

УДК 004.02

ОРГАНІЗАЦІЯ ЗАХИЩЕНОГО ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В МЕРЕЖАХ ЕЛЕКТРОННОГО УРЯДУВАННЯ

¹Гарасим О.Р., ¹Комова М.В., ²Литвин В.В.

Національний університет «Львівська політехніка»

¹Кафедра історії, теорії та практики культури

²Кафедра інформаційних систем та мереж

E-mail: garasym-oleg@rambler.ru

Анотація

Гарасим О.Р., Комова М.В., Литвин В.В. Організація захищеного електронного документообігу в мережах електронного урядування. В статті проводиться аналіз проблем побудови мереж електронного урядування та досліджується комплексний підхід до захисту електронного документообігу. Проведений аналіз програмного та апаратного забезпечення з метою вибору оптимального рішення проблеми витоку інформації з мережі електронного урядування. Розглянуто систему засобів і методів інформаційної взаємодії між урядом і громадянами/організаціями з метою створення ефективної системи зворотного зв'язку.

Загальна постановка проблеми. Технології електронного документообігу повинні вдосконалюватись згідно із загальними тенденціями розвитку телекомунікації з метою створення єдиного інформаційного простору та забезпечення інформаційної взаємодії споживачів із врахуванням аспектів інформаційної безпеки. Традиційні мережі загального користування еволюціонують: відбувається поступовий перехід від спеціалізованих систем і мереж зв'язку (телефонних, телеграфних, телексних, передавання даних) до мультисервісних та поліфункціональних мереж наступного покоління (NGN – Next Generation Network). Для NGN характерними рисами є пакетизація, цифровізація, конвергенція, універсалізація інформаційних та телекомунікаційних технологій, зростання кількості та якості інформаційних і телекомунікаційних послуг, загострення питання забезпечення захисту інформації.

Задачі дослідження. Системи захищеного електронного документообігу можуть існувати або як окрема Національна система конфіденційного зв'язку, або як підсистема гарантованого транспортування електронних документів та телекомунікаційної підтримки інтегрованої автоматизованої системи, що забезпечує вироблення рішень на основі автоматизації інформаційної діяльності, – а саме діє система електронного документообігу в самій галузі телекомунікацій.

При організації захищеного електронного документообігу виникає проблема узгодження методів та засобів захисту інформації різних компонентів документальних телекомунікацій, таких як: інформаційні ресурси, прикладні програми, телекомунікаційні протоколи тощо. Обладнання, лінії зв'язку та відповідні споруди повинні бути захищеними від несанкціонованого доступу. Дотримання комплексного підходу для забезпечення інформаційної безпеки зумовлює необхідність створення мережевої інфраструктури інформаційної безпеки.

Аналіз останніх досліджень та публікацій.

Технологічне забезпечення повинне бути націлене на створення комплексної системи забезпечення інформаційної безпеки (КСЗІБ). Склад КСЗІБ залежить від структури і складу системи зв'язку, але в загальному випадку включає наступні підсистеми:

- захист від витоку конфіденційної інформації;
- захист від вірусів і спаму;

- аналіз вразливостей;
- виявлення та запобігання втручань;
- міжмережеве екранування;
- розмежування доступу;
- криптографічний захист;
- моніторинг інформаційної безпеки.

Напрямок «Е-урядування. Е-демократія» в Україні є частиною програми МФВ (Міжнародний валютний фонд) «Посилення впливу громадянського суспільства». Завданнями напряму згідно затверджених Стратегії діяльності програми на 2007 рік та Звіту про реалізацію стратегії на 2008-2010 рік було «створення Українського центру розвитку електронного урядування та Регіонального центру розвитку електронного урядування в АР Крим та підтримка діяльності впродовж трьох років після створення».

Впродовж 2007-2009 років МФВ ініційовано та підтримано ряд комплексних і системних заходів на розбудову електронного урядування та становлення електронної демократії в Україні, які направлені на:

- організацію та проведення досліджень, аналізу та вироблення рекомендацій;
- вдосконалення нормативно-правового забезпечення;
- взаємодію із органами державної влади та місцевого самоврядування. Лобіювання та підтримку змін у державній політиці та управлінні процесами;
- створення Українського центру розвитку електронного урядування;
- створення та діяльність Регіонального центру розвитку електронного урядування в АР Крим;
- підтримку пілотних проектів з відпрацювання можливостей взаємодії органів місцевого самоврядування та громадськості;
- посилення впливу діяльності громадських об'єднань та недержавних громадських організацій;
- залучення та налагодження партнерства із міжнародними організаціями, провідними бізнес-структурами та іншими установами;
- презентація ініціатив та проектів МФВ.

Суть е-урядування полягає в застосуванні досягнень інформаційно-комунікаційних технологій до організації управління державою та взаємодії органів влади всіх рівнів з громадянами, громадськими організаціями, підприємцями. Е-урядування є невід'ємною складовою інформаційного суспільства і не може бути реалізованим без активної участі всіх зацікавлених у ньому сторін – органів державної влади та місцевого самоврядування, підприємств всіх форм власності, громадських організацій та громадян.

На сьогодні у світі не існує єдиної загальноприйнятої моделі е-урядування. Існує лише набір загальних вимог, яких повинні дотримуватись органи влади, громадяни та бізнес-структури, реалізуючи свої функції чи здійснюючи свої права у взаємовідносинах один з одним. Усіх користувачів адміністративних послуг об'єднує одне спільне прагнення – отримати більш ефективні засоби доступу до інформації, до послуг, щоб зменшити витрати часу, матеріальних та людських ресурсів, зробити взаємодію з органами влади простішою, швидшою та зручнішою, збільшити вплив суспільства на прийняття рішень.

Ухвалення Законів України «Про телекомунікації», «Про електронний цифровий підпис» та «Про електронні документи та електронний документообіг», а також низки указів Президента України й Постанов Кабінету Міністрів України «Про заходи щодо розвитку національної складової глобальної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні», «Про заходи щодо створення електронної інформаційної системи «Електронний Уряд» створило нову нішу в галузі телекомунікацій, що потребує перегляду підходів до побудови системи електронного документообігу. Технології електронного

документообігу застосовуються у сферах державної, суспільної та особистої діяльності, зокрема в системах:

- електронного документообігу та електронного цифрового підпису;
- державного управління «Електронний уряд»;
- електронних платежів – у діяльності банківських структур;
- електронної комерції;
- телемеханіки та телеавтоматики;
- служб передавання даних, телеграфних, факсимільних, Telex, Teletex, бюрофакс, датафакс, електронної пошти, зокрема ЕП. X.400;
- інформаційно-довідкових, мультимедійних служб-відеотекст, телетекст, Інтернет;
- телеконференцій з обміном документами, даними, графічною інформацією, аудіо;
- конференцзв'язку, зокрема документального, відеоконференцій.

Виходячи з досвіду країн, в яких е-урядування використовується давно і успішно, можна проаналізувати його структуру. Функціональна модель е-урядування в Німеччині зображена на рис. 1.

Відповідно до цієї моделі клієнти системи електронного урядування можуть отримати доступ до неї трьома способами: за допомогою телефонного зв'язку (центри виклику), електронного зв'язку (Інтернет) або через бюро звернень громадян.

Центри взаємодії створюються з метою:

- реєстрації учасників обміну інформацією;
- синхронізації загальнодоступних довідників;
- підтримка протоколів обміну;
- гарантування інформаційної безпеки та захищеного передавання даних.

Деякі зі служб електронного документообігу ще не досягли достатнього розвитку в той час, як на зміну прийшли нові технології. Сьогодні до характерних ознак електронного документообігу додається функція підтримки систем електронних документів, функціонування системи «Електронний уряд», електронної комерції. Новий образ документальних телекомунікацій повинен формуватися з врахуванням властивостей електронних документів.

Виходячи з досвіду країн, в яких е-урядування використовується давно і успішно, можна проаналізувати його структуру. Функціональна модель е-урядування в Німеччині зображена на рис. 1.

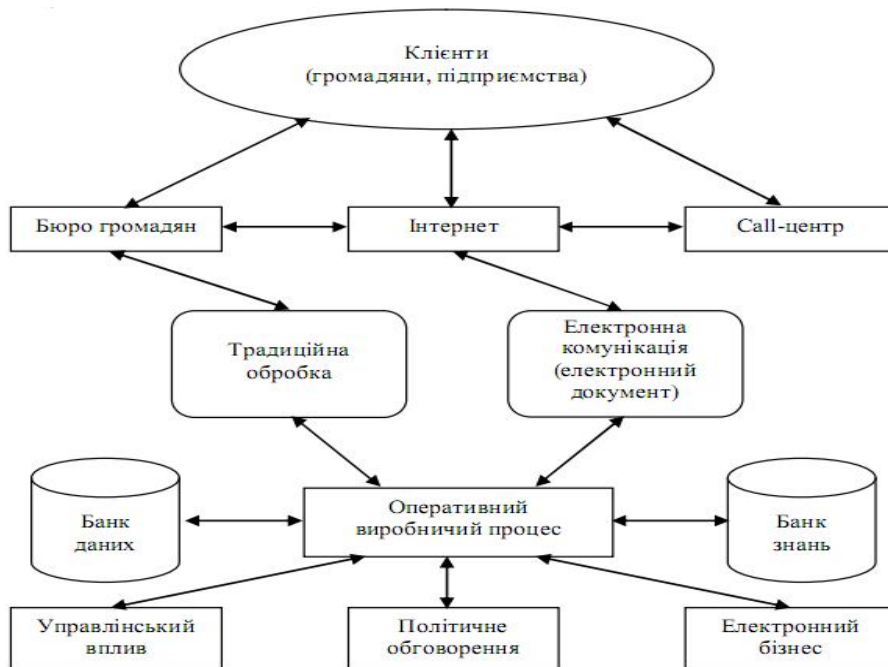


Рисунок 1. Функціональна модель е-урядування в Німеччині

Відповідно до цієї моделі клієнти системи електронного урядування можуть отримати доступ до неї трьома способами: за допомогою телефонного зв'язку (центри виклику), електронного зв'язку (Інтернет) або через бюро звернень громадян.

Центри взаємодії створюються з метою:

- реєстрації учасників обміну інформацією;
- синхронізації загальнодоступних довідників;
- підтримка протоколів обміну;
- гарантування інформаційної безпеки та захищеного передавання даних.

Сьогодні основною вимогою до систем електронного документообігу постає захист інформаційних ресурсів. Головні вимоги до підсистеми захисту електронного документообігу окреслено в Законі України «Про телекомунікації». Адекватного рівня інформаційної безпеки можна досягти лише на основі комплексного підходу, що передбачає використання фізичних, програмно-технічних і організаційних заходів та засобів захисту інформації.

Функції захисту повинні гарантувати безпеку:

- інформації, яка передається;
- даних абонентів, які зберігаються в системі;
- ресурсів системи документальних телекомунікацій;
- телекомунікаційних послуг;
- керування системою.

Аналіз отриманих наукових результатів. Інформаційна безпека неможлива без захисту самої системи захисту інформації. Для досягнення ефективності комплексної системи інформаційної безпеки необхідними є підсистеми керування та контролю в рамках управління системою. Розроблення підсистеми інформаційної безпеки, її впровадження, технічну експлуатацію та керування нею необхідно здійснювати на базі сучасної нормативно-правової бази у сфері технічного захисту інформації. Варто зазначити, що вимоги до інформаційної безпеки повинні висуватись не лише до Національної системи конфіденційного зв'язку. Частина вимог з інформаційної безпеки повинна задовольняти й телекомунікаційна мережа загального користування як первинний транспортний агент системи документообігу.

Для того щоб підвищити ефективність роботи органів державної влади необхідно використовувати систему в електронному урядуванні поряд із впровадженням електронного урядування, яка б відповідала усім вимогам ефективного опрацювання електронних документів та надійного їхнього захисту.

Основою інформаційної безпеки в електронному урядуванні є програмно-технічна архітектура. Для підвищення інформаційної безпеки слід використовувати термінальні технології (технологія тонких клієнтів). Термінал представляє собою монітор з клавіатурою і мишкою, і позбавлений таких складових ПК: материнської плати і універсальних процесорів, жорсткого диска, приводу для компакт-дисків, портів для підключення принтера. Термінал призначений для розміщення і виконання на ньому програм, служить лише для доступу через локальну мережу до сервера, на якому відбувається збереження і оброблення інформації, керування користувачами та реалізація інших функцій інформаційної системи. Така технологія зменшує можливість витоку інформації, оскільки позбавляє користувачів таких можливостей, які породжують загрози інформаційній безпеці або, які не передбачені функціональними обов'язками працівника. Немає можливості скопіювати на диск, флеш-пам'ять інформацію, не можливо встановити на робоче місце шкідливі або недозволені програми. Доступ до такого терміналу користувач може одержати ввівши ім'я і пароль або за допомогою смарт-карти, система проводить аутентифікацію і визначає, якими правами доступу володіє користувач. Таким чином, вирішуються задачі запобігання несанкціонованого доступу до системи. Для додаткового захисту слід використовувати мандатний доступ або

«мітки» безпеки. Приклад її використання – порівняння «мітки» документа, відправленого на друк з міткою принтера, це дозволяє гарантувати, що конфіденційні документи будуть видрукувані тільки на довірених принтерах.

Для захисту від НСД до серверів комп'ютерів системи, слід використовувати електронні замки. Вони забезпечують розмежування доступу до серверів і їхніх апаратних ресурсів, а також контроль цілісності програмного середовища.

Для ефективного електронного документообігу необхідно забезпечити надійний захист та автоматизацію ділових процесів. Системи електронного документообігу (Documentum, Lotus) дозволяють досягнути високої продуктивності праці зі збереженням надійного захисту. Вони оперують двома видами об'єктів для збереження інформації. По-перше: файли, папки і каталоги, в яких зберігаються опрацьовані документи. По-друге: таблиці і записи бази даних, в яких зберігається метадані (наприклад, картка документа, відомості про його історію, маршрут руху документа).

Висновки.

Проблеми впровадження «електронного урядування» в Україні мають внутрішню та зовнішню природу. Серед останніх особливе місце займають такі загальносвітові тенденції як глобалізація та її наслідки у вигляді світової фінансово-економічної кризи; зростання кількості та рівня традиційних загроз (небезпек) особі, суспільству, державі, світовому суспільству в цілому, а також поява нових загроз, ускладнення їхньої взаємодії; посилення конкуренції між країнами за енергоресурси, лідерство в світі та на регіональному рівні. У зв'язку із сьогоdnішнім становищем основною вимогою до систем електронного документообігу є надійний захист інформації.

Захист інформації в мережах електронного урядування з використання систем електронного документообігу (Documentum, Lotus тощо), забезпечується декількома методами: 1) використання термінальних технологій; 2) використання в системі сертифікованих замків. Побудова системи на основі типових сегментів дозволяє легко розширити її у масштабі, збільшуючи кількість сегментів і включаючи в них технічні засоби. В сегментах використовується однакова схема і технологія побудови системи інформаційної безпеки.

Список літератури

1. Всемирная встреча на высшем уровне по вопросам информационного общества. 10-12 декабря, Женева. План действий. [Електр. ресурс]. – Спосіб доступу: URL: www.itu.int/dms_pub/itus/md/03/wsis/doc/S03-wsis-doc-005!!msw-r.doc
2. Черешкин Д.С., Кононов А.А. Концепция создания национальной инфраструктуры защиты информации // Научно-техническая информация. Сер.1. – 2003. – №11
3. Балашов В.А. Обеспечения всеобщего доступа к инфокоммуникационным услугам и технологиям в сельских районах Украины. [Електр. ресурс]. – Спосіб доступу: URL: <http://www.euriadnik.org.ua/modules.php?name=news&file=article&sid=1130>. – Заголовок з екрана.
4. Кисельова Л. Розділ III. До концепції створення електронних архівів. Деякі правові аспекти визначення характеристик електронних документів. [Електр. ресурс]. – Спосіб доступу: URL: <http://www.archives.gov.ua>. – Заголовок з екрана.
5. Шейн И. Электронное развитие документооборота // Computer-world. – 2003. – № 18.