'язані з ними і призначені для ідентифікації»[17]. Практичний досвід використання електронного підпису дає підстави розширити це формулювання: завдання електронного підпису – реалізувати за допомогою технічних засобів основні ознаки і функції власноручного підпису, а саме: 1) функцію ідентифікації: автор документа – особа, чиє ім'я у ньому зазначено; 2) функцію підтвердження цілісності: поданий документ – справжній; 3) функцію підтвердження завершеності: версія документа остаточна; 4) функцію зобов'язання: документ підлягає ознайомленню і виконанню[18].

Технологію електронного підпису не можна вважати абсолютно надійною: вона фіксує несанкціоновані операції з документом, здійснені лише у відомий або передбачений спосіб. Асиметричні алгоритми накладання і перевірки електронного підпису – це, найчастіше, уже відомий *RSA, DSA (Digital Signature Algorithm)*. Технологіями електронного підпису допускається використання симетричного алгоритму *MAC* – переважно для гарантування цілісності документів, що зберігаються на сервері; для ініціалізації цього алгоритму потрібен тільки ключ автора (власника) документа, перевірці сторонніми особами такий ключ не підлягає, тому виконувати основну функцію електронного підпису – підтвердження авторства – *MAC* не в змозі.

Найпоширеніші нині технології захисту електронних документів – кодування та електронний підпис – стикаються з проблемою їхнього практичного застосування при архівації документів: алгоритми у зв'язку з розвитком цифрових технологій мають дуже обмежений «термін надійності» – значно коротший, ніж строк зберігання документів в архіві, і підлягають регулярній перевірці на розкодування та постійній модернізації[19].

[16] Вимога щодо збереження цілісності електронного документа є чинною для процесів не лише його пересилання, але й зберігання перед відправкою або після отримання. Див. E-Government-Handbuch: Phasenplan, Кар. 3.4.

[17] Див. Gesetz uber Rahmenbedingungen fur elektronische Signaturen.

[18] E-Government-Handbuch: Verschlusselung und Signatur.

[19] Для накладання і перевірки електронного підпису обрано такі математичні алгоритми, що за нинішніх технологій його підробка або непомітні маніпуляції із засвідченими документами практично виключаються. "Термін придатності" використовуваного методу було встановлено на шість років, його подовжують щороку на один рік – доки надійність методу не викликатиме сумнівів. Див. Erber-Faller, S. 15, 71.

Список використаної літератури

1. Abgabenordnung. http://bundesrecht.juris.de/ao_1977/index.html.
2. Bischoff, F.: Archivierung digitaler Unterlagen: Neue Anforderungen an die Archive. – Vortrag auf dem Hessischen Archivtag am 5.Juli 2000. – S. 1-2. http://www.stadtgeschichte-ffm.de/aktuelles/buecher/archivtag/archiv3.pdf.
3. Bischof, F.: Ende der Aktenzeit? – eine Herausforderung fur die Archivare – Erfahrungen eines Kommunalarchivars. http://www.stadtgeschichte-ffm.de/aktuelles/publikationen/archivtag/archivtag_1.html.
4. Borghoff, R.; Rodig, R.; Scheffszyk, S.: Langzeitarchivierung. Dpunkt Verlag, 2003; Hohmann, G.: Digitale Ewigkeit und virtuelle Museen. In: Telepolis. Heise-Verlag 30. Oktober 2003.
5. E-Government-Handbuch. http://www.bsi.de/fachthem/egov/6.htm.
6. Erber-Faller, S.: Elektronischer Rechtsverkehr. – Luchterhand Verlag: Neuwied, Kriftel, 2000.
7. Gesetz uber Rahmenbedingungen fur elektronische Signaturen. http:// bundesrecht. juris. de/sigg_2001.
8. Grundsatze ordnungsma?iger DV-gestutzter Buchfuhrungssysteme (GoBS). Schreiben des Bundesministeriums des Finanzen an die Oberfinanzbehorden der Lander vom 7.November 1995.
9. Handelsgesetzbuch. http://www.handelsgesetzbuch.de.
10. Henstorf, K.-G.; Kampffmeier, U.; Prochnow, J.: Grundsatze der Verfahrensdo-kumenta-tion nach GoBS. Code of Practice Band 2. VOI Verband Organisations- und Informa-tionssysteme e.V., Bonn, 1999.
11. Kampffmeier, U.; Rogalla, J.: Grundsatze der elektronischen Archivierung. Code of Practice Band 1. VOI Verband Organisations- und Informationssysteme e.V., Bonn, 2.Auflage 1996.
12. NESTOR Kompetenznetzwerk zur Langzeitarchivierung digitaler Quellen in Deutschland. http://www.langzeitarchivierung.de.
13. Netlexikon. http://www.lexikon-definition.de.
14. PK-DML Prufkriterien fur Dokumentenmanagement-Losungen. VOI Verband Organisations- und Informationssysteme e.V., Bonn, 2.Auflage 2004.

ЕЛЕКТРОННІ РЕСУРСИ БІБЛІОТЕК УКРАЇНИ В ІНФОРМАЦІЙНОМУ ЗАБЕЗПЕЧЕННІ НАУКИ: СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

НОВІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

На підставі аналізу наукових електронних ресурсів бібліотек України обґрунтовується роль бібліотек у формуванні масивів наукових знань та організації доступу до них. Визначаються основні електронні ресурси в системі наукових комунікацій. Також йдеться про доцільність створення корпоративних електронних каталогів, шляхи удосконалення їхнього довідково-пошукового апарату, формування електронних бібліотек на основі повнотекстового розширення електронних каталогів. Як перспективні напрями розвитку системи електронних ресурсів розглядаються репозитарії, наукові портали. Окреслюються головні завдання бібліотек України в умовах формування інформаційно-когнітивного електронного середовища

Г. Шемаєва

НАУКОВО-ІНФОРМАЦІЙНИЙ потенціал стає головним індикатором сучасного рівня соціально-економічного розвитку кожної країни. Саме цим зумовлено особливу увагу до науки та знань у світі. Знання виступають важливим інструментом підвищення ефективності наукової та іншої діяльності. Інформаційні ресурси і технології, що реалізуються, є основними рушійними силами суспільного прогресу в сучасних умовах.

Одним із головних чинників розвитку науки є здобуття знань, їхнє розповсюдження та використання, що досягається в умовах сьогодення, в основному, шляхом доступу до наукових електронних ресурсів. Можна стверджувати, що наука в Україні все ще відчуває значний інформаційний голод. Про це свідчить ряд факторів.

По-перше, вітчизняні бібліотеки майже не комплектуються науковими виданнями зарубіжних країн.

По-друге, незважаючи на низку заходів на різних рівнях щодо організації доступу до світових наукових електронних ресурсів (програма "Електронна інформація для бібліотек", європейський проект INTAS "Доступ до електронних журналів для вчених нових незалежних держав" – видавництв EBSCO, Springer, Blackwell Science), більшість українських вчених не знають про таку можливість одержання інформації.

По-третє, немає цілісної системи представлення інформації в Інтернеті стосовно наукових досягнень України та надання доступу до них.

По-четверте, відсутні єдині методичні та методологічні основи функціонування системи електронних наукових комунікацій.

Розв'язання зазначених проблем вбачається у створенні сучасної ресурсної бази інформаційного забезпечення науки України з потужною пошуковою системою на засадах Інтернет-технологій, яка, з одного боку, буде інтегратором української наукової думки, а з другого – основною складовою системи наукових комунікацій. Головним компонентом такої бази мають стати наукові електронні ресурси бібліотек країни на національному, регіональному, галузевому, спеціалізованому рівнях, що потребує їхнього вивчення, аналізу стану та визначення перспектив розвитку.

Напрями розвитку системи наукових комунікацій накреслено у Державній програмі "Інформаційні та комунікаційні технології в освіті і науці" на 2006-2010 роки, ухваленій Кабінетом Міністрів України у 2005 році, а також у рамках затвердженої на факультеті бібліотекознавства та інформатики Харківської державної академії культури комплексної наукової теми досліджень "Бібліотечно-інформаційне забезпечення науки, виробництва, освіти та культури".

Про актуальність проблеми створення, представлення електронних ресурсів бібліотек України в Інтернеті