

Територіальна інформаційна система повинна бути призначена для автоматизації адміністративних функцій органів місцевого самоврядування та територіальних структур органів державної влади (БТІ, земельні комітети, казначейство, органи з праці та зайнятості, ЗАГС-и та ін.).

Для зменшення витрат на впровадження типових компонентів ТІС доцільно, щоб Департамент освіти і науки Полтавської обласної державної адміністрації взяв на себе функції базової муніципальної освіти щодо впровадження типових компонентів ТІС в Полтавській області з подальшим тиражуванням типових компонентів в інших муніципальних утвореннях регіону.

ЗАХИСТ ДІЛОВОГО ЕЛЕКТРОННОГО ЛИСТУВАННЯ

Довбня О. Д. Вищий навчальний заклад Укоопспілки «Полтавський університет економіки і торгівлі», напрям підготовки «Документознавство та інформаційна діяльність», студент групи ДІД-51м.

Ольховський В. О. Вищий навчальний заклад Укоопспілки «Полтавський університет економіки і торгівлі», доцент кафедри документознавства та інформаційної діяльності в економічних системах, к. т. н., доцент – науковий керівник.

Сучасний глобалізований світ і тенденції розбудови засад інформаційного суспільства характеризуються збільшенням потоків управлінської інформації, захист якої потребує дедалі більше часу, людських та матеріальних ресурсів.

В останні роки в Україні відбувається перехід від традиційних форм відпрацювання документів до їх електронного вигляду. Перехід до електронного документообігу несе цілий ряд переваг, серед яких: суттєве скорочення термінів відпрацювання та проходження документів в установах, спрощення пересилання документів між установами, що в свою чергу, зумовлює відчутну економічну вигоду.

Одним із важливих питань на шляху переходу до електронного документообігу є необхідність захисту інформації в системах електронного документообігу. Для передачі електронних документів широке застосування набуває використання відкритих каналів зв'язку та мережі Інтернет в яких найважливішим питанням є забезпечення захисту інформації, що передається.

Найбільш поширеними і в більшості випадків ефективними є криптографічні методи та засоби захисту інформації – методи шифрування, кодування або іншого перетворення інформації, в результаті якого її вміст стає недоступним без пред'явлення ключа криптограми і зворотного перетворення. При застосуванні криптографічних методів

захисту інформації охороняється безпосередньо сама інформація, а не доступ до неї (наприклад зашифрований файл не можна прочитати навіть у випадку крадіжки носія). Дані методи захисту інформації реалізуються у вигляді програмних або апаратно-програмних засобів.

Наряду з криптографічними методами захисту інформації можливе застосування стегаграфічних методів. Існує значна кількість методів, що пов'язані з використанням комп'ютерних форматів зображень, аудіо та відео в якості контейнера для приховування конфіденційних даних. Вибір конкретних засобів захисту інформації буде залежати від цінності інформації, яка обробляється. Чим складніші засоби захисту інформації, комбінація методів та засобів криптографічного та стегаграфічного захисту інформації, тим вони будуть дорожчі. Але в будь-якому випадку для забезпечення захисту інформації, що циркулює в електронному документообігу повинні бути спочатку впроваджені хоч б елементарні, найдешевші засоби.

Отже, ми вважаємо, що доцільно для забезпечення ефективного захисту інформації в електронному документообізі необхідно комбінувати різні методи, створивши оптимальне співвідношення, ціна – надійність. Виходячи з цього розробки раціональних методів захисту в системі електронного документообігу мають набути найактуальнішого характеру вже в наступні роки, коли усі види підприємств будуть використовувати електронний документообіг, а основними засобами передачі інформації будуть відкриті канали зв'язку та мережа Інтернет.

Саме тому, нашому суспільству необхідно значно поглибити поняття захисту інформації в електронному документообізі. Ще одним цікавим напрямом є не просто розроблення системи захисту інформації в електронному документообізі, а й зрозуміла адаптація систем електронного документообігу для смартфонів, адже за останніми даними вже близько половини населення України використовує смартфони, а це значить що у найближчому майбутньому відбудеться перехід до застосування мобільного обладнання для ділового листування та скорочення трудовитрат завдяки синхронизації програмного забезпечення електронного документообігу на мобільних пристроях зв'язку.

Загрозами для системи електронного документообігу крім порушень конфіденційності також є і загрози цілісності – можливе пошкодження, знищення чи спотворення інформації – як випадкове, так і зловмисне. Також при застосуванні електронних систем існує загроза працездатності системи, реалізація якої призведе до порушення або припинення роботи системи; сюди входять як умисні атаки, так і помилки користувачів, а також збої в обладнанні та програмному

забезпеченні. Тому сучасна система електронного документообігу повинна як мінімум передбачити механізм захисту від основних загроз – забезпечення конфіденційності та збереження документів, забезпечення безпечного доступу, забезпечення достовірності документів, протоколювання дії користувачів. Система повинна забезпечити збереження документів від втрати чи псування і мати можливість їх швидкого відновлення. При цьому важливо забезпечити розподілене збереження даних – зручним інструментом тут є використання «хмарних» сервісів зберігання даних в Інтернеті. Тому доцільним слід вважати застосування в системах електронного документообігу сумісної роботи з Інтернет-сховищами даних, причому зберігання та передавання конфіденційних даних повинно відбуватись у захищеному вигляді автоматично.

У справі захисту конфіденційної інформації організації від різного виду загроз значне місце займає персонал підприємства. Співробітники сучасного підприємства повинні мати можливість використовувати для доступу до службових інформаційних систем Інтернет і працювати з документами вдома, у відрядженні, чи у відпустці. Але працівники звичайно мають різну кваліфікацію по роботі з засобами зв'язку, що неминуче буде призводити до випадків неправильного використання інформаційних ресурсів і ненавмисного нанесення шкоди. Також треба враховувати, що є люди, які свідомо бажають завдати шкоди своєму підприємству. Це і скривджені, і корисливі співробітники, і навіть впроваджені шпигуни. Блокування таких загроз забезпечує дотримання системою документообігу принципу мінімальних повноважень. Кожен співробітник повинен володіти тільки тим набором повноважень, який необхідний для виконання його посадових обов'язків. Основним технічним засобом для реалізації цього принципу є системи аутентифікації та авторизації співробітників, а так само метод поділу мережі та інформаційних систем на різні зони довіри в залежності від оброблюваної інформації і груп співробітників, що мають до неї доступ і забезпечення контролю доступу між ними. Другий принцип захисту – це обов'язкове ведення журналів обліку. Система електронного документообігу повинна протоколювати доступ до інформаційних ресурсів підприємства, доступ до публічних інформаційних ресурсів, адміністративний доступ до систем і устаткування і таке інше.

Список використаних джерел

1. Підходи щодо захисту інформації в системах електронного документообігу / Р. М. Штонда, Ю. О. Процюк, В. В. Овсянніков, О. М. Маковецький, І. Р. Мальцева // Сучасні інформаційні техно-

- логії у сфері безпеки та оборони. – 2015. – № 3. – С. 129–132. – Режим доступу: http://nbuv.gov.ua/UJRN/sitsbo_2015_3_24.
2. Малиновський В. Сучасний стан та перспективи розвитку криптографічних засобів захисту систем електронного документообігу [Електронний ресурс] / В. Малиновський // Студії з архівної справи та документознавства. – 2012. – Т. 20. – С. 210–214. – Режим доступу: http://nbuv.gov.ua/UJRN/sasd_2012_20_33.
 3. Шерман М. І. Навчальна дисципліна «Електронний документообіг та захист інформації» як складова системи формування комп'ютерно-інформаційної компетентності магістрів державної служби [Електронний ресурс] / М. І. Шерман // Теорія та практика державного управління і місцевого самоврядування. – 2013. – № 1. – Режим доступу: http://nbuv.gov.ua/UJRN/Ttpdu_2013_1_20.

ДОКУМЕНТНО-ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ОРЕНДНИХ ВІДНОСИН В АГРАРНІЙ СФЕРІ

Мищенко Д. В. Вищий навчальний заклад Укоопспілки «Полтавський університет економіки і торгівлі», спеціальність «Документознавство та інформаційна діяльність», магістр.

Макарова М. В. Вищий навчальний заклад Укоопспілки «Полтавський університет економіки і торгівлі», д. е. н., завідувач кафедри документознавства та інформаційної діяльності в економічних системах, професор – науковий керівник.

Згідно статті 93 Земельного Кодексу України [2] право оренди земельної ділянки визначено наступними категоріями.

Право оренди земельної ділянки – це засноване на договорі строкове платне володіння і користування земельною ділянкою, необхідною орендареві для проведення підприємницької та іншої діяльності.

Земельні ділянки можуть передаватися в оренду громадянам та юридичним особам України, іноземним громадянам і особам без громадянства, іноземним юридичним особам, міжнародним об'єднанням та організаціям, а також іноземним державам.

Оренда земельної ділянки може бути короткостроковою – не більше 5 років та довгостроковою – не більше 50 років.

Орендована земельна ділянка або її частина може за згодою орендодавця передаватися орендарем у володіння та користування іншій особі (суборенда).

Згідно Закону України «Про оренду землі» [3] – оренда землі – це засноване на договорі строкове платне володіння і користування земельною ділянкою, необхідною орендареві для проведення підприємницької та інших видів діяльності.