**Міністерство освіти і науки України**

**Національний авіаційний університет**

###### Конфіденційне діловодство

**Методичні рекомендації**

**до самостійної роботи**

**для студентів напряму підготовки**

**6.020105 «Документознавство**

**та інформаційна діяльність»**

**Київ 2016**

Міністерство освіти і науки України

Національний авіаційний університет

 Конфіденційне діловодство

Методичні рекомендації до самостійної роботи

для студентів напряму підготовки

6.020105 «Документознавство

та інформаційна діяльність»

Київ 2016

УДК 651.4/9:65.012.8(076.5)

ББК С844р

 К652

Укладач *О. Г. Ількова*

Рецензент *Н. В. Бем*

*Затверджено методично-редакційною радою Національного авіаційного університету (протокол № 3/15 від 21.05.2015 р.).*

**Конфіденційне діловодство :** методичні рекомендації до К652 самостійної роботи / уклад. О. Г. Ількова. – К. : НАУ, 2016. – 32 с.

Містять методичні рекомендації до індивідуальних занять, понятійний апарат, тематику курсових робіт та список рекомендованої літератури.

Для студентів напряму підготовки 6.020105 «Документознавсто та інформаційна діяльність»

**Вступ**

## Метою навчальної дисципліни «Конфіденційне діловодство» є надання студентам відомостей про особливості становлення, функціонування та правила організації конфіденційного діловодства в Україні; формування у них цілісного уявлення про класифікацію інформації за рівнем доступу, документування конфіденційної інформації та організацію конфіденційного документообігу.

Завданнями вивчення навчальної дисципліни є формування у студентів напряму «Документознавство та інформаційна діяльність» знань та навичок організації конфіденційного діловодства та документообігу установ.

Навчальний матеріал дисципліни структурований за модульним принципом і складається з двох модулів.

У результаті засвоєння навчального матеріалу студент повинен:

**Знати:**

* історію розвитку конфіденційного діловодства в Україні та особливості сучасного конфіденційного діловодства;
* класифікацію інформації за ступенем доступу;
* основні види роботи з документами з різними грифами секретності;

## закони та державні програми в галузі інформації та інформаційної безпеки;

* правила підготовки, обліку та зберігання конфіденційних документів;

## специфіку правової відповідальності за розголошення інформації з обмеженим доступом;

## особливості електронного конфіденційного документообігу.

**Вміти*:***

* самостійно аналізувати сучасний стан та перспективи розвитку конфіденційного діловодства в Україні;
* характеризувати схему класифікації інформації і наводити її підтвердження;
* визначати склад інформації з обмеженим доступом;
* організовувати конфіденційне діловодство;
* застосовувати конфіденційний документообіг у практиці українських підприємств та організацій;
* аналізувати проблеми і перспективи українського законодавства в галузі інформації, інформатизації, інформаційної безпеки та електронного документообігу;
* використовувати набуті знання на заняттях з інших курсів циклу професійно-орієнтованих дисциплін, при написанні курсових і дипломних робіт та при проходженні практики.

У результаті підготовки до індивідуальних занять та виконання курсової роботи студент повинен:

**Знати:**

* монографічні й періодичні видання з обраної теми й аналізувати їх зміст;
* історію досліджуваної проблеми та сучасний стан її опрацювання;
* предмет, об’єкт, мету і методи дослідження;
* сутність і особливості конфіденційного діловодства;
* вимоги до написання, структурування, мовного оформлення науково-дослідної роботи;

**Вміти:**

* систематизувати отримані теоретичні знання з конфіденційного діловодства;
* самостійно осмислити наукову проблему, творчо й критично її дослідити;
* збирати, аналізувати і систематизувати науково-теоретичні джерела;
* формулювати висновки, пропозиції та рекомендації з предмета дослідження.

Знання, вміння та навички отримані під час вивчення цієї навчальної дисципліни, будуть використані під час проходження переддипломної практики.

**Методичні рекомендації до індивідуальних занять**

**Тема:**

**Історія розвитку конфіденційного діловодства України.**

**Створення переліків відомостей інформації з обмеженим доступом**

**План**

1. Розвиток конфіденційного діловодства України на сучасному етапі.
2. Створення переліків відомостей, що містять інформацію з обмеженим доступом.

**Основні поняття:** діловодство, державна таємниця, інформація з обмеженим доступом, комерційна таємниця, конфіденційне діловодство, Постійно діюча експертна комісія (ПДЕК).

**Література:** [1]; [7]; [8]; [14]; [17]; [21]; [22]; [23]; [24].

**Методичні рекомендації**

Готуючи відповідь на **перше питання**, необхідно зважати на сучасні реалії. Конкурентна боротьба – супутник комерційної діяльності та умова виживання комерційних підприємств. Звідси – прагнення зберегти в секреті від конкурентів ті прийоми та особливості своєї діяльності, які забезпечують перевагу над ними, звідси і прагнення конкурентів виявити ці секрети, щоб використовувати їх у своїх інтересах. Отримання, використання, розголошення таких секретів без згоди їх власників віднесені законодавством до однієї з форм недобросовісної конкуренції, званої промисловим шпигунством. Секрети комерційної діяльності, які потребують захисту, отримали назву комерційної таємниці. Поняття комерційної таємниці також має свою історію.

У відповіді варто наголосити, що відродження в другій половині 1980-х років підприємницької діяльності спричинило за собою розробку, пов'язаних з нею, нормативних документів, в тому числі що стосуються комерційної таємниці. У першу чергу потурбувалися сформулювати визначення комерційної таємниці. Таке визначення було надане в 1990 році у Законі «Про підприємства в СРСР». У ньому сказано: «Під комерційною таємницею підприємства розуміються відомості, що не є державними секретами, пов’язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю підприємства, розголошення (передача, витік) яких може завдати шкоди його інтересам».

Зі здобуттям незалежності, Україна починає самостійно створювати і розвивати власну систему державних органів та національне законодавство. Одним з перших законодавчів актів, який закріпив право громадян на інформацію, заклав правові основи інформаційної діяльності був принятий 2 жовтня 1992 року Закон України «Про інформацію». Саме цим законом вперше було введено в обіг термін «конфіденціальна інформація». Відповідно до ст. 28 Закону України «Про інформацію», інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Інформація з обмеженим доступом – це відомості конфіденційного або таємного характеру, правовий статус яких передбачений законодавством України, які визначені такими до встановлених юридичних процедур і право на обмеження доступу до яких надано власнику таких відомостей. Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну (ст. 30 Закону України «Про інформацію»). Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов (ст. 32 Закону України «Про інформацію»). Роботу з документами, які містять конфіденційну інформацію, що є власністю держави, регламентує «Інструкція про порядок обліку, зберігання і використання документів, справ та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави». Хоча ця Інструкція регулює питання конфіденційного діловодства щодо документів, які містять конфіденційну інформацію, що є власністю держави, зазначимо, що багато підприємств взяли її «на озброєння» для організації конфіденційного діловодства у власному бізнесі.

Організація і технологія конфіденційного діловодства не регламентовані державними нормативними актами. Їх повинен

визначати власник конфіденційних документів, з огляду на специфіку діяльності підприємства. Однак при цьому йому необхідно керуватися визначеними нормами і правилами роботи з конфіденційними документами, що забезпечують потрібний рівень функціонування підприємства, збереженість документів і конфіденційність інформації, що міститься в них.

Пам’ятайте, що склад документованої конфіденційної інформації залежить від компетенції і функцій підприємства, характеру його діяльності, взаємозв'язків з іншими підприємствами, порядку вирішення питань. Перелік відомостей, що складають комерційну таємницю, розробляється для кожного підприємства самим підприємством‑ власником інформації. Це випливає з чинного законодавства, яким встановлено, що склад і обсяг таких відомостей визначається власником інформації. Таким чином, право підприємця на зміст комерційної таємниці є безумовним. Ніхто не може диктувати йому, що відносити до комерційної таємниці, за винятком зведень, що не можуть складати комерційну таємницю відповідно до державних нормативних актів.

Починаючи готувати відповідь на друге питання майте на увазі, що правовою підставою для встановлення складу відомостей, які відносяться до комерційної таємниці, є закони, а також визначення поняття «комерційна таємниця», якими передбачено, що відомості, які складають комерційну таємницю, можуть бути в будь-якій сфері підприємницької діяльності. Отже, комерційна таємниця може поширюватися на всі напрямки і види діяльності підприємства.

Розробкою переліку відомостей, що складають комерційну таємницю, повинна займатися постійно діюча експертна комісія (ПДЕК).

Зазначте, шо на першому етапі роботи на основі аналізу задач, функцій, компетенції, напрямків діяльності підприємства необхідно встановити весь склад циркулюючої на підприємстві інформації, відображеної на будь-якому носії, будь-яким способом і у будь-якому вигляді, а також з урахуванням перспектив розвитку підприємства і його взаємин з партнерами, визначити характер додаткової інформації, що може виникнути в результаті діяльностіпідприємства. Ця інформація класифікується за тематичною ознакою.

Вкажіть, що на другому етапі визначається, яка з встановленої інформації повинна бути конфіденційною і віднесена до комерційної таємниці. Пам’ятайте, що базовим критерієм при цьому є можливість одержання переваг від використання інформації за рахунок невідомості її третім особам. Цей критерій має ніби дві складові: невідомість інформації третім особам і отримання переваг в силу цієї невідомості. Конфіденційність є правовою формою й водночас інструментом забезпечення невідомості інформації.

Зазначте, що у сфері комерційної діяльності цінність інформації обумовлена насамперед ринковою потребою в інформації як джерелі отримання прибутку, тому віднесення інформації до комерційної таємниці дозволяє отримати прибуток і не зазнати збитків. Конфіденційність такої інформації створює для її власника переваги в конкурентній боротьбі і виступає як засіб захисту від несумлінної конкуренції.

Зазначте, що перелік відомостей, що становлять обмеження доступу, розробляється для кожного підприємства самим підприємством – власником інформації. Таким чином, право підприємця на зміст конфіденційної інформації є незаперечним.

У висновку зазначте, що у сфері комерційної діяльності цінність інформації обумовлена насамперед ринковою потребою в інформації як джерелі одержання прибутку, тому віднесення інформації до комерційної таємниці дозволяє дістати прибуток і запобігти збиткам. Конфіденційність такої інформації створює для її власника переваги в конкурентній боротьбі й виступає як засіб захисту від несумлінної конкуренції.

**Тема:**

#  Правова відповідальність у конфіденційному діловодстві України

**План**

1. Відповідальність за розголошення інформації з обмеженим доступом.
2. Перевірка наявності документів, що містять інформацію з обмеженим доступом.

**Основні поняття:** адміністративна відповідальність, кримінальна відповідальність, цивільна відповідальність.

**Література:** [1]; [2]; [3]; [4]; [5]; [6]; [7]; [8]; [9]; [10]; [13]; [18]; [19]; [20]; [24]; [29]; [30].

**Методичні рекомендації**

Готуючи відповідь на **перше питання**, зверніть увагу на те, що громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною за власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушують передбаченої законом таємниці, мають право самостійно визначати режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту. Наголосіть, що виняток становить інформація, для якої встановлено правові обмеження щодо можливості її віднесення до категорії конфіденційної. Поясніть, що це окремі відомості комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої створює загрозу життю і здоров’ю людей (ч. 3-4 ст. 30 Закону України «Про інформацію»).

Обов’язково вкажіть, що в Україні питання захисту інформації з обмеженим доступом регламентується Законами України «Про інформацію», «Про захист інформації в автоматизованих системах», «Про державну таємницю», «Про телекомунікації» та іншими.

Дайте визначення поняття «державна таємниця». Державною таємницею є вид таємної інформації, що охоплює відомості у сфері оборони, економіки, нау­ки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані державною таємницею у Зводі відомостей, що становлять державну таємницю і підлягають охороні державою (закріплюється у вигляді відкритого наказу Голови СБ України).

Зазначте, що в Україні є три ступені секретності (державної таємниці): «особливої важливості», «цілком таємно» та «таємно», гриф «Для службового користування» застосовується для позначення матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави.

Наголосіть, що в Україні до інформації з обмеженим доступом, що не є власністю держави, належить комерційна таємниця. Для розуміння поняття «комерційної таємниці», скористайтеся визначенням поданим Господарським кодексом України (ст. 36).

З юридичної точки зору визначте, що об’єктивна сторона злочину має дві форми: несанкціонований збут інформації з обмеженим доступом та її розповсюдження. І для кваліфікації діяння особи за ст. 361-2 ККУ достатнім є доведення, хоча б однієї із них.

Не забувайте, що під розповсюдженням слід розуміти повідомлення інформації будь-яким способом (усно, письмово, друкованим способом, за допомогою комп’ютерної мережі тощо) невизначеному колу осіб (хоча б одній людині).

Вкажіть, що суб’єкт злочину ст. 361-2 КК України загальний, тобто відповідно до ст. 18 КК України, це фізична осудна (усвідомлює свої дії і керує ними – ст. 19) особа, якій до вчинення злочину виповнилося 16 років (ч. 1 ст. 22 КК України). Однак варто зауважити, що втрата документів, що містять державну таємницю (ст. 329) передбачає необережну форму вини, а у ст. 361-2 діяння може бути вчинено тільки з прямим умислом.

Далі переходьте до розкриття змісту поняття «доступ до інформації». Це поняття використовується у чинному законодавстві України, однак визначення його не розкривається.

Продемонструйте, як Закон України «Про інформацію» дає визначення поняття «режим доступу до інформації». А саме, «режим доступу до інформації – це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації» [ст. 28].

Обгрунтуйте, як Закон України «Про державну таємницю» закріплює визначення поняття «доступ до державної таємниці». А саме, «доступ до державної таємниці – надання повноважною посадовою особою дозволу громадянинові на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов’язаної із державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов’язаної із державною таємницею, цією посадовою особою відповідно до її службових повноважень» [ст. 1].

Починаючи давати відповідь на **друге** **питання**, наголосіть, що метою перевірки наявності документів, справ і носіїв конфіденційної інформаціїє встановлення їх реальної відповідності записам в облікових формах, зберігання цілісності і комплектності, а також своєчасне виявлення фактів втрати конфіденційних матеріалів і визначення правильності виконання процедур і операцій щодо їхнього обліку, зберігання і використання. Зазначте, що перевірка завжди здійснюється стосовно облікових даних та документів, екземплярів кожного документа та їх складових частин або справи. Пам’ятайте, що окрім того, під час перевірки розглядаються питання можливості зняття з документів грифа конфіденційності.

Треба мати на увазі, що перевірки наявності конфіденційних матеріалів можуть бути регламентованими (періодичними) і нерегламентованими (неперіодичними).

Регламентовані, обов’язкові перевірки здійснюються здебільшого щокварталу і наприкінці календарного року або в інші встановлені на підприємстві терміни. Вони охоплюють весь масив конфіденційних матеріалів.

Нерегламентовані перевірки здійснюються при зміні керівників підприємства, режимно-секретного підрозділу чи підрозділів напрямків діяльності підприємства, звільненні співробітників цих підрозділів, після завершення екстремальної ситуації, при виявленні факту можливої втрати інформації тощо. Цей вид перевірки зазвичай обмежується конкретною частиною конфіденційних матеріалів.

Не забувайте, що щоденні самоперевірки чи перевірки наявності документів здійснюють наприкінці робочого дня всі співробітники підприємства, які працюють з конфіденційними матеріалами.

Вкажіть, що квартальні і річні перевірки наявності документів здійснюються спеціально призначеною комісією. За результатами квартальної і річної перевірок складається акт. Зазначте, що кожен вид перевірки закінчується лише після виявлення фактичної наявності всіх документів, що значаться в облікових формах.

Пам’ятайте, що під час проведення квартальної перевірки наявності конфіденційних матеріалів контролюється зберігання традиційних і електронних документів, що перебувають на виконанні у співробітників підприємства і не підшиті у справи. Наголосіть, що перевірка здійснюється лише в присутності самого співробітника. Скажіть, що у процесі проведення річної перевірки контролюється зберігання усіх традиційних і електронних документів: як тих, що перебувають на виконанні, так і виконаних, підшитих у справи незалежно від часу їхнього надходження чи видання. Зауважте, що справи перевіряються поаркушно. Відсутність конфіденційного документа, справи чи носія інформації у співробітника, якому вони були видані, вважається втратою цих матеріалів. Зазначте, що у такому разі комісія складає відповідний акт і негайно доповідає про втрату першому керівникові підприємства для ухвалення рішення. Підкресліть, що акт складається також у випадку виявлення в базі даних комп’ютера співробітника чи на дискеті неврахованої чи не санкціоновано збереженої копії електронного документа.

Отже, у висновку повідомте, що перевірка наявності документів, справ і носіїв інформації реалізує одну з головних частин функції контролю за роботою співробітників з конфіденційними матеріалами і дає можливість вірогідно визначити міру відповідального ставлення кожного співробітника до цієї роботи. Водночас виявляються факти втрати конфіденційних матеріалів, що є підставою для початку службового розслідування.

**Тема:**

**Облік та оформлення паперових носіїв конфіденційної інформації**

**План**

1. Приймання і облік документів з обмеженим доступом.
2. Порядок та особливості розмноження конфіденційних документів.

**Основні поняття:** внутрішній документ, вхідний документ, копія, оригінал, резолюція, реєстрація документа.

**Література:** [7]; [10]; [14]; [15]; [17]; [18]; [19]; [20]; [21]; [22]; [23]; [24]; [28]; [29].

**Методичні рекомендації**

Облік конфіденційних документів включає присвоєння і реєстрацію в облікових формах і документах реєстраційних номерів, запис облікових і пошукових даних про документи (дата, автор, заголовок, кількість аркушів, місцезнаходження тощо). Основною вимогоюобліку конфіденційних документів є забезпечення схоронності документів, створення можливостей для швидкого знаходження, контролю виконання, наведення необхідних довідок

про документи без залучення самих документів, а також для перевірки наявності документів, що є однією з обов’язкових вимог до конфіденційного діловодства

Обліку підлягають усі без винятку виготовлені на підприємстві, в установі чи організації й отримані ними конфіденційні документи.

Документи з грифом обмеження доступу, які надходять на підприємство, зокрема документи, створені за допомогою автоматизованої електронно-обчислювальної системи, приймаються і обліковуються (реєструються) канцелярією організації, яка веде облік несекретної документації. Як правило, таку роботу виконує працівник, якому доручена робота з такими документами. Облік виданих документів охоплює документи, виготовлені на даному підприємстві в рукописний, машинописний спосіб або з використанням друкувальних пристроїв ЕОМ незалежно від того, направляються ці документи на інші підприємства чи є внутрішніми. Облік документів, що надійшли, охоплює документи, які надійшли від інших підприємств, установ чи організацій.

Облік документів виділеного зберігання (інвентарний облік) охоплює всі документи, що надійшли, та документи, яким присвоюється обліковий номер документів виділеного зберігання на стадії їхнього створення або одержання. До таких документів належать текстові й креслярсько-графічні документи, які через виробничі умови, режим доступу до них або зовнішні особливості (вид носія, формат тощо) неможливо або недоцільно підшивати до справ.Попередня реєстрація (облік) охоплює всі паперові носії, призначені для складання чернеток і проектів документів.

Метою реєстрації (обліку) є забезпечення зберігання та запобігання втрати документів, перевірки наявності, контролю виконання документів, наведення необхідних довідок про документи без використання самих документів, а також максимальне обмеження кола осіб, допущених до роботи з документами, забезпечення їхнього обліку за інформованістю.

При великому документообігу доцільно використати картковий спосіб обліку, адже він скорочує час на пошук документів за рахунок розміщення карток у відповідних рубриках картотек, дає можливість здійснювати ручний контроль виконання документів без виготовлення спеціальних контрольних карток, прискорює і підвищує якість проведення перевірок наявності документів.

При картковому способі обліку документів (як і носіїв) необхідно вести контрольний журнал для кожного виду карткового обліку документів та окремо для носіїв. Журнальна форма реєстрації документів доцільна в установах з обсягом документообігу до 500-600 документів на рік. Для карткової реєстрації всіх документів має застосовуватися єдина реєстраційно-контрольна картка, придатна для оброблення автоматизованою системою. Реєстраційні картки групують у довідкові картотеки, які створюються окремо на кожний календарний рік.

Зазвичай довідкова картка складається з двох частин: невиконані та виконані документи. Перша частина картки використовується для пошуку документа в процесі його виконання за виконавцями, кореспондентами або термінами виконання. Друга частина картки використовується для пошуку виконаних документів з окремих питань.

З метою обмеження доступу до інформації, що містить комерційну таємницю (КТ), керівник повинен видати спеціальний наказ про введення «Переліку відомостей, що містять комерційну таємницю підприємства», заходи щодо охорони цих відомостей, визначення кола осіб, які мають доступ до цієї інформації, правила роботи з документами, що мають гриф «Комерційна таємниця». Відповідальні працівники підприємства повинні під розписку ознайомитися з наказом та додатком до нього. Це можуть бути працівники, для яких робота з документами належить до основних службових обов'язків, або відповідальний працівник, для якого виконання цих функцій становитиме додаткове навантаження.

Зауважте, що гриф конфіденційності, на відміну від грифа таємності, означає, що право власності на інформацію, яка міститься в документі, належить підприємству.

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

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

## Документи з грифом обмеження доступу формують в окрему справу (справи), на обкладинці якої в правому верхньому куті роблять позначку «Комерційна таємниця». На звороті обкладинки вказують список працівників, які мають право користуватися документами, внесеними в цю справу.

## Зберігають такі справи у сейфі, що опечатується посадовою особою, яка відповідає за їхнє зберігання. Доступ до цього сейфа іншим працівникам має бути забороненим.

## Відповідаючи на друге питання вкажіть, що розмноження конфіденційних документів повинне здійснюватися тільки при нагальній службовій необхідності в їхніх додаткових примірниках.

## Конфіденційні документи можуть розмножуватися в підрозділі конфіденційного діловодства або в спеціальному розмножувальному підрозділі підприємства. Розмноження (тиражування) конфіденційних документів у друкарнях методом набору і друкування тексту, як правило, не здійснюється, головним чином, через відсутність потреби у великому тиражі.

## Розмноження конфіденційних документів не повинне відбуватися разом із розмноженням відкритих документів. Під час розмноження конфіденційних документів усе, що не має відношення до їх розмноження, повинно бути прибране з робочих місць, використовуваних при розмноженні, доступ сторонніх осіб у приміщення, в якому відбувається розмноження, не дозволяється.

## При виникненні в процесі розмноження аркушів браку вони поміщуються у спеціальну папку.

## Дозвіл на розмноження документів можуть давати за вимогою керівника підприємства керівники відповідних структурних підрозділів самостійно або разом з керівником служби безпеки (підрозділу конфіденційного діловодства) підприємства. Підписаний керівником підприємства список осіб, що мають право давати дозвіл на розмноження конфіденційних документів, повинен знаходитися в розмножувальному підрозділі.

## Зверніть увагу, на документи, що надійшли з інших підприємств, – вони можуть розмножуватися тільки з письмового дозволу підприємств, що їх видали. Вкажіть, що дозвіл на виготовлення додаткових примірників документа оформляється на звороті останнього листка примірника, з якого повинне проводитися розмноження. Цей примірник не повинен у майбутньому направлятися на інші підприємства, він підшивається в справу або переводиться на облік документів виділеного збереження.

## При неможливості оформлення дозволу на розмноження на самому документі він оформляється у формі обліку даного документа.

## Наголосіть, що розмноженню підлягають документи, які реєструються в підрозділі конфіденційного діловодства або у спеціальному розмножувальному підрозділі у журналі обліку розмноження конфіденційних документів.

## На розмножених примірниках працівник підрозділу конфіденційного діловодства проставляє їхні номери. При цьому, якщо документ був виданий даним підприємством, то номери розмножених примірників продовжують номери раніше виготовлених примірників, якщо документ був виданий іншим підприємством, то на розмножених примірниках їхні номери проставляються дрібно: у чисельнику на всіх примірниках залишається номер, привласнений підприємством, що видало документ, а в знаменнику на кожному примірнику проставляється привласнений йому порядковий номер, починаючи з № 1.

## Розмноження конфіденційних документів у формі зняття копій здійснюється у випадках, коли документи підшиті до справи і зняті з обліку по журналах (картках) обліку цих документів. Технологія виготовлення копій документів аналогічна технології виготовлення додаткових примірників, крім наступних особливостей.

## На примірнику документа, з якого знімалася копія, під дозволом на зняття копії працівником підрозділу конфіденційного діловодства робиться запис «Знята копія в \_\_\_прим. за зв. № \_\_\_\_», що завіряється його підписом із проставленням дати.

## Заповнення граф журналу обліку щодо виданих документів при зніманні копій здійснюється аналогічно заповненню на знову створювані документи.

**Тема:**

**Складання номенклатур, формування і оформлення конфіденційних справ**

**План**

1. Формування і оформлення конфіденційних справ.
2. Складання номенклатур справ, що містять конфіденційні справи.

**Основні поняття:** конфіденційна справа, номенклатура справ, справа, формування справи.

**Література:** [12]; [14]; [17]; [18]; [20]; [21]; [22]; [23]; [24].

## Методичні рекомендації

При розгляді **першого питання**, варто наголосити, що документи з грифом «Для службового користування» після їх виконання формують у справи. Порядок формування цих справ передбачається зведеними номенклатурами справ установи. Документи з грифом «Для службового користування» залежно від виробничої потреби дозволяється формувати у справи окремо або разом з іншими документами з того самого питання. Якщо в установі створюється велика кількість однакових видів документів (наказів, інструкцій, планів тощо) з грифом «Для службового користування» та без цього грифа, доцільно формувати їх в окремі справи. При цьому в графі «Індекс справи» із номенклатури справ до номера справи із документами, що мають гриф «Для службового користування», додається позначка «ДСК».

Якщо документ із грифом «Для службового користування» додається до справи з документами, що не мають такого грифа, на справі ставлять позначку «ДСК», а до номенклатури справ вносять відповідні зміни. В установах, у яких створюють незначну кількість документів із грифом «Для службового користування» загальною номенклатурою справ може бути передбачене запровадження однієї справи із заголовком «Документи із грифом «Для службового користування».

Термін зберігання такої справи не встановлюється, а у відповідній графі номенклатури справ проставляють позначку «ЕК» (експертна комісія). Після закінчення діловодного року справи «Документи з грифом «Для службового користування» переглядають постійні члени експертної комісії установи та у разі потреби приймають рішення про переоформлення документів. Документи постійного зберігання, що містяться у цій справі, формують в окрему справу, якій надають окремий заголовок і яку додатково включають до номенклатури справ. Документи тимчасового зберігання залишають у цій справі згідно із затвердженою номенклатурою справ.

Якщо у справі документи з грифом «Для службового користування» містяться тільки документи тимчасового зберігання, вона може не переоформлятися. Термін зберігання такої справи встановлюють відповідно до найбільшого терміну зберігання документів, що містяться в цій справі. Позначка «ЕК» у графі номенклатури справ «Термін зберігання» закреслюють і зазначають уточнений термін зберігання.

Справи з документами без грифа обмеження доступу, у яких накопичуються окремі документи з грифом «Для службового користування», неохідно віднести до категорії обмеженого розповсюдження і використання. На обкладинках і на титульному аркуші цих справ також проставляють гриф «Для службового користування», а в загальну номенклатуру справ вносять відповідні уточнення. Кожна справа повинна мати не більш 250 аркушів (якщо більше, то заводиться новий том з тим самим заголовком, що і заголовок даної справи). Формування справ відбувається шляхом підшивки документів в обкладинки. Оформлення конфіденційної справи включає опис справи на обкладинці, проставляння на внутрішній стороні обкладинки ініціалів і прізвищ осіб, допущених до справи, заклад картки обліку видачі справи, заповнення опису справи, складання завірчого напису, прошивання справи. Написи на обкладинках повинні робитися чітко, світлостійким чорнилом або тушшю.

Готуючи відповідь на **друге питання**, варто зазначити, що номенклатура справ із грифом «Для службового користування» – це оформлений у встановленому порядку систематизований перелік найменувань справ, які створюються в установі, із вказівкою їхніх індексів, термінів збереження й осіб, яким надане право користування справами.

Водночас номенклатура є й обліковим документом для заведених конфіденційних справ з грифом «Для службового користування». Крім того, вона використовується для перевірки наявності конфіденційних справ, може бути використана як схема побудови довідкової картотеки для документів і складання описів справ постійного і довгострокового (понад 10 років) збереження, переданих в архів підприємства.

Підкресліть, що номенклатура справ із грифом «Для службового користування» повинна бути самостійним документом, її не потрібно поєднувати з номенклатурою відкритих справ, тому що склад граф цих номенклатур має істотні розходження. Номенклатура конфіденційних справ із грифом «Для службового користування» розробляється для підприємства в цілому (зведена номенклатура справ). Вона складається на кожен рік (наприкінці поточного року на наступний рік ) підрозділом конфіденційного діловодства на основі письмових пропозицій структурних підрозділів установи. Крім того, у номенклатуру включаються конфіденційні справи із грифом «Для службового користування», що надійшли з інших підприємств: закриті справи минулих років – у номенклатуру справ відповідного року, незакриті – у номенклатуру справ поточного року. До розроблення номенклатури повинні залучатися кваліфіковані фахівці, номенклатура підписується керівником підрозділу конфіденційного діловодства (начальником канцелярії) установи, візується керівниками зацікавлених структурних підрозділів, узгоджується з архівом установи, розглядається на засіданні постійно діючої експертної комісії підприємства і затверджується керівником установи. Якщо таких змін немає, то на кожен наступний рік (до 5 років) номенклатура передруковується (з можливими незначними змінами), підписується керівником підрозділу конфіденційного діловодства, затверджується керівником підприємства і вводиться в дію без вищеперерахованих погоджень.

Номенклатура повинна мати відповідний гриф конфіденційності, видаватися в двох екземплярах і реєструватися в журналі обліку виданих документів з грифом «ДСК». Перший екземпляр номенклатури зберігається в підрозділі конфіденційного діловодства і по закінченні року підшивається в спеціальну справу, другий передається в архів установи. Після затвердження номенклатури справ можливі протягом року зміни в неї вносяться керівником підрозділу конфіденційного діловодства (із проставленням підпису) на підставі доповідних записок керівників підрозділів установи.

Систематизація конфіденційних справ у номенклатурі повинна здійснюватися з врахуванням їхньої важливості і взаємозв'язку, що прискорює пошук документів. Справи з планами і звітами розташовуються в послідовності термінів їхнього збереження.

Справа з номенклатурою конфіденційних справ, конфіденційні і відкриті журнали (картотеки) обліку конфіденційних документів, а також відкриті справи з матеріалами на конфіденційні документи (реєстри, квитанції, розписки на відправлені документи, акти перевірок наявності документів та ін.) містяться наприкінці номенклатури, що не має розподілу за розділами, а при наявності розділів у розділі, що відповідає назві підрозділу конфіденційного діловодства за умови структурної побудови номенклатури справ.

Кожній справі привласнюється самостійний цифровий індекс, що складається з номера структурного підрозділу (при структурній схемі побудови номенклатури) або номера напрямку (при виробничо-галузевій схемі) і через тире порядкового номера справи в межах кожного розділу, наприклад: 01-01, 01-02, 02-01 і т.д. У номенклатурі, що не має розподілу на розділи, замість індексу справи проставляється його порядковий номер за номенклатурою. Після закінчення року в номенклатурі зазначається кількість заведених справ постійного і тимчасового зберігання та перехідних на наступний рік.

**Тема:**

**Організація захисту інформації з обмеженим доступом в електронному документообігу**

1. Особливості роботи з конфіденційними документами в електронному документообігу.
2. Захист інформації з обмеженим доступом в електронному документообігу.

**Основні поняття:** електронний документообіг, електронний підпис, електронний цифровий підпис, захист інформації в системі, комплексна система захисту інформації, центри сертифікації ключів.

**Література:** [6]; [7]; [9]; [15]; [16]; [25]; [26]; [27]; [32].

**Методичні рекомендації**

Підготовка відповіді на **перше питання** повинна розпочатися з визначення електронного документа. Скористайтеся для цього «Законом про електронні документи» (ст.5), а саме електронний документ – це документ, інформація в якому зафіксована у формі електронних даних, включаючи обов’язкові реквізити документа. Склад та порядок розміщення обов’язкових реквізитів електронних документів визначається законодавством.

Наголосіть, що електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму. Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для сприймання його змісту людиною. Детальні вимоги щодо складу і порядку розміщення обов'язкових реквізитів електронних документів будуть визначатися спеціальними нормативними актами.

Оригіналом електронного документа вважається електроннийпримірник документа з обов’язковими реквізитами, у такому разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації, передбачає що кожний з електронних примірників буде вважатися оригіналом електронного документа.

Якщо автором створюється ідентичний за документальною інформацією і реквізитами електронний документ та документ на папері, – кожен з документів є оригіналом і має однакову юридичну силу.

Продовжуючи відповідь, зазначте, що відповідно до ст. 1 Закону України «Про електронний цифровий підпис», під терміном ЕЦП розуміють вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати особу, що його підписувала.

Закон України «Про електронні документи та електронний документообіг» в статті 6 також зазначає, що електронний підпис є обов'язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу.

Накладанням електронного підпису завершується створення електронного документа. Відносини, пов'язані з використанням електронних цифрових підписів, регулюються законом. Дійсність ЕЦП перевіряється за допомогою відкритого ключа – коду перевірки, доступного решті суб'єктів електронного документообігу.

Щоб кожний «підписант» мав свій, унікальний, підпис, використовується так званий особистий ключ – код, який має бути відомий лише його власникові. Якщо цей код повідомити програмі, то відповідно до криптографічного алгоритму вона сформує унікальне контрольне значення і додасть його до документа. Тобто підпише електронний документ унікальним ЕЦП господаря даного особистого ключа.

Для перевірки вірогідності ЕЦП та цілісності електронного документа використовується інший код – так званий відкритий ключ. На відміну від особистого, відкритий ключ доступний усім іншим зацікавленим учасникам електронного документообігу. Цей код не дозволяє підробити ЕЦП автора електронного документа, але дозволяє перевірити його справжність. Відкритий ключ має бути сертифікований центром сертифікації ключів. Застосування будь-яких інших видів електронного підпису допускається на договірних засадах.

Отримавши цей код, програма, використовуючи вже згаданий алгоритм, звірить його з отриманим разом з документом ЕЦП автора. Якщо ці контрольні значення зійдуться, підпис вважатиметься справжнім, а отриманий документ – цілісним.

Щоб підвищити ступінь довіри суб’єктів правовідносин до системи ЕЦП і зменшити ймовірність підробки таких підписів, законодавці передбачили в Законі «Про ЕЦП» першу «лінію оборони» ‑ сертифікацію відкритих ключів спеціальними організаціями ‑ Центрами сертифікації ключів (ЦСК), і другу «лінію оборони» ‑ посилені сертифікати ключів.

У разі неможливості зберігання електронних документів на електронних носіях інформації протягом певного строку, встановленого законодавством для відповідних документів на папері, суб’єкти електронного документообігу повинні вживати заходів із дублювання документів на кількох електронних носіях інформації та здійснювати періодичне копіювання їх відповідно до порядку обліку й копіювання документів, встановленого законодавством. Якщо виконати зазначені вимоги неможливо, електронні документи повинні зберігатись у вигляді копії документа на папері (за відсутності оригіналу цього документа на папері).

Якщо автор і адресат у письмовій формі попередньо не домовилися про інше, датою і часом відправлення електронного документа вважаються дата і час, коли відправлення електронного документа не може бути скасовано особою, яка його відправила. У разі відправлення електронного документа шляхом пересилання його на електронному носії, на якому записано цей документ, датою і часом відправлення вважаються дата і час здавання його для пересилання. Електронний документ вважається одержаним адресатом з часу надходження авторові повідомлення в електронній формі від адресата про одержання цього електронного документа автора, якщо інше не передбачено законодавством або попередньою домовленістю між суб’єктами електронного документообігу.

Зверніть увагу, що при копіюванні електронного документа з електронного носія інформації обов’язково здійснюється перевірка цілісності даних на цьому носії. Основним безпосереднім об’єктом злочину є встановлений режим інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або на носіях такої інформації. Пам’ятайте, що додатковим об’єктом може бути авторське право або інші нематеріальні блага. Ст. 361-2 передбачає спеціальний предмет злочину. Це інформація з обмеженим доступом (ІзОД), яка зберігається в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або на носіях такої інформації.

Інформація, яка зберігається (обробляється) в ЕОМ, автоматизованних системах, комп’ютерних мережах або на носіях такої інформації – це текстова, цифрова, графічна чи інша інформація (дані, відомості) про осіб, предмети, події, явища, що існує в електронному вигляді, і може використовуватися, оброблятися чи змінюватися за допомогою ЕОМ (комп’ютерів).

**Методичні рекомендації до виконання та оформлення курсових робіт**

Курсова робота (КР) допомагає студентові оволодіти навичками проведення сучасних наукових досліджень. Оскільки «Конфіденційне діловодство» є професійно-орієнтованою дисципліною у підготовці фахівців зі спеціальності «Документознавство та інформаційна діяльність, тому написання курсової роботи є також підготовчим етапом до виконання та захисту дипломної роботи на здобуття освітнього рівня «Магістр» або «Спеціаліст». Виконання курсової роботи необхідно розпочати зі складання бібліографії проблеми та списку (джерел) літератури за темою роботи. Після того починається новий етап — **робота над джерелами** (літературою). Починати треба із вивчення спеціальної наукової літератури. Це дає можливість студентові ознайомитися з рівнем розроблення в документознавчій літературі обраної ним теми. Вагоме значення для написання курсової роботи мають **джерела.** Тому, чим ширша залучена документальна база, тим переконливішими будуть висновки і якість самої роботи.

На наступному етапі необхідно розробити **зміст** курсової роботи, який традиційно містить три розділи. Зміст курсової роботи складається залежно від тих питань, які досліджуються, але, як правило, він включає такі структурні елементи:
1) вступ; 2) розділи, у яких висвітлюється основний зміст обраної теми; 3) висновки; 4) список використаних джерел (літератури). Однією з найскладніших і найважливіших частин курсової роботи є **вступ,** у якому визначається актуальність теми. Формулюється мета та завдання роботи, подається стислий історіографічний огляд літератури з означеної теми. При цьому недостатньо обмежуватися лише переліком авторів чи назвами книг, а потрібно стисло охарактеризувати значення тієї чи іншої праці, яка згадується при розробленні проблеми. Курсова робота складається з розділів, які в свою чергу, можуть поділятися на підрозділи, пункти і підпункти, де викладається основний матеріал теми відповідно до змісту. Виклад матеріалу має бути логічним, послідовним та лаконічним. Необхідно уникати повторювань, нечітких формулювань. Цитуючи джерела (літературу) під час викладу матеріалу, обов’язково треба робити на них посилання із зазначенням номерів сторінок. **Висновки** мають відповідати основному змісту роботи, бути конкретними і підсумовувати відповіді на питання змісту.

**Список літератури** оформлюють відповідно до вимог вищої школи: в алфавітному порядку, з наведенням усіх вихідних даних джерел.

**Обсяг** курсової роботи 25-30 друкованих аркушів формату

А-4 (шрифт – 14, інтервал – 1,5).

**Орієнтовні теми курсових робіт**

1. «Конфіденційна інформація» і «таємна інформація»: сутність та зміст понять.
2. «Комерційна таємниця» і «банківська таємниця»: сутність та зміст понять.
3. «Державна таємниця»: сутність та зміст поняття і використання у конфіденційному діловодстві.
4. Нормативно-законодавче забезпечення конфіденційного діловодства України: проблеми та перспективи.
5. Організаційно-технологічні особливості конфіденційного діловодства.
6. Поняття і принципи організації конфіденційного документообігу.
7. Дозвільна система доступу до конфіденційних документів.
8. Специфіка відправлення конфіденційних документів.
9. Проведення експертизи цінності конфіденційних документів.
10. Порядок зберігання конфіденційних документів і користування ними.
11. Відбір та підготовка конфіденційних справ і документів для архівного зберігання.
12. Відбір та підготовка конфіденційних справ і документів для знищення.
13. Режим зберігання конфіденційних документів.
14. Зберігання архівних документів з обмеженим доступом у державних архівних установах.
15. Специфіка розмноження і розсилання конфіденційних документів.
16. Державна статистична звітність з питань Державної таємниці.
17. Специфіка електронного документообігу в конфіденційному діловодстві.
18. Місце та специфіка конфіденційного діловодства в загальному діловодстві.
19. Аналіз видів конфіденційної інформації.
20. Організаційно-правові засади роботи з конфіденційними документами.
21. Конфіденційне діловодство як важлива складова системи захисту конфіденційної інформації, що є власністю юридичних осіб.
22. Гриф «Для службового користування»: специфіка використання у конфіденційному діловодстві.
23. Значення конфіденційного діловодства для забезпечення ефективності та вдосконалення управлінської діяльності в бізнесі.
24. Національна система конфіденційного зв’язку: правові засади та функціонування.
25. Організаційні та технологічні аспекти розмежування доступу в інформаційні системи захищеного електронного документообігу.

**Список рекомендованої літератури**

Основний

1. Конституція України [Електронний ресурс] : Прийнята на п’ятій сесії Верхов. Ради України 28 червня. 1996 р. / Верхов. Рада України. – Офіц. вид. – К. : Алерта, 2013. – 30 с. – Поточна редакція Тлумачення від 15 травня 2014 р.. – Режим доступу : zakon.rada.gov.ua. – Заголовок з екрана.
2. Кодекс законів про працю України [Електронний ресурс] : Закон від 10 грудня 1971 р. № 332-08. – Поточна редакція від 8 лютого 2015 р. – Ст. 147‑151. – Режим доступу : zakon.rada.gov.ua. – Заголовок з екрана.
3. Кримінальний кодекс України [Електронний ресурс] : Закон України від 5 квітня 2011 р. – № 2341-14. – Поточна редакція від 8 лютого 2015 р. – Ст. 52‑53, 55‑57, 60‑61, 111, 361‑2. – Режим доступу : zakon.rada.gov.ua. – Заголовок з екрана.
4. Кодекс України про адміністративні порушення [Електронний ресурс] : Закон від 7 грудня 1984 р. – № 8073-Х. – Поточна редакція від 8 лютого 2015 р. – Ст. 9, 12, 14, 24, 31. ‑ Режим

доступу : zakon.rada.gov.ua. – Заголовок з екрана.

1. Про доступ до публічної інформації [Електронний ресурс] : Закон України від 13 січня 2011 р.. – Режим доступу : zakon.rada.gov.ua. – Заголовок з екрана.
2. Про захист інформації в автоматизованих системах [Електронний ресурс] : Закон України від 5 липня 1994 р. – Режим доступу : zakon.rada.gov.ua. – Заголовок з екрана.
3. Про інформацію [Текст] : Закон України від 2 жовтня 1992 р. № 2657-ХII // Відомості Верховної Ради України. – 1992. – № 48. – Зміни внесено законом України: про внесення змін до Закону України «Про інформацію» від 13 січня 2011 р. № 2938-VI // Відомості Верховної Ради України. – 2011. – № 32.
4. Про державну таємницю [Електронний ресурс] : Закон України від 21 вересня 1999 р. № 3855-XII. – Режим доступу : zakon.rada.gov.ua. – Заголовок з екрана.
5. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : Закон України від 5жовтня 1994 р. № 31 // Відомості Верховної Ради. – Режим доступу : zakon.rada.gov.ua. – Заголовок з екрана.
6. Про електронні документи та електронний документообіг [Текст] : Закон України від 22 травня 2003 р. // Відомості Верховної Ради України. – 2003. ‑ № 36. – Зміни внесено Законом України «Про електронні документи та електронний документообіг» від 31 травня 2005 р. № 2599-ІV // Відомості Верховної Ради України. – 2005. – № 126.
7. Про Національний архівний фонд і архівні установи [Текст] :Закон України від 24 грудня 1993 р. № 3814-ХII (зі змінами) // Відомості Верховної Ради України. – 1994. – № 15. Зміни внесено законом України: Про внесення змін до Закону України «Про Національний архівний фонд і архівні установи» від 13 грудня 2001 р. № 2888-ІІІ // Відомості Верховної Ради України. – 2002. – № 11.
8. Про обов’язковий примірник документів [Текст] : Закон України від 9 квітня 1999 р. № 595-ХІV // Відомості Верховної Ради України. – Закону 1999. – № 22/23. – зміни внесено Законом України: Про внесення змін до ст. 8 закону України «Про обов’язковий примірник документів» // Відомості Верховної Ради України. – 2007. – № 27.
9. Цивільний кодекс України [Електронний ресурс] : Закон України від 16 січня 2003 р. – № 435-IV. – Поточна редакція

від 6 лютого 2015 р. – Ст. 200. – Режим доступу : zakon.rada.gov.ua. – Заголовок з екрана.

1. Діловодство й архівна справа. Терміни та визначення понять [Текст] : ДСТУ 2732-2004. – Чинний від 2004-05-28. – К. : Держспоживстандарт України, 2005. – 31 с.
2. Захист інформації. Технічний захист інформації. Основні положення [Текст] : ДСТУ 3396.0-96 Введ. 1 січня 1997 р. – К. : Держкомстандарт України, 1996. – 26 с.
3. Захист інформації. Технічний захист інформації. Порядок проведення робіт [Текст] : ДСТУ 3396.1-96 Введ. 1 липня 1997 р. – К. : Держкомстандарт України, 1996. – 18 с.
4. Інформація та документація. Базові поняття. Терміни та визначення [Текст] : ДСТУ 2392-94. – Вид. офіц. – К. : Держстандарт України, 1994. – 41 с.
5. Інструкція про порядок обліку, зберігання і використання документів, справ та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави. [Текст] : Затверджена постановою Кабінету Міністрів України від 27 листопада 1998 р. ‑ № 48. – Cт. 1764.
6. Головань С. М. Ведення документів з грифом секретності: [Текст] : навч. посіб. / С. М. Головань. – К. : НАУ, 2003. – 176 с.
7. Головань С. М. Загальне діловодство та ведення документів, що містять інформацію з грифом «Для службового користування» [Текст] : навч.-метод. посіб. / С. М. Головань. – К. : НАУ, 2003. – 92 с.
8. Конфіденційне діловодство [Текст] : підруч. / О. Л. Голубенко, В. О. Хорошко, О. С. Петров, С. М. Головань. – Луганськ : СНУ ім. В. Даля, 2009. – 208 с.
9. Конфіденційне діловодство. Практикум [Текст] : навч. посіб. / О. Л. Голубенко, В. О. Хорошко, О. С. Петров, С. М. Головань. – Луганськ : СНУ ім. В. Даля, 2010. – 180 с.
10. Конфіденційний документообіг [Текст] : навч. посіб. / С. М. Головань, В. В. Поповський, В. О. Хорошко. – К. : ДУІКТ, 2007. – 264 с.
11. Організація конфіденційного діловодства [Текст] : підруч. / А. Г. Габович, С. М. Головань, С. І. Жлобін, В. О. Хорошко. – К. : ДУІУТ, 2005. – 376 с.

**Додатковий**

25.Актуальні проблеми забезпечення інформаційної безпеки держави [Текст] : зб. Матеріалів науково-практ. конфер. (2009, Київ) 20 березня 2009 / В. П. Мікулін; Нац. акад.. служби безпеки України. – К., 2009. – 200 с.

1. Головань С. М. Концепція створення системи електронних документів [Текст] / С. М. Головань, О. О. Мелешко, Л. М. Щербак // Науково-технічний журнал «Захист інформації». – 2005. – № 2. – С. 63‑67 с.
2. Головань С. М. Процеси оцінки безпеки електронного документообігу [Текст] / С. М. Головань, А. М. Давиденко, Л. М. Щербак // Науково-технічний журнал «Захист інформації». – 2005. – № 4. – С. 107‑111.
3. Головань С. М. Організація роботи підрозділу захисту інформації з обмеженим доступом [Текст] / С. М. Головань, А. М. Давиденко, В. О. Хорошенко, Л. М. Щербак // Науково-технічний журнал «Захист інформації». – 2006. – № 1. – С. 79‑825.
4. Документаційне забезпечення робіт із захисту інформації з обмеженим доступом [Текст] : підруч. / С. М. Головань, В. Б. Дудикевич, В. С. Зачепило, В. О. Хорошко, Л. М. Щербак. – Львів : Львівська політехніка, 2005. – 288 с.
5. Правові основи захисту інформації з обмеженим доступом [Текст] : курс лекцій / А. І. Марущак. – К. : КНТ, 2007. – 208 с.
6. Сучасне діловодство: зразки документів, діловий етикет [Текст] : довідник / Уклад. В. Бріцин. – К. : Довіра, 2010. – 687 с.
7. Філіпова Л*.* Системи управління електронним документообігом: загальні поняття термінології, організації, технології (зарубіжний досвід) [Текст] / Л. Філіпова // Вісник Книжкової палати. – 2001. – № 4. – С. 15–18.

**Зміст**

Вступ………………………………………………………………...4

Методичні рекомендації до індивідуальних занять……………. 6

Методичні рекомендації до виконання та оформлення курсових робіт…………………………………………………………….… 25

Список рекомендованої літератури….……………………….… 27

*Навчальне видання*

Конфіденційне

діловодство

Методичні рекомендації

до самостійної роботи

для студентів напряму підготовки

6.020105 «Документознавство

та інформаційна діяльність»

Укладач

Ількова Оксана Григорівна

Редактор *Є. Г. Кравченко*

Технічний редактор *А. І. Лавринович*

Коректор *О. О. Крусь*

Комп’ютерна верстка *Н. В. Чорної*

Підп. до друку 31.03.2016. Формат 60х84/16. Папір офс.

Офс. друк Ум. друк. арк. 1,86. Обл.-вид. арк. 2,0.

Тираж 100 прим. Замовлення № 36-1.

Видавець і виготівник

Національний авіаційний університет

03680, Київ-58, проспект Космонавта Комарова, 1

Свідоцтво про внесення до Державного реєстру ДК № 977 від 05.07.2002