ЗАТВЕРДЖЕНО
Наказ Вищого навчального закладу
Укоопспілки «Полтавський університет
економіки і торгівлі»
18 квітня 2019 року № 88-Н

Форма № П-4.04

Вищий навчальний заклад Укоопспілки
«ПОЛТАВСЬКИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТОРГІВЛІ»
Навчально-науковий інститут бізнесу та сучасних технологій
Форма навчання заочна
Кафедра менеджменту

Допускається до захисту
Завідувач кафедри _____ Л.М. Шимановська-Діанич
«_____» червня 2021 р.

ДИПЛОМНА РОБОТА

на тему «Керування потоками робіт і організація конфіденційного документообігу» (за матеріалами Товариства з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком»)

зі спеціальності 029 Інформаційна, бібліотечна та архівна справа
освітня програма «Документознавство та інформаційна діяльність»

Виконавець роботи Бондаренко Богдан Едуардович

_____
(підпис, дата)

Науковий керівник д.і.н., професор Оніпко Тетяна Володимирівна

_____
(підпис, дата)

Рецензент Молчанова Наталія Юріївна

ПОЛТАВА 2021

ЗМІСТ

ВСТУП

Сучасний період розвитку суспільства та держави характеризується значним зростанням ролі інформації, інформаційних ресурсів, інформаційних технологій, що призводить до активізації інформаційних відносин, які виникають в усіх сферах життєдіяльності держави і суспільства в процесі здійснення певного виду інформаційної діяльності, а саме: створення, збирання, одержання, зберігання, використання, поширення, охорона та захист різноманітних відомостей.

Інформація набуває важливого значення і в економічній сфері, зокрема в підприємницькій діяльності, виступаючи як самостійним об'єктом господарського обороту, так і важливою передумовою успішного ведення справ суб'єктами господарювання. Тому сьогодні особливо актуальним стає дослідження законодавчого врегулювання і забезпечення захисту прав власників так званих «інформаційних об'єктів», до числа яких належить інформація з обмеженим доступом.

Специфіка господарювання в умовах ринкової економіки та конкуренції між суб'єктами господарювання, примушує серйозно ставитися не лише до правової, але й інформаційної безпеки господарської діяльності. У сучасних умовах здійснення підприємницької діяльності науково-технічна, технологічна, економічна та інша актуальна інформація, що дозволяє отримати пріоритет на ринку товарів та послуг, є рушійною силою конкуренції, а в багатьох випадках – основною умовою економічного виживання суб'єкта господарювання.

У сучасній ринковій економіці обов'язковою умовою успіху підприємця у бізнесі, отримання прибутку та збереження в цілісності створеної ним організаційної структури є забезпечення економічної безпеки його діяльності. Одна з головних складових частин економічної безпеки – інформаційна безпека, яка досягається за рахунок використання комплексу систем, методів та засобів захисту інформації підприємця від можливих зловмисних дій конкурентів та з метою збереження її цілісності та конфіденційності.

Інформація, що використовується підприємцем у бізнесі та управлінні підприємством, банком, компанією чи іншою структурою є його власною або приватною інформацією, яка являє собою істотну цінність. Ця інформація є його інтелектуальною власністю.

В умовах тотальної інформатизації суспільства важливу роль відіграють питання захисту інформації, особливо – інформації з обмеженим доступом, насамперед через недопущення її спотворення, порушення цілісності, неправомірного використання тощо. Захист ділової, фінансової, технологічної та іншої інформації від крадіжок, несанкціонованого використання, її зміни чи знищення набуває важливого значення в сучасних умовах розвитку інформаційних технологій. Жорстка конкурентна боротьба комерційних структур змушує їх вживати заходів щодо захисту такої інформації, спираючись на відповідні норми чинного законодавства та власну нормативно-правову основу, а захист інформації із обмеженим доступом є одним з першочергових завдань забезпечення інформаційної безпеки.

З огляду на це проблема керування потоками робіт і організації конфіденційного документообігу на підприємствах є актуальною і такою, що потребує досліджень.

Проблемі керування потоками робіт і організації конфіденційного документообігу на підприємствах приділяли увагу такі дослідники: О.В. Адабаш, А.О. Антонюк, В.Ю. Баскаков, А.Г. Габович, О.Р. Гарасим, О.В. Гладківська, С.М. Головань, С.Г. Гордієнко, С.Л. Ємельянов, І.М. Забара, О.О. Коренюк, О.Б. Кукарін, О.О. Кулініч, В.А. Ліпкан, А.І. Марущак, Т.М. Мужанова, А.С. Нерсесян, О.С. Петров, В.Т. Савицький, О.О. Федоренко, В.О. Хорошко, Л.Б. Чирун, О.О. Шарабурина, Л.М. Щербак та ін.

Мета дипломної роботи полягає у теоретичному обгрунтуванні проблеми керування потоками робіт і організації конфіденційного документообігу та за результатами виконаного дослідження надання рекомендацій щодо удосконалення організації конфідеційного документообігу у Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком».

Згідно з даною метою було визначено такі завдання:

– розкрити сутність та види конфіденційної інформації;

– розглянути теоретичні аспекти документування інформації конфіденційного характеру;

– з’ясувати поняття та основні принципи конфіденційного документообігу;

– охарактеризувати діяльність Товариства з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком»;

– дослідити основні етапи кофіденційного документообігу у Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком»;

– проаналізувати особливості роботи з конфіденційною кадровою документацією у Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком»;

– визначити складові системи захисту конфіденційної інформації на підприємстві;

– з’ясувати порядок зняття грифу обмеженого доступу та забезпечення збереженості конфіденційних документів на підприємстві;

– обґрунтувати основні шляхи підвищення ефективності конфіденційного документобігу у Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком».

Об’єктом дослідження є процеси керування потоками робіт і організації конфіденційного документообігу на підприємстві.

Предметом дослідження є теоретико-методологічні засади керування потоками робіт і організації конфіденційного документообігу на підприємстві й методичні підходи до його вдосконалення.

Суб’єктом дослідження є Товариство з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком».

Для вирішення завдань, спрямованих на досягнення мети роботи, було використано комплекс загальнонаукових методів дослідження.

Методи систематизації й використання інформаційного матеріалу (аналізу, синтезу, абстрагування, індукції, дедукції, теоретичного узагальнення,

порівняння, класифікації) використані для дослідження теоретичних основ організації конфіденційного документообігу, зокрема з'ясування сутності понять «конфіденційна інформація», «конфіденційний документ», «конфіденційний документообіг», «конфіденційне діловодство» тощо, а також визначенні напрямів удосконалення організації конфіденційного документообігу на досліджуваному підприємстві.

За домогою методу контент-аналізу здійснено аналіз інформаційного наповнення сайту досліджуваного підприємства.

Метод причинно-наслідкового аналізу застосований для з'ясування впливу сучасних інформаційно-комунікаційних технологій на організацію конфіденційного документообігу на підприємстві.

Графічний метод використаний для унаочнення окремих теоретичних положень і висновків дипломної роботи.

Інформаційно-методологічною базою дослідження є: вітчизняна законодавча й нормативно-правова база, зокрема Закон України «Про інформацію» (1992 р.), Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (1994 р.), Закон України «Про електронні документи та електронний документообіг» (2003 р.); «Про захист персональних даних» (2010 р.), Закон України «Про доступ до публічної інформації» (2011 р.); монографії; навчальні посібники; статті з досліджуваної проблеми у періодичних виданнях; електронні ресурси мережі Інтернет; документи суб'єкта дослідження, матеріали сайту суб'єкта дослідження тощо.

Практичне значення одержаних результатів полягає в наданні рекомендацій щодо удосконалення організації конфіденційного документообігу на підприємстві, зокрема у Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком».

Структура і обсяг роботи. Робота складається зі вступу, трьох розділів, дев'яти підрозділів, висновків, рекомендацій, списку інформаційних джерел. Робота містить 90 сторінок основного тексту, 14 рисунків, 2 таблиці, 8 додатків. Список інформаційних джерел налічує 78 найменувань.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ КЕРУВАННЯ ПОТОКАМИ РОБІТ І ОРГАНІЗАЦІЇ КОНФІДЕНЦІЙНОГО ДОКУМЕНТООБІГУ

1.1 Сутність та види конфіденційної інформації

Сучасний період розвитку суспільства характеризується значним зростанням ролі інформації, інформаційних ресурсів, інформаційних технологій, що призводить до активізації інформаційних відносин, які виникають в усіх сферах життєдіяльності суспільства.

Згідно Закону України «Про інформацію», інформація – це будь-які відомості та (або) дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом [10]. Відкритою є будь-яка публічна інформація, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Загальновизнано, що інформація з обмеженим доступом має як моральну, так і матеріальну цінність для осіб, що нею володіють. На відміну від відкритої інформації, інформація з обмеженим доступом не призначена для широкого розповсюдження. Інформація з обмеженим доступом – це така інформація, доступ до якої має лише обмежене коло осіб і оприлюднення якої заборонено розпорядником інформації відповідно до закону [20]. Обмеження доступу до інформації здійснюється в інтересах національної безпеки або охорони законних прав фізичних та юридичних осіб. Обмеженню доступу підлягає інформація, а не документ. Якщо документ містить інформацію з обмеженим доступом, для ознайомлення надається інформація, доступ до якої необмежений [77].

Згідно статті 21 Закону України «Про інформацію» та статті 6 Закону України «Про доступ до публічної інформації» до інформації з обмеженим доступом належать конфіденційна інформація, службова інформація та таємна інформація (рис. 1.1).

Рисунок 1.1 – Види інформації з обмеженим доступом, складено автором за [6; 10]

Конфіденційна інформація – це підвид інформації з обмеженим доступом. Стосовно визначення поняття «конфіденційна інформація», то слід зазначити, що лексичним значенням слова «конфіденційний» є таке поняття: «який не підлягає розголошенню, довірчий, таємний» [47].

Конфіденційна інформація (від англ. confidence – довіра) – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням [45]. У законодавстві України наводяться визначення поняття «конфіденційна інформація» (табл. 1.1).

Таблиця 1.1 – Визначення поняття «конфіденційна інформація» у законодавстві України, складено автором за [6; 10]

Стаття 21 Закону України «Про інформацію» (1992 р.)	Стаття 7 Закону України «Про доступ до публічної інформації» (2011 р.)
Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.	Конфіденційна інформація – це інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов. Не може бути віднесена до конфіденційної інформація, зазначена в частині першій і другій статті 13 цього Закону.

У статті 21 Закону України «Про інформацію» зазначено: конфіденційна інформація – це інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних

повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом [10]. Відносини, пов’язані з правовим режимом конфіденційної інформації, регулюються законом.

У статті 7 Закону України «Про доступ до публічної інформації» наведено таке визначення: конфіденційна інформація – це інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов [6].

О.В. Адабаш зазначає, що конфіденційна інформація – це інформація, обмежений доступ до якої та порядок поширення визначено фізичною або юридичною особою (крім суб’єктів владних повноважень). Правове регулювання суспільних відносин, які виникають з приводу інформації з обмеженим доступом, чітко не врегульовані у національному законодавстві України. Слід вести мову не лише про відсутність чіткого розмежування конфіденційної та таємної інформації, але й досить безсистемним викладенням положень, які стосуються будь-якої інформації з обмеженим доступом [11].

Одним із суттєвих проявів недосконалості інформаційного законодавства є відсутність чітких законодавчих критеріїв для визначення конфіденційної інформації, порядку та умов віднесення інформації до конфіденційної.

У науковій літературі здійснювались спроби визначити окремі види відомостей, що можуть належати до конфіденційної інформації у сфері господарської (підприємницької) діяльності.

На думку О. О. Кулініч, конфіденційною інформацією може бути будь-яка інформація з обмеженим доступом, не віднесена чинним законодавством до державної таємниці [51].

Конфіденційну інформацію в сфері господарської діяльності можна умовно поділити на три сектори: ділова інформація суб'єкта господарювання; інформація, що стосується безпосередньо фактичних даних про суб'єкта

господарювання (інформація персонального характеру); ноу-хау – так звані секрети виробництва [52, с. 143].

Перша частина інформації стосується безпосередньо інформації про діяльність суб'єкта господарювання в певній сфері, а саме: різноманітні бази даних (клієнтів, адрес, контрагентів), результати досліджень статистичного, маркетингового характеру, коньюктури споживчого ринку, тощо.

Другий блок інформації стосується інформації, яка характеризує суб'єкта господарювання та нерозривно пов'язана із ним, як наприклад: відомості про банківські рахунки, масштаби виробництва та різноманітні угоди, що укладаються даним підприємством, тощо.

Третій блок інформації можна умовно позначити як «ноу-хау» – сукупність технічних, технологічних, комерційних та інших знань, оформлених у вигляді технічної документації, навиків та виробничого досвіду, необхідних для організації того чи іншого виду виробництва, але не запатентованих [52, с. 145].

Х. Буртник, аналізуючи проблему визначення конфіденційної інформації робить висновок про те що:

– конфіденційною є інформація про фізичну або юридичну особу, крім суб’єктів владних повноважень, яка обмежена у доступі цією особою, а також попередньо обмежена законодавством до моменту, поки особа не відкриє таку інформацію за власним бажанням;

– така інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом;

– законодавством може бути заборонено віднесення певної інформації до обмеженої у доступі, зокрема і конфіденційної [13].

Розпорядники інформації, які володіють конфіденційною інформацією, можуть поширювати її лише за згодою осіб, які обмежили доступ до інформації, а за відсутності такої згоди – лише в інтересах національної безпеки, економічного добробуту та прав людини, що передбачено статтею 7 Закону України «Про доступ до публічної інформації» [6].

Конфіденційну інформацію можна поділити на дві категорії: конфіденційна інформація, що є власністю держави, конфіденційна інформація, що не є власністю держави.

Конфіденційна інформація, що є власністю держави, знаходиться в користуванні органів державної влади або органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності.

Конфіденційна інформація, що не є власністю держави, належить громадянам, юридичним особам, які володіють інформацією ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їхнього професійного, ділового, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці. Власники такої інформації самостійно визначають режим доступу до неї, включаючи належність до категорії конфіденційної, та встановлюють для неї систему (спосіб) захисту. Склад і обсяг таких відомостей та порядок їх захисту визначає суб'єкт господарювання [45].

Комерційна таємниця належить до різновидів конфіденційної інформації, що не є власністю держави. Комерційна таємниця – це виробнича, науково-технічна, управлінська, фінансова та інша інформація, що використовується для досягнення комерційних цілей (одержання прибутку, уникнення збитків, чесного здобуття переваги над конкурентами) і яка вважається конфіденційною [24]. До конфіденційної інформації належать також ідеї, винаходи, відкриття, технології, індивідуальні особливості комерційної діяльності, що дають змогу успішно конкурувати тощо.

У статті 36 Господарського Кодексу України поняття «комерційна таємниця» визначається як відомості, що не є державною таємницею, пов'язані з виробництвом, технологією, управлінням, фінансовою та іншою діяльністю підприємства, розголошення яких може завдати шкоди інтересам цього підприємства. Статтею 420 Цивільного кодексу України визначено, що комерційна таємниця є одним з об'єктів інтелектуальної власності. Відповідно майнові права інтелектуальної власності на комерційну таємницю належать

особі, яка правомірно визнала інформацію комерційною таємницею, якщо інше не встановлено договором [78].

Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

Власна інформація підприємства з метою її захисту може бути віднесена до комерційної таємниці та є конфіденційною при дотриманні таких умов:

– інформація не повинна відображати негативні сторони діяльності фірми, порушення законодавства та інші подібні факти;

– інформація не повинна бути загальнодоступною чи загальновідомою;

– виникнення чи отримання інформації повинно бути законним і пов’язано з витрачанням матеріального, фінансового чи інтелектуального потенціалу фірми;

– персонал фірми повинен знати про цінність такої інформації та навчений правилам роботи з нею;

– на підприємстві повинні бути виконані дії щодо захисту цієї інформації.

У Законі України «Про доступ до публічної інформації» зазначено, що таємна інформація – це інформація, доступ до якої обмежується відповідно до частини другої статті 6 цього Закону, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю [6].

До службової може належати така інформація:

– що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу 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;

– зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Згідно Закону України «Про інформацію», до інформації з обмеженим доступом не можуть бути віднесені такі відомості:

– про стан довкілля, якість харчових продуктів і предметів побуту;

– про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;

– про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

– про факти порушення прав і свобод людини і громадянина;

– про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

– щодо діяльності державних та комунальних унітарних підприємств, господарських товариств, у статутному капіталі яких більше 50 відсотків акцій (часток) належать державі або територіальній громаді, а також господарських товариств, 50 і більше відсотків акцій (часток) яких належать господарському товариству, частка держави або територіальної громади в якому становить 100 відсотків, що підлягають обов’язковому оприлюдненню відповідно до закону;

– інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов’язковість яких надана Верховною Радою України [10].

Конфіденційна інформація умовно поділяється на конфіденційну інформацію про фізичну особу та конфіденційну інформацію про юридичну особу (рис. 1.2).

Рисунок 1.2 – Види конфіденційної інформації, складено автором за [45; 71]

Підставою для визначення інформації конфіденційною є бажання фізичної чи юридичної особи вважати певну інформацію про неї чи інформацію, що знаходиться у її володінні, конфіденційною.

Інформація про фізичну особу (персональні дані) – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [10].

До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження. Не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини.

Кожному забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законом. Відповідно до статті 10 Закону України «Про доступ до публічної інформації» кожна особа має право:

– знати у період збирання інформації, але до початку її використання, які відомості про неї та з якою метою збираються, як, ким і з якою метою вони використовуються, передаються чи поширюються, крім випадків, встановлених законом;

– доступу до інформації про неї, яка збирається та зберігається;

– вимагати виправлення неточної, неповної, застарілої інформації про себе, знищення інформації про себе, збирання, використання чи зберігання якої здійснюється з порушенням вимог закону;

– на ознайомлення за рішенням суду з інформацією про інших осіб, якщо це необхідно для реалізації та захисту прав і законних інтересів;

– на відшкодування шкоди у разі розкриття інформації про цю особу з порушенням вимог, визначених законом [6].

Конфіденційна інформація про юридичну особу – це інформація, яка міститься в договорах, контрактах, листах, звітах, аналітичних матеріалах, випискаx з бухгалтерських рахунків, схемах, графіках, специфікаціях, інших

документах, що фігурують в діяльності юридичної особи. Розголошення даних, що містяться в таких документах, може бути використано конкурентами і, відповідно, завдати економічної та іншої шкоди юридичній особі. Особливістю відомостей, що складають комерційну таємницю, як вид конфіденційної інформації, є їх комерційний і господарський характер. Іншими словами, це інформація, що має економічну цінність, здатна впливати на фінансове становище суб'єкта підприємницької діяльності, розмір одержуваного ним прибутку [35].

У статті 6 Закону України «Про доступ до публічної інформації» зазначено, що обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог:

– виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи кримінальним правопорушенням, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

– розголошення інформації може завдати істотної шкоди цим інтересам;

– шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні [6].

Останнім часом питання, пов'язані з конфіденційною інформацією, викликають загострену увагу, адже будь-яка інформація має цінність для її власника та потребує захисту від нецільового використання та розголошення іншим особам.

Конфіденційна інформація – це відомості, що перебувають у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. Відповідно до статті 21 Закону України «Про інформацію» конфіденційна інформація разом із службовою та таємною інформацією належить до інформації з обмеженим доступом.

1.2 Теоретичні аспекти документування інформації конфіденційного характеру

Для документування інформації підприємства, яка є результатом творчої інтелектуальної праці в науці та виробництві, найбільш характерні не текстові, а зображувальні способи. Досить часто конфіденційна інформація документується фотографічними, відеографічними та іншими способами. Цінність інформації може бути кошторисною категорією і відображати конкретний розмір прибутку при її використанні чи розмір збитків при її втраті. Інформація стає часто цінною через її правове значення для організації чи розвитку бізнесу, наприклад, установчі документи, програми та плани, договори з партнерами та посередниками тощо. Цінність може відображати її перспективне, наукове, технічне чи технологічне значення.

Власна цінна інформація підприємства не обов'язково є конфіденційною. Часто звичайний правовий документ важливо зберегти в цілісності та безпеці від викрадача чи стихійного лиха. Цінну конфіденційну ділову інформацію, як правило, містять: плани розвитку виробництва, ділові плани, плани маркетингу, бізнес-плани, списки власників акцій та інші документи.

Найбільш цінними є відомості: про виробництво і продукцію, ринок, наукові розробки, матеріально-технічне забезпечення, умови контрактних переговорів, відомості про персонал, принципи управління підприємством, систему безпеки підприємства. Комерційна цінність інформації, як правило, недовготривала і визначається часом, необхідним конкуренту для створення тієї ж ідеї, її викрадення та відтворення [60].

Склад цінної інформації визначається її власником і фіксується в спеціальному переліку. Перелік цінних відомостей, що складають таємницю фірми, є постійним робочим матеріалом керівництва фірми, служб безпеки та конфіденційної документації. Він регулярно оновлюється, коректується та являє собою інвентарний список відомостей про конкретні роботи, конкретну продукцію, конкретні дослідження, конкретні контракти тощо.

Конфіденційний характер включеної в документ інформації позначається грифом обмеження доступу до документа, який виділяє його з загального потоку і ініціює обробку в спеціальному автономному режимі, а також поширює на документ захисні та інші міри підвищеної уваги та контролю.

Конфіденційна інформація зазвичай міститься у вигляді будь-яких документів – традиційних паперових або електронних. Документи, що містять конфіденційну інформацію, прийнято називати конфіденційними, а процес виготовлення таких документів і організацію роботи з ними – конфіденційним діловодством [15].

Конфіденційне діловодство – це діяльність, що забезпечує документування конфіденційної інформації, організацію роботи з конфіденційними документами та захист інформації, що міститься в них. При цьому, під документуванням інформації розуміється процес підготовки та виготовлення документів. Під організацією роботи з документами – їх облік, проходження, виконання, відправлення, класифікація, систематизація, підготовка до архівного зберігання, знищення, режим зберігання та використання, перевірка наявності [17].

За Т.М. Мужановою, конфіденційне діловодство – це сукупність процесів, що забезпечують документування конфіденційної інформації, організацію роботи з конфіденційними документами і захист інформації, що міститься в них [57, с.14]. Отже, документування конфіденційної інформації, а також організація роботи з конфіденційними документами та захист інформації, що міститься в них, забезпечується шляхом ведення конфіденційного діловодства.

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

За сферою діяльності відкрите діловодство поширюється на управлінські дії і включає переважно управлінські документи. Конфіденційне діловодство поширюється як на управлінську, так і на різні види виробничої діяльності, включаючи не тільки управлінські, але й науково-технічні документи (науково-дослідні, проектні, конструкторські, технологічні тощо). До конфіденційних

документів належать і деякі документи з особового складу. Крім того, конфіденційне діловодство розповсюджується не лише на офіційні документи, але й на їх проекти, різні робочі записи, що не мають усіх необхідних реквізитів, але містять інформацію, що підлягає захисту [75].

Відмінність конфіденційного діловодства від відкритого полягає у тому, що конфіденційну інформацію необхідно захищати не тільки від утрати, а й від недозволеного виходу за межі зони функціонування або встановленого кола осіб, які мають право працювати з нею. Завдання конфіденційного діловодства представлено на рис. 1.3.

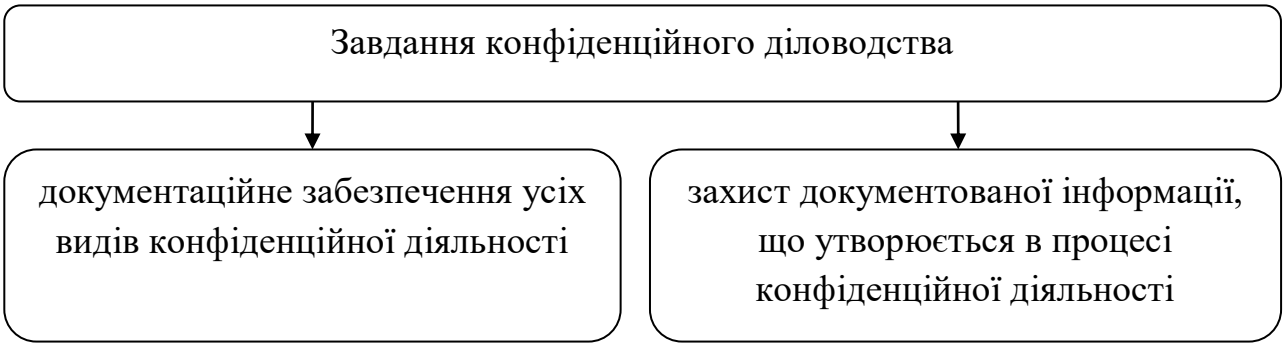

Рисунок 1.3 – Завдання конфіденційного діловодства, складено автором за [60]

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 поаркушний облік кожного примірника усіх без винятку документів та їх проектів;

– максимально необхідна 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 та обов'язкова відповідальність за облік, збереженість документів і порядок користування ними [63].

Ці особливості водночас є й вимогами до конфіденційного діловодства.

В установі, залежно від специфіки її діяльності, конфіденційна інформація може міститися в договорах, ділових листах, звітах, аналітичних матеріалах, базах даних клієнтів, споживачів, отримувачів соцдопомоги тощо. Крім того, конфіденційною інформацією вважаються і виписки з бухгалтерських, банківських рахунків, схеми, графіки, специфікації та інші документи. Правила роботи з інформацією конфіденційного характеру визначаються законами і деталізуються в локальних нормативних актах міністерств, відомств, підприємств (установ, організацій) усіх форм власності.

До конфіденційних документів відносяться документи з обмеженим доступом, тобто такі документи, до роботи з якими надається спеціальний допуск. П.О. Добродумов наводить таке визначення: конфіденційний документ – таємний, довірчий, той, що не підлягає розголошенню чи публікації [30].

Під конфіденційним (закритим, що захищається) документом розуміється необхідним чином оформлений носій документованої інформації, що містить відомості обмеженого доступу або використання, які становлять інтелектуальну власність юридичної або фізичної особи [46].

Під конфіденційним документом розуміється оформлений носій інформації, що містить відомості, які відносяться до недержавної таємниці і складають інтелектуальну власність юридичної або фізичної особи. Обов'язковою ознакою конфіденційного документа є наявність в ньому інформації, що підлягає захисту [23]. Конфіденційні документи не слід називати секретними або ставити на них гриф секретності, так як конфіденційні і секретні документи відображають різні види таємниці.

Конфіденційні документи включають в себе:

– у державних структурах: службову інформацію обмеженого поширення, іменовану в чиновницькому побуті інформацією для службового користування, тобто інформацією, що віднесена до службової таємниці, а також документи, що мають робочий характер і не підлягають публікації у відкритій пресі (проекти документів, супутні матеріали тощо);

– у підприємницьких структурах: відомості, які їх власник відповідно до законодавства має право віднести до комерційної (підприємницької) таємниці, таємниці фірми, інших видів недержавної таємниці;

– незалежно від приналежності: будь-які персональні (особисті) дані про громадян, а також відомості, що містять професійну таємницю, технічні та технологічні нововведення (до їх патентування), таємницю підприємств зв'язку, сфери обслуговування тощо [62].

Залежно від призначення конфіденційні документи поділяють на:

– вхідні;

– вихідні;

– внутрішні [61].

Конфіденційні документи також можна поділити на такі види: організаційні, керівні, розпорядчі, кадрові (по особовому складу), фінансово-бухгалтерські, нормативно-методичні, інформаційно-довідкові (рис. 1.4).

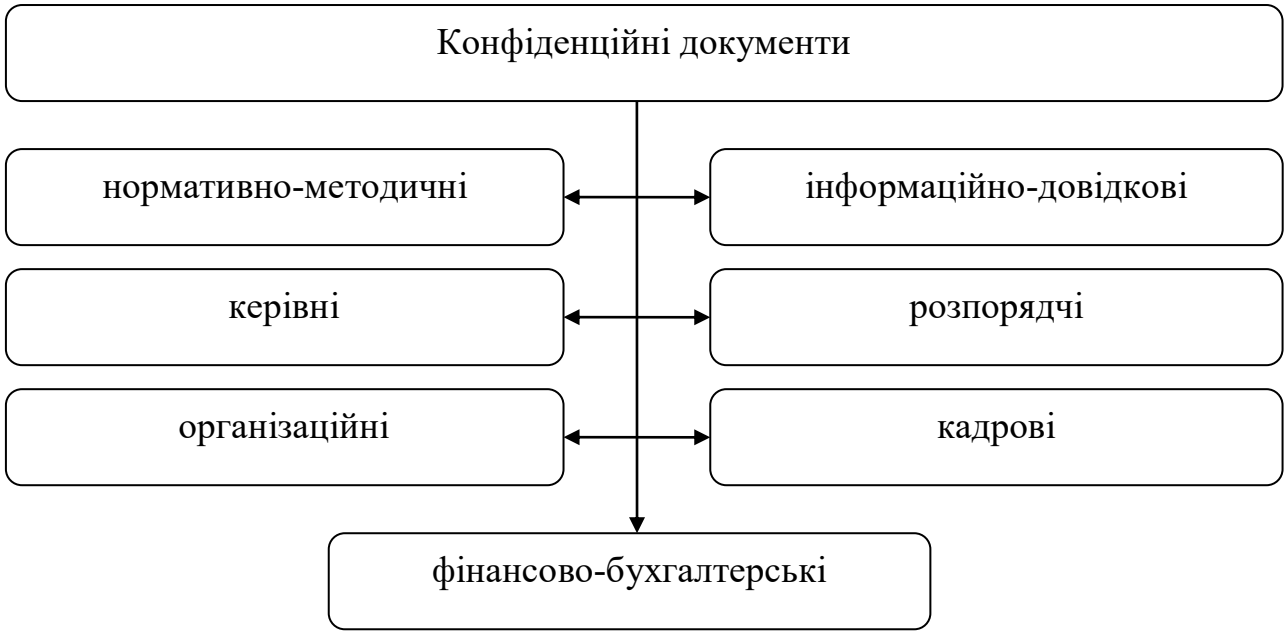

Рисунок 1.4 – Види конфіденційних документів, складено автором за [14]

Особливістю конфіденційного документа є те, що він представляє собою одночасно:

– масовий носій цінної інформації, що захищається;

– основне джерело накопичення та розповсюдження цієї інформації, а також її неправомірного розголошення або витоку;

– обов’язковий об’єкт захисту [23].

Конфіденційність документів завжди має значні розбіжності за термінами обмеження вільного доступу до них персоналу фірми (від декількох годин до декількох років). Слід враховувати, що основна маса конфіденційних документів після закінчення їх використання або роботи з ними втрачає свою цінність і конфіденційність. Наприклад, листування до укладення контракту може мати гриф конфіденційності, але після його підписання цей гриф з письмового дозволу першого керівника фірми знімається.

Виконані документи, які зберегли конфіденційний характер і цінність для діяльності фірми, формуються у справи відповідно до номенклатури справ. Період перебування конфіденційних документів у справах може бути короткочасним або тривалим залежно від цінності інформації, що міститься в документах справи. Період конфіденційності документів визначається відповідно до вказаного вище переліку конфіденційних відомостей і залежить від специфіки діяльності фірми. Наприклад, виробничі, науково-дослідні фірми мають значно більше цінних документів, ніж торговельні, посередницькі підприємства.

Документи довготривалого періоду конфіденційності (програми і плани розвитку бізнесу, технологічна документація ноу-хау, ноу-хау, винаходи тощо.) мають ускладнений варіант обробки і зберігання, що забезпечує безпеку інформації та її носія. Документи короткочасного періоду конфіденційності, що мають оперативне значення для діяльності фірми, обробляються і зберігаються за спрощеною схемою і можуть не виділятися з технологічної системи обробки відкритих документів при наявності в цій системі мінімальних захисних, контрольних та аналітичних елементів [41].

Таким чином, конфіденційні документи характеризуються специфічними особливостями, які відображають їх сутність як носіїв інформації обмеженого доступу і визначають побудову системи захисту цієї інформації.

При документуванні конфіденційної інформації варто враховувати такі аспекти:

– обсяг конфіденційних відомостей, включених у документ, має бути мінімальним і визначатися реальною ситуацією;

– документ завжди має стосуватися лише одного питання (теми) – це є важливим не стільки для швидкого доведення документа до виконавців, скільки для забезпечення чіткого функціонування системи доступу персоналу до конфіденційної інформації, необхідної лише певному співробітнику, і запобігання несанкціонованому ознайомленню співробітників установи та інших осіб з інформацією, що має обмежений доступ;

– зведені планові, організаційні, розпорядчі (зокрема, накази з основної діяльності), звітні та інші документи, що передбачають кількох виконавців, не слід розсилати підрозділам і виконавцям у повному обсязі – такі документи доводять до виконавців вибірково у вигляді витягів, персоніфікованих додатків-завдань;

– інформацію з обмеженим доступом необхідно максимально локалізувати в конкретній частині документа, його розділі, додатку, фотоілюстрації, графіку, на окремому диску, електронному масиві з ускладненою системою доступу (наприклад, великий за обсягом документ може мати окремий розділ, що містить комплекс інформації обмеженого доступу) [63].

Склад документованої конфіденційної інформації залежить від компетенції і функцій установи, характеру її діяльності, взаємозв’язків з іншими установами, порядку розв’язання питань.

Конфіденційним документам надається гриф обмеженого доступу, що засвідчує особливий характер інформації, до якої має доступ обмежене коло осіб. Гриф обмеження доступу (Таємно, Для службового користування, Конфіденційно тощо) проставляють у верхньому правому куті на лицьовому боці першого аркуша документа над реквізитами «Адресат» або «Гриф затвердження документа». Обмеження доступу до друкованих видань позначають на обкладинці та титульному аркуші. Нижче грифа обмеженого доступу проставляється номер примірника. Приклади оформлення грифа обмеженого доступу:

Для службового користування Прим. 2

або

Конфіденційно Прим. 1

Якщо гриф обмеженого доступу не можна розташувати на магнітному носії, слід скласти супровідний лист, в якому обумовити обмеження. Гриф обмеженого доступу проставляється виконавцем та особою, яка підписує документ, на виданні – автором (укладачем) і керівником, який підписав видання до друку. Відповідальність за забезпечення правильного ведення обліку, зберігання і використання конфіденційних документів несуть керівники установ [22].

Облік (реєстрацію), зберігання, розмноження конфіденційних документів здійснює, як правило, служба діловодства (секретар), що обліковує несекретну документацію. А відповідальність за нерозголошення відомостей, що містяться у конфіденційних документах, покладається на режимно-секретний підрозділ установи. Проте керівники установ, що володіють конфіденційною інформацією, можуть встановлювати інший порядок приймання і обліку такої документації, тобто покладати ці функції на режимно-секретні підрозділи.

Облік, зберігання, розмноження конфіденційних документів здійснює, як правило, служба діловодства (секретар), що обліковує несекретну документацію. Облік конфіденційних документів включає присвоєння та зазначення в облікових формах і на документах реєстраційних номерів, запис облікових і пошукових даних про документи (дата, автор, заголовок, кількість сторінок, місцезнаходження тощо) [17].

Обліку підлягають усі без винятку виготовлені в установі документи з грифом обмеженого доступу. Вони обліковуються за кількістю сторінок, а друковані видання (книги, журнали, брошури) – за кількістю примірників.

Документи, що містять конфіденційну інформацію, реєструються один раз. Облік ведеться в журналах чи на картках, як правило, окремо від обліку документів відкритого діловодства. Облік магнітних носіїв інформації з грифом обмеженого доступу ведеться окремо від обліку паперових документів.

Одержуючи конфіденційний документ, співробітник повинен звірити номер отриманого документа з його номером у журналі реєстрації, перевірити кількість аркушів і розписатися за отриманий документ. При поверненні конфіденційного документа співробітник служби діловодства (секретар) повинен звірити номер цього документа з номером у журналі, перевірити кількість аркушів документа і в присутності співробітника, що повертає документ, поставити в журналі (у відповідній графі) свій підпис і дату повернення документа.

Сторінки журналів реєстрації нумеруються, прошнуровуються та опечатуються. На останній обліковій сторінці слід зробити запис про кількість сторінок у журналі, який підписує працівник служби діловодства (секретар) і засвідчує печаткою «Для пакетів».

Якщо обсяг документів з грифом обмеженого доступу незначний, можна вести їх облік (реєстрацію) разом із документами загального діловодства. При цьому на картці (у журналі) до реєстраційного номера документа чи видання додається відповідна позначка, наприклад ДСК, КТ тощо [60].

Тираж видання з грифом обмеженого доступу, отриманий для розсилання, реєструється під одним вхідним номером у журналі обліку і розподілу видань із відповідними грифами. Додатково розмножені примірники документа (видання) враховуються за номером цього документа (видання), про що робиться позначка на розмноженому документі (виданні) та в усіх облікових формах. При цьому нумерація розмножених примірників продовжується від останнього номера примірників, які були розмножені раніше.

Друкування документів, що містять конфіденційну інформацію, здійснюється в друкарському бюро чи в структурних підрозділах. Відповідальність за збереження і нерозголошення інформації несуть керівники цих підрозділів.

На звороті останньої сторінки кожного примірника документа друкарка має зазначити кількість надрукованих примірників, прізвище виконавця, власне прізвище і дату друкування документа.

Надруковані та підписані примірники документів з грифом обмеженого доступу разом із чернетками чи варіантами передаються для реєстрації

працівнику служби діловодства (секретарю), який здійснює їх облік. Чернетки та варіанти знищуються виконавцем і співробітником служби діловодства (секретарем), про що на копії вихідного документа робиться запис: Чернетки і варіанти знищено. Проставляються дата і підписи.

Розмножувати конфіденційні документи можна лише з дозволу керівника установи чи структурного підрозділу під контролем служби діловодства (секретаря). Облік розмножених документів ведеться за кількістю примірників. У реєстраційних формах, що заповнюються у друкарні, до реєстраційного номера чи назви документа додається відповідна позначка ДСК або КТ. Копіювально-розмножувальну техніку слід обладнати технічними засобами захисту інформації. Документи з грифом обмеженого доступу, отримані від інших установ, дозволяється розмножувати лише за їх згодою [75].

Розсилають конфіденційні документи на підставі рознарядок, підписаних керівником установи і керівником служби діловодства, із зазначенням облікових номерів примірників, що розсилаються (відправляються). Конфіденційні документи можна пересилати цінними або рекомендованими поштовими відправленнями або з кур'єрами, які доставляють документи під підпис в реєстрі.

Документи, що розсилаються в інші установи, вкладають у конверти або упаковують таким чином, щоб виключити можливість доступу до них. Конверти застосовують світлонепроникні, пакети заклеюють. На конвертах (упаковках) зазначають адреси та назви одержувача і відправника, номери вкладених документів із відповідною позначкою. При цьому на конвертах забороняється зазначати прізвища, посади адресата, а також прізвища виконавців документів і назви структурних підрозділів.

Конфіденційне діловодство – це діяльність, що забезпечує документування конфіденційної інформації, організацію роботи з конфіденційними документами і захист інформації, яка міститься в них. Конфіденційний документ – це носій інформації, що містить відомості обмеженого доступу, які становлять інтелектуальну власність юридичної або фізичної особи. Конфіденційні документи вимагають специфічних умов їх створення і організації роботи з ними.

1.3. Поняття та основні принципи організації конфіденційного документообігу

Згідно Закону України «Про інформацію», документ – це матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі [10].

Документообіг – це рух документів в організації з моменту їх отримання чи створення до завершення виконання чи відправки [2]. Документообіг – це складний технологічний процес, який характеризується різними параметрами, пов'язаними з процесами документування і з усією діяльністю організації. Тому документообіг є важливою ланкою діловодства, так як визначає не лише інстанції проходження документа, але і швидкість цього руху.

Під документообігом П.О. Добродумов розуміє рух документів у підприємстві з моменту їх отримання або створення до завершення виконання або відправки на архівне зберігання [30, с. 135].

Єдиною державною системою діловодства (ЄДСД) встановлено основні принципи організації документообігу – проходження документів у підприємстві повинно бути оперативним, цілеспрямованим, тобто виключати зворотні, зигзагоподібні та інші маршрути. Має діяти принцип одноразового перебування документа в одному структурному підрозділі або в одного виконавця.

Існує чітка система здійснення всіх послідовних операцій з документами: прийняття і реєстрація, розгляд керівником, порядок проходження документів в організації, їх виконання, контроль виконання, формування справ, підготовка і передача справ до архіву.

Основу правильної організації обігу документів становить чітке розмежування функцій та обов’язків між працівниками підприємства. Точне знання обов’язків підвищує відповідальність кожного співробітника, в той же час виключає дублювання операцій під час роботи з документами. Відповідний розподіл праці в таких випадках закріплюється в посадових інструкціях і функціональних обов’язках.

Порядок документообігу в організації регламентується інструкцією з діловодства, регламентами роботи з документами, положеннями про структурні підрозділи, посадовими інструкціями.

Виділяють такі види документообігу:

– централізований документообіг (вся документація централізовано реєструється);

– децентралізований документообіг (реєстрація документів у кількох місцях за умови річного документообігу 100 тисяч і більше документів, а також за наявності територіально уособлених структурних підрозділів та певних особливих умов роботи);

– змішаний документообіг (найбільш важлива внутрішня документація та листування керівництва реєструється у канцелярії, решта документів – у структурних підрозділах) [67, с. 16].

О.В. Матвієнко та М.Н. Цивін говорять про те, що організація документообігу підприємства залежить від масштабу діяльності підприємства, його функцій, кількості ланок управління і обсягу документопотоків [56].

Здійснюючи аналіз документообігу, в якості об’єкта дослідження можна розглядати окремий документ, документопотік, документаційний технологічний процес. Однак основоположним об’єктом дослідження і удосконалення можна назвати документопотік. Документопотік – це структурована сукупність документів (документованої інформації), що переміщуються в заданому напрямі, призначених для забезпечення виконання персоналом управлінських функцій і прийняття рішень [29].

Документопотік – це комплекс заходів передавання інформації в установі, зафіксованих на певних носіях. Формування документопотоків залежить від побудови і структури установи, форми організації ведення обліку документів, типів, кількості і виду програмно-технічних та організаційних засобів, обчислювальної техніки, що використовуються в процесі організації документопотоку. Вони бувають різної інтенсивності, що вимагає особливої уваги при організації процесу документообміну.

Виділяють три потоки документів на підприємстві:

– вхідні документи від зовнішніх адресатів, оброблювані структурними підрозділами (вхідна кореспонденція, нормативні й законодавчі документи, договори, проекти); більшість із них повинна породжувати вихідні, причому в заздалегідь установлений термін;

– вихідні документи, що випускаються структурними підрозділами для відправлення в зовнішні організації (вихідна кореспонденція, договори, проекти, довідки, тощо);

– внутрішні документи, що видаються керівництвом підприємства або структурними підрозділами (накази, інструкції, довідки) й використовуються для організації роботи підприємства [74].

Отже, виділяють такі види документопотоків на підприємстві:

– документопотік вхідних документів (листи, угоди, рекламні оголошення, відомчі розпорядження та інструкції тощо). Більша частина документів, які обробляються, адресовані керівнику підприємства, лише менша частина – заступникам керівника, керівникам структурних підрозділів і конкретним виконавцям;

– документопотік внутрішніх документів – це документи які циркулюють між підрозділами (службами) однієї організації. Як правило, це: накази, розпорядження, інструкції керівництва, службові записки, акти тощо;

– документопотік вихідних документів – це документи які виходять з установи, як правило це відповіді на листи, угоди, запити, звіти, контракти, прес-релізи тощо (рис. 1.5).

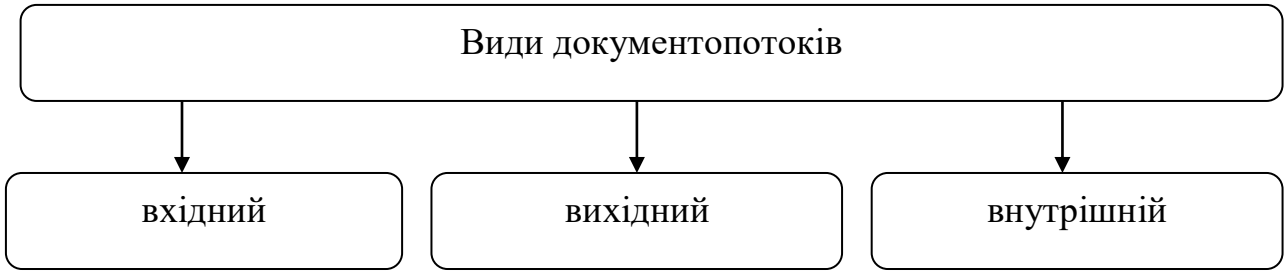

Рисунок 1.5 – Види документопотоків на підприємстві,
складено автором за [67]

Документопотік характеризують за такими параметрами:

– зміст документопотоку (склад документів, включених до нього, та склад інформації, зафіксованої в цих документах);

– структура документопотоку (описується ознаками, відповідно до яких документи можуть бути класифіковані, індексовані, сформована система довідкового апарату за документами установи);

– режим або циклічність документопотоку (періодичність руху документів через пункти опрацювання);

– напрям документопотоку (визначають пунктами відправлення і призначення);

– обсяг (об'єм) документопотоку (визначають кількістю документів, які проходять за одиницю часу, вимірюється фізичною кількістю документів створюваних упродовж року або обсягом інформації в документах) [43].

Обсяг документопотоку – кількість документів, які надійшли в установу і створені за певний період. Даний показник використовують як критерій при виборі організаційної форми діловодства (традиційна, автоматизована), а також впливати на структуру служби діловодства та її штатний склад [65].

Отже, документообіг складається з потоків вхідних, вихідних та внутрішніх документів організації. Потік вхідних документів – це документи, які надходять з інших (вищих) інстанцій і які скеровують керівникам, структурним підрозділам, окремим виконавцям. Потік вихідних документів – документи, створені в установі для скерування адресатам за її межами. Потік внутрішніх документів формують документи, які створені і циркулюють в установі з одного підрозділу в інший та не виходять за її межі [70].

Організація конфіденційного документообігу – це створення необхідних умов для виготовлення й одержання конфіденційних документів, організації роботи з ними, запобігання втрати і витоку документованої конфіденційної інформації [61].

Метою як «відкритого», так і конфіденційного документообігу є забезпечення своєчасного виконання документів або їх використання. На відміну від «відкритого» документообігу конфіденційний документообіг має

ще одну мету – захист документів від несанкціонованого доступу і запобігання розголошенню конфіденційної інформації. З цієї причини конфіденційний документообіг називають ще захищеним документообігом. Захищений документообіг – це контрольований рух конфіденційних документів по регламентованим пунктам обробки в жорстких умовах організаційного та технологічного забезпечення безпеки носія інформації і самої інформації [23].

Отже, важливою відмітною рисою і особливістю конфіденційного документообігу є необхідність захисту документів від несанкціонованого доступу до них з метою запобігання витоку конфіденційної інформації.

Таким чином, організація конфіденційного документообігу повинна будуватися на основі певних принципів (рис. 1.6).

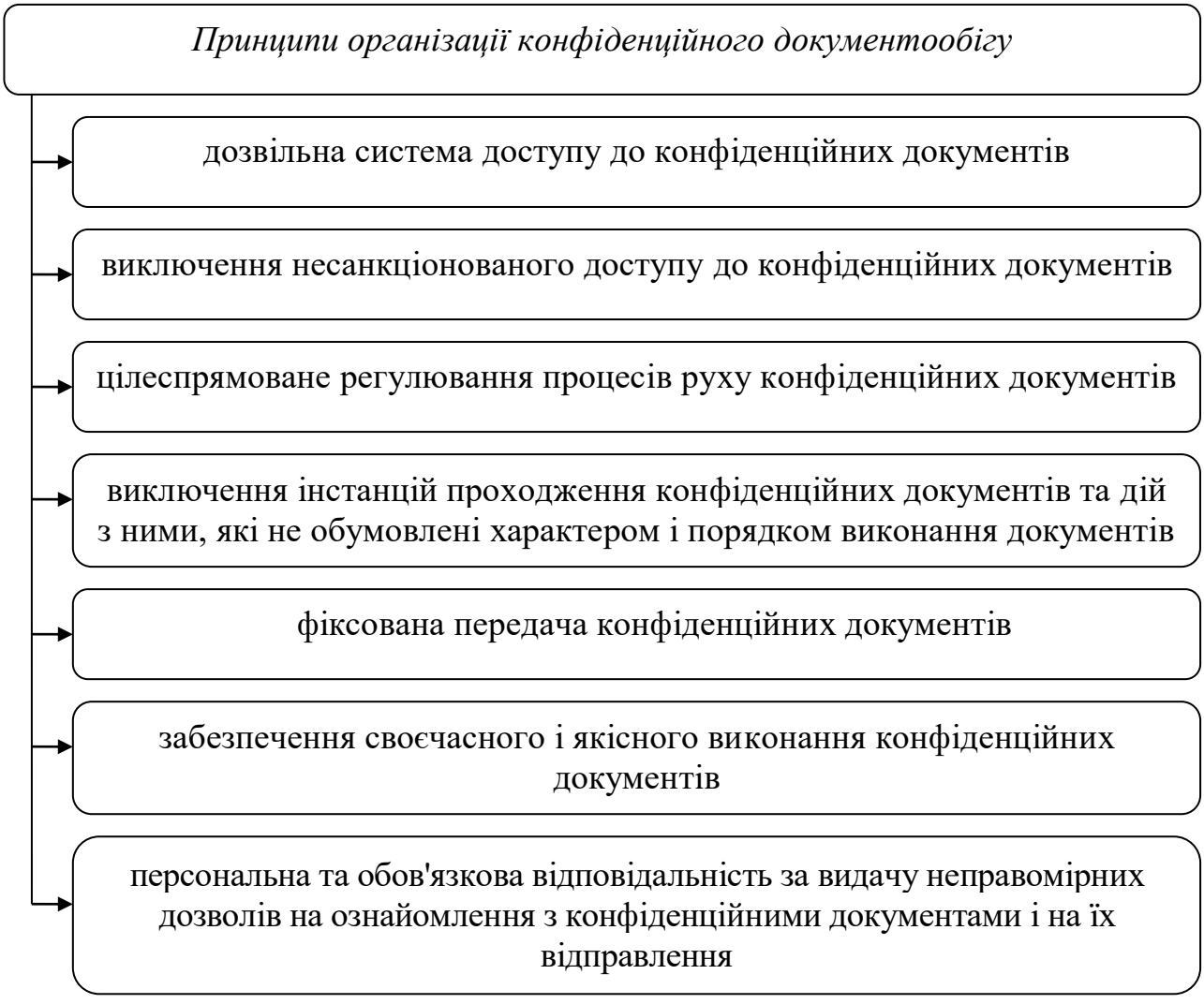

Рисунок 1.6 – Основні принципи організації конфіденційного документообігу, складено автором за [23; 61]

Основою організації конфіденційного документообігу є облік конфіденційної документованої інформації на кожному етапі її проходження.

Життєвий цикл документів, які містять конфіденційну інформацію, розпочинається в діловодстві з моменту надходження документа в організацію або з моменту його створення і завершується знищенням документа (проекту документа) чи передачею документа на архівне зберігання. Рух документів, які містять конфіденційну інформацію протягом їх життєвого циклу в організації, називається конфіденційним документообігом [61].

Розглянемо найбільш важливі правила конфіденційного документообігу:

1. Централізація всіх стадій, процедур і операцій з обробки та зберігання конфіденційних документів. Всі операції, пов'язані з прийомом, відправленням, обробкою, зберіганням конфіденційних документів в організації здійснюються в підрозділі (відділі, групі) конфіденційного діловодства або окремим працівником підрозділу загального діловодства.

Типовою помилкою в організації конфіденційного документообігу є його побудова за аналогією з «відкритим» документообігом. Виражається це, зокрема, в тому, що спеціаліст з конфіденційного діловодства при обробці вхідних конфіденційних документів привласнює документу, що надійшов порядковий номер, фіксує дату надходження, передає документ керівництву, а потім в підрозділ або ж відразу в підрозділ, після чого вся відповідальність за організацію роботи з конфіденційними документами, відстеження їх переміщень в процесі виконання лягає на співробітника, що організує роботу з документами в тому чи іншому підрозділі. В цьому випадку у співробітника, який відповідає за роботу з конфіденційними докукментами в рамках всієї організації, формується не повний масив даних про переміщення документів, він може простежити переміщення документа, в кращому випадку, до структурного підрозділу.

2. Пооперацийний облік усіх дій, що реалізуються з конфіденційними документами, облік кожного факту «життєвого циклу» документа. Дотримання цього правила є необхідним для формування такого масиву даних про конфіденційні документи, який в будь-який момент часу може надати

інформацію про місце знаходження кожного конфіденційного документа, а також про операції, що здійснені або здійснюються з ним. Головне у конфіденційному документообігу – це облік як документів, так і всіх дій, що здійснюються з документом. Це правило суттєво відрізняє конфіденційний документообіг від «відкритого» документообігу.

3. Облік всіх без винятку конфіденційних документів, включаючи їх копії. У конфіденційному діловодстві не існує понять «зареєстровані» і «незареєстровані» документи. Всі конфіденційні документи, і ті які надходять, і ті, що створюються в організації, підлягають обліку. Крім того, в системі конфіденційного діловодства обліку підлягають не лише конфіденційні документи, але і проекти документів, носії інформації, які використовуються для підготовки документів (листи паперу, блокноти, магнітні та інші носії), пакети (конверти) при їх надходженні в організацію. Якщо конфіденційний документ копіюється, то обліку підлягають всі екземпляри (копії) документа [23].

4. Виконання будь-яких переміщень конфіденційних документів та інших операцій під розпис керівників, виконавців і технічного персоналу. При реалізації операцій, пов'язаних з прийомом-передачею конфіденційних документів, перевіркою їх збереженості, цілісності і комплектності тощо, запис про вчинені дії в обліковій формі здійснюється під розпис тієї особи, на яку переходить відповідальність за документ після реалізації операції. Наприклад, надрукований у підрозділі конфіденційного діловодства документ передається виконавцю, виконавець повинен розписатися в обліковій формі, підтверджуючи факт отримання документа. Співробітник підрозділу конфіденційного діловодства має ретельно слідкувати за дотриманням цього правила. Навіть при передачі документа на розгляд керівника організації не можна нехтувати цим правилом, інакше, якщо станеться втрата документа, важко буде довести, хто несе за це відповідальність. При відсутності підпису керівника в обліковій формі відповідальність буде лежати на підрозділі конфіденційного діловодства.

5. Перевірка комплектності, цілісності конфіденційного документа при будь-якому його переміщенні. Для виконання цього правила працівник підрозділу

конфіденційного діловодства повинен при кожному отриманні або передачі документа перераховувати кількість сторінок основного документа, кількість додатків і кількість сторінок додатків. При цьому в обліковій формі і на самому документі зазначається кількість сторінок основного документа, кількість додатків і сторінок додатків. На документі ці відомості проставляються в складі позначки про надходження, поряд з датою і номером надходження.

6. Письмова фіксація всіх звернень персоналу до документа. Дотримання цього правила вимагає фіксувати в облікових формах не лише ті дії, які санкціоновані і здійснюються відповідно до нормативних актів організації, але й несанкціоновані дії, що здійснюються з конфіденційними документами. Наприклад, можуть мати місце факти отримання доступу (навіть випадкового) до конфіденційних документів тими працівниками або сторонніми особами, яким доступ до цих документів недозволений. Ця інформація може виявитися важливою в тому випадку, якщо відбудеться витік і розголошення конфіденційної інформації і необхідно буде встановити канал витоку інформації. Відомості про факти несанкціонованого доступу до конфіденційних документів фіксуються в обліковій формі (журналі, картці документа або в базі даних, якщо в організації ведеться автоматизований облік конфіденційних документів) [62].

7. Облік і забезпечення збереженості не лише документів, але й облікових форм. Оскільки в основі організації конфіденційного документообігу лежить облік документів і всіх дій, що здійснюються з документом, великого значення набувають безпосередньо облікові форми: журнали, картотеки, автоматизовані бази даних. Оскільки конфіденційний документообіг базується на пооперaційному обліку, а самі операції здійснюються під розпис працівника, найчастіше в якості облікових форм використовуються журнали або реєстраційно-облікові картки на паперовому носії. З огляду на, що обліку підлягають не лише документи, але й проекти документів, пакети тощо, в підрозділі конфіденційного діловодства, як правило, ведеться багато облікових форм. Це й змушує вводити ще й облік самих облікових форм, як правило, журнал обліку облікових форм, який може вестися як на паперовому носії, так і в електронному вигляді.

8. Письмове санкціонування керівником процедур копіювання конфіденційних документів, контроль технології виконання цих процедур. Кількість копій конфіденційних документів має бути обмеженою і визначатися діловими потребами. Рішення про копіювання документа може приймати керівник організації чи його заступники. Як правило, з конфіденційного документа знімається обмежена кількість копій.

9. Колегіальність процедури знищення документів, справ і баз даних. Це правило вимагає, щоб у процедурі знищення проектів, чернеток, конфіденційних документів брало участь не менше двох працівників. Знищення документів, проектів документів, чернеток проводиться лише за актом.

10. Контроль за виконанням персоналом правил роботи з конфіденційними документами, справами, базами даних. Одна з вимог правильної організації роботи з конфіденційними документами – це постійний контроль, особливо в період перебування документів у виконавців. Практика показує, що конфіденційний документ піддається найбільш сильним загрозам саме тоді, коли перебуває у виконавця. Підрозділ конфіденційного діловодства має проводити планові та позапланові перевірки організації роботи виконавців з документами. У той же час керівництво організації проводить перевірки організації роботи з конфіденційними документами в підрозділі конфіденційного діловодства [68].

Документи, що містять конфіденційну інформацію, в процесі документообігу піддаються різним ризикам та загрозам:

– крадіжка (розкрадання) документа або окремих його частин, носія чорнового варіанту документа (проекту документа) або робочих записів;

– несанкціоноване копіювання паперових і електронних документів, запам'ятовування тексту документа;

– таємне або дозволене ознайомлення співробітника фірми з документом і повідомлення інформації зловмиснику;

– підміна документів, носіїв і їх окремих частин;

– дистанційний перегляд документів і зображень на моніторі персонального комп'ютера за допомогою технічних засобів;

– помилкові (умисні або випадкові) дії персоналу при роботі з документами (порушення дозвільної системи доступу, правил поводження з документами);

– випадкове або навмисне знищення документів, несанкціонована модифікація і спотворення тексту тощо;

– втрата документів в умовах екстремальних ситуацій [44].

Для електронних документів загрози є особливо реальними, так як факт крадіжки інформації практично важко виявити. Загрози, пов’язані з конфіденційною інформацією, що обробляється і зберігається в комп'ютерах, класифікують таким чином:

– ненавмисні помилки користувачів, операторів, референтів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи;

– крадіжки і підробки інформації;

– стихійні ситуації зовнішнього середовища;

– зараження вірусами.

Враховуючи характер зазначених загроз, визначаються завдання щодо забезпечення захисту інформації в документопотоках, спрямовані на запобігання або послаблення цих загроз. Головним напрямом захисту документованої інформації від можливих небезпек є формування захищеного документообігу, використання в обробці і зберіганні документів спеціалізованої технологічної системи, що забезпечує безпеку інформації на будь-якому типі носія.

Підхід щодо захисту конфіденційних документів має бути комплексним. Необхідно зважено оцінювати ймовірні загрози і ризики, а також величину можливих втрат внаслідок дії цих загроз. Обираючи методи організації захищеного документообігу, слід шукати розумний баланс між необхідністю і можливістю, між безпекою даних і вартістю рішення щодо їх захисту.

Звичайно, для захисту конфіденційних документів від несанкціонованого доступу і розголошення недостатньо лише заходів, що вживаються в рамках конфіденційного документообігу, на це спрямована вся система безпеки організації. Однак значна частина вжитих заходів реалізується саме в рамках конфіденційного документообігу.

РОЗДІЛ 2
АНАЛІЗ ОРГАНІЗАЦІЇ КОНФІДЕНЦІЙНОГО ДОКУМЕНТООБІГУ У ТОВАРИСТВІ З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «КЕРУЮЧА КОМПАНІЯ «ДОМ.КОМ»

2.1 Характеристика діяльності Товариства з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком»

Керуюча Компанія «Дом.Ком Україна» (м. Київ, пл. Бесарабська, 9/1Б) здатна не лише вирішувати поточні питання житлового фонду, але й впроваджувати комплексні рішення з оптимізації управління та утримання житлово-комунального господарства (ЖКГ) міст України.

Свою діяльність Керуюча Компанія «Дом.Ком Україна» здійснює шляхом створення в містах України підприємств – керуючих компаній «Дом.Ком», які згідно з укладеними з органами місцевого самоврядування договорами здійснюють управління та утримання комунального житлового фонду місцевих рад. Компанія активно працює в таких містах як Київ, Житомир, Кривий Ріг, Суми, Нікополь, Рубіжне, Хмельницький. Діяльність керуючих компаній здійснюється у відповідності до законодавства України та спрямована на покращення надання житлово-комунальних послуг споживачам [31].

Керуюча Компанія «Дом.Ком Україна» співпрацює з Міністерством регіонального розвитку, будівництва та житлово-комунального господарства України, Громадською спілкою «Фонд розвитку та інновацій ЖКГ», Громадською спілкою «Асоціація управителів житла». Керуюча Компанія «Дом.Ком Україна» входить до Фонду розвитку та інновацій ЖКГ, завдяки чому має можливості залучати інвестиції в ЖКГ, та має партнерські відносини з багатьма провідними виробниками сучасного обладнання і техніки.

Завдяки професійному досвіду та використанню сучасних технологій, компанія займає лідируючі позиції на ринку житлово-комунальних послуг. Клієнтам надається широкий спектр послуг з індивідуальним підходом до

кожного. Мета компанії – це постійний рух у бік поліпшення й оптимізації її діяльності. І це, насамперед, кваліфіковане управління прийнятим на обслуговування житловим і нежитловим фондом, забезпечення його якісного змісту та підтримання стану прибудинкової території на високому рівні.

На сайті Керуючої Компанії «Дом.Ком Україна» представлено такі розділи: діяльність компанії, проекти компанії, новини, новітні технології, для ОСББ, контакти. Є також дані про підприємства компанії у містах України (рис. 2.1).

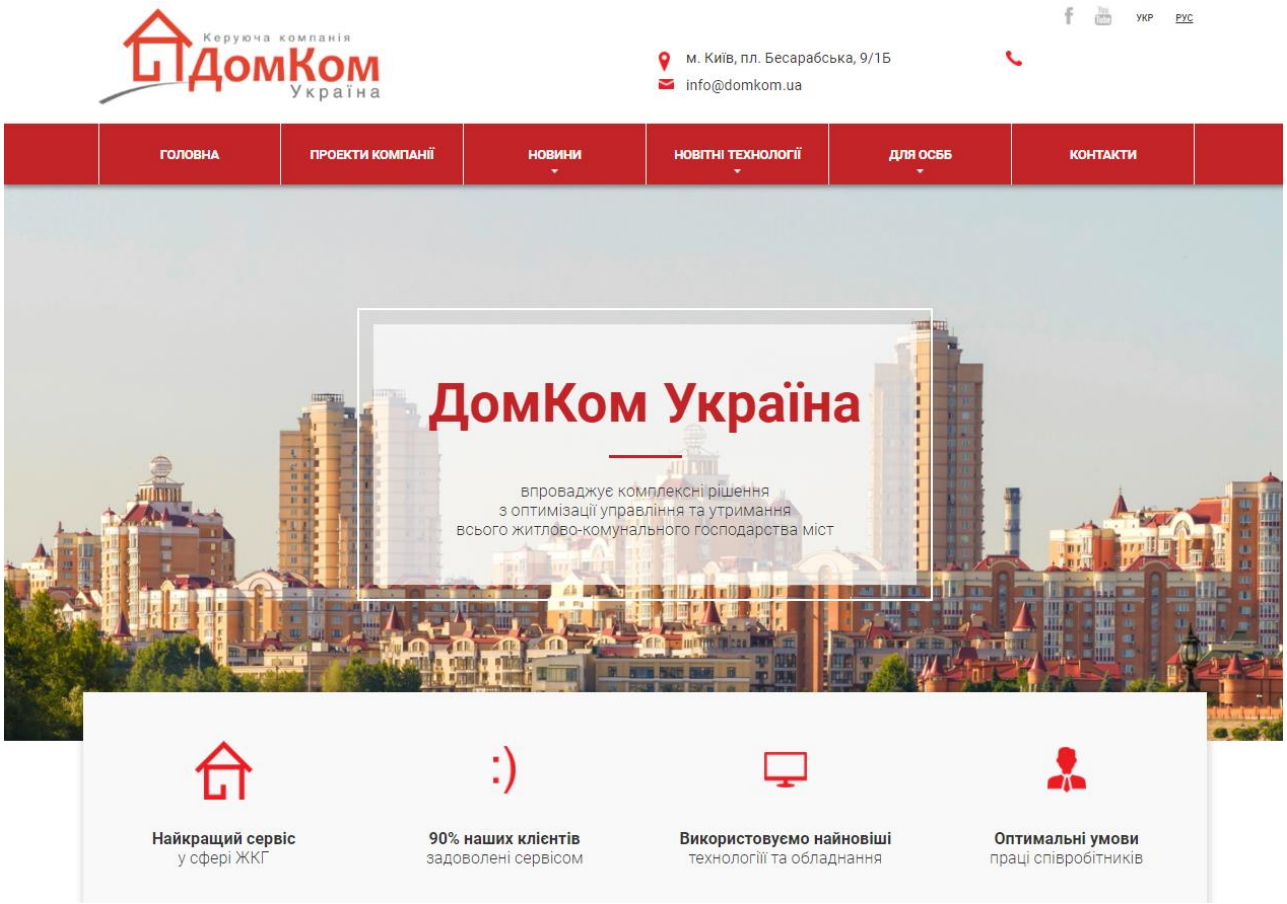

Рисунок 2.1 – Скриншот головної сторінки сайту Керуючої Компанії «Дом.Ком Україна» [31]

Програмні комплекси Керуючої Компанії «Дом.Ком Україна»:

1. Бухгалтерія ЖКГ. Побудинковий облік. Ведення побудинкового обліку доходів та витрат на базі бухгалтерської програми 1С, автоматичне формування бухгалтерського, податкового, фінансового та управлінського обліку як у цілому по підприємству так і в розрізі окремих будинків. Основні можливості програми:

– професійний облік в рамках єдиної системи з автоматизацією та синхронізацією процесів управління, планування, обліку та контролю всіх етапів діяльності в сфері утримання будинків;

– автоматизований розрахунок тарифів та фактичних витрат по управлінню та утриманню в розрізі будинків на базі офіційного бухгалтерського обліку 1С;

– формування аналітичних звітів (фінансових, економічних, виробничих тощо) як по групі будинків так і по кожному будинку окремо;

– облік витрат в розрізі будинків за видами виконаних робіт та статей тарифу;

– порівняльний аналіз доходів і витрат за статтями тарифу та формування балансів в розрізі будинків: нараховано-сплачено-фактично витрачено;

– автоматизований розрахунок та облік заробітної плати з розширеним функціоналом;

– облік технічних характеристик житлових будинків.

2. Абонентський облік та управління будинком ОСББ. Програма складається з двох модулів, які можуть використовуватись як в межах єдиної системи, так і окремо.

2.1. Модуль «Абонентський облік». Автоматизація всіх процесів по веденню особових рахунків споживачів: нарахування, облік оплат, пільг та субсидій, формування квитанцій та довідок. Основні можливості програми:

– автоматизація нарахувань по особовим рахункам споживачів за послуги з управління та утримання будинків;

– облік фактичних платежів по особовим рахункам;

– автоматичне формування квитанцій на сплату за ж-к послуги;

– формування звітів і реєстрів по пільгах та субсидіях для обміну даними з УПСЗН в електронному форматі;

– автоматичний облік даних від банків щодо платежів абонентів;

– облік споживачів по особовим рахункам (спрощений «паспортний стіл»);

– автоматичне формування стандартних довідок;

– облік показань приладів обліку по особовим рахункам;

– допомога юридичній службі: формування позовів, претензій, приписів, договорів тощо.

2.2. Модуль «Управління будинком ОСББ». Спрощений бухгалтерський облік процесів діяльності ОСББ. Основні можливості програми:

– спрощений бухгалтерський облік для ОСББ;

– ведення технічних даних по житловому будинку;

– автоматичне формування офіційної звітності та управлінських звітів;

– формування річних кошторисів на утримання будинку;

– облік фактичних витрат по будинку в розрізі статей кошторису;

– порівняльний аналіз фактичних витрат з річним кошторисом;

– автоматизований облік заявок мешканців;

– ведення бази контрагентів та постачальників [32].

3. Програма «Аварійно-диспетчерська служба ЖКГ». Ведення автоматизованого обліку та контролю приймання та виконання звернень споживачів. Основні можливості програми:

– єдина служба для звернення абонентів щодо всіх питань, пов’язаних з обслуговування будинків;

– прийом та облік заявок щодо аварійних ситуацій, поточних питань обслуговування будинку та заявок на платні послуги;

– можливість приймання дзвінків за допомогою IP-телефонії для підвищення якості обслуговування;

– обробка та аналітика заявок за різними категоріями: аварійні, поточні, тарифні, платні, виконані, в роботі тощо;

– контроль виконання заявок (термін та якість виконання);

– швидкий пошук і перегляд інформації по конкретній заявці, будинку, категорії звернення, типу ушкодження тощо;

– архівація даних щодо заявок та виконаних робіт в розрізі кожного будинку за довільний проміжок часу;

– формування довідок, аналітичних звітів, діаграм та графіків за завданий період часу по будь-якому будинку або виду заявки чи категорії звернення.

На сайті Керуючої Компанії «Дом.Ком Україна» в розділі «Контакти» є також електронна форма для написання повідомлень (рис. 2.2.)

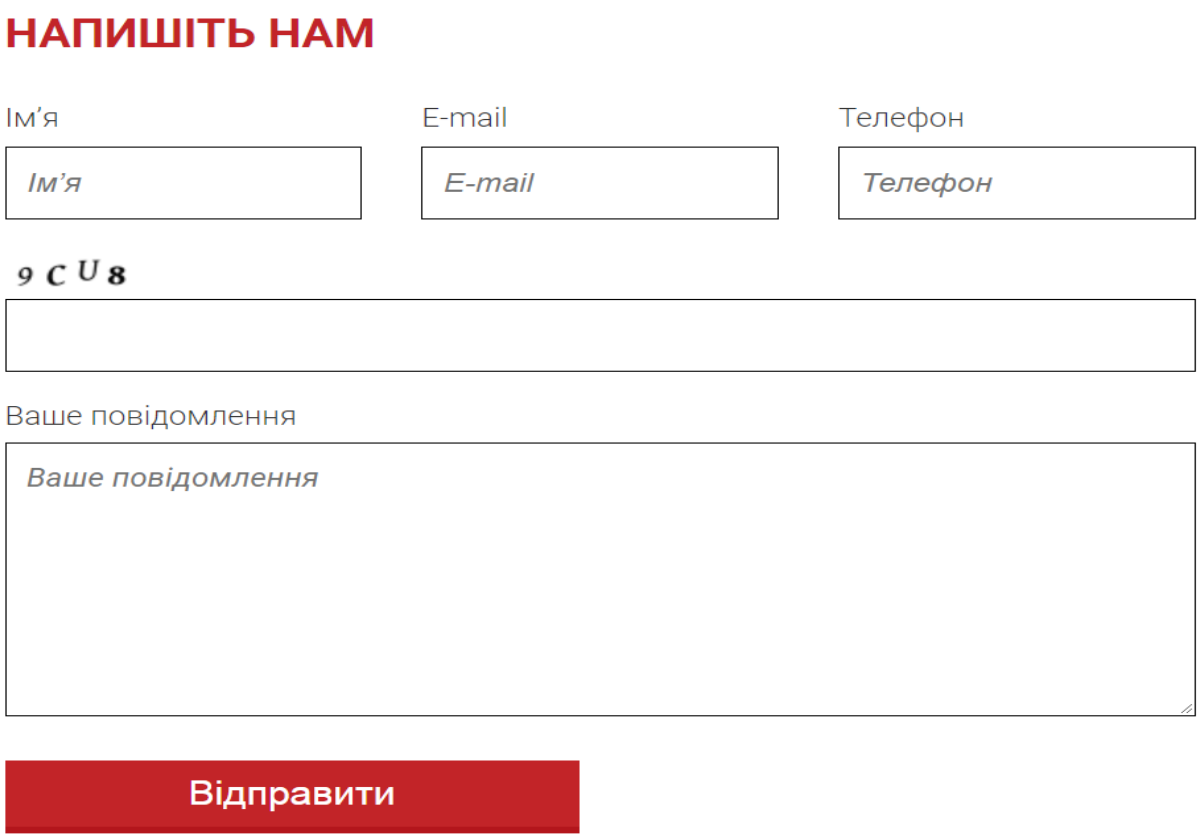

Рисунок 2.2 – Електронна форма для написання повідомлення на сайті Керуючої Компанії «Дом.Ком Україна» [31]

Товариство з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» працює в сфері житлово-комунальних послуг з 2011 р. Підприємство надає послуги з утримання будинків, споруд та прибудинкових територій, обслуговує Покровський (до 2016 р. – Жовтневий) район м. Кривий Ріг. Підприємство знаходиться за адресою: Дніпропетровська область, м. Кривий Ріг, вул. Мусоргського, 15А. E-mail: office_kr@domkom.org.ua [33].

Перший досвід управління житловим фондом підприємство отримало, обслуговуючи низку ОСББ м. Кривий Ріг. За два роки успішного розвитку та плідної роботи, підприємству була передана в управління та обслуговування частина житлового фонду Жовтневого району м. Кривий Ріг загальною площею 901,3 тис. кв. метрів та прибудинковою територією 1004,4 тис. кв. метрів.

Нині в обслуговуванні підприємства знаходиться 416 житлових багатоквартирних будинків, з них: 9-поверхових – 19 будинків; 6-поверхових – 1 будинок; 5-поверхових – 158 будинків; 4-поверхових – 106 будинків; 3-поверхових – 37 будинків; 2-поверхових – 41 будинок; 1-поверхових – 54 будинки. Кількість особових рахунків – 18340. Кількість мешканців – 35660 чол.

Стан житлового фонду, що обслуговується підприємством (будинки за термінами експлуатації): від 20 до 30 років – 14; від 30 до 40 років – 25; від 40 до 50 років – 77; 50 років та вище – 300 [33].

Будь-яке підприємство є хорошим настільки, наскільки хорошою є його команда. ТОВ «Керуюча Компанія «Дом.Ком» є майданчиком для найкращих фахівців житлово-комунальної галузі. Нині на підприємстві працює понад 150 професійних штатних співробітників. Добре підготовлений персонал, інноваційні матеріали, комплектуючі та обладнання провідних вітчизняних і європейських виробників – все це допомагає гарантувати високоякісний сервіс.

Приділяється постійна увага удосконаленню технічної бази підприємства, підбору кваліфікованих кадрів і поліпшенню якості обслуговування населення.

Для ТОВ «Керуюча Компанія «Дом.Ком» характерним є:

– досвід у керуванні житловим фондом;

– системний підхід (проблеми мешканців вирішуються комплексно);

– використання найсучашніших досягнень в ІТ-технологіях;

– наявність сучасної матеріальної бази (сучасний парк техніки, для швидкого і якісного виконання робіт);

– прозорість у роботі (діяльність компанії здійснюється у відповідності до законодавства україни та спрямована на покращення надання житлово-комунальних послуг споживачам);

– клієнтоорієнтованість (надання клієнтам широкого спектру послуг з індивідуальним підходом до кожного).

За понад десять років діяльності підприємством зроблено чимало:

– створено потужну виробничо-технічну базу зі спеціалізованою комунальною технікою, сучасним обладнанням, засобами малої механізації та інвентарем;

– створено оперативну аварійно-диспетчерську службу, укомплектовану спеціальним транспортом та обладнанням, а також засобами зв’язку;

– впроваджуються заходи з енергозбереження, насамперед установка лічильників обліку електроенергії в місцях загального користування;

– при виконанні ремонтів по житлофонду застосовуються тільки сучасні матеріали, що дозволяють значно підвищити якість робіт;

– налагоджено роботу і зворотний зв’язок з населенням, знижено кількість звернень мешканців до органів місцевого самоврядування з питань житлово-комунального обслуговування.

Крім того, підприємством налагоджено соціальне партнерство з містом:

– пристрій і оновлення дитячих майданчиків;

– утримання дитячих майданчиків, скверів та меморіалів;

– участь в інших соціальних заходах міста.

Підприємство використовує нові стандарти обслуговування, впроваджує комплексні рішення з оптимізації управління та утримання житлово-комунального господарства району міста:

– якість обслуговування (підприємство слідкує за якістю виконаних робіт);

– сучасні методи обслуговування (втілення сучасних методів обслуговування житлового фонду);

– ІТ-технології у житлово-комунальному господарстві (розроблено програмні комплекси, які адаптовані для роботи в сфері ЖКГ);

– оплата послуг онлайн Privat24 та IPay.

Програмні комплекси підприємства:

– бухгалтерія ЖКГ. Ведення побудинкового обліку доходів та витрат на базі бухгалтерської програми 1С, автоматичне формування бухгалтерського, податкового, фінансового та управлінського обліку як у цілому по підприємству так і в розрізі окремих будинків;

– абонентський облік. Автоматизація всіх процесів по веденню особових рахунків споживачів: нарахування, облік оплат, пільг та субсидій, формування квитанцій та довідок;

– аварійно-диспетчерська служба. Ведення автоматизованого обліку та контролю приймання та виконання звернень споживачів.

На сайті Товариства з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» є дані про підприємство, новини, досягнення, звіти про виконі види робіт, інформація для споживачів. У контактах можна знайти адресу підприємства, телефони приймальні, аварійно-диспетчерської служби (рис. 2.3).

Рисунок 2.3 – Скриншот головної сторінки сайту Товариства з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» [33]

У 2020 р. в Україні офіційно запустилася ЖКГ-платформа «Діджітал-ЖЕК» (скорочено – ДЖЕК), яка позиціонується як «пульт управління будинком». Цей новий онлайн-сервіс дасть можливість жителям багатоквартирних будинків вирішити всі свої проблеми, пов’язані з житлово-комунальними умовами, через смартфон або ПК – не виходячи з будинку [16].

«ДЖЕК» – це по суті діджиталізація ЖКГ в Україні. У першу чергу, це комунікаційна платформа, через яку мешканці багатоквартирних будинків

можуть спілкуватися зі своїми управителями і сусідами та ефективно вирішувати проблеми ЖКГ в онлайні.

Ідея створення такого рішення виникла з введенням в Україні карантину, коли жителі багатоквартирних будинків виявилися замкненими в своїх оселях і не змогли відвідувати ЖЕКи і зборів мешканців для вирішення комунальних проблем.

Сьогодні реєстрація в «ДЖЕК» доступна для всіх бажаючих. Жителі можуть скористатися низкою базових послуг:

– швидко та безпечно оплатити комунальні рахунки в одному місці (оплати виробляються через платіжний сервіс iPay, у подальшому планують підключати інші сервіси),

– викликати майстра – сантехніка, електрика, слюсаря тощо;

– отримувати новини по будинку.

Для мешканців, чиї управителі вже підключені до системи, доступні ще й додаткові можливості:

– онлайн-звернення до управителя (наприклад, заявка на ремонт або установку лавки біля під'їздів);

– участь в онлайн-опитуваннях від управителів замість довгих зібрань біля під’їзда;

– оперативне інформування з важливих питань (наприклад, про планові відключення комунальних послуг, ремонти і т.д.).

На платформі «ДЖЕК» управитель може публікувати оперативну інформацію про дезінфекцію під’їзду, ремонтні роботи, а жителі – активно допомагати один одному, адже зараз це надзвичайно важливо.

З 1 липня 2020 р. будинки, що обслуговуються Товариством з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком», підключені до платформи «ДЖЕК». Відтоді мешканцям будинків пропонуються такі послуги:

– новий персональний кабінет на платформі www.djek.org з реєстрацією лише у три кроки;

– зручна і проста оплата квитанцій онлайн;

– електронні квитанції в персональному кабінеті;

– новини того чи іншого будинку та важливі оголошення в Viber, Telegram.

Платформа безкоштовна як для мешканців будинків, так і для управителів та доступна через смартфон (Android, iOS) або у веб-версії. Так, тепер лише з допомогою мобільного додатку можна викликати сантехніка, оплатити послуги і навіть провести зібрання жителів багатоквартирних будинків.

На сайті підприємства розміщено новину про те, що відтепер зручним пультом управління будинком можна скористатися через смартфон. Для цього необхідно завантажити мобільний додаток на Play Market і App Store і можна користуватися усіма опціями безкоштовно (рис. 2.4).

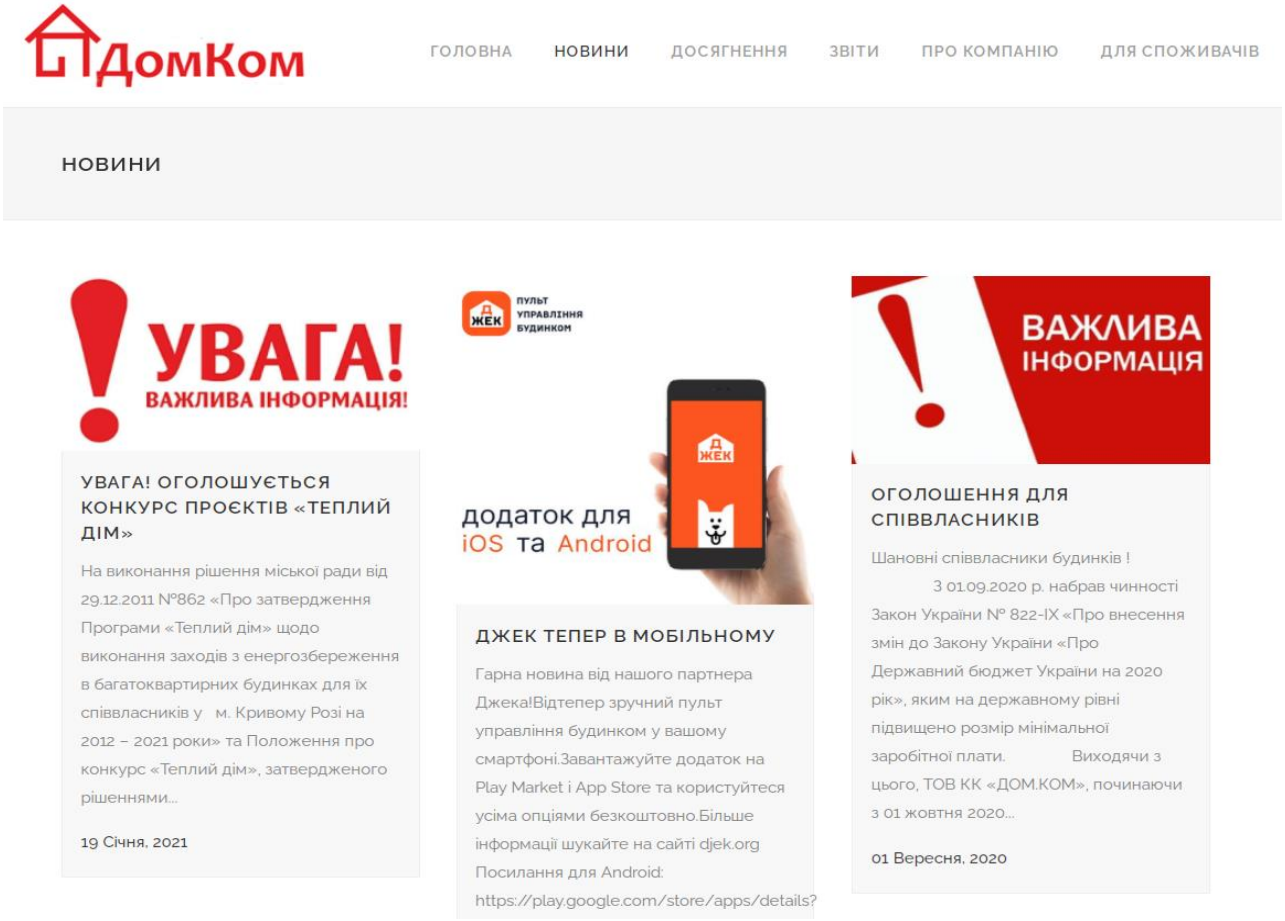

Рисунок 2.4 – Скриншот сторінки «Новини» сайту Товариства з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» [34]

Отже, «ДЖЕК» – це сервіс для вирішення житлово-комунальних проблем у режимі онлайн – від оплати житлово-комунальних послуг до заявок на ремонт.

2.2 Основні етапи конфіденційного документообігу у Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком»

Конфіденційне діловодство у Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» у цілому базується на тих самих принципах, що й загальне, але водночас має відмінності, зумовлені обмеженням доступу до документованої інформації.

Основними завданнями конфіденційного діловодства у Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» є:

– документаційне забезпечення усіх видів конфіденційної діяльності;

– захист документованої інформації, що утворюється в процесі конфіденційної діяльності.

Документуючи конфіденційну інформацію у Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» враховують такі аспекти:

– обсяг конфіденційних відомостей, включених у документ, має бути мінімальним і визначатися реальною ситуацією;

– документ завжди має стосуватися лише одного питання (теми) – це є важливим не стільки для швидкого доведення документа до виконавців, скільки для забезпечення чіткого функціонування системи доступу персоналу до конфіденційної інформації, необхідної лише певному співробітнику, і запобігання несанкціонованому ознайомленню співробітників організації та інших осіб з інформацією, що має обмежений доступ;

– планові, організаційно-розпорядчі (зокрема, накази з основної діяльності), звітні та інші документи, що передбачають кількох виконавців, не слід розсилати підрозділам і виконавцям у повному обсязі – такі документи доводять до виконавців вибірково у вигляді витягів, персоніфікованих додатків-завдань;

– інформацію з обмеженим доступом необхідно максимально локалізувати в конкретній частині документа, його розділі, додатку, фотоілюстрації, графіку, на окремому диску, електронному масиві з ускладненою системою доступу

(наприклад, великий за обсягом документ може мати окремий розділ, що містить комплекс інформації обмеженого доступу).

Прийом вхідних конфіденційних документів здійснюється співробітником конфіденційного діловодства. При цьому перевіряється:

– кількість сторінок документа;
– кількість екземплярів;
– наявність додатків (якщо вони вказані в супровідному листі) [57].

У разі відсутності в пакеті (конверті) деяких перерахованих документів – складається акт в 2-х примірниках. Один примірник акта надсилається на адресу відправника.

Обов'язковою є реєстрація конфіденційних документів у спеціальних журналах. Сторінки журналу представляють собою таблицю, що містить графи: номер по порядку, дата реєстрації документа, дата підписання та номер документа, адресант, найменування і короткий зміст, кількість аркушів документа, кількість аркушів додатка, кількість примірників, виконавець, примітки.

На кожному вхідному документі при реєстрації повинен бути проставлений відбиток штампа, в якому вказуються найменування документа, його реєстраційний номер і дата надходження.

Після реєстрації документи передаються керівництву підприємства для прийняття рішення. Керівник після розгляду документа визначає виконавця та дає вказівки по виконанню документа. Ці вказівки оформляються на самому документі у вигляді резолюції. З резолюцією керівника конфіденційний документ передається виконавцю під розписку в журналі реєстрації вхідних конфіденційних документів.

По завершенні роботи над документом на ньому проставляється відмітка про виконання. Після цього документ підшивається в справу співробітником конфіденційного діловодства.

Рішення про подальше використання конфіденційного документа визначається його значенням і практичною цінністю. Залежно від цього конфіденційні документи можуть: використовуватися в подальшому;

передаватися в архів на зберігання; знищуватися. Всі ці дії повинні виконуватися з дотриманням вимог до конфіденційних документів (рис. 2.5).

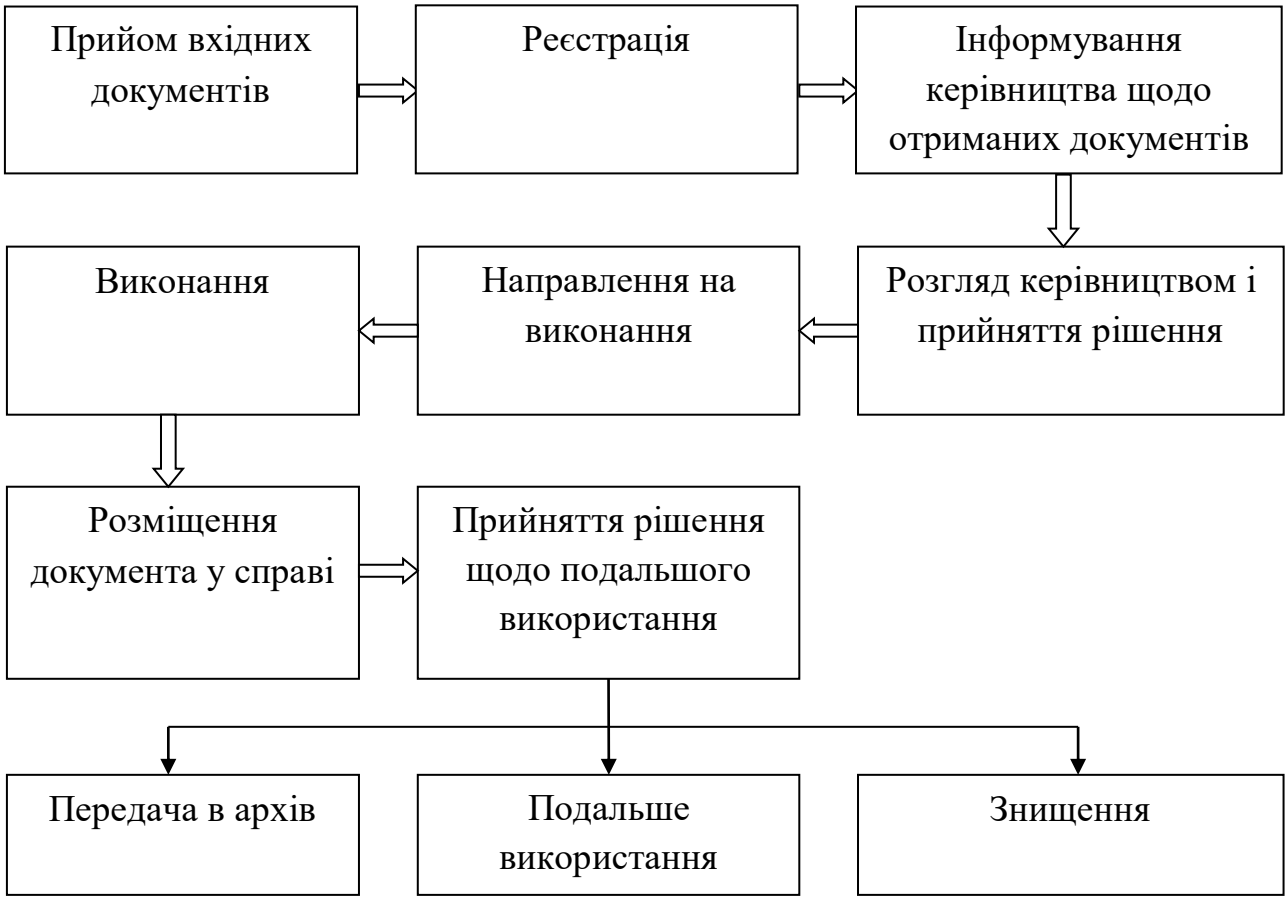

Рисунок 2.5 – Порядок роботи з вхідними конфіденційними документами у Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком», складено автором за [23; 61]

Що стосується регламенту роботи з вихідними конфіденційними документами, то можна визначити низку стандартних процедур, за допомогою яких формується зміст документа і відстежується його шлях від адресанта до адресата. Підготовчий етап – розробка проекту документа, потім його узгодження з керівництвом і підписання, заключний етап – реєстрація в журналі вихідних конфіденційних документів і відправлення документа.

Проект вихідного конфіденційного документа розробляється виконавцем документа у двох примірниках. Далі проект документа надається на затвердження керівництву підприємства. Після підписання документ

реєструється співробітником конфіденційного діловодства в журналі (картці) реєстрації вихідних конфіденційних документів.

Відправка конфіденційних документів здійснюється відповідно до затвердженого керівництвом підприємства переліком адресатів із зазначенням реєстраційного номера вихідного конфіденційного документа.

Отже, робота з вихідними конфіденційними документами включає такі етапи: розробка проекту документа; узгодження документа; підписання документа; реєстрація документа; відправка документа (рис. 2.6).

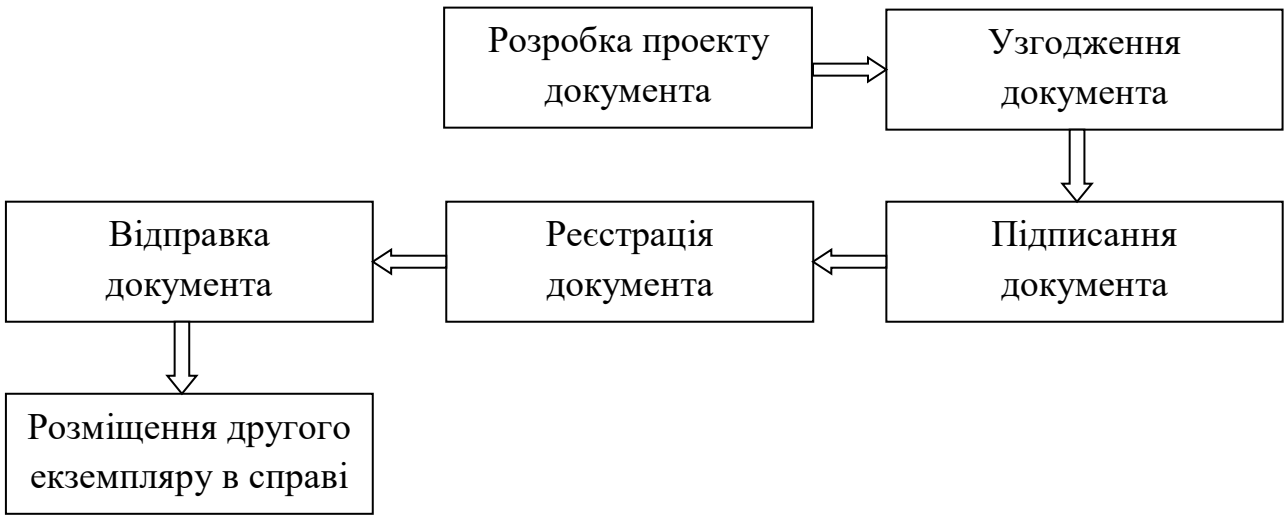

Рисунок 2.6 – Порядок роботи з вихідними конфіденційними документами у Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком», складено автором за [23; 62]

Видача і повернення конфіденційних документів повинні своєчасно відображатися в журналі обліку і видачі конфіденційних документів. Для реєстрації видачі та повернення заводиться спеціальний журнал за аналогією до журналу реєстрації вхідних документів з різницею в найменування граф таблиці.

У таблиці журналу реєстрації видачі – повернення конфіденційних документів є такі графи: номер за порядком, номер документа, дата видачі, найменування документа і його короткий зміст, кількість сторінок у документі, кількість сторінок у додатку, кількість примірників, ПІБ особи, яка отримала документ, розписка в отриманні, відмітка про повернення з підписом і датою, примітки.

Порядок роботи з внутрішніми конфіденційними документами у Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» відображено на рис. 2.7.

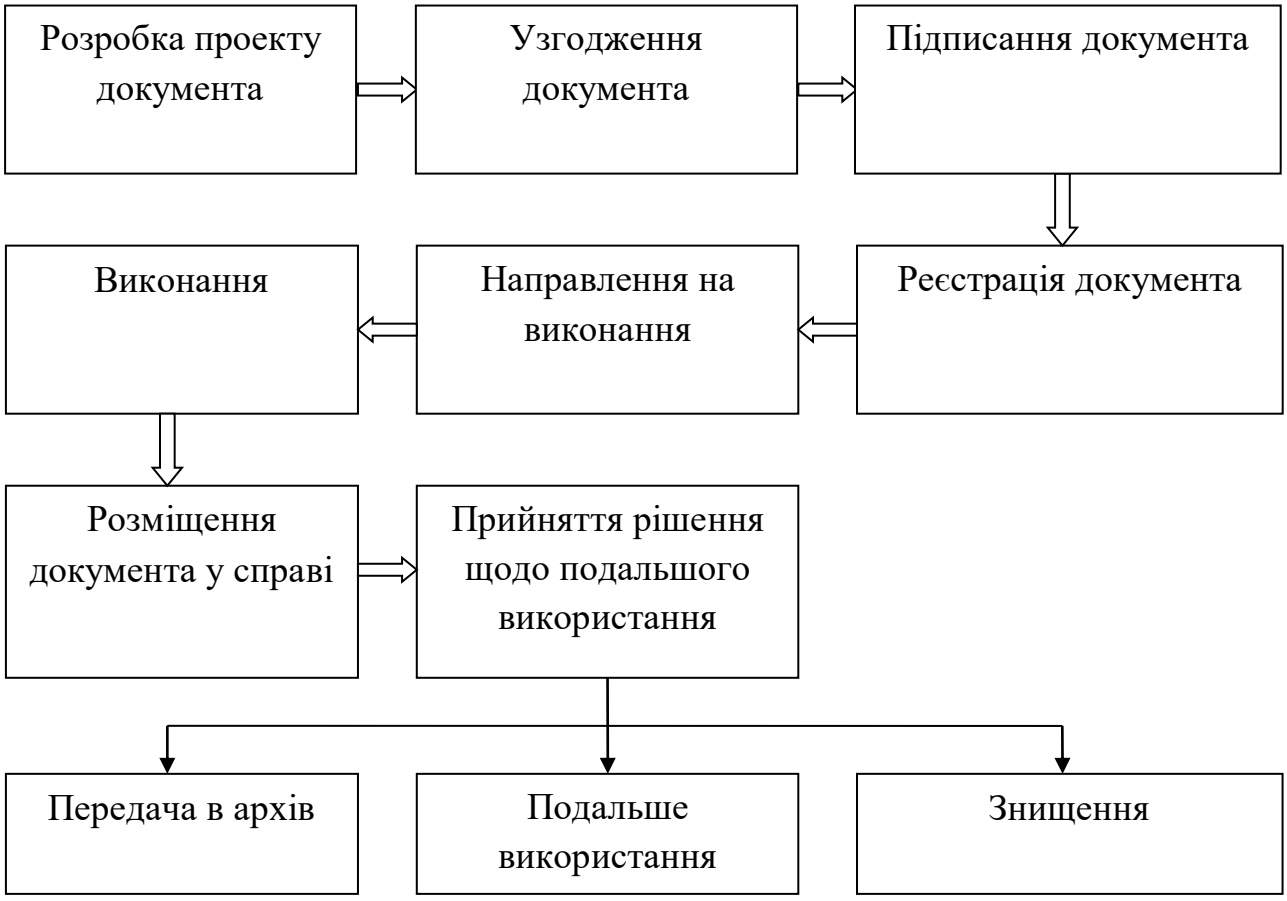

Рисунок 2.7 – Порядок роботи з внутрішніми конфіденційними документами у Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком», складено автором за [61; 62]

У Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» конфіденційним документам надається гриф обмеженого доступу, що засвідчує особливий характер інформації, до якої має доступ обмежене коло осіб. Гриф обмеження доступу («Комерційна таємниця», «Таємно», «Для службового користування», «Конфіденційно» тощо) проставляють у верхньому правому куті на лицьовому боці першого аркуша документа над реквізитами «Адресат» або «Гриф затвердження документа» (Додаток А). Гриф обмеженого доступу проставляється виконавцем та особою, яка підписує документ, на виданні – автором (укладачем) і керівником, який підписав видання до друку.

Відповідальність за забезпечення правильного ведення обліку, зберігання і використання конфіденційних документів несе керівництво Товариства з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком».

Облік конфіденційних документів включає присвоєння та зазначення в облікових формах і на документах реєстраційних номерів, запис облікових і пошукових даних про документи (дата, автор, заголовок, кількість сторінок, місцезнаходження тощо). Обліку підлягають усі без винятку виготовлені у Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» документи з грифом обмеженого доступу.

Документи, що містять конфіденційну інформацію, реєструються один раз. Облік ведеться в журналах обліку конфіденційних документів, як правило, окремо від обліку документів відкритого діловодства (Додаток Б).

Одержуючи конфіденційний документ, співробітник звіряє номер отриманого документа з його номером у журналі реєстрації, перевіряє кількість аркушів і розписується за отриманий документ. При поверненні конфіденційного документа співробітник служби діловодства звіряє номер цього документа з номером у журналі, перевіряє кількість аркушів документа і в присутності співробітника, що повертає документ, проставляє в журналі (у відповідній графі) свій підпис і дату повернення документа [60].

Сторінки журналів реєстрації нумеруються, прошнуровуються та опечатуються. На останній обліковій сторінці робиться запис про кількість сторінок у журналі, який підписує працівник служби діловодства і засвідчує печаткою.

Облік, зберігання, розмноження конфіденційних документів здійснює служба діловодства (секретар), що обліковує несекретну документацію (він також несе відповідальність за нерозголошення інформації даного документа).

Друкування документів, що містять конфіденційну інформацію, здійснюється в структурних підрозділах Товариства з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком». Відповідальність за збереження і нерозголошення інформації несуть керівники цих підрозділів. На звороті останньої сторінки кожного примірника документа особа, яка друкувала його,

має зазначити кількість надрукованих примірників, прізвище виконавця, власне прізвище і дату друкування документа.

Надруковані та підписані примірники документів з грифом обмеженого доступу разом із чернетками чи варіантами передаються для реєстрації працівнику служби діловодства (секретарю), який здійснює їх облік. Чернетки та варіанти знищуються виконавцем і співробітником служби діловодства (секретарем), про що на копії вихідного документа робиться запис: «Чернетки і варіанти знищено». Проставляються дата і підписи.

Розмножувати конфіденційні документи можна лише з дозволу керівника організації чи структурного підрозділу під контролем служби діловодства (секретаря). Облік розмножених документів ведеться за кількістю примірників. У реєстраційних формах, що заповнюються у друкарні, до реєстраційного номера чи назви документа додається відповідна позначка ДСК або КТ [63].

Документи з грифом обмеженого доступу, отримані від інших установ, дозволяється розмножувати лише за їх згодою.

Розсилають конфіденційні документи у ТОВ «Керуюча Компанія «Дом.Ком» на підставі рознарядок, підписаних керівником підприємства і керівником служби діловодства, із зазначенням облікових номерів примірників, що відправляються. Конфіденційні документи пересилають цінними або рекомендованими поштовими відправленнями або з кур’єрами, які доставляють документи під підпис в реєстрі.

Документи, що розсилаються в інші установи, вкладають у конверти або упаковують таким чином, щоб виключити можливість доступу до них. Конверти застосовують світлонепроникні, пакети заклеюють. На конвертах (упаковках) зазначають адреси та назви одержувача і відправника, номери вкладених документів із відповідною позначкою. При цьому на конвертах забороняється зазначати прізвища, посади адресата, а також прізвища виконавців документів і назви структурних підрозділів.

Документи, що містять конфіденційну інформацію, після їх виконання формують у справи. Порядок їх формування передбачений номенклатурою

справ відкритого діловодства. При цьому до номенклатури включаються всі довідкові та реєстраційні картотеки, журнали та документи з відповідними грифами. Документи, що містять конфіденційну інформацію, залежно від виробничої та інформаційної потреби дозволяється формувати у справи окремо або разом з несекретними документами з одного і того самого питання.

Якщо у Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» створюється значна кількість однакових видів документів (наказів, інструкцій, планів тощо) з грифом обмеженого доступу, то передбачено їх формування в окремі справи. При цьому в графі номенклатури справ «Індекс справи» до номера справи з документами, що містять конфіденційну інформацію, додається відповідна позначка.

У разі долучення документа з грифом обмеженого доступу до справи з документами, що не мають такого грифу, на справі ставиться відповідна позначка, наприклад ДСК, а до номенклатури справ вносяться відповідні зміни.

Якщо у процесі діяльності Товариства з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» створюється незначна кількість документів, що містять конфіденційну інформацію, номенклатурою справ передбачено запровадження однієї справи із заголовком «Документи з грифом «Для службового користування»» або «Документи з грифом «Комерційна таємниця»». Строк зберігання такої справи не встановлюється.

Після закінчення діловодного року справу з конфіденційними документами поаркушно переглядають та у разі потреби приймають рішення про переформування справи [17].

Документи постійного зберігання формують в окрему справу, якій надають заголовок і додатково включають до номенклатури справ. Документи тимчасового зберігання залишаються у справі згідно із затвердженою номенклатурою справ.

Якщо у справі з грифом обмеженого доступу містяться лише документи тимчасового зберігання, її можна не переформовувати. Строк зберігання такої справи встановлюється відповідно до найбільшого строку зберігання

документів, що містяться у справі. При цьому у графі номенклатури справ «Строк зберігання» зазначають уточнений строк зберігання.

Справи, в яких нагромаджуються окремі документи, що містять конфіденційну інформацію, належать до категорії обмеженого розповсюдження і використання. На обкладинках і титульних аркушах цих справ також проставляється гриф обмеженого доступу, а до номенклатури справ вносяться відповідні уточнення. Справи з документами, що містять конфіденційну інформацію, повинні мати внутрішні описи.

Доступ до конфіденційних документів у Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» здійснюється лише на основі письмового дозволу керівника підприємства.

Дозвіл на доступ до конфіденційних документів оформлюється у вигляді:

– резолюції керівника на документі;

– завдання (вказівки) про виконання документа та прізвища виконавця в змісті розпорядчих документів (наказ, розпорядження);

– письмового дозволу на видачу документів (для архівних справ) [23].

Доступ до конфіденційних документів, що надійшли до Товариства з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком», здійснюється на підставі резолюції керівника на самому документі або на супровідному листі. Із супровідного листа резолюція переноситься на документ і засвідчується підписом особи, відповідальної за облік, обробку та зберігання конфіденційних документів із зазначенням дати.

Доступ виконавців до документів, що містять конфіденційну інформацію, здійснюється відповідно до затвердженого списку посадових осіб, які мають право працювати з такими документами. Зміни до цих списків, пов’язані з розширенням або обмеженням кола осіб, що допускаються до документів, вносяться з письмового дозволу керівника на підставі доповідних записок керівників структурних підрозділів.

Виконавець документа (якщо він продовжує працювати з тими ж питаннями, що порушені у документі) і особи, які візували та підписували документ,

допускаються до нього без спеціального дозволу. У разі відсутності виконавця (відрядження, відпустка, хвороба) його документами мають право користуватися керівник структурного підрозділу, в якому він працює, або за письмовим дозволом останнього – інші працівники того ж підрозділу, яким доручено виконання документа. Із сейфа документи за відсутності виконавця вилучаються в установленому порядку комісією зі складанням акту.

Не дозволяється використовувати відомості, що містяться в конфіденційних документах, у відкритих виступах чи опубліковувати в ЗМІ, експонувати такі документи на відкритих виставках, демонструвати на стендах, вітринах [46].

Знімати копії, а також робити витяги з документів, що мають гриф обмеженого доступу, можна тільки з дозволу керівника Товариства з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» чи структурного підрозділу.

Копіювати документи з грифом обмеженого доступу, що отримані від інших установ, можна лише з дозволу установ – авторів цих документів.

Видавати справи з грифом обмеженого доступу з архіву можна:

– працівникам своєї організації за списком, затвердженим керівником Товариства з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» (структурного підрозділу) або за його письмовим дозволом;

– працівникам інших установ – за їх письмовим зверненням і на підставі письмового дозволу керівника організації (структурного підрозділу).

Справи з грифом обмеженого доступу видаються виконавцям і приймаються від них під підпис у журналі обліку конфіденційних справ (Додаток В).

Таким чином, документування конфіденційної інформації є важливою складовою конфіденційного діловодства Товариства з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком», оскільки від кількості, складу і правильності оформлення конфіденційних документів залежать якість і ефективність управлінської діяльності, достовірність і юридична сила документів, трудомісткість їхньої обробки, а також якість організації конфіденційного документообігу.

2.3 Особливості роботи з конфіденційною кадровою документацією у Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком»

Одним із видів конфіденційної документації є кадрова документація, тому кадрова служба як підрозділ, що працює з конфіденційною інформацією, повинна дотримуватися правил роботи, які установлені для даного виду інформації.

У процесі роботи з документами з особового складу необхідно враховувати, що за Законом України «Про інформацію» персональні дані (відомості про факти, події та обставини трудової діяльності й особистого життя) громадян відносять до категорії конфіденційної інформації [10].

Згідно Закону України «Про захист персональних даних», персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою [9].

До конфіденційної кадрової документації відноситься трудова книжка. Трудова книжка – це основний документ, де фіксується і накопичується інформація про стаж роботи працівника, яка в майбутньому використовується для визначення соціальних та інших виплат [42].

Трудові книжки на працівників ведуться на всіх підприємствах і організаціях незалежно від форм власності. Трудова книжка є основним документом, що підтверджує загальний, безперервний і спеціальний стаж роботи. Законом забороняється мати одній особі кілька трудових книжок.

Трудова книжка заводиться на працівника, який вперше приймається на роботу. Її заповнюють у присутності прийнятого на роботу не пізніше тижневого строку після підписання наказу про зарахування на роботу. Записи до трудової книжки вносять на підставі паспорта та документів про освіту і професію. Дані про освіту (середня, середня спеціальна, вища) та спеціальність чи професію вказуються на підставі атестатів, дипломів, сертифікатів, а також довідок, якщо освіта незакінчена вища.

Порядок заповнення трудових книжок та вкладок до них, обліку їх та видачі в разі звільнення або втрати тощо регламентує «Інструкція про порядок ведення трудових книжок на підприємствах, в установах та організаціях».

У Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком приділяють значну увагу збереженню та правильному оформленню трудових книжок.

На титульній сторінці трудової книжки вказується прізвище, ім'я та по батькові повністю, без скорочень. Дата народження вказує число, місяць і рік.

На титульній сторінці обов'язково ставиться підпис особи, відповідальної за видачу трудових книжок, і печатка підприємства, де книжка вперше була заповнена. Запис на наступних сторінках трудової книжки починається із проставлення штампу підприємства або написання від руки його назви.

У відповідних графах трудової книжки обов'язковими є записи:

1) порядковий номер запису;

2) дата прийому чи звільнення;

3) вказівка на дію і посаду (прийнятий на посаду старшого інженера, звільнений за власним бажанням, переведений на посаду завідувача лабораторії);

4) підстава (наказ за №... від 00.00.00) [30, с. 107].

Усі дати вказуються в точній відповідності до наказу про прийняття, переведення або звільнення акуратно, без виправлень і помарок. Якщо все-таки виникає необхідність зробити виправлення, то це обумовлюється і завіряється підписом посадової особи та печаткою.

Бланки трудових книжок і вкладок до них є документами суворої звітності (Додаток Г).

У Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» з метою збереження та контролю за використанням бланків трудових книжок і вкладок до них ведеться книга обліку бланків трудових книжок і вкладок до них (Додаток Д). Книга ведеться у бухгалтерії Товариства з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком». Для цієї мети в плані

рахунків бухгалтерського обліку активів, капіталу, зобов'язань і господарських операцій організації виділено окремий позабалансовий рахунок «Бланки суворого обліку».

У книзі обліку бланків трудових книжок і вкладок до них фіксують усі операції, що пов'язані з одержанням та витрачанням бланків трудових книжок і вкладок до них із зазначенням серії й номера кожного бланка. Основними реквізитами книги обліку бланків трудових книжок і вкладок до них є:

– дата (число, місяць, рік);

– від кого отримано або кому відпущено документ;

– підстава операції (найменування документа, номер та дата);

– надходження книжок (кількість книжок із зазначенням серії й номера, кількість вкладок із зазначенням серії й номера, сума);

– витрачання книжок (кількість книжок із зазначенням серії й номера, а також кількість вкладок із зазначенням серії й номера, сума) [28].

Особа, яка призначена відповідальною на підприємстві за ведення трудових книжок працівників повинна звітувати перед бухгалтерією щодо кількості наявних бланків трудових книжок і вкладок до них.

Для обліку руху трудових книжок і вкладок до них відділом кадрів Товариства з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» ведеться книга обліку руху трудових книжок і вкладок до них (Додаток Е). У цій книзі реєструють усі трудові книжки, одержані від працівників під час влаштування їх на роботу, а також трудові книжки і вкладки до них, виписані працівникам які раніше їх не мали. При отриманні трудової книжки у зв'язку зі звільненням працівник розписується в особовій картці й у книзі обліку.

До відомостей, що вносяться до книги обліку руху трудових книжок і вкладок до них, належать:

– нумерація записів за порядком;

– дата приймання або заповнення трудової книжки чи вкладки до неї (число, місяць, рік);

– прізвище, ім'я та по батькові власника трудової книжки;

– посада, професія працівника, який здав або на якого заповнено трудову книжку чи вкладку;

– назва структурного підрозділу;

– дата й номер документа, на підставі якого прийнято працівника;

– підпис відповідальної особи, яка приймала або заповнювала трудову книжку (вкладку);

– серія й номер трудової книжки або вкладки до неї;

– сума, одержана при виписуванні трудової книжки чи вкладки до неї;

– дата й підстави для видачі трудової книжки працівникові;

– підпис власника трудової книжки про її отримання [75].

Книга обліку руху трудових книжок і вкладок до них надає можливість отримати оперативну інформацію про рух і нинішнє місцезнаходження документа суворої звітності. У книзі також відображається основна інформація про початок і закінчення професійної діяльності працівника на підприємстві, підстави прийому та звільнення. Така інформація може стати затребуваною під час відновлення загубленої трудової книжки чи її вкладки.

Книга обліку бланків трудових книжок і вкладок до них та книга обліку руху трудових книжок і вкладок до них мають бути пронумеровані, прошнуровані та затверджені підписом керівника підприємства й відбитком печатки.

Бланки трудових книжок і вкладок до них зберігаються в бухгалтерії як документи суворої звітності й видаються під звіт особі, котра відповідає за ведення трудових книжок.

Особа, яка відповідає за ведення трудових книжок, щомісяця подає до бухгалтерії звіт про наявність бланків трудових книжок і вкладок до них. На зіпсовані під час заповнення бланки трудових книжок і вкладок до них складають акт за типовою формою № П-11 (Додаток Ж).

Якщо працівник попередньо вирішує питання про перехід на інше місце роботи чи оформляється на роботу за сумісництвом, то йому у разі потреби видають завірений витяг із його трудової книжки, який оформлюють на трансферному бланку А4 машинописним способом або від руки.

Трудові книжки та їх дублікати, не одержані працівниками при звільненні, зберігаються протягом двох років у відділі кадрів Товариства з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» окремо від трудових книжок працівників, які перебувають на роботі. Після цього строку непотрібні трудові книжки (дублікати) зберігаються в архіві підприємства протягом 50 років, а по закінченні зазначеного строку їх можна знищити у встановленому порядку.

Також до конфіденційної кадрової документації Товариства з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» відносяться й особові справи.

Особова справа – це сукупність документів, що містять найважливіші відомості про працівника. Особова справа – це добір різних документів, які характеризують біографічні, ділові та особисті якості працівника. Вона необхідна для вивчення, добору і використання персоналу на підприємстві [30, с. 105].

На кожного працівника Товариства з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» у відділі кадрів формують особову справу. Кожній особовій справі присвоюють порядковий номер, який відповідає номеру в штатно-посадовій книзі.

До особової справи заносять документи, що їх заповнює чи складає працівник при вступі на роботу (заяву, особовий листок з обліку кадрів чи анкету, автобіографію), копії документів про освіту, витяг з наказу про зачислення на роботу та інші документи по особовому складу, що стосуються даного працівника. Усі ці документи підшивають в окрему папку, на обкладинці якої зазначають інформацію в такій послідовності: назва підприємства, «Відділ кадрів», «Особова справа. №»; ім’я, по батькові, прізвище працівника, на якого оформлено особову справу.

Особові справи зберігаються окремо від інших документів, у спеціальних сейфах. Доступ до особових справ мають працівники, які визначені наказом керівника Товариства з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком». Опис документів особової справи містить їх порядкові номери, індекси, найменування, кількість сторінок. Опис документів складає працівник відділу кадрів під час первісного оформлення документів особової справи, а

подальші записи заносять після одержання відповідних документів. Форма опису особової справи дає можливість працівникові відділу кадрів враховувати тимчасове вилучення з неї документів. У разі необхідності вилучення документа з особової справи працівник відділу кадрів робить в описі відповідну позначку: ким вилучено документ і з якої причини (Додаток И).

Найбільш раціональним вважається такий склад і порядок розміщення документів в особовій справі:

– опис документів;

– доповнення до особового листка з обліку кадрів (записуються відомості про накази про переведення на іншу роботу, заохочення, дисциплінарні стягнення; зміни облікових даних працівника);

– особовий листок з обліку кадрів;

– автобіографія;

– копії документів про освіту, вчений ступінь, підвищення кваліфікації;

– перелік наукових праць (для працівників із вченим ступенем чи званням);

– різного роду характеристики чи рекомендаційні листи;

– копія документа про затвердження на посаді (у випадках, передбачених чинним законодавством);

– копії документів, на основі яких видаються накази про призначення, переведення, звільнення працівника;

– заява про прийняття на роботу;

– матеріали проведення атестації;

– згода на обробку персональних даних [42].

У подальшому, в хронологічній послідовності, до особової справи додаються: накази (розпорядження) про зміни анкетних даних; копії документів, які підтверджують підвищення кваліфікації, перепідготовку, стажування; характеристики; атестаційні листки та ін.

У Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» приділяють значну увагу оформленню та збереженню конфіденційної кадрової документації.

РОЗДІЛ 3
ОСНОВНІ НАПРЯМИ УДОСКОНАЛЕННЯ ОРГАНІЗАЦІЇ КОНФІДЕНЦІЙНОГО ДОКУМЕНТООБІГУ НА ПІДПРИЄМСТВІ

3.1 Складові системи захисту конфіденційної інформації на підприємстві

Останнім часом питання конфіденційної інформації викликає загострену увагу, адже будь-яка інформація має цінність для її власника та потребує захисту від нецільового використання та розголошення іншим особам.

Захист інформації – це сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації [3].

У Законі України «Про інформацію» зазначено, що захист інформації – це сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї [10].

Основними цілями захисту конфіденційної інформації є:

– запобігання витоку, розкрадання, спотворення, підробки інформації;

– забезпечення безпеки особистості, суспільства, держави;

– запобігання несанкціонованим діям зі знищення, перекручення, блокування інформації;

– захист конституційних прав громадян на збереження особистої таємниці та конфіденційності персональних даних;

– збереження державної таємниці, конфіденційності документованої інформації [26].

Підприємством має бути створена система захисту конфіденційної інформації, яка б унеможливила несанкціонований (незаконний) доступ до неї. Заходи щодо захисту конфіденційної інформації на підприємстві можна умовно класифікувати на зовнішні та внутрішні, які, в свою чергу, поділяються на

правові, організаційні, технічні та психологічні (табл. 3.1). Дотримання заходів збільшує захищеність інформації і робить її більш стійкою до різних загроз.

Таблиця 3.1 – Заходи щодо захисту конфіденційної інформації підприємства, складено автором за [8; 62]

Заходи щодо захисту конфіденційної інформації			
Зовнішні		Внутрішні	
Правові: 1) прийняття положення про забезпечення цілісності конфіденційної інформації; 2) укладання договорів про повну матеріальну відповідальність; 3) прийом розписок про нерозголошення конфіденційної інформації і попередження про відповідальність за її розголошення.	*Організаційні:* 1) створення спеціального режиму, спеціальних підрозділів; 2) розробка дозвільної системи доступу до інформації; 3) введення відповідної відмітки документів та інших носіїв інформації; 4) організація конфіденційного діловодства; 5) призначення відповідального за збереження конфіденційності.	*Технічні:* 1) виявлення можливих джерел витоку інформації; 2) придбання спеціальної апаратури і програмних продуктів для захисту інформації; 3) проведення регулярних оперативних заходів по технічному захисту і пошуку каналів витоку інформації.	*Психологічні:* 1) проведення роз'яснювальної роботи з персоналом, партнерами і клієнтами; 2) створення сприятливої атмосфери в колективі; 3) проведення регулярних перевірок (гласних і негласних) з виявлення ненадійних осіб.

Загроза інформаційної безпеки – це сукупність умов і факторів, що створюють небезпеку порушення інформаційної безпеки. Носіями загроз безпеки інформації є джерела загроз. Всі джерела загроз інформаційної безпеки можна поділити на три основні групи:

– обумовлені діями суб'єкта (антропогенні джерела) – суб'єкти, дії яких можуть призвести до порушення безпеки інформації, дані дії можуть бути кваліфіковані як навмисні або випадкові злочини. Джерела, дії яких можуть призвести до порушення безпеки інформації можуть бути як зовнішніми, так і внутрішніми. Ці джерела можна спрогнозувати, і прийняти адекватні заходи.

– обумовлені технічними засобами (техногенні джерела) – ці джерела загроз менш прогнозовані, безпосередньо залежать від властивостей техніки і тому

вимагають особливої уваги. Дані джерела загроз інформаційній безпеці, також можуть бути як внутрішніми, так і зовнішніми;

– стихійні джерела – дана група об'єднує обставини, що становлять непереборну силу (стихійні лиха або інші обставини, які неможливо передбачити або запобігти чи можливо передбачити, але неможливо запобігти), такі обставини, які носять об'єктивний і абсолютний характер, поширюється на всіх. Такі джерела загроз абсолютно не піддаються прогнозуванню і тому заходи проти них повинні застосовуватися завжди. Стихійні джерела, як правило, є зовнішніми по відношенню до захищеного об'єкта і під ними, як правило, розуміються природні катаклізми [37].

Основною загрозою безпеки інформаційних ресурсів обмеженого поширення є несанкціонований (незаконний, недозволений) доступ зловмисника чи сторонньої особи до документованої інформації і як результат оволодіння інформацією і протиправне її використання або вчинення інших дестабілізуючих дій.

Під сторонньою особою розуміється будь-яка особа, яка не має безпосереднього відношення до діяльності підприємства (працівники інших організаційних структур, відвідувачі підприємства тощо), а також співробітники цього підприємства, що не володіють правом доступу до певних приміщень, до конкретного документу, інформації, баз даних.

Метою і результатами несанкціонованого доступу може бути не тільки оволодіння цінними відомостями і їх використання, а й їх видозміна, модифікація, знищення, фальсифікація, підміна і тому подібне.

Основним винуватцем несанкціонованого доступу до інформаційних ресурсів є, як правило, персонал, що працює з документами, інформацією та базами даних. При цьому треба мати на увазі, що втрата інформації відбувається в більшості випадків не в результаті навмисних дій зловмисника, а через неуважність і безвідповідальність персоналу.

Отже, втрата інформаційних ресурсів обмеженого доступу може настати при:

– наявності зацікавленості конкурентів, установ, фірм або осіб до конкретної інформації;

– виникненні ризиків і загроз, організованих зловмисником, або при випадкових обставинах;

– наявності умов, що дозволяють зловмисникові здійснити необхідні дії і оволодіти інформацією. Ці умови можуть включати:

– відсутність системної аналітичної роботи з виявлення та вивчення загроз, каналів і ступеня ризику порушень безпеки інформаційних ресурсів;

– неефективну систему захисту інформації або відсутність цієї системи, що утворює високий ступінь уразливості інформації;

– непрофесійно організовану систему обробки і зберігання конфіденційних документів;

– невпорядкований підбір персоналу і плинність кадрів, складний психологічний клімат у колективі;

– відсутність системи навчання працівників правилам захисту інформації обмеженого доступу;

– відсутність контролю зі сторони керівництва підприємства за дотриманням персоналом вимог нормативних документів по роботі з інформаційними ресурсами обмеженого доступу;

– безконтрольне відвідування приміщень фірми сторонніми особами.

Отже, загроза порушення конфіденційності полягає в тому, що інформація стає відомою тому, хто не володіє повноваженнями доступу до неї. Конфіденційна інформація повинна захищатися і від втрати, і від витоку.

Система захисту інформації представляє собою комплекс організаційних, технічних і технологічних засобів, методів і заходів, які перешкоджають несанкціонованому (незаконному) доступу до інформації. Власник інформації особисто визначає не тільки склад цінної інформації, яка належить захисту, але й відповідні способи та засоби захисту [62].

Комплексність системи захисту досягається її формуванням з різних елементів – правових, організаційних, технічних. Співвідношення елементів та їх зміст забезпечують індивідуальність системи захисту інформації на підприємстві. Конкретну систему захисту можна уявити у вигляді цегляної

стіни, яка складається з безлічі різноманітних елементів (цегли). Отже, можна виокремити три рівня системи захисту конфіденційної інформації: правовий, організаційний та технічний (рис. 3.1).

Рисунок 3.1 – Основні способи захисту конфіденційної інформації, складено автором за [3; 8; 26]

Елемент правового захисту інформації передбачає: наявність в засновницьких та організаційних документах підприємства, контрактах, що укладаються із співробітниками, і в посадових інструкціях положень та зобов'язань щодо захисту конфіденційних відомостей, формулювання і доведення до відома всіх співробітників підприємства механізму правової відповідальності за розголошення конфіденційних відомостей. У правовий елемент системи захисту може також включатись страхування цінної інформації від різних ризиків [27].

Елемент організаційного захисту інформації містить заходи управлінського та обмежувального характеру, які спонукають персонал дотримуватися правил захисту конфіденційної інформації і включає в себе:

– регламентацію та регулярне оновлення переліку (списку) цінної, конфіденційної інформації, яка підлягає захисту, складання і ведення переліку конфіденційних документів підприємства;

– регламентацію системи (ієрархічної схеми) обмеження доступу персоналу до конфіденційної інформації;

– регламентацію технології захисту і обробки конфіденційних документів;

– побудову захищеного традиційного або безпаперового документообігу;

– побудову технології документування цінної інформації, складання, оформлення, виготовлення і видавництва конфіденційних документів;

– побудову технологічної системи збереження конфіденційних документів;

– організацію архівного зберігання конфіденційних документів;

– регламентацію захисту інформації від несанкціонованих дій персоналу;

– порядок і правила роботи персоналу з конфіденційними документами та конфіденційною інформацією, контроль за виконанням всіма співробітниками цього порядку і правил;

– відбір персоналу для роботи з конфіденційною інформацією, навчання та інструктування співробітників;

– порядок захисту інформації при веденні переговорів, проведенні нарад по конфіденційним питанням, прийомі відвідувачів, здійснення рекламної, виставочної та іншої діяльності;

– регламентацію аналітичної роботи з виявлення загроз цінній інформації і каналів витоку інформації;

– обладнання і атестацію приміщень і робочих зон, виділених для здійснення конфіденційної діяльності, ліцензування технічних систем і засобів захисту інформації та охорони;

– регламентацію пропускного режиму на території, приміщеннях підприємства, ідентифікацію персоналу;

– регламентацію системи охорони території, будівлі, приміщень, обладнання і персоналу підприємства;

– регламентацію дій персоналу в екстремальних ситуаціях;

– регламентацію роботи по управлінню системою захисту інформації.

Елемент організаційного захисту є стержнем, який зв'язує в систему всі елементи. Центральною проблемою при розробці методів організаційного захисту інформації є формування дозвільної (обмежувальної) системи доступу персоналу до конфіденційних відомостей, документів, баз даних. Важливо чітко встановити: хто, кого, до яких відомостей, коли, на який період і як допускає.

Дозвільна система доступу вирішує такі задачі: забезпечення співробітників всіма необхідними для роботи документами і інформацією; обмеження кола осіб, які допускаються до конфіденційних документів; виключення несанкціонованого ознайомлення з документами. Ієрархічна послідовність доступу реалізується за принципом «чим вища цінність конфіденційних відомостей, тим менша чисельність співробітників можуть їх знати» [61].

Доступ співробітника до конфіденційних відомостей, який здійснюється у відповідності з дозвільною системою, називається санкціонованим. Дозвіл (санкція) на доступ до цих відомостей завжди є строго персоніфікованим і видається керівником в письмовому вигляді: наказом, що затверджує схему посадового чи іменного доступу до інформації, резолюцією на документі, списком-дозволом в карточці видачі справи.

Елемент технічного захисту включає: засоби захисту технічних каналів витоку інформації, що виникають під час роботи ЕОМ, засобів зв'язку,

копіювальних апаратів, принтерів, факсів та інших приладів і обладнання; засоби захисту приміщень від візуальних та акустичних способів технічної розвідки; засоби охорони будівель і приміщень від проникнення сторонніх осіб (засоби спостереження, сповіщення, сигналізації, інформування і ідентифікації, інженерні споруди); засоби протипожежної охорони; засоби виявлення приладів і пристроїв технічної розвідки (підслуховувальних та передавальних пристроїв, звукозаписувальної та телевізійної апаратури тощо) [62].

Система захисту конфіденційної інформації на підприємстві є індивідуалізованою сукупністю необхідних елементів захисту, кожний з яких окремо вирішує свої специфічні для даного підприємства завдання. У комплексі ці елементи формують багатогранний захист секретів підприємства і дають відносну гарантію безпеки підприємницької діяльності.

Захист конфіденційної інформації підприємства може забезпечуватися низкою управлінських інструментів, основними з яких є:

– установлення правил віднесення інформації до конфіденційної;

– розроблення та доведення до осіб, допущених до конфіденційної інформації, інструкцій щодо дотримання режиму конфіденційності;

– обмеження доступу до носіїв інформації, які вміщують конфіденційну інформацію;

– використання організаційних, технічних та інших засобів збереження (захисту) конфіденційної інформації;

– здійснення контролю за дотриманням установленого режиму збереження (захисту) конфіденційної інформації.

Водночас захист конфіденційної інформації передбачає:

– визначення конфіденційної інформації, строків її захисту за категоріями;

– систему допуску працівників підприємства, інших осіб до конфіденційної інформації;

– обов’язки осіб, допущених до конфіденційної інформації;

– визначення порядку роботи з паперовими та електронними документами, що містять конфіденційну інформацію;

– забезпечення збереження документів і справ (архівів), що містять конфіденційну інформацію;

– механізми організації та проведення контролю за забезпеченням установленого порядку під час роботи з конфіденційною інформацією;

– відповідальність за розголошення конфіденційної інформації та втрату документів, що містять конфіденційну інформацію [15].

Комплексність системи захисту конфіденційної інформації досягається її формуванням із різних елементів – правових, організаційних, програмно-технічних. Співвідношення елементів, їх зміст забезпечують індивідуальність системи, гарантують її неповторність та складність подолання.

У цілому для створення правових основ захисту конфіденційної інформації та комерційної таємниці на підприємстві необхідно попередньо зробити таке:

– розробити Перелік відомостей, що складають комерційну таємницю та конфіденційну інформацію підприємства;

– розробити Положення про інформаційну політику підприємства та договір про конфіденційність наданої інформації;

– при укладенні трудових договорів (контрактів) із співробітниками підприємства внести пункт про обов’язок співробітника зберігати комерційну таємницю та конфіденційну інформацію підприємства;

– при прийманні на посаду співробітників, робота яких буде пов’язана з конфіденційною інформацією, підписувати Зобов’язання про нерозголошення комерційної таємниці та конфіденційної інформації [49].

Як свідчить практика, попри наявність на підприємстві організаційних заходів щодо захисту конфіденційної інформації, ознайомлення значної кількості працівників із нею підвищує ризик її витікання. Через це правильна організація роботи персоналу з такими документами є дуже важливою. Основні принципи та правила управління персоналом з урахуванням вимог інформаційної безпеки визначено в міжнародному стандарті ISO 17799. Суть їх полягає в необхідності виконання певних вимог під час наймання та звільнення працівників, забезпеченні обізнаності із правилами роботи та застосуванні

запобіжних заходів до порушників. Дотримання цих заходів дає змогу істотно знизити вплив людського фактора, уникнути характерних помилок і здебільшого запобігти витіканню інформації та її неналежному використанню.

Для більш надійного збереження конфіденційна інформація має перебувати переважно в електронному вигляді і бути захищена електронними засобами захисту. Практика показує, що в нинішніх умовах крадіжки (витікання) інформації відбуваються і по електронних каналах зв'язку або за допомогою різних носіїв інформації. Виходячи з цього, головні зусилля в боротьбі з витіканням конфіденційної інформації потрібно зосередити саме на цьому напрямі. Зокрема, насамперед слід налагодити чітку систему контролю та аудиту за використанням у роботі працівників тих чи інших документів. Для цього використовуються спеціальні установки програмного забезпечення для обмеження доступу груп користувачів до окремих частин корпоративної мережі і до документів.

Сучасні технології уможливлюють розроблення та впровадження різноманітних багатоступінчастих засобів контролю доступу і запобігання витіканню інформації. Для обмеження доступу до інформації та протоколювання фактів здійснення несанкціонованого доступу використовують стандартні сервіси безпеки.

Для запобігання несанкціонованому копіюванню конфіденційної інформації на зовнішні носії використовується спеціалізоване програмне забезпечення, призначене для контролю зовнішніх комунікаційних портів комп'ютера (типу USB тощо). Користувачам присвоюються права доступу до контрольованих пристроїв за аналогією з правами доступу до файлів [15].

Це лише декілька найбільш популярних і використовуваних на практиці систем боротьби із втратою конфіденційної інформації. Насправді їх, звісно ж, набагато більше, і вибирати треба самому підприємству виходячи з його фінансових можливостей, цінності інформації та ступеня загрози.

Для ефективного захисту конфіденційної інформації, її необхідно врегулювати, насамперед, на рівні локальних актів (у Положенні про конфіденційну інформацію, посадовій інструкції) з якими працівники підприємства повинні ознайомитися під підпис. Крім того, необхідно визначити

перелік інформації, яка виступає носієм комерційної таємниці і належить до конфіденційної інформації.

Разом з умовами використання та захистом конфіденційної інформації, закріплених нормативним актом підприємства, правовідносини з усіма учасниками, які мають доступ до конфіденційної інформації (працівниками, особами, які надають послуги, контрагентами) мають бути врегульовані в договірному порядку. У відносинах з контрагентами питання конфіденційної інформації регулюються зазвичай у вигляді окремого договору про нерозголошення, або як один із розділів основного договору.

Незважаючи на вид договору, в ньому повинні бути такі складові: визначення конкретного переліку інформації, яка є конфіденційною; коло осіб, які мають доступ до неї; права та обов'язки сторін щодо її використання; порядок її знищення та строк дії зобов'язання (дана умова досить розповсюджена у західних країнах), а також вартість зобов'язання про нерозголошення (за умови що договір є оплатним) та юридична відповідальність за порушення умов договору (як правило у вигляді штрафних санкцій).

Для убезпечення власника конфіденційної інформації в договорі доречно детально виписувати, що сторонами визнається неправомірним розголошенням конфіденційної інформації, яка відповідальність із зазначенням конкретного її розміру покладається на винну особу, що допустила неправомірне розголошення конфіденційної інформації, а також строк протягом якого діє сам договір [59].

Отже, кожне підприємство з урахуванням особливостей його діяльності, а відповідно, складу конфіденційної інформації, має розробити та затвердити:

– Положення про конфіденційну інформацію підприємства;

– Перелік категорій відомостей, що складають конфіденційну інформацію підприємства;

– форму Договору (Зобов'язання) про нерозголошення конфіденційної інформації підприємства;

– Інструкцію про порядок роботи з документами підприємства, що містять конфіденційну інформацію тощо.

3.2 Порядок зняття грифу обмеженого доступу та забезпечення збереженості конфіденційних документів на підприємстві

Інформація – це продукт, який має таку властивість як старіння. Певна категорія інформації, яка включена до переліку конфіденційної інформації, з часом може втратити свою комерційну цінність. Відповідно в даному випадку відпадає необхідність захищати цю інформацію від неправомірних посягань або втрати. Відтак дана категорія відомостей має бути виключена з переліку конфіденційної інформації підприємства, що передбачає подальше проведення процедури зняття грифу конфіденційності з документів, що містять таку інформацію.

Для того щоб зняти гриф конфіденційності з документа, необов'язково чекати, коли закінчиться зазначений в переліку термін дії режиму обмеження доступу до інформації, що міститься в документі.

Підставою для зняття грифу конфіденційності може бути також зміна об'єктивних обставин, внаслідок яких подальший захист певних конфіденційних відомостей підприємства є недоцільним.

Взагалі, розглядаючи питання зняття грифу конфіденційності, варто відзначити, що підставами для цього можуть бути:

– виключення інформації, що міститься в документі (носії), з переліку конфіденційної інформації підприємства;

– закінчення встановленого терміну дії режиму обмеження доступу до інформації;

– наявність події, при якому подальший захист конфіденційної інформації стає недоцільним (наприклад, патентування винаходу, розголошення інформації тощо);

– встановлення факту неправильності присвоєння грифу конфіденційності документу (носію) [40].

Підготовка пропозицій щодо зняття грифу конфіденційності покладається, як правило, на експертну комісію, яка створюється за рішенням керівництва

підприємства. До комісії в обов'язковому порядку включають працівника, відповідального за ведення конфіденційного діловодства.

Висновок комісії оформляють актом, який затверджується керівництвом підприємства. На документі гриф конфіденційності закреслюють однією рискою і поруч з ним за допомогою спеціального штампа або від руки роблять позначку про зняття грифа: Гриф знятий. Акт №__від_ (вказують номер акта і дату його затвердження керівником), завірену підписом особи, відповідальної за ведення конфіденційного діловодства, і печаткою підприємства (структурного підрозділу). Аналогічні відмітки вносяться до опису справ, журналів реєстрації конфіденційних документів.

Звичайно, про зняття грифу конфіденційності з документів необхідно письмово поінформувати всіх адресатів, яким ці матеріали направлялися, адже вони не знають про те, що гриф обмеження доступу з матеріалів був знятий.

На документи з грифом обмеженого доступу, що мають постійний строк зберігання або «до ліквідації організації», а також тривалий (понад 10 років) строк зберігання, складають описи справ, оформлюють обкладинки справ та формують справи відповідно до архівних правил [60].

Відібрані для знищення документи, строк зберігання яких закінчився, включаються в акт про вилучення цих документів для знищення. Якщо документи з грифом обмеженого доступу включаються до загального акту разом з іншими, несекретними справами, то в графі «Заголовок справи» після номерів справ проставляється відповідна позначка. Документи знищуються після затвердження акту керівником підприємства.

Відібрані для знищення документи з грифом обмеженого доступу перед відправленням на переробку як макулатуру слід подрібнити до стану, що виключає можливість їх прочитання. Якщо обсяг справ, відібраних для знищення, незначний, вони можуть бути спалені, про що в акті необхідно зробити позначку.

Після знищення документів із грифом обмеженого доступу в облікових документах (журналах, номенклатурах, описах справ тимчасового зберігання) зазначається: Знищено. Акт №___ від (дата).

Інформаційні видання, телефонні й адресні довідники, копії документів, стенографічні записи та друкований брак можна знищувати без акту, але з позначкою в облікових формах, що засвідчуються підписами виконавця і працівника, відповідального за їх облік і зберігання.

Для забезпечення збереженості конфіденційних документів, справ і носіїв, а також для запобігання витоку інформації, що міститься в них, повинен бути встановлений спеціальний режим їх зберігання.

Організація зберігання конфіденційних документів повинна виключати можливість несанкціонованого доступу до них.

Всі документи, справи і видання, що мають гриф конфіденційності, повинні зберігатися в службових приміщеннях у шафах, які надійно замикаються і опечатуються.

Приміщення, в яких зберігаються конфіденційні документи повинні відповідати вимогам внутрішньооб'єктового режиму, який забезпечує фізичну збереженість документації, що знаходиться в даних приміщеннях.

Основний принцип зберігання конфіденційних документів – це персональна відповідальність співробітника підприємства, відповідального за роботу з конфіденційними документами, а також виконавців за збереженість цих документів [69].

Для документів, що містять конфіденційну інформацію, на підприємстві створюють особливий режим зберігання: у службових приміщеннях встановлюють шафи (сейфи), обладнують сховища, що надійно замикаються та опечатуються.

Отже, роботу підлеглих доцільно організувати за принципом «чистих столів». Суть його полягає в тому, що співробітник за своєї відсутності не повинен залишати жодного документа на своєму робочому місці. Вся інформація, а особливо та, що має конфіденційний характер, повинна надійно зберігатися у сейфі, металевій шафі.

Приміщення, які призначені для цілодобового зберігання конфіденційних документів, повинні відповідати нормам, встановленим для зберігання таких

документів: віддалені від приміщень з харчовими продуктами і хімічними речовинами, не мати з ними вентиляційних каналів, відповідати вимогам пожежної безпеки, санітарним нормам, а також бути гарантованими від затоплення.

Вхід в такі приміщення необхідно строго регламентувати. Крім керівника підприємства і співробітників, що мають пряме відношення до обробки і зберігання конфіденційних документів, в приміщення можуть допускатися особи, що забезпечують їх обслуговування.

Для запобігання несанкціонованого входу в приміщення, в яких зберігаються конфіденційні матеріали, на дверях, по можливості, встановлюють електронні замки. Вікна приміщень повинні мати надійні засоби захисту, що виключають можливість проникнення в приміщення сторонніх осіб. Крім того, на них повинна бути захисна сітка або жалюзі, що запобігають можливості випадання документів, а також візуального перегляду документів і екранів відеомоніторів з вулиці.

Вхідні двері, вікна приміщень, а також сейфи, шафи і стелажі слід оснастити охоронною сигналізацією, яка пов’язана зі службою охорони підприємства або службою позавідомчої охорони.

Конфіденційні документи в приміщеннях повинні зберігатися в сейфах, металевих шафах або металевих стелажах, які після закінчення робочого дня закриваються і опечатуються співробітниками, відповідальними за облік і зберігання документів. Зберігання відкритих документів разом з конфіденційними допускається тільки у випадках, коли вони є додатками до конфіденційних документів [17].

Електронні версії конфіденційних документів зберігають за допомогою врахованих в конфіденційному діловодстві зовнішніх електронних носіїв, що мають відповідні інвентарні номери і грифи конфіденційності (електронні носії з грифом конфіденційності повинні зберігатися окремо від інших зовнішніх електронних носіїв інформації в сейфі або шафі, яка замикається), а також на жорстких дисках комп'ютерів, які не підключені до внутрішньої комп'ютерної мережі підприємства і мережі Інтернет, з використанням парольного захисту.

Необхідно встановити заборону на розміщення і обробку конфіденційної інформації на комп’ютерах, підключених до мережі Інтернет. У випадку роботи користувачів на комп’ютерах, підключених до внутрішньої комп’ютерної мережі підприємства, електронні версії конфіденційних документів повинні зберігатися на захищеному диску (інформація на захищених дисках стає доступною тільки тоді, коли адміністратор мережі надає користувачеві відповідні повноваження).

Резервне копіювання конфіденційної інформації здійснюють з використанням зовнішніх електронних носіїв, що мають відповідні грифи конфіденційності та інвентарні номери [60].

За збереженість конкретного конфіденційного документа (матеріального носія інформації) відповідає працівник, який отримав цей документ (матеріальний носій інформації) у користування з проставленням ним особистого підпису у відповідному журналі реєстрації (обліку). Після закінчення робочого дня всі документи слід прибирати в сейф (шафу).

У разі зміни або звільнення працівника, відповідального за ведення конфіденційного діловодства, складають акт прийому-передачі конфіденційних справ (документів на паперових та інших носіях конфіденційної інформації), що затверджується керівником підприємства.

При звільненні працівник підприємства зобов'язаний здати особі, відповідальній за ведення конфіденційного діловодства, всі наявні в його розпорядженні матеріальні носії конфіденційної інформації.

Документи, видані для роботи працівникам-виконавцям, повертають до служби діловодства (секретарю) або в архів того самого дня.

У деяких випадках з дозволу керівника служби діловодства чи особи, відповідальної за архів підприємства, документи можуть зберігатися у працівника протягом терміну, потрібного йому для виконання завдання, за умови цілковитого забезпечення їх збереженості. При цьому документи не дозволяється залишати на столі, закінчивши роботу, їх треба покласти до шафи, що замикається, або сейфа.

На підприємстві має бути встановлена заборона на винесення конфіденційних документів (матеріальних носіїв) зі службових приміщень для роботи з ними вдома, в готелі тощо, хоча, звичайно, в окремих випадках керівник може дозволити виконавцям документів винести конфіденційні документи для їх узгодження, підпису тощо.

Документи, що містять конфіденційну інформацію, не дозволяється виносити за межі підприємства. Лише за умови потреби в погодженні чи підписанні документів організаціями, які розташовані в тому самому населеному пункті, керівник підприємства може видати працівникам письмовий дозвіл на винесення цих документів.

Працівникам, направленим у відрядження в інші населені пункти, забороняється мати при собі документи, що містять конфіденційну інформацію. Такі документи заздалегідь пересилають за призначенням.

Наявність документів, що містять конфіденційну інформацію підприємства, щорічно переглядає комісія, спеціально призначена наказом керівника підприємства. До складу комісії обов'язково входять особи, яким доручено облік і зберігання конфіденційних документів.

Результати перевірок оформляються протоколом. Якщо під час перевірки було виявлено втрату документів із грифом «КТ» чи розголошення відомостей що містять конфіденційну інформацію, про це терміново доповідають керівництву підприємства [75].

Для розслідування факту втрати конфіденційних документів або розголошення інформації, що міститься в них, наказом керівника підприємства призначається комісія, висновок якої затверджує керівник підприємства.

За порушення, що призвели до розголошення конфіденційної інформації, втрати чи незаконного знищення документів із грифом обмеженого доступу, винні особи несуть відповідальність згідно із законодавством.

Документи, що містять конфіденційну інформацію, потребують особливого режиму зберігання. Тому на підприємстві конфіденційні документи повинні зберігатися у сейфах та сховищах, що надійно замикаються й опечатуються.

3.3. Основні шляхи підвищення ефективності конфіденційного документообігу у Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком»

Основою сучасної організації раціональної та оперативної роботи зі створення й обробки великого потоку документів на підприємствах стали персональні комп'ютери (ПК). Комп'ютерні технології радикально змінили характер праці в діловодстві та управлінні. Перелічимо основні можливості комп'ютерних технологій у діловодстві:

– допомога у створенні документа (конструювання бланків для підприємства; підготовка документа і розміщення його в пам'яті; використання шаблонів у створенні документів; пошук, зберігання і редагування тексту документів);

– передача документа на відстань будь-якому адресату, у якого є факсимільний зв'язок або ПК і модем (документ передається в електронному вигляді з комп'ютера на комп'ютер, в комп'ютерній локальній мережі, а також за допомогою електронної пошти та мережі Інтернет);

– реєстрація документа (заповнюється реєстраційна картка на екрані ПК, а реєстраційний номер наносять на сам документ в штамп для відмітки про одержання документа);

– контроль за виконанням документа (в електронній картці робиться відмітка про контроль, і це автоматично дозволяє інформувати керівництво підприємства про рівень виконавчої дисципліни працюючих співробітників, а також складати різного роду довідки-звіти з документообігу);

– переклад тексту документа з однієї мови на іншу (здійснюється в автоматичному режимі за наявності відповідного пакету програм і додатковому редагуванні тексту);

– захист документів (від випадкового доступу до інформації в ПК; відновлення тексту; антивірусний захист) [43].

Впровадження електронного документообігу на підприємстві дозволяє підвищити ефективність праці його співробітників за рахунок скорочення часу

на пошук, розробку, тиражування і пересилку документів. У той же час слід врахувати, що використання ПЕОМ у документообігу може наштовхуватися на численні перешкоди – фінансові, програмно-технічні, психологічні.

До принципів впровадження електронного документообігу на підприємстві слід віднести:

– поступове збільшення питомої ваги ПЕОМ при створенні документів;

– своєчасну модернізацію технічного та програмного забезпечення;

– першочергове використання ПЕОМ для скорочення рутинних операцій при створенні документів;

– переважне використання ПЕОМ на етапах документообігу з найбільшими часовими витратами (як правило, при листуванні);

– чітке розуміння необхідності впровадження подібних систем керівництвом підприємства [38].

Автоматизована робота з документами здійснюється шляхом створення та впровадження спеціальних програм з використанням ПЕОМ та автоматизованих робочих місць (АРМ). При цьому повинна бути забезпечена інформаційно-технічна сумісність засобів обчислювальної техніки між собою і з централізованими базами даних.

Керівництво підприємства має нести відповідальність за ефективність використання автоматизованої технології роботи з документами, визначати право доступу співробітників до інформації, що зберігається на машинних носіях.

Упорядковуючи документи, керівники підприємств часто приймають організаційні рішення щодо впровадження ефективних схем розміщення файлів на сервері, щоб документи можна було знайти й ефективно використовувати. Але такі заходи спрацьовують лише до певного моменту.

Якщо підприємство ставить перед собою все складніші завдання та одночасно збільшується документообіг, такі засоби збереження інформації, забезпечення взаємодії і контролю виконання доручень не є достатніми. Негативним наслідком є втрата документів та контролю над функціонуванням документів, що є особливо недопустимим під час роботи з конфіденційною інформацією.

Впроваджуючи електронний документообіг, потрібно врахувати і те, що існують різні електронні системи, які мають певні переваги та недоліки, специфіку використання.

За даними Forrester Research, 38 % компаній зі списку Fortune 500 вважають, що придбання сучасної системи електронного документообігу (СЕД) є вкрай важливим для успішного ведення бізнесу. За даними Siemens Business Services, у разі використання СЕД:

– продуктивність праці персоналу збільшується на 20–25 %.

– вартість архівного зберігання електронних документів на 80% нижча порівняно із вартістю зберігання паперових архівів [18].

Система електронного документообігу (СЕД) – це типове рішення, призначене для автоматизації документообігу і діловодства як в державних, так і в недержавних підприємствах будь-яких за розмірами, формами власності та родом діяльності [56]. Система дає змогу автоматизувати традиційне діловодство, організувати електронний архів документів, упорядкувати процеси роботи з вхідною/вихідною кореспонденцією, підтримувати внутрішню документацію на підприємстві, працювати зі зверненнями громадян і виконувати інші завдання.

Прийнято також вважати, що від впровадження СЕД отримуються тактичні та стратегічні переваги. Тактичні переваги визначаються скороченням витрат при впровадженні СЕД, що пов'язане із: звільненням фізичного місця для збереження документів; зменшенням витрат на копіювання і доставку документів у паперовому вигляді; зниженням витрат на персонал і устаткування тощо.

До стратегічних належать переваги, що пов'язані з підвищенням ефективності роботи підприємства чи організації. До таких переваг можна зарахувати: появу можливості колективної роботи над документами (що неможливо у разі паперового діловодства); значне прискорення пошуку та вибірки документів (за різними атрибутами); підвищення безпеки інформації за рахунок того, що робота в СЕД з незареєстрованної робочої станції неможлива, а кожному користувачеві СЕД надаються свої повноваження доступу до інформації; підвищення рівня збереження документів і зручності їхнього збереження, тому що вони

зберігаються в електронному вигляді на сервері; покращення контролю за виконанням рішень документів [18].

Однак, впроваджуючи на підприємстві систему електронного документообігу, не можна забувати про її безпеку. Нині все більшого поширення набувають системи захищеного електронного документообігу. Це пов'язано із збільшенням кількості конфіденційних документів в організаціях різної форми власності і активним переходом систем документообігу до електронного вигляду.

Підхід до захисту електронного документообігу повинен бути комплексним. Необхідно тверезо оцінювати можливі загрози і ризики СЕД, а також величину можливих втрат від загроз.

Основні загрози для систем електронного документообігу можуть бути класифіковані таким чином:

– загроза цілісності – пошкодження, знищення або спотворення інформації, що може бути як ненавмисним у випадках помилок і збоїв, так і зловмисним;

– загроза конфіденційності – будь-яке порушення конфіденційності, в тому числі крадіжка, перехоплення інформації, зміна маршрутів слідування і т.д.;

– загроза працездатності системи – загроза, реалізація якої призводить до порушення або припинення роботи системи, включаючи навмисні атаки, помилки користувачів, а також збої в обладнанні і програмному забезпеченні;

– неможливість доказу авторства – загроза, що виражається у тому, що якщо в документообігу не використовується електронний цифровий підпис, то неможливо доказати, що саме даний користувач створив даний документ (при цьому неможливо зробити документообіг юридично значимим);

– загроза доступності – загроза, що порушує можливість за допустимий час отримати інформацію користувачам, які мають право доступу до неї [55].

Захист саме від цих загроз в тій чи іншій мірі повинна реалізовувати будь-яка система електронного документообігу. Відповідно, в комплекс захисту електронної документації повинні входити такі заходи: обмеження прав фізичного доступу до об’єктів системи документообігу; розмежування прав доступу до файлів і папок; підтвердження авторства електронного документу;

контроль цілісності електронного документу; конфіденційність електронного документу; забезпечення юридичної сили електронного документу; забезпечення надійності функціонування технічних засобів; забезпечення резервування каналів зв'язку; резервне дублювання інформації; захист від вірусів; захист від «злому» мереж.

Для забезпечення захисту конфіденційної інформації в інформаційних системах повинні обов'язково виконуватися такі процедури: аутентифікація – процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора; ідентифікація – процедура розпізнавання користувача в системі, як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою [50]. Отже, процедура ідентифікації і аутентифікації користувачів є невід'ємним елементом системи захищеного електронного документообігу.

Можна констатувати, що основними завданнями СЕД на основі процедури ідентифікації і аутентифікації є:

– жорстка ідентифікація і аутентифікація користувачів для організації доступу до інформаційно важливих ресурсів, що захищаються;

– обмеження доступу до конфіденційної інформації і персональних даних;

– блокування несанкціонованого доступу;

– забезпечення доступності публічної інформації [66].

Необхідно звернути увагу на методи ідентифікації і аутентифікації користувачів комп'ютерних систем. Найпоширеніший з них – парольний. Головна перевага парольної ідентифікації – це простота реалізації й використання. Проблема, яка сильно знижує надійність цього способу – це людський чинник. Більшість людей використовують ненадійні ключові слова, які легко підбираються. Тому деякі фахівці в області інформаційної безпеки радять використати довгі паролі, що складаються з випадкового сполучення букв, цифр і різних символів.

Апаратний (електронний) принцип ідентифікації ґрунтується на визначенні особи користувача по якомусь предмету, ключу, що перебуває в його ексклюзивному користуванні. На даний момент найбільше поширення

одержали два типи пристроїв: різноманітні карти (проксіміті-карти, смарт-карти, магнітні карти тощо) та так звані токени (token), які підключаються безпосередньо до одного з портів комп'ютера. Але серйозною небезпекою у випадку використання апаратної ідентифікації є можливість крадіжки зловмисниками токенів або карт у зареєстрованих користувачів. Також вони можуть бути втрачені, передані іншій особі, дубльовані.

Максимально надійним способом ідентифікації і аутентифікації вважають біометричний, при якому користувач ідентифікується за своїми біометричними даними (відбиток пальця, сканування сітківки ока, голос тощо). Проте в цьому випадку вартість рішення вища, а сучасні біометричні технології ще не настільки досконалі, щоб уникнути помилкових спрацьовувань або відмов [55].

Ще один важливий параметр ідентифікації і аутентифікації – кількість факторів, що враховуються. Тобто, цей процес може бути однофакторним або багатофакторним, коли для визначення особи користувача застосовується відразу кілька параметрів. Також можливе комбінування різних методів: парольного, апаратного, біометричного. Утім, сьогодні найчастіше використовується лише одна пара: парольний захист і токен. Впровадження комбінованих систем збільшує кількість ідентифікаційних ознак і тим самим підвищує рівень безпеки і захисту систем електронного документообігу.

З метою підвищення ефективності конфіденційного документобігу Товариству з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» доцільно впровадити систему захищеного електронного документообігу, наприклад FossDoc, розробником якої є ТОВ «ФОСС-Он-Лайн» (м. Харків).

СЕД FossDoc – це рішення на платформі FossLook, призначене для створення електронного архіву документів, організації корпоративного документообігу і автоматизації бізнес-процесів на підприємствах, в установах і організаціях будь-якого роду діяльності. Програма дозволяє вирішити велику кількість завдань, реалізація яких покладена на відповідні модулі [72]. Однією з переваг платформи FossLook є її здатність забезпечувати захищене сховище документів, у тому числі конфіденційних, необхідних для роботи.

Крім того, підприємство може впровадити систему електронного захисту «FossProtect». ТОВ «ФОСС-Он-Лайн» пропонує послуги криптозахисту каналів зв'язку за допомогою системи FossProtect. Дана система захищає передачу інформації як у локальній мережі, так і у мережі Інтернет.

У 2019 р. ТОВ «ФОСС-Он-Лайн» отримало експертний висновок Державної служби спеціального зв’язку та захисту інформації України в якому зазначено, що комплекс засобів захисту програмної системи електронного захисту «FossProtect» версії 2.х відповідає вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених у технічному завданні «Програмна система електронного захисту «FossProtect». Часткове технічне завдання. Вимоги щодо забезпечення захисту інформації від несанкціонованого доступу» [73].

Отже, система електронного захисту «FossProtect» призначена для створення криптографічного захисту даних підприємства, що передаються через внутрішню мережу підприємства або мережу Інтернет.

Для захисту від витоків інформації широке розповсюдження отримали спеціалізовані продукти, до яких, зокрема, слід віднести Information Protection and Control (IPC) – технологію захисту конфіденційної інформації від внутрішніх загроз. Рішення класу IPC призначені для захисту інформації від внутрішніх загроз, запобігання різних видів витоків інформації, корпоративного шпигунства і бізнес-розвідки. IPC-система поєднує у собі дві основні технології: шифрування носіїв інформації у всіх точках мережі; контроль технічних каналів витоку інформації за допомогою технологій Data Loss Prevention (DLP) [12].

Основним завданням IPC-систем є запобігання передачі конфіденційної інформації за межі корпоративної інформаційної системи. Додаткові завдання систем класу IPC:

– запобігання передачі зовні не тільки конфіденційної, але й іншої небажаної інформації (образливих виразів, спаму, зайвих обсягів даних тощо);

– запобігання передачі небажаної інформації не тільки зсередини назовні, а й ззовні всередину інформаційної системи;

– запобігання використання працівниками Internet-ресурсів і ресурсів мережі в особистих цілях;

– захист від спаму та захист від вірусів;

– оптимізація завантаження каналів, зменшення нецільового трафіку;

– архівація інформації на випадок випадкового видалення або псування оригіналу тощо [44].

Data Leak Prevention (DLP) – це технології запобігання витоку конфіденційної інформації з інформаційної системи назовні, а також технічні пристрої (програмні або програмно-апаратні) для такого запобігання витокам [45].

DLP-системи будуються на аналізі потоків даних, які перетинають периметр інформаційної системи, що захищається. При детектуванні в цьому потоці конфіденційної інформації спрацьовує активна компонента системи, і передача повідомлень (пакета, потоку, сесії) блокується.

Технологія DLP в IPC підтримує контроль таких технічних каналів витоку конфіденційної інформації: корпоративна електронна пошта; веб-пошта; соціальні мережі й блоги; файлообмінні мережі; форуми та інші інтернет-ресурси, у тому виконані на AJAX-технології; засоби миттєвого обміну повідомленнями (ICQ, Skype, AOL AIM, Google Talk, Windows Live Messenger); p2p-клієнти; периферійні пристрої (USB, LPT, COM, WiFi, Bluetooth тощо); локальні та мережеві принтери [12].

Для ТОВ «Керуюча Компанія «Дом.Ком» доцільним є використання сучасних технологій захисту конфіденційної інформації від можливих витоків. Для запобігання навмисних або випадкових витоків конфіденційної інформації розробник програмних рішень з інформаційної безпеки – Компанія ТОВ «Софтліст» (м. Київ) пропонує підприємствам DLP-системи. За допомогою DLP-захисту відбувається постійний контроль усіх каналів передачі конфіденційної інформації в електронному вигляді, у тому числі передачі даних через Інтернет [39]. Система забезпечує можливість блокування витоків даних (припинення відправки електронних повідомлень, передачі файлів) шляхом контролю життєвого циклу та переміщення конфіденційних даних.

ВИСНОВКИ

У процесі виконання дипломної роботи виконано всі поставлені завдання та досягнута мета роботи. За результатами проведеного дослідження доцільно зробити такі висновки:

1. Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням. Конфіденційна інформація умовно поділяється на конфіденційну інформацію про фізичну особу та конфіденційну інформацію про юридичну особу. Відповідно до статті 21 Закону України «Про інформацію» конфіденційна інформація разом із службовою та таємною інформацією належить до інформації з обмеженим доступом.

2. Конфіденційна інформація зазвичай міститься у вигляді будь-яких документів – традиційних паперових або електронних. Документи, що містять конфіденційну інформацію, прийнято називати конфіденційними, а процес виготовлення таких документів і організацію роботи з ними – конфіденційним діловодством. Під конфіденційним документом розуміється необхідним чином оформлений носій документованої інформації, що містить відомості обмеженого доступу або використання, які становлять інтелектуальну власність юридичної або фізичної особи.

3. Життєвий цикл документів, які містять конфіденційну інформацію, розпочинається в діловодстві з моменту надходження документа в організацію або з моменту його створення і завершується знищенням документа (проекту документа) чи передачею документа на архівне зберігання. Рух документів, які містять конфіденційну інформацію протягом їх життєвого циклу в організації, називається конфіденційним документообігом. Особливістю конфіденційного документообігу є необхідність захисту документів від несанкціонованого доступу до них з метою запобігання витоку конфіденційної інформації.

4. Товариство з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» працює в сфері житлово-комунальних послуг з 2011 р.

Підприємство надає послуги з утримання будинків, споруд та прибудинкових територій, обслуговує Покровський район м. Кривий Ріг. На сайті підприємства є дані про його діяльність, новини, досягнення, звіти про виконі види робіт, інформація для споживачів. У контактах можна знайти адресу підприємства, телефони приймальні, аварійно-диспетчерської служби.

5. Досліджено порядок роботи з вхідними, вихідними та внутрішніми конфіденційними документами у Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком». Конфіденційним документам надається гриф обмеженого доступу, що засвідчує особливий характер інформації, до якої має доступ обмежене коло осіб. Документування конфіденційної інформації є важливою складовою конфіденційного діловодства підприємства.

6. Одним із видів конфіденційної документації є кадрова документація, тому кадрова служба як підрозділ, що працює з конфіденційною інформацією, повинна дотримуватися правил роботи, які установлені для даного виду інформації. У Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» приділяють значну увагу оформленню та збереженню конфіденційної кадрової документації.

7. Підприємством має бути створена система захисту конфіденційної інформації, яка б унеможливила несанкціонований (незаконний) доступ до неї. Заходи щодо захисту конфіденційної інформації на підприємстві можна умовно класифікувати на зовнішні та внутрішні, які, в свою чергу, поділяються на правові, організаційні, технічні та психологічні.

8. Документи, що містять конфіденційну інформацію, потребують особливого режиму зберігання. Тому на підприємстві конфіденційні документи повинні зберігатися у сейфах та сховищах, що надійно замикаються й опечатуються.

9. З метою підвищення ефективності конфіденційного документобігу Товариству з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком» доцільно впровадити систему захищеного електронного документообігу. Також доцільним є використання сучасних технологій захисту конфіденційної інформації від можливих витоків.

РЕКОМЕНДАЦІЇ

За результатами дослідження визначено рекомендації щодо удосконалення організації конфіденційного документообігу у Товаристві з обмеженою відповідальністю «Керуюча Компанія «Дом.Ком»:

1. Доцільно впровадити систему захищеного електронного документообігу, наприклад FossDoc, розробником якої є ТОВ «ФОСС-Он-Лайн» (м. Харків). FossDoc – це рішення на платформі FossLook, призначене для створення електронного архіву документів, організації корпоративного документообігу і автоматизації бізнес-процесів на підприємствах, в установах і організаціях будь-якого роду діяльності. Однією з переваг платформи FossLook є її здатність забезпечувати захищене сховище документів, у тому числі конфіденційних.

Доцільно також впровадити систему електронного захисту «FossProtect», яка може бути інтегрована із СЕД FossDoc. Дана система захищає передачу інформації як у локальній мережі, так і у мережі Інтернет.

В експертному висновку Державної служби спеціального зв'язку та захисту інформації України від 15 лютого 2019 р. № 934 йдеться про те, що комплекс засобів захисту програмної системи електронного захисту «FossProtect» версії 2.х відповідає вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених у технічному завданні «Програмна система електронного захисту «FossProtect». Часткове технічне завдання. Вимоги щодо забезпечення захисту інформації від несанкціонованого доступу».

2. Для запобігання витоків конфіденційної інформації використовувати сучасні програмні продукти, що базуються на технології детектування конфіденційної інформації. Розробник програмних рішень з інформаційної безпеки Компанія ТОВ «Софтліст» (м. Київ) пропонує DLP-систему, яка забезпечує: постійний контроль каналів передачі конфіденційної інформації в електронному вигляді, у тому числі передачі даних через Інтернет; можливість блокування витоків даних (припинення відправки електронних повідомлень, передачі файлів) через контроль за переміщенням конфіденційних даних.

СПИСОК ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. ДСТУ 4163-2003: Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлювання документів. – Київ: Держспоживстандарт України, 2003. – 22 с.
2. ДСТУ 2732:2004: Діловодство й архівна справа. Терміни та визначення понять. – Київ: Держспоживстандарт України, 2005. – 31с.
3. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення. – Київ: Держкомстандарт України, 1996. – 26 с.
4. Правила організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях: Наказ Міністерства юстиції України від 18.06.2015 р. № 10005 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0736-15#Text (дата звернення: 19.02.2021) – Назва з екрана.
5. Про державну таємницю: Закон України від 21.01.1994 р. № 3855-XII [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/ laws/show/3855-12#Text (дата звернення: 11.02.2021) – Назва з екрана.
6. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/ laws/show/2939-17 (дата звернення: 11.02.2021) – Назва з екрана.
7. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV [Електронний ресурс]. – Режим доступу : https://zakon3.rada.gov.ua/laws/show/851-15 (дата звернення: 10.02.2021) – Назва з екрана.
8. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5.07.1994 р. № 80/94-ВР [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 15.02.2021) – Назва з екрана.

9. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297–VI [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 19.02.2021) – Назва з екрана.
10. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 15.02.2021) – Назва з екрана.
11. Адабаш О. В. Інформація з обмеженим доступом: проблеми законодавчого визначення [Електронний ресурс] / О.В. Адабаш // Наше право. – 2013. – № 13. – С. 61–66. – Режим доступу: http://nbuv.gov.ua/UJRN/Nashp_2013_13_12 (дата звернення: 15.03.2021) – Назва з екрана.
12. Антонюк А.О. Технології захисту конфіденційної інформації від внутрішніх загроз / А.О. Антонюк, В.С. Портяной, В.П. Шилін // Проблеми програмування. – 2011. – № 1. – С. 78–88.
13. Буртник Х. Конфіденційна інформація, інформація про особу та персональні дані: співвідношення і регулювання [Електронний ресурс] / Х. Буртник. – Режим доступу: https://cedem.org.ua/analytics/konfidentsijna-informatsiya-informatsiya-pro-osobu-ta-personalni-dani-spivvidnoshennya-i-regulyuvannya/ (дата звернення: 15.04.2021) – Назва з екрана.
14. Види конфіденційних документів [Електронний ресурс]. – Режим доступу: https://studopedia.org/14-34599.html (дата звернення: 11.04.2021) – Назва з екрана.
15. Вимоги до роботи з конфіденційною інформацією установи [Електронний ресурс]. – Режим доступу: https://balance.ua/news/post/trebovaniya-k-rabote-s-konfidencialnoy-informaciey-uchrezhdeniya (дата звернення: 25.04.2021) – Назва з екрана.
16. Вирішуйте житлово-комунальні проблеми онлайн: в Україні запустилася платформа ДЖЕК [Електронний ресурс]. – Режим доступу: https://www.ipay.ua/blog/news/virishujte-zhitlovo-komunalni-problemi-onlajn-v-ukraini-zapustilasya-platforma-dzhek (дата звернення: 30.04.2021) – Назва з екрана.

17. Габович А.Г. Організація конфіденційного діловодства: підручник / А. Г. Габович, С. М. Головань, С. І. Жлобін, В. О. Хорошко. – Київ : ДУІУТ, 2015. – 376 с.
18. Гарасим О.Р. Аналіз засобів управління корпоративною конфіденційною інформацією [Електронний ресурс] / О.Р. Гарасим, Л.Б. Чирун // Вісник Національного університету «Львівська політехніка». Інформаційні системи та мережі. – 2010. – № 689. – С. 117–128. – Режим доступу : http://ena.lp.edu.ua:8080/bitstream/ntb/20163/1/13-117-128.pdf (дата звернення: 15.03.2021) – Назва з екрана.
19. Гладківська О. В. Забезпечення доступу до інформації та її захисту: термінологічний аспект [Електронний ресурс] / О. В. Гладківська // Інформація і право. – 2013. – № 2. – С. 17–25. – Режим доступу: http://nbuv.gov.ua/UJRN/Infpr_2013_2_4 (дата звернення: 18.03.2021) – Назва з екрана.
20. Гладківська О.В. Інформація з обмеженим доступом: проблема неузгодженості термінології [Електронний ресурс] / О. В. Гладківська // Інформація і право. – 2014. – № 1. – С. 49–58. – Режим доступу: http://nbuv.gov.ua/UJRN/Infpr_2014_1_8 (дата звернення: 25.03.2021) – Назва з екрана.
21. Головань С.М. Документаційне забезпечення робіт із захисту інформації з обмеженим доступом: підручник / С. М. Головань, В. Б. Дудикевич, В. С. Зачепило, В. О. Хорошко, Л. М. Щербак. – Львів: Вид.-во «Львівська політехніка», 2015. – 288 с.
22. Головань С. М. Загальне діловодство та ведення документів, що містять інформацію з грифом «Для службового користування»: навчально-методичний посібник / С.М. Головань. – Київ: НАУ, 2013. – 92 с.
23. Головань С.М. Конфіденційний документообіг: навч. посіб. / С. М. Головань, В. В. Поповський, В. О. Хорошко. – Київ : ДУІКТ, 2017. – 264 с.
24. Гордієнко С. Г. Конфіденційна інформація та «таємниці»: їх співвідношення [Електронний ресурс] / С. Г. Гордієнко // Часопис Київського університету

права. – 2013. – № 4. – С. 233–238. – Режим доступу: http://nbuv.gov.ua/UJRN/Chkup_2013_4_57 (дата звернення: 29.03.2021) – Назва з екрана.

25. Гордієнко С.Г. Проблеми систематизації нормативно-правового регулювання захисту конфіденційної інформації в України [Електронний ресурс] / С. Г. Гордієнко // Правничий вісник Університету "КРОК". – 2010. – Вип. 6(1). – С. 76–85. – Режим доступу: http://nbuv.gov.ua/UJRN/Pvuk_2010_6(1)__14 (дата звернення: 11.04.2021) – Назва з екрана.
26. Гуз А.М. Організація захисту інформації з обмеженим доступом : підручник / А.М. Гуз, О.Д. Довгань, А.І. Марущак та ін. – Київ : Наук.-вид. відділ НА СБ України, 2011. – 378 с.
27. Гуцалюк М.В. Організація захисту інформації : навчальний посібник / М.В. Гуцалюк. – Київ : Альтерпрес, 2011. – 308 с.
28. Данюк В.М. Кадрове діловодство: навч. посібник / В.М. Данюк, Л.П. Кулаковська. – Київ: Каравела, 2018. – 240 с.
29. Діденко А.Н. Сучасне діловодство: навч. посібник / А.Н. Діденко. – Київ: Либідь, 2016. – 384 с.
30. Діловодство і документація: навчально-методичний посібник / Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України»; [уклад. П. О. Добродумов]. – Суми : ДВНЗ “УАБС НБУ”, 2014. – 209 с.
31. ДомКом Україна. Про нас [Електронний ресурс]. – Режим доступу: http://www.domkom.ua/uk/ (дата звернення: 15.04.2021) – Назва з екрана.
32. ДомКом Україна. Програмні комплекси [Електронний ресурс]. – Режим доступу: http://www.domkom.ua/uk/programni-kompleksi/ (дата звернення: 15.04.2021) – Назва з екрана.
33. ДомКом Кривий Ріг. Про нас [Електронний ресурс]. – Режим доступу: http://krrog.domkom.ua/pro-kompaniiu/ (дата звернення: 18.04.2021) – Назва з екрана.

34. ДомКом Кривий Ріг. Новини [Електронний ресурс]. – Режим доступу: http://krrog.domkom.ua/category/ukraine-ua/novini/ (дата звернення: 26.04.2021) – Назва з екрана.
35. Ємельянов С. Л. Проблемні аспекти класифікації інформації з обмеженим доступом в Україні [Електронний ресурс] / С. Л. Ємельянов // Наукові праці Національного університету "Одеська юридична академія". – 2012. – Т. 12. – С. 130–140. – Режим доступу: http://nbuv.gov.ua/UJRN/Nponyua_2012_12_16 (дата звернення: 15.04.2021) – Назва з екрана.
36. Забара І. М. Інформація з обмеженим доступом: міжнародно-правовий режим [Електронний ресурс] / І. М. Забара // Правова інформатика. – 2013. – № 4. – С. 41–47. – Режим доступу: http://nbuv.gov.ua/UJRN/Pinform_2013_4_8 (дата звернення: 19.03.2021) – Назва з екрана.
37. Загрози інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%D0%B8_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8 (дата звернення: 17.04.2021) – Назва з екрана.
38. Захарченко Н. В. Вплив електронного документообігу на ефективність діяльності підприємства [Електронний ресурс] / Н. В. Захарченко, Н. Д. Маслій, М. С. Мамуненко // Молодий вчений. – 2017. – № 5. – С. 582–587. – Режим доступу: http://nbuv.gov.ua/UJRN/molv_2017_5_131 (дата звернення: 11.04.2021) – Назва з екрана.
39. Захист від витоків конфіденційної інформації (DLP) [Електронний ресурс]. – Режим доступу : https://softlist.ua/rishennia/rishennia-z-informatsiinoi-bezpeky/dlp (дата звернення: 15.04.2021) – Назва з екрана.
40. Зняття грифу конфіденційності з документів [Електронний ресурс]. – Режим доступу : https://studref.com/470035/dokumentovedenie/snyatie_grifa_konfidentsialnosti_dokumentov (дата звернення: 29.04.2021) – Назва з екрана.

41. Кислюк К.В. Спеціальне документознавство: навчальний посібник / К.В. Кислюк. – Київ: Кондор, 2011. – 192 с.
42. Козоріз В.П. Загальне і кадрове діловодство: навч. посібник / В.П. Козоріз, Н.І. Лапицька. – Київ: Міжрегіональна академія управління персоналом, 2012. – 164 с.
43. Комова М.В. Діловодство: навч. посібник / М.В. Комова. – Львів: Тріада плюс, 2016. – 217 с.
44. Конфиденциальный документооборот: угрозы и риски [Електронний ресурс]. – Режим доступу: http://www.konspekt.biz/index.php?text=56236 (дата звернення: 15.04.2021) – Назва з екрана.
45. Конфіденційна інформація [Електронний ресурс]. – Режим доступу : https://wiki.legalaid.gov.ua/index.php/%D0%9A%D0%BE%D0%BD%D1%84%D1%96%D0%B4%D0%B5%D0%BD%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F (дата звернення: 16.03.2021) – Назва з екрана.
46. Конфіденційні документи [Електронний ресурс]. – Режим доступу: https://studopedia.su/5_1614_konfidentsiyni-dokumenti.html (дата звернення: 30.03.2021).
47. Коренюк О. Інформація з обмеженим доступом: об’єкт господарських відносин [Електронний ресурс] / О. Коренюк // Зовнішня торгівля: економіка, фінанси, право. – 2018. – № 2. – С. 91–100. – Режим доступу: http://nbuv.gov.ua/UJRN/uazt_2018_2_12 (дата звернення: 18.03.2021) – Назва з екрана.
48. Коц Д. В. Теоретико-правові засади інформації з обмеженим доступом / Д. В. Коц // Вісник НТУУ «КПІ». Політологія. Соціологія. Право : збірник наукових праць. – 2019. – № 2 (42). – С. 107–111.
49. Круглюк К. Як правильно встановити на підприємстві режим доступу до конфіденційної інформації та комерційної таємниці [Електронний ресурс] / К. Круглюк. – Режим доступу: http://jurist.ua/?article/188 (дата звернення: 25.03.2021) – Назва з екрана.

50. Кукарін О.Б. Електронний документообіг та захист інформації : навч. посіб. [Електронний ресурс] / О.Б. Кукарін. – Київ: НАДУ, 2015. – 84 с. – Режим доступу: http://www.academy.gov.ua/%5CNMKD%5Clibrary_nadu%5CNavch_Posybniky%5C157617ed-2d29-45aa-96bd-97e52b5051db.pdf (дата звернення: 25.03.2021) – Назва з екрана.
51. Кулініч О. О. Теоретико-методологічні підходи до визначення структури інформації з обмеженим доступом [Електронний ресурс] / О. О. Кулініч // Актуальні проблеми держави і права. – 2018. – Вип. 42. – С. 24–32. – Режим доступу: http://nbuv.gov.ua/UJRN/apdp_2008_42_5 (дата звернення: 25.03.2021) – Назва з екрана.
52. Кулініч О. О. Правова охорона конфіденційної інформації в сфері господарської діяльності [Електронний ресурс] / О. О. Кулініч // Актуальні проблеми політики : зб. наук. – Одеса: ОНЮА, 2019. – Вип. 36. – С. 138–146. – Режим доступу: http://dspace.onua.edu.ua/bitstream/handle/11300/128/app-36_Kulinich_O_O_%28138-146%29.pdf?sequence=1&isAllowed=y (дата звернення: 18.04.2021) – Назва з екрана.
53. Ліпкан В. Доступ до інформації з обмеженим доступом: проблеми вироблення уніфікованих дефініцій [Електронний ресурс] / В. Ліпкан, Л. Капінус // Публічне право. – 2013. – № 4. – С. 45–53. – Режим доступу: http://nbuv.gov.ua/UJRN/pp_2013_4_8 (дата звернення: 15.04.2021) – Назва з екрана.
54. Ліпкан В.А. Адміністративно-правовий режим інформації з обмеженим доступом в Україні : монографія / В.А. Ліпкан, В.Ю.Баскаков; за заг. ред. В.А. Ліпкана. – Київ: ФОП О.С. Ліпкан, 2013. – 344 с.
55. Мазниченко Н.І. Захист інформації в системах електронного документообігу на основі систем ідентифікації [Електронний ресурс] / Н.І. Мазниченко. – Режим доступу: https://dspace.nlu.edu.ua/bitstream/123456789/6710/1/Maznichenko.pdf (дата звернення: 28.04.2021) – Назва з екрана.
56. Матвієнко О. Основи організації електронного документообігу: навчальний посібник / О. Матвієнко, М. Цивін. – Київ: Центр учбової літератури, 2008. –112 с.

57. Мужанова Т.М. Організація конфіденційного діловодства: навчальний посібник [Електронний ресурс] / Т.М. Мужанова. – Київ: Державний університет телекомунікацій, 2019. – 143 с. – Режим доступу: http://www.dut.edu.ua/uploads/l_1895_14951894.pdf (дата звернення: 28.03.2021) – Назва з екрана.
58. Нерсесян А. С. Корпоративна інформація з обмеженим доступом як предмет службових злочинів в сфері господарювання [Електронний ресурс] / А. С. Нерсесян // Науковий вісник Академії муніципального управління. Серія : Право. – 2011. – Вип. 1. – С. 217–225. – Режим доступу: http://nbuv.gov.ua/UJRN/Nvamu_pr_2011_1_28 (дата звернення: 27.03.2021) – Назва з екрана.
59. Нікітін О. Конфіденційна інформація та її захист. Важливі поради для керівників підприємств [Електронний ресурс] / О. Нікітін. – Режим доступу : https://id-legalgroup.com/ua/blog/konfidencialnaya-informaciya-i-ee-zashita--vajnie-soveti-dlya-rykovoditelei-predpriyatii----oleg-nikitin--advokat-ID-Legal-Group- (дата звернення: 11.03.2021) – Назва з екрана.
60. Організація конфіденційного діловодства [Електронний ресурс]. – Режим доступу: https://works.doklad.ru/view/4_GT7TfjC_8/all.html (дата звернення: 24.03.2021) – Назва з екрана.
61. Організація конфіденційного документообігу [Електронний ресурс]. – Режим доступу: https://centr.expert/organizaciya-konfidencialnogo-dokumentooborota (дата звернення: 25.04.2021) – Назва з екрана.
62. Організаційно-правові засади конфіденційного документообігу на підприємстві [Електронний ресурс]. – Режим доступу: https://knowledge.allbest.ru/audit/3c0a65625a2ad69b5d43b89521316d27_0.html (дата звернення: 10.04.2021) – Назва з екрана.
63. Особливості організації конфіденційного діловодства [Електронний ресурс]. – Режим доступу: http://dilova.at.ua/publ/dilovodstvo/specialni_vidi_dilovodstva/osoblivosti_organizaciji_konfidencijnogo_dilovodstva/10-1-0-192 (дата звернення: 17.04.2021) – Назва з екрана.

64. Палеха Ю. І. Загальне документознавство: навч. посіб. / Ю. І. Палеха, Н. О. Леміш. – Київ: Ліра-К, 2008. – 393 с.
65. Палеха Ю. Загальне діловодство: теорія та практика керування документацією із загальних питань: навчальний посібник / Ю. Палеха. – Київ : Видавництво Ліра-К, 2014. – 624 с.
66. Піддубна Л. В. Інформаційна безпека в системах електронного документообігу [Електронний ресурс] / Л. В. Піддубна, В. М. Павліченко // Науковий вісник Полтавського університету економіки і торгівлі. Серія : Економічні науки. – 2019. – № 4. – С. 59–66. – Режим доступу: http://nbuv.gov.ua/UJRN/Nvpusk_2019_4_10 (дата звернення: 16.04.2021) – Назва з екрана.
67. Попчук О.В. Документне забезпечення управлінської діяльності організацій : навч.-метод. посіб. / О. В. Попчук. – Рівне: Рівнен. держ. гуманітар. ун-т, 2012. – 116 с.
68. Правила организации конфиденциального документооборота [Електронний ресурс]. – Режим доступу: http://naar.ru/articles/pravila-organizacii-konfidencialnogo-dokumentooborota/ (дата звернення: 19.04.2021) – Назва з екрана.
69. Режим зберігання конфіденційних документів і поводження з ними [Електронний ресурс]. – Режим доступу: http://um.co.ua/6/6-10/6-108385.html (дата звернення: 29.04.2021) – Назва з екрана.
70. Рожелюк В. М. Організація документообігу як основного інструмента забезпечення функціонування ефективної системи комунікації на переробному підприємстві [Електронний ресурс] / В. М. Рожелюк, П. Н. Денчук // Сталий розвиток економіки. – 2014. – № 2. – С. 114–121. – Режим доступу: http://nbuv.gov.ua/UJRN/sre_2014_2_18 (дата звернення: 23.04.2021) – Назва з екрана.
71. Савицький В. Т. Доступ і обмеження доступу до інформації: забезпечена свобода і застережена небезпека [Електронний ресурс] / В. Т. Савицький // Університетські наукові записки. –2017. – № 4. – С. 116–135. – Режим

доступу: http://nbuv.gov.ua/UJRN/Unzap_2017_4_12 (дата звернення: 15.04.2021) – Назва з екрана.

72. Система електронного документообігу FossDoc [Електронний ресурс]. – Режим доступу: https://fossdoc.com/elektronniy-dokumentooborot (дата звернення: 25.04.2021) – Назва з екрана.
73. Система електронного захисту «FossProtect» [Електронний ресурс]. – Режим доступу: https://fossprotect.com/ (дата звернення: 25.04.2021) – Назва з екрана.
74. Скібіцька Л.І. Діловодство: навч. посіб. для студентів ВНЗ / Л. І. Скібіцька. – 2-ге вид. – Київ : Кондор, 2012. – 219 с.
75. Спеціальні види діловодства [Електронний ресурс]. – Режим доступу: https://pidru4niki.com/1031020856490/dokumentoznavstvo/spetsialni_vidi_dilovodstva (дата звернення: 18.04.2021) – Назва з екрана.
76. Федоренко О.О. Проблемні питання правового регулювання обігу інформації з обмеженим доступом (державна таємниця та службова інформація) [Електронний ресурс] / О. О. Федоренко, С. О. Керсіцький, А. І. Курбатов // Право та інноваційне суспільство. – 2013. – № 1. – Режим доступу: http://nbuv.gov.ua/UJRN/pric_2013_1_17 (дата звернення: 29.03.2021) – Назва з екрана.
77. Шарабурина О. О. Новели законодавства України про інформацію з обмеженим доступом [Електронний ресурс] / О. О. Шарабурина // Часопис Київського університету права. – 2013. – № 2. – С. 147–150. – Режим доступу: http://nbuv.gov.ua/UJRN/Chkup_2013_2_36 (дата звернення: 26.03.2021) – Назва з екрана.
78. Щодо конфіденційної інформації та комерційної таємниці [Електронний ресурс]. – Режим доступу: https://www.kadrovik.ua/novyny/shchodo-konfidenciynoyi-informaciyi-ta-komerciynoyi-tayemnycі (дата звернення: 15.04.2021) – Назва з екрана.