ТЕОРІЯ І ПРАКТИКА РЕФЕРЕНТСЬКОЇ ТА ОФІСНОЇ ДІЯЛЬНОСТІ» (ДК-31)

Лекція

Тема 8. Робота секретаря-референта з конфіденційною інформацією

1. Поняття про інформацію з обмеженим доступом та її різновиди: інформація службова, таємна та конфіденційна.
2. Нормативно-методичне забезпечення роботи секретаря з конфіденційною інформацією.
3. Особливості діловодства з документами з обмеженим доступом.
4. Специфіка роботи з персональними відомостями співробітників фірми.

1. Поняття про інформацію з обмеженим доступом та її різновиди: інформація службова, таємна та конфіденційна

Інформація – це зміст повідомлення про сукупність явищ і подій, що представляють інтерес для зацікавлених осіб та організацій, підлягають реєстрації та обробці.

1. До службової може належати така інформація, що міститься в документах суб'єктів владних повноважень, які становлять внутрішню службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2. Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф «для службового користування». Доступ до таких документів надається відповідно до Закону України «*Про інформацію*».

3. Перелік відомостей, що становлять службову інформацію, який складається органами державної влади, органами місцевого самоврядування, іншими суб'єктами владних повноважень, у тому числі на виконання делегованих повноважень, не може бути обмеженим у доступі.

Залежно від доступності, інформація поділяється на *доступну і недоступну* для певного суб'єкта.

За режимом доступу інформація поділяється на *відкриту* інформацію та інформацію *з обмеженим доступом*.

З обмеженим доступом інформація поділяється на:

– з*акриту* або *секретну* (являє собою таємницю і розповсюдження якої можливе лише за згодою органів, уповноважених контролювати питання, пов'язані з цією інформацією);

– *таємну і конфіденційну*.

Таємна – інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі.

Конфіденційна – інформація, що містить відомості, які знаходяться у володінні, користуванні або розпорядженні юридичних та фізичних осіб і поширюється за їхнім бажанням згідно з передбаченими умовами (Закон України «*Про інформацію*»).

Відкрита – інформація, якою дозволено користуватися широкому загалу.

Можливість доступу до інформації для конкретного споживача часто залежить від платних чи безплатних умов її надання. Тому, відповідно до її місця у товарно-грошовому обігу, інформація поділяється на *комерційну та некомерційну*.

Комерційна інформація поширюється лише за бажанням її власника, в першу чергу на його умовах і переважно як об'єкт купівлі-продажу.

2. Нормативно-методичне забезпечення роботи секретаря з конфіденційною інформацією

Нормативно-методичне забезпечення захисту конфіденційної інформації призначено для регламентації процесів забезпечення інформаційної безпеки фірми, в тому числі при

роботі персоналу з конфіденційною інформацією, документами, справами і базами даних. Воно містить обов'язкові організаційні, інструктивні й інформаційні документи, що встановлюють принципи, вимоги і способи попередження пасивних і активних загроз цінній інформації, які можуть виникнути по вині персоналу, конкурентів, зловмисників та інших осіб.

Нормативно-методичне забезпечення базується на тих обов'язкових положеннях, які повинні міститися в засновницьких та інших основоположних документах фірми і визначати правовий статус інформаційної безпеки фірми.

Документи, що фіксують завдання, функції і відповідальність служб, які здійснюють захист цінної документованої інформації фірми: положення про службу безпеки, положення про службу конфіденційної документації, посадові інструкції співробітників цих служб, посадова інструкція менеджера (референта) з безпеки невеликої підприємницької фірми та інші документи.

Документи відрізняються за призначенням, складом, змістом і відображають вибрану фірмою систему захисту документованої інформації

Інструкція для забезпечення безпеки власної інформації підприємницької фірми необхідна для організації роботи із захисту конфіденційної і цінної документованої інформації містить:

1. Обов'язки співробітників фірми при роботі з конфіденційною документацією.

2. Порядок доступу співробітників до конфіденційних документів і баз даних, оформлення доступу.

3. Забезпечення збереження документів на паперових та інших носіях у роботі з ними керівників, виконавців (спеціалісти) і технічного персоналу.

4. Порядок збереження таємниці фірми під час проведення нарад, засідань і переговорів.

5. Вимоги до приміщень для роботи з конфіденційною інформацією.

6. Порядок охорони території, будівлі, приміщень, транспортних засобів і персоналу' фірми.

7. Пропускний режим приміщень фірми, облік і порядок видачі посвідчень, пропусків і візуальних ідентифікаторів.

8. Порядок прийому, обліку і контролю діяльності відвідувачів.

9.Організаційні забезпечення захисту інформації в ПЕОМ та лініях зв'язку, у використанні в обробці документів засобів організаційної техніки.

10. Відповідальність співробітників фірми за розголошення конфіденційної інформації і втрату цінних документів.

11. Інструкція з обробки, зберігання і руху конфіденційних документів підприємницької фірми, призначених для організації роботи співробітників служби конфіденційної документації, менеджера (референта) з безпеки, що керує справами фірми.

Ключові розділи цієї інструкції: Структура захищеного документообігу фірми. Встановлення, зміна і зняття грифу конфіденційності документів. Порядок складання, виготовлення та видання конфіденційних документів. Копіювання і розмноження документів з конфіденційною інформацією. Прийом і розподіл вхідних документів. Контроль виконання документів. Перевірка наявності документів, справ, баз даних і носіїв та ін.

3. Особливості діловодства з документами з обмеженим доступом

Конфіденційне діловодство базується на принципах, що й загальне діловодство, але водночас має відмінності, зумовлені конфіденційністю документованої інформації.

Відмінність конфіденційного діловодства полягає в тому, що в ньому конфіденційна інформація повинна захищатися не тільки від утрати, але й від недозволеного виходу такої інформації за межі її функціонування, що захищається, або встановленого кола осіб, які мають право працювати з нею.

Сутність конфіденційного діловодства зумовлена його організаційними і технологічними особливостями, до яких належать:

– суворе регламентування складу документів установи, що містять конфіденційну інформацію, та їх видання;

– обов'язковий облік кожного примірника; поаркушний облік усіх без винятку документів та їх проектів;

– якнайбільша повнота реєстраційних даних про кожен документ;

– фіксація проходження і місцезнаходження кожного документа;

– проведення систематичних перевірок наявності документів;

– дозвільна система допуску до документів і справ;

– жорсткі вимоги до умов зберігання документів і користування ними;

– персональна відповідальність за облік, збереженість документів і порядок користування ними.

Вимоги до конфіденційного діловодства:

– документаційне забезпечення усіх видів конфіденційної діяльності;

– захист документованої інформації, що утворюється в процесі конфіденційної діяльності

Діловодство в разі роботи з документами, що містять комерційну таємницю, має свої особливості. Наказом керівника призначається посадова особа (особи), яка відповідає за облік, зберігання та використання документів, що мають гриф обмеження доступу. Нею може бути і секретар, для якого робота з документами належить до основних службових обов'язків, або відповідальний працівник, для якого виконання цих функцій становитиме додаткове навантаження.

Гриф конфіденційності означає, що право власності на інформацію, яка міститься в документі, належить підприємству.

Якщо інформація, що становить комерційну таємницю, міститься в документах, які належать підприємствам-партнерам, то про нерозголошення її має бути зазначено в тексті, договорі між цими підприємствами.

Якщо на документі не проставлено гриф обмеження доступу й у тексті немає вказівок на конфіденційність, то це означає, що автор та особи, які підписали чи затвердили документ, передбачили всі можливі наслідки вільної (без обмеження доступу) роботи з документом.

На документі з грифом «КТ» («Конфіденційно») зазначається кількість при-мірників документа і місце знаходження кожного з них.

Наприклад:
Складений у двох примірниках:
Прим. 1 – на адресу прим.
№2-до справи 01.08.

На звороті або в резолюції документа з грифом «КТ» керівник пише прізвище тих посадових осіб, яким дозволено користуватися цим документом.

Наприклад:
Дозволяю:
Кучуку В.О.
Сидорчуку Д.М.
Підпис керівника Дата

Друкування документів з грифом «КТ» здійснюється централізовано, у спеціально відведеному для цього приміщенні або на робочому місці, куди заборонено вхід стороннім. Віддруковані та підписані документи передаються для реєстрації посадовій особі, яка відповідає за їх облік. Чернетки і варіанти документа знищуються цією особою з підтвердженням факту знищення записом на копії вхідного документа. Наприклад*: чернетка (і варіанти) знищено. Підпис. Дата.*

Усі документи з конфіденційною інформацією повинні реєструватися окремо від решти

документів у Журналі реєстрації документів з грифом КТ.

Усі документи, що надходять з грифом *«Комерційна таємниця»,* одержує відповідальна особа чи секретар-референт, яка обов'язково перевіряє кореспонденцію на цілісність. Якщо якихось документів не вистачає, то складають акт (у двох примірниках, один з яких направляють адресантові).

Документи з грифом обмеження доступу формують в окрему справу, на обкладинці якої в правому верхньому куті роблять позначку *«Комерційна таємниця».* На звороті обкладинки вміщують список працівників, які мають право користуватися документами внесеними до даної справи.

Зберігаються такі справи у сейфі, що опечатується посадовою особою, яка відповідає за їх зберігання. Доступ до цього сейфа іншим працівникам має бути заборонений.

Обіг (видача та повернення) документів з грифом «КТ» відображається в Журналі обліку видачі документів з грифом «КТ».

Документи, що мають гриф обмеження доступу, видають та приймають під розписку, при цьому забороняється:

– вилучати зі справи чи переносити до іншої справи документи, що мають гриф обмеження доступу, без дозволу керівника та позначок у «Журналі реєстрації документів з грифом обмеження доступу»;

– виносити з приміщення документи без спеціального дозволу керівника;

– розмножувати документи без дозволу керівника (якщо є дозвіл, то розмноження здійснюють у присутності відповідальної особи, а браковані примірники одразу знищують).

Усі справи, доступ до яких обмежено, обов'язково вносять до номенклатури справ підприємства.

Після закінчення календарного року наказом керівника призначається спеціальна комісія, яка обов'язково має:

– перевірити наявність усіх документів;

– відібрати документи для зберігання в архіві;

– визначити документи для знищення.

Перевірка наявності документів з грифом «КТ» за рішенням керівництва підприємства може здійснюватися з іншою періодичністю, наприклад, після закінчення кварталу. При втраті конфіденційного документа про це негайно інформують керівника підприємства. Вживаються всі заходи, щоб розшукати документ. Для розслідування факту втрати керівник підприємства створює спеціальну комісію. У випадку, коли розшук не дав позитивних наслідків, складається акт, а до журналу реєстрації вноситься про це відповідний запис.

Після звільнення з роботи співробітника, відповідального за документи з грифом «КТ», проводять перевірку наявних документів, які передають заново призначеній для цього особі. Складають акт приймання-передачі, який затверджується керівником підприємства або його заступником.

На особу, яка на підприємстві була допущена до КТ і звільнилася з роботи, зобов'язання про нерозголошення конфіденційної інформації поширюється ще протягом двох років після звільнення, якщо інший термін не був обумовлений трудовою угодою. При передачі справ до архіву на документи з грифом «КТ» складається окремий опис. Архівне зберігання таких документів здійснюється в опечатаних коробках у приміщенні, куди забороняється несанкціонований доступ. На документи з грифом «КТ», що відібрані для знищення, складається акт. Передаючи справи до архіву, складають окремий опис документів, що мають гриф обмеження доступу. У приміщенні архіву такі документи зберігають в опечатаних скриньках. Несанкціонований доступ до них суворо заборонено.

4. Специфіка роботи з персональними відомостями співробітників фірми

Інформація про особу – це сукупність документованих або публічно оголошених відомостей про особу. Основними даними (персональними даними) є національність, освіта, сімейний стан, релігійна приналежність, стан здоров’я, а також адреса, дата і місце народження.

Кожна особа має право на ознайомлення з інформацією, зібраною про неї. Ця інформація охороняється законами України.

Відомості про працівників відображені в кадрових документах, зокрема про вік, дату і місце народження, місце проживання, ідентифікаційний номер, соціальний статус, пільги відповідно до закону.

Документація підприємств, установ та організацій в електронній формі та/або у формі картотек, що містить певним чином структуровані персональні дані працівників є базою персональних даних або її частиною.

Робота з персональними даними відбувається не тільки через автоматизовані інформаційні системи (сайти і програмні застосунки). Використовують бланки, анкети та інші паперові форми збору персональних даних. Правила і вимоги, передбачені законодавством, поширюються на всі можливі форми.

Збирання і зберігання персональних даних може бути у різних формах (у «паперовій» і в цифровій). У цифровій формі фірма (керівник, секретар) може зберігати відомості локально, використовуючи свої власні потужності і технічні засоби. Програмні і технічні заходи безпеки мають бути актуальними, дієвими та відповідати потенційним загрозам, характеру і масштабам наявної бази персональних даних. Саме у процесі зберігання персональних даних проявляється роль і значення технічної спеціалізації секретаря (спеціаліста).

Можливі порушення і проблеми криються у наступних документах, процесах роботи з персональними даними:

У роботі секретар-референт з конфіденційною інформацією повинен керуватися Законом України «Про захист персональних даних».

Необхідно дотримувати письмову згоду співробітника на обробку його персональних даних, які стосуються: расового або етнічного походження; політичних, релігійних або світоглядних переконань; членства в політичних партіях і професійних спілках; притягання до кримінальної відповідальності; стану здоров'я, біометричних або генетичних даних.

Проте при звичайному виконанні функцій роботодавця немає потреби у збиранні та обробленні таких відомостей.

Щоб відповідно до закону забезпечити захист персональних даних працівників, потрібно:

1. Наказом затвердити список осіб, які мають право доступу до персональних даних співробітників. У наказі треба визначити, які саме особи із цього списку для яких цілей можуть використовувати персональні дані працівників. Тобто чітко зазначити, хто і навіщо. Кожний співробітник має доступ лише до тих персональних даних, які необхідні йому у зв'язку з виконанням посадових (службових) обов'язків.

2. Розробити форму під назвою «Зобов'язання про нерозголошування персональних даних». Цю форму повинні підписати всі співробітники, які мають доступ до персональних даних працівників підприємства (наприклад, співробітники бухгалтерії, відділу кадрів, члени комісії із соціального страхування тощо). Строк дії такого зобов'язання не припиняється навіть після припинення роботи з персональними даними (це може бути як звільнення, так і переведення до іншого структурного підрозділу підприємства, де не доведеться працювати з персональними даними інших співробітників)

Форму треба давати працівникові на підпис під час прийняття на роботу (або переведення з іншого відділу, де немає доступу до персональних даних). Датою отримання доступу до персональних даних уважається дата підписання співробітником зобов'язання, а датою позбавлення такого права вважається дата його звільнення (переведення на іншу посаду, де не буде доступу до персональних даних) –Типового порядку.

Зразок зобов'язання:

Директорові ТОВ «Сніг»Луценку В. Н.
Інспектора кадрів Роменко М. К.

Зобов'язання

Я, інспектор кадрів ТОВ «Сніг» Роменко Марія Кирилівна, зобов'язуюся не розголошувати персональні дані співробітників, які стали мені відомі у зв'язку з виконанням мною посадових обов'язків.

11.11.20 р. *(підпис) М. К. Ромашкіна*

Згідно з Типовим порядком роботодавець зобов'язаний вести облік працівників, які мають доступ до персональних даних (секретар, інспектор кадрів та ін.). Для цього ведуть журнал обліку таких працівників.

3. Повідомити працівників про роботодавця, пояснення його персональних даних, склад і зміст зібраних даних, їх права, а також про мету збору персональних даних.

4. Розробити Положення про порядок обробки і захисту персональних даних. За основу можна взяти Типовий порядок. Чинним законодавством передбачено як адміністративну, так і кримінальну відповідальність за порушення вимог про захист персональних даних.