УДК 003.26:004.056.55 (045) **С.В. Толюпа, О.О. Гаврилюк**

СИСТЕМА ЗАХИСТУ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ НА ОСНОВІ ЗАСТОСУВАННЯ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

У статті досліджено систему забезпечення захисту електронного документообігу на базі Lotus Notes; досліджена структура та функціональні особливості системи електронного документообігу; реалізовано систему забезпечення захисту електронного документообігу на базі Lotus Notes. Запропонована удосконалена СЕД на базі LOTUS DOMINO/NOTES, що може бути використаною у діяльності реального підприємства для підвищення ефективності його роботи.

Ключові слова: електронний документообіг, ЕЦП, Lotus Notes, система захисту.

Постановка проблеми

XXI сторіччя зарекомендувало себе як вік інформаційних технологій тому не дивно, що кількість і обсяги використовуваних в сучасному світі електронних документів ростуть. Тому з кожним роком у всьому світі зростає кількість проектів, згідно з якими процеси обміну паперовими документами стають не тільки неефективними, а й неможливими. При цьому варто зазначити, що однією з основних вимог до електронних документів є наявність можливості перевірити їх цілісність, одним із способів забезпечення цього- є електронно цифровий підпис (ЕЦП).

Мета статті

Метою даної статті є аналіз системи забезпечення захисту електронного документообігу для корпоративних інформаційних ресурсів на базі програми Lotus Notes

Основні матеріали дослідження

Запуск будь-якої комплексної інформаційної системи вимагає не тільки установки обладнання і настроювання програмного засобу, але і перебудови бізнес-процесів і перенавчання службовців. Чим нижче обсяг зміни бізнес-процесів при впровадженні системи – тим вище шанс дотримання строків впровадження, а інколи і взагалі запуску системи. Тому комплексні інформаційні системи завжди впроваджують поодинці, послідовно автоматизуючи відносно замкнуті сфери діяльності, згодом поєднуючи їх інтеграційною системою.

З технологічної точки зору система електронного документообігу являє собою інтеграційну систему, що охоплює діловодство і підготовку документів і поєднує їх із зовнішнім середовищем електронного обміну. Таким чином, для підвищення шансів завершення автоматизації органу влади в необхідний строк треба попереднє впровадження систем автоматизованого діловодства і засобів організації колективної роботи при підготовці документів.

Основною технологічною проблемою для державних службовців при переході до електронного документообігу є використання електронного аналога власноручного підпису на документах. Без розуміння і впровадження цієї технології неможливо перейти на цілком безпаперову обробку документів в органах державної влади і місцевого самоврядування.

Повного переводу прийому вхідних і розсилання вихідних документів на безпаперову технологію не потрібно. Подібне обмеження може бути порушенням прав окремих громадян, що не мають доступу до засобів обчислювальної техніки та Інтернету. Класичні функції реєстрації вхідних паперових документів із традиційними підписами заявників також є атрибутами системи електронного документообігу. Це необхідно для скасування «інформаційної нерівності» [1]. Як вже йшлося вище, електронний документообіг – це сукупність нових технологій роботи з документами. Застосовувані технології дозволяють

організувати «безшовну» взаємодію систем, що забезпечують різні операції обробки документів.

У першу чергу до таких технологій можна віднести:

- технології розпізнавання текстів, що трансформують паперові вхідні документи в цілком електронну форму представлення;
- електронний аналог власноручного підпису;
- засоби передачі даних;
- засоби збереження електронної інформації [2, 3, 4, 1].

Перераховані технології дозволяють підсистемам, що виконують різні функції, органічно доповнювати одна одну. Подібна взаємодія дозволяє різко підвищити ефективність праці держслужбовців при роботі з документами [5, 6].

Електронний документообіг дозволяє створити в органі влади єдиний інформаційний простір, інтегруючи в інформаційний вузол усі документальні системи. Інтеграція здійснюється без втрати якості роботи з документами, зі збереженням традицій російського діловодства.

Основа подібної інтеграції — надійне сховище документів і взаємодіючі з ним системи документообігу. Всі оброблювані документи зберігаються в єдиному сховищі, що дозволяє за [5, 2]

Схема взаємодії систем електронного документообігу з єдиним сховищем документів органу влади на прикладі найбільш протяжного циклу обробки документів відображена на рис. 1. Під найбільш протяжним циклом мається на увазі випадок, що коли вхідний документ породжує підготовку вихідного документа, що включає аналіз архівних документів і внутрішніх робочих матеріалів [7].

Усі ці операції регламентовані загальнодержавними і відомчими інструкціями з діловодства і виконуються за допомогою системи автоматизованого діловодства та електронного документообігу (скорочено — САДЕД).

Система також автоматизує операції [5, 6]:

- узгодження проекту внутрішнього чи вихідного документа;
- затвердження внутрішнього чи вихідного документа;
- розсилання і публікації документів.

Це обумовлено необхідністю використання в перерахованих вище операціях електронного аналога власноручного підпису і криптозахисту. Обидві ці технології регламентовані федеральним законодавством і повинні здійснюватися за допомогою ПЗ, що має необхідні сертифікати. Однак робота з архівними документами є важливим етапом при підготовці нових матеріалів. Інтеграція архіву електронних документів у єдиний інформаційний простір органу влади дозволить зробити доступ до архівних матеріалів оперативним і ефективним.

Інші відображені на рис. 1. операції:

- підготовка текстів документів;
- підтримка робочих матеріалів (інформаційні документи, довідники, статті, загальні списки, розклади тощо) і єдиних шаблонів документів;
- підтримка бази нормативно-довідкової інформації і керівних матеріал — оперують «неофіційними» документами, робота з якими не регламентована загальнодержавними чи відомчими інструкціями. На даний момент у більшості органів влади і місцевого самоврядування дані операції вже виконуються із застосуванням ЗОТ. Задача автоматизованої системи — організувати ефективну колективну роботу над текстами документів і надати кожному держслужбовцю насичений інформаційний простір для забезпечення діяльності.

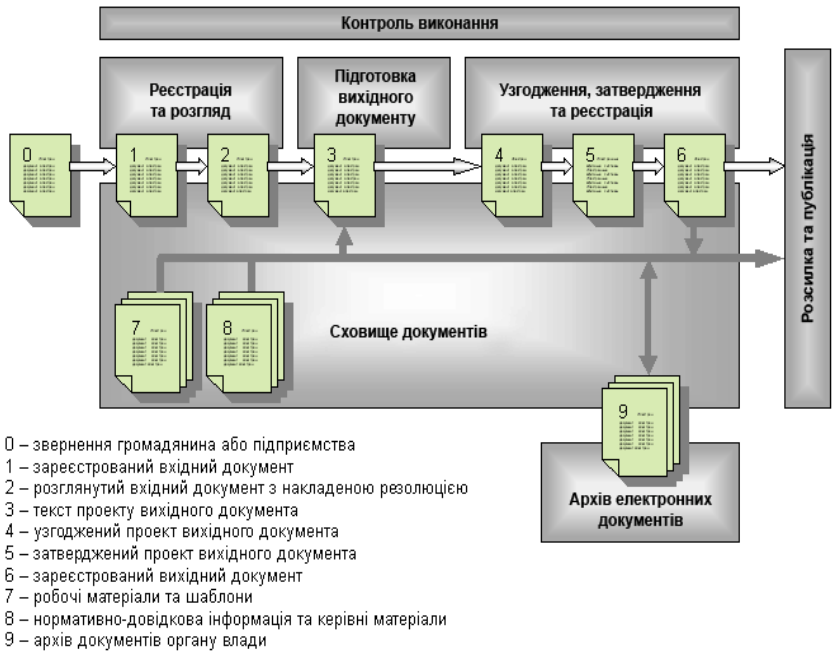

Рис.1. Схема електронного документообігу

Основною метою при розробці технологій електронного документообігу було досягнення максимальної наступності правил і прийомів паперового документообігу і журнально-картотечного діловодства, що дозволяє забезпечити безболісний перехід від традиційних технологій до сучасних.

Технологію електронного документообігу підтримують наступні функціональні можливості системи [5, 6]:

- реєстрація в автоматизованому режимі переданих електронною поштою або через Інтернет-портал вхідних документів, у тому числі таких, що мають електронний цифровий підпис (ЕЦП) і криптозахист;
- сканування і розпізнавання паперових документів;
- прикріплення до реєстраційної картки (РК) електронного образу документу у вигляді файлу (файлів) будь-якого формату;
- розмежування прав доступу до прикріплених файлів електронного образу документу;
- надання кожній посадовій особі — учаснику діловодного процесу — свого особистого віртуального кабінету, чим досягається доступ посадової особи тільки до документів, що відноситься до її компетенції;
- розсилання електронних документів і доручень по них по мережі (по кабінетах посадових осіб);
- забезпечення процесу узгодження (візування) проектів документів;
- повнотекстовий і атрибутивний пошук електронних документів, включаючи віддалений повнотекстовий пошук;
- відправлення електронною поштою або публікація на Інтернет-порталі органу влади електронних вихідних документів (з використанням будь-якої електронної пошти, що підтримує MAPI), захищених ЕЦП і шифруванням за допомогою сертифікованих засобів;
- формування і оформлення справ, тобто групування виконаних документів у справи відповідно до номенклатури справ і систематизацією документів всередині справи;
- архівне збереження електронних документів, справ органу влади [8].

Програма електронного документообігу з використанням ЕЦП на сьогодні активно впроваджується в державних установах і органах державної влади, що істотно розширює можливості застосування ЕЦП і розвиток електронного документообігу в Україні.

Електронний цифровий підпис функціонально аналогічний звичайному рукописному підпису на папері і володіє всіма його основними перевагами:

- засвідчує, що підписаний документ надходить від особи, що його підписала;
- гарантує цілісність підписаного документа (захист від модифікацій);
- не дає можливості особі, що підписала документ, відмовитися від зобов'язань, пов'язаних з підписаним документом [9].

Безпека використання ЕЦП забезпечується тим, що засоби, які використовуються для роботи з ЕЦП, проходять експертизу та сертифікацію в Департаменті спеціальних телекомунікаційних систем СБУ, що гарантує неможливість злому і підробки ЕЦП.

Функціональні особливості системи

Система захисту у складі користувач-сервер призначена для:

- автентифікації користувачів системи при підключенні до сервера та забезпечення конфіденційності і цілісності даних, які передаються між користувачами та сервером;
- забезпечення цілісності та неспростовності авторства електронних даних та документів, що циркулюють у системі, з використанням електронного цифрового підпису.

Зазначені функції система виконує шляхом застосування механізмів криптографічного захисту інформації, яка обробляється у системі.

Автентифікація користувачів системи на сервері здійснюється під час підключення користувачів до сервера (встановлення з'єднання з сервером) шляхом реалізації протоколу взаємної автентифікації сторін. Забезпечення конфіденційності та цілісності інформації, яка передається між користувачем та сервером системи під час їх взаємодії, реалізується шляхом шифрування інформації та формування і перевіряння криптографічних контрольних сум.

Забезпечення цілісності та неспростовності авторства електронних даних та документів, що циркулюють у системі, реалізуються шляхом формування та перевіряння електронного цифрового підпису від даних та документів, як на стороні користувача системи так і на стороні сервера.

Система в цілому відноситься до типу апаратно-програмних комплексів КЗІ виду «Б», категорії «Ш», «П» та «Р2, класу Б2. Окремі засоби, що входять до його складу, відносяться до типів апаратно-програмних та програмних засобів КЗІ видів «Б» та «В», категорії «Ш», «П» та «Р» класу Б2.

Найвищий гриф обмеження доступу інформації, яка може захищатися засобами системи – конфіденційна, що не є власністю держави.

Для організації ключової системи (управління ключовими даними) засобів системи використовується центр сертифікації ключів.

Розробка структури системи

Структурна схема комплексу захисту наведена на рис. 2.

До складу комплексу входять:

- програмні засоби (бібліотеки) КЗІ (користувача ЦСК);
- апаратні засоби КЗІ.

Програмні засоби КЗІ реалізують логіку роботи комплексу та інтегровані безпосередньо у користувальницьку та серверну частини системи (користувача та сервер), через визначені інтерфейси.

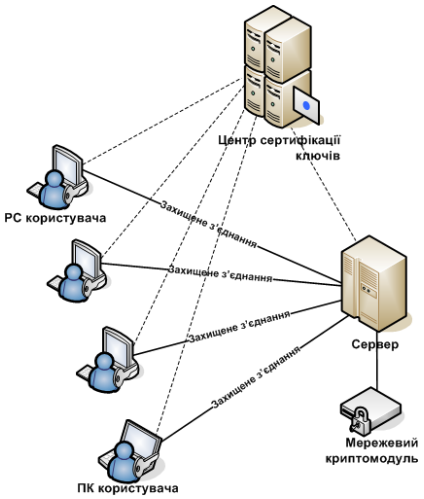

Рис. 2. Структурна схема комплексу у складі системи

Програмні засоби КЗІ комплексу можуть використовувати зовнішні апаратні засоби КЗІ, такі як електронні ключі, мережні криптомодулі тощо.

До складу апаратних засобів комплексу можуть входити:

- електронний ключ;
- мережний криптомодуль

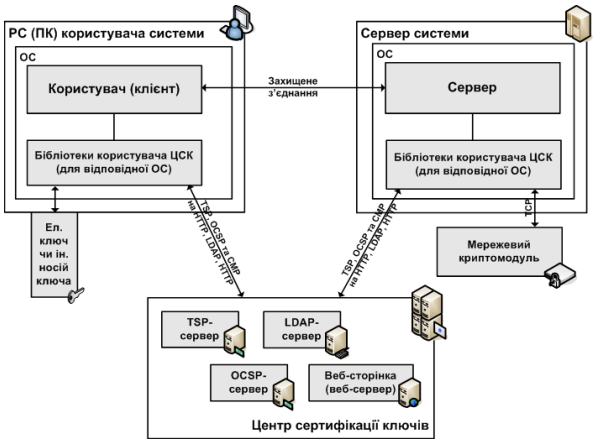

Рис. 3. Функціональна схема комплексу у складі системи

До складу комплексу входять:

- програмні засоби (бібліотеки) КЗІ (користувача ЦСК);
- апаратні засоби КЗІ.

Програмні засоби КЗІ реалізують логіку роботи комплексу та інтегровані безпосередньо у користувальницьку та серверну частини системи (користувача та сервер), через визначені інтерфейси.

Програмні засоби КЗІ комплексу можуть використовувати зовнішні апаратні засоби КЗІ, такі як електронні ключі, мережні криптомодулі тощо.

До складу апаратних засобів комплексу можуть входити:

- електронний ключ;
- мережний криптомодуль .

Бібліотеки користувача центру сертифікації ключів (ЦСК) призначені для використання в якості базових засобів КЗІ та виконують наступні функції у їх складі:

- роботу з носіями ключової інформації (зчитування особистих ключів з носіїв);
- роботу з файловим сховищем сертифікатів та списків відкликаних сертифікатів (СВС), що включає: зчитування сертифікатів та списків відкликаних сертифікатів із файлового

сховища; визначення статусу сертифіката за допомогою списків відкликаних сертифікатів; завантаження списків відкликаних сертифікатів з веб-сторінки ЦСК (з веб-серверу ЦСК);

- зашифрування та розшифрування даних;

- формування та перевірку ЕЦП від даних;

- захист сеансів передачі даних (захист з'єднань), що включає: реалізацію протоколу взаємної автентифікації сторін під час встановлення сеансу захищеної передачі даних (захищеного з'єднання); захист (шифрування та контроль цілісності) сегментів захищеної передачі даних (даних захищеного з'єднання);

- інтерактивну перевірку статусу сертифікатів у ЦСК за протоколом OCSP (через OCSP-сервер ЦСК);

- пошук сертифікатів у LDAP-каталозі ЦСК (на LDAP-сервері ЦСК);

- отримання позначок часу у ЦСК (через TSP-сервер ЦСК) тощо.

Бібліотеки користувача ЦСК інтегруються зазначену у систему (та інші прикладні системи) через визначені інтерфейси та реалізовані для ОС Microsoft Windows 98/2000/XP/2003 Server/2008 Server/7, ОС Microsoft Windows Mobile 5/6/6.5, Linux (SUSE/Red Hat/Slackware та ін.), UNIX (AIX/Solaris/BSD та ін.) у вигляді бібліотек підключення (DLL/COM, SO) або у вигляді java-аплетів (J2SE/J2ME).

Електронний ключ призначений для апаратної реалізації криптографічних перетворень усередині пристрою у складі засобів користувача системи.

Мережевий криптомодуль призначений для апаратної реалізації криптографічних перетворень усередині модуля у складі сервера системи.

Розміщення складових частин комплексу на технічних засобах системи

На сервері системи встановлюються та використовуються наступні складові частини комплексу:

- програмний комплекс захисту сервера, який включає бібліотеки користувача ЦСК (для відповідної серверної ОС);

- апаратний засіб КЗІ – криптомодуль мережі .

На засобах користувачів системи (робочих станціях чи портативних комп'ютерах – РС та ПК) встановлюються та використовуються наступні складові частини комплексу:

- програмний комплекс захисту користувача, який включає бібліотеки користувача ЦСК (для відповідної ОС);

- апаратний засіб КЗІ – електронний ключ.

Інсталяційні пакети програмних засобів комплексу

Програмні засоби комплексу передаються на об'єкт впровадження у вигляді інсталяційних пакетів на оптичному компакт-диску. Формат інсталяційного пакету залежить від цільової ОС.

До складу інсталяційних пакетів входять:

- інсталяційний пакет з програмним комплексом захисту сервера;

- інсталяційний пакет з програмним комплексом захисту користувача.

До складу кожного з інсталяційних пакетів входить комплект експлуатаційних документів на відповідні програмні комплекси у електронному вигляді.

Опис апаратних засобів

Електронний ключ призначений для:

- автентифікації користувача системи перед початком роботи;

- зберігання та захисту особистого ключа користувача;

- апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні користувача.

Електронний ключ має електричний USB-інтерфейс для підключення до ПЕОМ.

Апаратна реалізація електронного ключа забезпечує захищеність виконання усіх криптографічних перетворень усередині пристрою та унеможливлює доступ до особистих ключів користувача з боку ПЕОМ користувача.

Мережевий криптомодуль призначений для:

- автентифікації сервера системи перед початком роботи;

- зберігання та захисту особистого ключа сервера;

- апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні сервера.

Мережевий криптомодуль має мережевий електричний інтерфейс Ethernet 100/1000 для підключення до сервера системи безпосередньо або через комутатори локальної обчислювальної мережі.

Апаратна реалізація мережевого криптомодуля забезпечує захищеність виконання усіх криптографічних перетворень усередині модуля та унеможливлює доступ до особистих ключів сервера з боку ЕОМ сервера системи.

Опис рішень щодо криптографічного захисту інформації

У засобах системи використовуються такі криптографічні алгоритми та протоколи:

- алгоритм шифрування за ДСТУ ГОСТ 28147:2009 (режим простої заміни, режим гамування та режим вироблення імітовставки);

- алгоритм ЕЦП за ДСТУ 4145-2002;

- алгоритм гешування за ГОСТ 34.311-95;

- протокол розподілу ключових даних Діффі-Хелмана в групі точок еліптичної кривої (направлене шифрування).

Протокол розподілу ключових даних реалізований згідно методики розподілу ключових даних на основі протоколу Діффі-Хелмана в групі точок еліптичної кривої, яка погоджена з Державною службою спеціального зв’язку та захисту інформації України і відповідає вимогам ДСТУ ISO/IEC 15946-3. Генерація ключових даних виконується згідно методики генерації ключових даних, яка погоджена з Державною службою спеціального зв’язку та захисту інформації України.

Протокол встановлення захищеного сеансу передачі даних реалізовано на основі протоколу взаємної автентифікації з двома проходами згідно стандарту ДСТУ ISO/IEC 9798-3. Протокол взаємної автентифікації включає:

- формування користувачем та передачу даних автентифікації (запиту) на сервер, при цьому користувач виконує наступні дії: генерує випадкове число; підписує випадкове число та власний сертифікат (за необхідності) власним особистим ключем ЕЦП; передає сформовані дані автентифікації (запит) на сервер;

- обробку запиту від користувача сервером, при цьому сервер виконує наступні дії: отримує дані автентифікації від користувача;

- здійснює пошук (за відсутності сертифіката у запиті) та перевірку чинності сертифіката користувача; перевіряє ЕЦП на даних; у разі успішної обробки отриманих даних автентифікації – генерує сеансові ключі шифрування та вектори початкової ініціалізації; підписує отримане випадкове число та сеансові ключі з векторами початкової ініціалізації власним особистим ключем ЕЦП; зашифровує сформовані дані разом з ЕЦП спрямовано на користувача; передає підписані та зашифровані дані автентифікації (відповідь) користувачу;

- прийом та обробку відповіді користувача від сервера, при цьому користувач виконує наступні дії: отримує відправлені дані автентифікації (відповідь) від сервера; здійснює пошук та перевірку чинності сертифіката сервера; розшифровує дані автентифікації; перевіряє ЕЦП на даних;

- перевіряє відповідність випадкового числа у отриманих даних; у разі успішної обробки отриманих даних автентифікації (відповіді) завершує роботу протоколу.

Структурно-функціональна схема взаємодії користувача та сервера наведена на рис. 4.

За результатом роботи протоколу на сервері та користувачеві встановлюються два сеансових ключа та два вектори початкової ініціалізації для поточного шифрування даних у захищеному з'єднанні у дуплексному режимі. Шифрування даних у захищеному з'єднанні здійснюється за алгоритмом шифрування згідно ДСТУ ГОСТ 28147:2009 у режимі гамування. В якості криптографічної контрольної суми для контролю цілісності даних у захищеному з'єднанні використовуються імітовставки, які обчислюються за алгоритмом шифрування згідно ДСТУ ГОСТ 28147:2009 у режимі вироблення імітовставки.

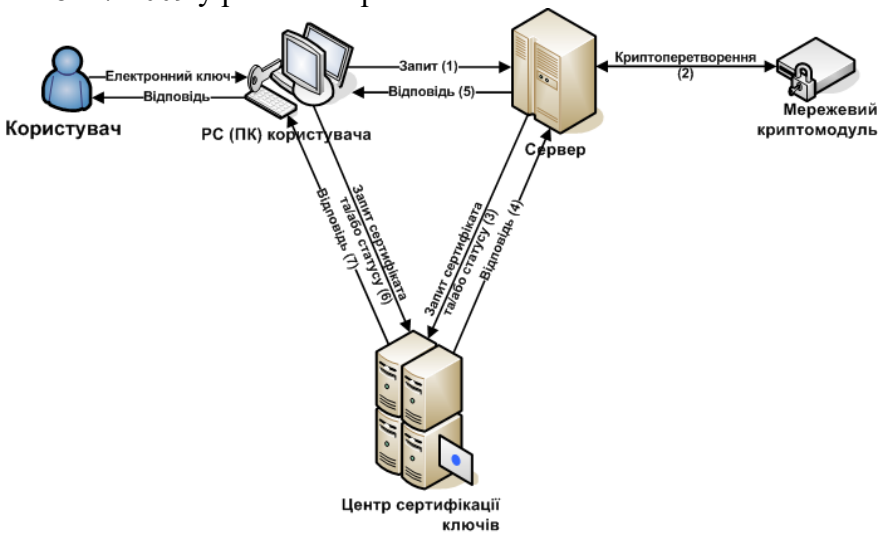

Рис. 4. Структурно-функціональна схема взаємодії користувача та сервера

Шифрування даних та обчислення імітовставок у захищеному з'єднанні здійснюється на основі сеансових ключів та векторів початкової ініціалізації (синхромаркерів), які розподіляються між користувачем та сервером у результаті виконання протоколу взаємної автентифікації.

Склад та організація ключової системи

Організацію ключової системи засобів комплексу виконує центр сертифікації ключів (ЦСК).

У комплексі використовуються дві підгрупи ключових даних:

- ключові дані ЦСК;

- ключові дані користувачів та сервера системи.

До складу ключових даних ЦСК відносяться сертифікати ЦСК та серверів ЦСК (TSP-сервера та OCSP-сервера), які використовуються для перевірки ЕЦП сертифікатів, списків відкликаних сертифікатів, позначок часу тощо.

До ключових даних користувачів та сервера системи відносяться особисті ключі та сертифікати відповідно користувачів та сервера.

Параметри еліптичних кривих для алгоритму ЕЦП ДСТУ 4145-2002, та довгострокові ключові елементи (ДКЕ) для алгоритму шифрування ДСТУ ГОСТ 28147:2009, постачаються відповідно до вимог Держспецзв'язку України.

Окрім електронних ключів, в якості носіїв ключової інформації для особистих ключів користувачів можуть використовуватися:

- гнучкі диски 3,5” (дискети);
- електронні диски (flash-диски);
- компакт-диски (CD-R, CD-RW, DVD-R або DVD-RW);
- інші електронні ключі: Технотрейд uaToken; Aladdin eToken R2, PRO; Актив ruToken; Автор SecureToken; CIC Almaz; смарт-карти Aladdin, Автор, Криптомаш, та інші модулі з бібліотеками підтримки.

Формати ключових даних та іншої спеціальної інформації відповідають вимогам міжнародних стандартів, рекомендацій та діючих нормативних документів, а саме:

- формати сертифікатів та списків відкликаних сертифікатів згідно технічних специфікацій форматів представлення базових об’єктів національної системи ЕЦП (затверджені спільним наказом ДСТСЗІ СБ України і Держзв’язку України від 11.09.2006 р. за № 99/166);
- формати захищених даних (даних з ЕЦП та зашифрованих даних) – згідно міжнародних технічних рекомендацій RFC 3630 (PKCS#7) та проекту технічних специфікацій національної системи ЕЦП;
- формати запитів на отримання інформації про статус сертифіката та інформації про статус – згідно міжнародних технічних рекомендацій RFC 2560 та проекту технічних специфікацій національної системи ЕЦП;
- формати запитів на формування позначок часу та самих позначок часу – згідно міжнародних технічних рекомендацій RFC 3161 та проекту технічних специфікацій національної системи ЕЦП.

Опис взаємодії з центром сертифікації ключів

ЦСК призначений для обслуговування сертифікатів відкритих ключів користувачів та сервера системи, надання послуг фіксування часу, а також надання (за необхідності) користувачам системи засобів генерації особистих та відкритих ключів.

ЦСК забезпечує:

- обслуговування сертифікатів користувачів та сервера системи, що включає: реєстрацію користувачів та сервера; сертифікацію відкритих ключів користувачів та сервера; розповсюдження сертифікатів; управління статусом сертифікатів та розповсюдження інформації про статус сертифікатів;
- надання послуг фіксування часу;
- надання користувачам системи (за необхідності) засобів генерації особистих та відкритих ключів

Для взаємодії з центром сертифікації ключів (використання його інтерактивних служб) користувачі та сервери системи повинні мати можливість мережевого підключення до ЦСК. Усі механізми взаємодії з ЦСК виконують бібліотеки користувача ЦСК.

Структурно-функціональна схема комплексу у складі системи із зазначеним порядком взаємодії з ЦСК наведена на рис. 5.

Зміна статусу сертифікатів (блокування, поновлення або скасування) та знищення особистих ключів користувачів та сервера системи здійснюється у відповідності до порядку, який визначений ЦСК (згідно регламенту ЦСК).

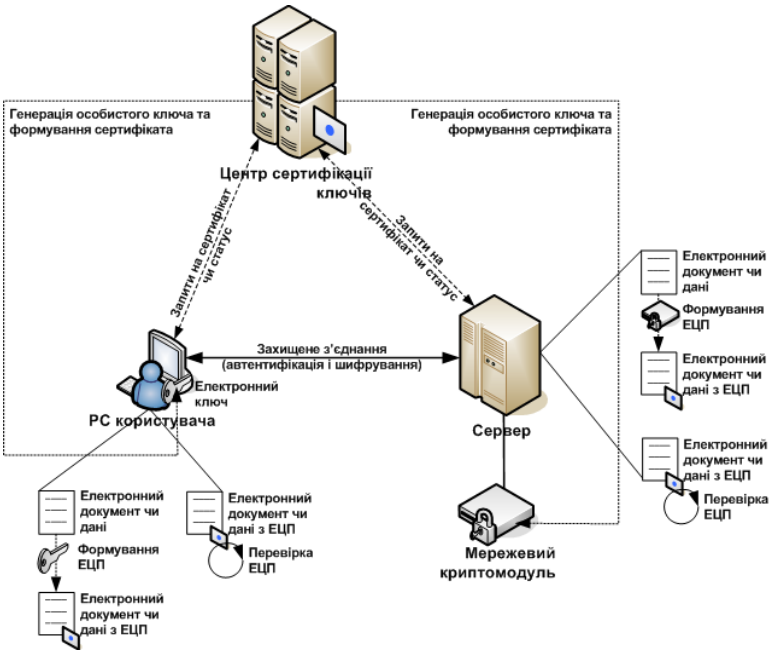

Рис. 5. Структурно-функціональна схема системи

Висновки

У статті досліджено систему забезпечення захисту електронного документообігу на базі Lotus Notes; досліджена структура та функціональні особливості системи електронного документообігу; реалізовано систему забезпечення захисту електронного документообігу на базі Lotus Notes.

З технологічної точки зору система електронного документообігу являє собою інтеграційну систему, що охоплює діловодство і підготовку документів і поєднує їх із зовнішнім середовищем електронного обміну.

Практична цінність роботи полягає у тому, що запропонована удосконалена СЕД на базі LOTUS DOMINO/NOTES, що може бути використаною у діяльності реального підприємства для підвищення ефективності його роботи.

Література

1. Нестеренко О.В. Теоретичні та методологічні основи побудови автоматизованих інформаційно-аналітичних систем органів державної влади. Автореферат ... доктора техн. наук / НАН України. Національна бібліотека України ім. В. І. Вернадського. – К., 2006. – 41 с.

2. Джефф С. Документооборот по сети Internet // ComputerWorld Россия. – 1996. – 243 с.

3. Жовтенко В. В. Формування системи документальних ресурсів електронного урядування: досвід зарубіжних країн щодо її впровадження // Документознавство. Бібліотекознавство. Інформаційна діяльність: проблеми науки, освіти, практики: Зб. матеріалів III Міжнар. наук.-практ. конф., Київ, 16-18 травня 2006 р. / Редкол.: Г.В. Боряк, Г.В. Власова, Л.А. Дубровіна, М.С. Слободяник та ін. – К. : 2006. – С. 21-23

4. Колесов А. Автоматизация документооборота в Восточной Сибири // PCWeek/RE, Проекты. – 1997. – № 39 (113). – С. 71–81.

5. Гавриш С. ДІЛО – система автоматизації діловодства та електронного документообігу // Довідник секретаря та офіс-менеджера. – 2007. – № 2. – С. 25–31.

6. Правила посиленої сертифікації. Затверджені наказом ДСТСЗІ СБ України №3 від 13.01.2005 р. та зареєстрованих в Міністерстві юстиції України за №104/10384 від 27.01.2005 р.

7. Козоріз В.П., Лаписька Н.І. Загальне і кадрове діловодство: навч. Посіб. – К.: МАУП, 2002. – 128 с.

8. Кулешів С.Г. Управлінське документознавство: навч. посіб. – К.: ДАКККіМ, 2003. – 229 с.

9. Чирський Ю. Електронний цифровий підпис: правові аспекти застосування // Довідник секретаря та офіс-менеджера. – 2007. – № 1. – С. 17–22.

Надійшла 26.11.2016 р. Рецензент: д.т.н., проф. Дружинін В.А.