Модуль 3. Документаційне обслуговування діяльності з урахуванням особливостей архівної справи

Тема № 7. Робота з діловою кореспонденцією

Тема уроку №81: Опрацювання та відправлення кореспонденції

Мета: сформувати поняття ділових документів, розвивати вміння застосовувати теоретичні знання на практиці, виховувати інтерес до професії.

Матеріал уроку:

Вихідні документи надсилаються адресатам з використанням засобів поштового зв'язку, електронного зв'язку, а також доставляються кур'єрською або поштовою службою.

Опрацювання документів для відправлення поштовим зв'язком здійснюється службою діловодства установи відповідно до Правил надання послуг поштового зв'язку.

З використанням засобів електрозв'язку служба діловодства здійснює передачу телеграм, факсограм, телефонограм, електронних документів із застосуванням електронного цифрового підпису та документів у сканованій формі без електронного цифрового підпису.

У разі надсилання факсограм і документів у сканованій формі без електронного цифрового підпису необхідно надіслати також оригінал документа в паперовій формі.

Види документів, інформація з яких передається каналами електрозв'язку, а також необхідність і порядок посилання адресатові їх оригіналу в паперовій формі визначаються інструкцією установи з урахуванням наявних в установі технічних і програмних засобів.

Інформаційні, телекомунікаційні та інформаційно-телекомунікаційні системи повинні забезпечувати захист від несанкціонованих дій, які можуть призвести до випадкових або умисних змін чи знищення інформації.

Вихідні документи опрацьовуються і надсилаються централізовано в день їх надходження від структурних підрозділів - виконавців або не пізніше наступного робочого дня.

Не допускається надсилання або передача документів без їх реєстрації у службі діловодства

Домашнє завдання:

1. § 2, ст.437-441, конспект
2. Складіть перелік того, що перевіряється під час приймання від виконавців вихідних документів.

Відповіді надсилати на адресу anylesik@gmail.com. В темі листа зазначайте прізвище, групу, назву предмета; в тексті листа – номер та дату уроку.

Модуль 3. Документаційне обслуговування діяльності з урахуванням особливостей архівної справи

Тема № 6. ОРГАНІЗАЦІЯ ДОКУМЕНТІВ У ДІЛОВОДСТВІ

Тема уроку №82: Застосування електронного підпису

Мета: засвоїти поняття нормативної бази діловодства, розвивати вміння застосовувати теоретичні знання на практиці, виховувати інтерес до професії.

Матеріал уроку:

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

Сучасні інформаційні технології дають можливість установам, підприємствам та організаціям, фізичним особам, суб'єктам господарювання більш ефективно і творчо вирішувати економічні та соціальні проблеми.

Електронний документообіг є одним з тих інструментів, що в змозі забезпечити потреби сьогодення в швидкому інформаційному обміні. А використання електронного цифрового підпису, що підтверджує оригінальність документа і надійно захищає його від підробок, - ефективне рішення для всіх, кому необхідно оперативно перевірити дійсність отриманої інформації або підтвердити факт укладення договору.

Документи можуть бути засвідчені електронним цифровим підписом і передані до місця призначення протягом декількох секунд, адже електронний документ передається за допомогою швидкісних телекомунікаційних систем, однією з яких є, приміром, мережа Інтернет. За таких умов усі учасники обміну електронними документами незалежно від відстані мають однакові можливості в електронному інформаційному обміні.

Електронний документообіг з використанням електронного цифрового підпису невдовзі посяде домінуюче місце у системі опрацювання, підготовки, підписання та надсилання документа, оскільки традиційні схеми: розроблення проекту документа в електронному вигляді, створення паперової копії для підпису, пересилання паперової копії з підписом, розгляд паперової копії, перенесення її на комп'ютер - малоефективні, трудомісткі й такі, що потребують забагато часу.

Електронний цифровий підпис (ЕЦП) можна отримати за результатом криптографічного перетворення набору електронних даних, який логічно поєднується з документом і дає змогу підтвердити його цілісність та ідентифікувати підписувача.

ЕЦП додається до вхідного документа (або розміщується в окремому полі документу) і така комбінація даних (документ + ЕЦП) утворює захищений електронний документ.

Накладається електронний цифровий підпис за допомогою особистого (таємного) ключа та перевіряється за допомогою відкритого ключа. Особистий ключ відомий лише його володільцеві й може зберігатись у нього на дискеті, пристрої Touch Memory, Smart-карті і т.і.

Відкритий ключ доступний всім учасникам електронного документообігу. Такий ключ включається до сертифіката відкритого ключа та може

розповсюджуватись в електронній формі або у формі документа на папері (публікується в загальнодоступному або спеціалізованому довіднику).

Алгоритм роботи системи мусить бути побудовано таким чином, що маючи доступ до відкритого ключа неможливо відтворити таємний ключ або поставити цифровий підпис - його можна тільки перевірити.

Для повноцінного функціонування систем ЕЦП необхідно забезпечити доступ отримувача до достовірної копії відкритого ключа відправника (підписувача) та можливість перевірити, що ця копія відкритого ключа належить саме цьому підписувачу.

Для виконання цього створюються спеціальні захищені довідники ключів, які ведуться спеціальними установами - центрами сертифікації ключів.

Центри сертифікації ключів (ЦСК) - це установи, які перевіряють дані власника відкритого ключа та видають захищені електронні документи спеціального зразка - сертифікати відкритих ключів, в яких міститься відкритий ключ та перевірена центром сертифікації інформація про власника ключа.

Перелік акредитованих центрів сертифікації ключів, з якими ДПС України укладено договір для подання податкової звітності платниками податків із застосуванням електронного цифрового підпису наведено в додатку 5.17.

Сертифікат відкритого ключа - електронний документ, що підписується електронним цифровим підписом центру сертифікації ключів. Достатньо отримати достовірним каналом сертифікат самого центру сертифікації ключів, щоб мати можливість перевірити достовірність будь-якого сертифікату, що виданий цим центром.

Зазначена особливість дає можливість поряд із звичайним електронним цифровим підписом виділити цифровий підпис, підтверджений посиленим сертифікатом відкритого ключа.

Посилений сертифікат ключа - тобто сертифікат, виданий із додержанням певних стандартизованих та затверджених законом вимог та правил (в тому числі - правил щодо проведення процедури засвідчення особи - власника ключа). Для того щоб мати право видавати сертифікати такого зразка, центри сертифікації мають пройти процедуру акредитації (засвідчення відповідності вимогам законодавства).

Юридичні та фізичні особи можуть на договірних засадах засвідчувати чинність відкритого ключа сертифікатом відкритого ключа, а також використовувати електронний цифровий підпис без сертифіката відкритого ключа.

Щодо органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій державної форми власності, то для них встановлено імперативну (обов'язкову) норму, згідно з якою зазначені організації можуть застосовувати електронний цифровий підпис лише за умови використання надійних засобів ЕЦП, що повинно бути підтверджено сертифікатом відповідності або позитивним висновком спеціально уповноваженого центрального органу виконавчої влади, та наявності посилених сертифікатів відкритих ключів у своїх працівників-підписувачів.

За правовим статусом електронний цифровий підпис прирівнюється до власноручного підпису (печатки) лише в тому разі, якщо:

- - електронний цифровий підпис підтверджено з використанням посиленого сертифіката відкритого ключа за допомогою надійних засобів цифрового підпису;

- - під час перевірки використовувався посилений сертифікат відкритого ключа, чинний на момент накладення електронного цифрового підпису;
- - особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті.

Підробити електронний цифровий підпис, а разом з ним і засвідчений документ неможливо, адже це потребуватиме величезної кількості обчислень, які, як вважається, не можуть бути реалізовані за сучасного рівня математики й обчислювальної техніки за прийнятний час, тобто поки інформація, що міститься в підписаному документі, є актуальною.

Домашнє завдання:

1. § 2, ст.441-447, конспект
2. Які умови має забезпечити держава для введення масового використання електронно-цифрового підпису?

Відповіді надсилати на адресу anylesik@gmail.com. В темі листа зазначайте прізвище, групу, назву предмета; в тексті листа – номер та дату уроку.

Документаційне обслуговування підприємства

Модуль 3. Документаційне обслуговування діяльності з урахуванням особливостей архівної справи

Тема № 7. Робота з діловою кореспонденцією

Тема уроку №83: Створення корпоративного центру сертифікації ключів

Мета уроку: сформувати знання про особливості роботи з документами, розвивати практичні уявлення про сервіс, виховувати любов до професії.

Матеріал уроку:

Якщо передбачається обмін підписаними документами між підрозділами всередині великої установи, корпорації, то можна створити корпоративний центр сертифікації ключів (КЦСК), діяльність якого б поширювалася тільки на власну організацію і підвідомчі їй дочірні підприємства (наприклад, філії банку).

Склад подібного КЦСК може бути мінімальний: окремий комп'ютер, що працює під керуванням ОС Windows Server, програмне забезпечення (ПО), що керує Microsoft Certificate Services і ПО криптопровайдера, що має відповідний сертифікат для формування ключів ЕЦП.

Секретні ключі, записані КЦСК на ключових носіях (можуть використовуватися дискети, інтелектуальні карти і т.п.) передаються користувачам, які будуть мати право підпису. Головний комп'ютер КЦСК і комп'ютери всіх користувачів, що одержала ключі, повинні бути обладнані пристроями для читання ключових носіїв.

Сертифікати ключів і списки відкликаних сертифікатів записуються в базу даних установи й можуть бути підписані КЦСК відкритим способом, й направлені підписувачам електронною поштою. Одержавши секретні ключі, користувачі, що мають право підпису, будуть в змозі підписувати файли документів безпосередньо на своїх робочих місцях.

Витрати на програмне забезпечення для роботи з ключами й апаратуру для читання ключів, хоча і незначні (порядку сотні доларів на одне місце), але пропорційно зростають зі збільшенням кількості робочих місць.

Крім того, запровадження в дію ЕЦП це не разовий захід, а досить тривалий процес. У цьому процесі потрібно і навчання користувачів, і видання відповідних інструкцій і нормативних документів. І уже в міру освоєння технології ЕЦП кількість користувачів із правом підпису зросте до оптимального для кожної конкретної організації значення.

Всі інші користувачі Системи можуть упевнитися в дійсності підписів одержуваних ними документів, використовуючи загальний сервер верифікації підпису. Сертифікати підписів, що зберігаються в базі даних Системи, використовуються для перевірки підписів. При поширенні сертифікатів по всіх установах корпоративної системи користувачі зможуть упевнитися в дійсності документа, незалежно від того, де він був підписаний.

Для забезпечення цілісності переданих електронною поштою електронних документів, також може використовуватися ЕЦП. У цьому випадку ЕЦП використовується вже для підпису всього електронного повідомлення, включаючи РКК документа і його файли.

Після одержання електронною поштою повідомлення одержувачу необхідно перевірити підпис, зареєструвати отриманий документ, зберігши при цьому підпис у файлів документу. Таким чином, користувачі Системи можуть бути упевнені в дійсності документів, що надійшли до них.

Регламент одержання, використання і відкликання підписів, а також дозвіл можливих конфліктів застосування ЕЦП - внутрішня справа учасників корпоративної системи і може вирішуватися їх внутрішніми нормативними документами. До того ж приведена технологія застосування ЕЦП не припускає виникнення правових відносин, що виходять за рамки учасників установи.

Домашнє завдання:

1. Підручник 2, с. 447-449, написати конспект.
2. Опишіть, як можна отримати сертифікат ключа

Відповіді надсилати на адресу anylesik@gmail.com. В темі листа зазначайте прізвище, групу, назву предмета; в тексті листа – номер та дату уроку.

Модуль 3. Документаційне обслуговування діяльності з урахуванням особливостей архівної справи

Тема № 7. Робота з діловою кореспонденцією

Тема уроку №84: Організація контролю за ходом виконання документів

Мета: сформувати поняття побудови документів у сучасному суспільстві, розвивати вміння застосовувати теоретичні знання на практиці, виховувати інтерес до професії.

Матеріал уроку:

Завдання контролю - забезпечення своєчасного та якісного виконання документів. Контролю підлягають зареєстровані документи, в яких встановлено завдання.

Обов'язковий контроль виконання: законів України, постанов Верховної Ради України, указів, розпоряджень президента України; постанов і розпоряджень Кабінету Міністрів України.

Відповідальність за виконання документа несуть особи, зазначені у розпорядчому документі (наказі, розпорядженні), резолюції керівника, безпосередні виконавці. Коли документ виконується кількома працівниками, відповідальним за організацію виконання є перший зазначений у резолюції.

Безпосередній контроль за виконанням документів покладається на канцелярію. У структурних підрозділах безпосередній контроль за виконання документів здійснює секретар.

Документи можуть бути із зазначенням і без зазначення строку виконання. Строк - у самому документі чи встановлений актом законодавства. Наприклад: листи-доручення і листи-запити установ вищого рівня - до зазначеного в них терміну або протягом 30 днів, телеграми, в яких порушуються питання, що потребують термінового вирішення - до 2 днів. Документи без зазначення строку виконання - повинні виконуватись не пізніше як за 30 календарних днів. "Терміново" - 7 днів.

Контроль за виконанням документів включає такі види робіт:

постановку документів на контроль, формування картотеки контрольованих документів;

перевірку своєчасного доведення документів до виконавців;

попередні перевірки і регулювання ходу виконання;

облік і узагальнення результатів контролю за виконанням документів;

інформування керівника про хід та підсумки виконання документів (на оперативних зборах, засіданнях колегіальних органів);

зняття документів з контролю; - формування картотеки виконаних документів. Контроль за виконанням документів здійснюється на реєстраційно-контрольних картках (РКК). Проставляють літеру К на лівому полі документа, документ передають виконавцю, а додатковий примірник РКК ставлять до контрольної картотеки.

РКК групуються у контрольну картотеку чи у розділі довідкової картотеки за термінами виконання документів, за виконавцями, групами документів (постанови, накази, рішення).

В установі з обсягом документообігу більше 25 тис. документів на рік періодично складаються переліки не виконаних у встановлений термін документів і надсилаються до структурних підрозділів.

При контролі за допомогою ПК пошук необхідної інформації здійснюється за видом документа, датою, виконавцем, кореспондентом, терміном виконання і змістом.

Після виконання документ знімається з контролю, та ж особа робить помітку на документі (РКК) про зняття з контролю.

Домашнє завдання:

1. 2, ст.449-450, конспект.
2. Наведіть 10 прикладів документів і термін їх виконання та контролю.

Відповіді надсилати на адресу anylesik@gmail.com. В темі листа зазначайте прізвище, групу, назву предмета; в тексті листа – номер та дату уроку.