

Список використаних джерел

1. Матвієнко О. Менеджмент інформаційних офісних систем : навч. посіб. для студ. вищ. навч. закл. і системи післядипломної освіти за спец. «Менеджмент організацій» і «Документознавство та інформаційна діяльність». – К., 2001. – 154 с.
2. Інтернет-ресурс – <http://www.experts.in.ua/baza/analytic>.

УДОСКОНАЛЕННЯ ДОКУМЕНТАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ В КОМЕРЦІЙНИХ ПІДПРИЄМСТВАХ

В. О. Ольховський, к. т. н., доцент;

В. О. Горобець, студентка групи ДІД-71м

*ВНЗ Укоопспілки «Полтавський університет економіки і торгівлі»,
м. Полтава, Україна*

Одним з головних елементів захисту на підприємстві є захищений документообіг. Конфіденційні документи, як і відкриті, знаходяться в постійному русі по безлічі ієрархічних рівнів управління, що створює серйозні передумови для втрати цінної інформації. Тому, щодо документопотоків та документообігу конфіденційних документів потрібно здійснення певних захисних заходів. Документообіг конфіденційних документів, як об'єкт захисту, являє собою упорядковану сукупність каналів об'єктивного, санкціонованого поширення конфіденційної інформації (документів) в процесі управлінської та виробничої діяльності споживачів цієї інформації. При русі конфіденційних документів по інстанціях і рівнями управління збільшується число джерел інформації, що володіють цінними відомостями, і розширюються потенційні можливості для втрати конфіденційної інформації, її розголошення персоналом, витоку інформації технічними каналами, зникнення носія цієї інформації.

В кожній організації розробляється комплекс заходів щодо захисту інформації в документопотоках, спрямований на запобігання або ослаблення загроз втрати інформації. Головним заходом захисту конфіденційної інформації є застосування в діловодстві захищеного документообігу. Під захищеним документообігом розуміється контрольований рух конфіденційної документованої інформації по регламентованим пунктам прийому, обробки, розгляду, виконання, використання і зберігання в жорстких умовах організаційного та технологічного забезпечення безпеки як носія інформації, так і самої інформації.

Додатковими заходами, проведеними в організації, в рамках захищеного документообігу можуть бути:

1) обмеження доступу персоналу до документів, справ і базам даних рамками виконуваних ними службових обов'язків;

2) персональна відповідальність посадових осіб за видачу дозволу на доступ співробітників до конфіденційних відомостей і документів;

3) персональна відповідальність кожного співробітника організації за збереження довіреного йому носія і конфіденційність інформації;

4) жорстка регламентація порядку роботи з документами, справами і базами даних для всіх категорій персоналу, в тому числі перших керівників організації.

Будь-якому руху конфіденційного документа повинні обов'язково передувати операції з перевірки комплектності, цілісності та обліку нового місцезнаходження документа не ускладнювати роботу персоналу з документами і не збільшують терміни руху та виконання документів. Сукупність технологічних стадій, супроводжуючих потоки конфіденційних документів, дещо відрізняються від аналогічної сукупності технологічних стадій потоків відкритих документів, обумовлених заходами захищеного документопотока [1, 2].

Найбільш істотною відмінністю технології обробки та зберігання конфіденційних документів від звичайних є багатоступінчастий облік всіх процедур і операцій, які виконуються з документами.

Облік та реєстрація конфіденційних документів, перш за все, має на меті збереження документів і фіксація їх місцезнаходження. Тому, основна мета обліку конфіденційних документів – забезпечення їх фізичного збереження, комплектності та цілісності, контроль за доступом до них персоналу, перевірка реальної наявності документів та аналітична робота з обізнаності персоналу про зміст документів.

На відміну від відкритих документів конфіденційні документи на будь-якому носії враховуються відразу при надходженні або перед виготовленням чернетки документа, до розгляду, розподілу або погодження та підписання.

Облік конфіденційних документів завжди централізується за категоріями документів і ділиться на кілька видів, відповідних стадіям технологічної обробки документів у документопотоках і

забезпечують чіткий розподіл облікових операцій на кожній ділянці обробки документів. Це дозволяє дробити знання таємниці організації між декількома незалежними працівниками та здійснювати колегіальність при контролі за збереженням документів на кожній ділянці.

Важливим є встановлення порядку руху документів. Встановлення порядку руху документів або управління документацією на підприємстві полягає у створенні умов, що забезпечують зберігання необхідної документної інформації, її швидкий пошук і постачання нею споживачів у встановлені терміни і з найменшими витратами.

Правильна організація конфіденційного діловодства та електронного документообігу на підприємстві є складовою частиною комплексного забезпечення захисту інформаційних потоків і має важливе значення в досягненні мети її захисту. Як відомо, фахівці, що займаються в області інформаційної безпеки стверджують, що близько 80 % конфіденційної інформації знаходиться в документах діловодства. Тому питання конфіденційного документообігу на підприємстві безсумнівно грають важливу роль в досягненні нею економічних успіхів.

Конфіденційні документи повинні оброблятися в конфіденційному діловодстві підприємства, або в загальному діловодстві, спеціально призначеною посадовою особою, відповідальною за конфіденційні документи. Конфіденційні документи повинні зберігатися в окремому приміщенні в шафах, які замикаються і опечатуються.

Як і багато інших завдань, проблема захисту конфіденційного документообігу вирішується позитивно в тому випадку, коли посадова особа, що відповідає головним чином за «паперову» роботу, і служба інформаційних технологій, контролююча сьогодні електронні документи та матеріали, об'єднуються в єдине ціле і діють спільно.

Важливо організувати на підприємстві дозвільну систему доступу до конфіденційних документів. Дозвільна система доступу до конфіденційних документів являє собою сукупність встановлених керівництвом підприємства нормативних положень, які забезпечують обґрунтований і правомірний доступ користувачів до необхідного їм для виконання службових обов'язків обсягом конфіденційних документів. При цьому право давати дозвіл на ознайомлення і право працювати з конфіденційними

документами може бути надано тільки особам, які мають допуск до комерційної таємниці.

Отже, захищеність документопотоків досягається за рахунок:

- одночасного використання режимних (дозвільних, обмежувальних) заходів і технологічних прийомів, що входять в систему обробки та зберігання конфіденційних документів;

- нанесення відмінної позначки (грифа) на чистий носій конфіденційної інформації або документ, у тому числі супровідний, що дозволяє виділити їх в загальному потоці документів;

- формування самостійних, ізольованих потоків конфіденційних документів;

- використання автономної технологічної системи обробки і зберігання конфіденційних документів, що не стикаються з системою обробки відкритих документів;

- регламентації руху документів як всередині фірми, так і між фірмами;

- організації самостійного підрозділу конфіденційної документації або підрозділу служби безпеки;

- переміщення документів між керівниками, виконавцями та іншим персоналом тільки через службу конфіденційного діловодства.

Список використаних джерел

1. Кузнецов О. О. Захист інформації та економічна безпека підприємства / О. О. Кузнецов, С. П. Євсєєв, С. В. Кавун. – Х. : ХНЕУ, 2008. – 359 с.
2. Палеха Ю. І. Організація сучасного діловодства : [навч. посіб. для студ. вищ. навч. закл.] / Ю. І. Палеха. – К. : Кондор, 2007. – 189 с.

БІЗНЕС-МОДЕЛІ В ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ

Д. В. Заморьонова, аспірант

ВНЗ Укоопспілки «Полтавський університет економіки і торгівлі», м. Полтава, Україна

Мануель Кастельс наголошує якщо інформаційна технологія це еквівалент електрики в епоху індустріалізації, то сучасний Інтернет – енергетична система та електродвигун, тому що він здатний поставляти «інформаційну енергію» для будь-яких сфер