МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ЛЕСІ УКРАЇНКИ

Кафедра музеєзнавства, пам'яткознавства
та інформаційно-аналітичної діяльності

На правах рукопису

КРАСЬОХА ОЛЕКСАНДР ПЕТРОВИЧ

КОНФІДЕНЦІЙНА ІНФОРМАЦІЯ В ОРГАНІЗАЦІЙНИХ ДОКУМЕНТАХ: СТРАТЕГІЇ ТА МЕТОДИ ЗАХИСТУ

Робота на здобуття освітнього ступеня «Бакалавр»
за освітньо-професійною програмою
«Документаційне забезпечення управління та інформаційно-аналітична діяльність»
Спеціальності 029 «Інформаційна, бібліотечна та архівна справа»

Науковий керівник:
доктор історичних наук,
професор Гаврилюк С. В.

РЕКОМЕНДОВАНО ДО ЗАХИСТУ
Протокол № _____
засідання кафедри музеєзнавства,
пам'яткознавства та інформаційно-
аналітичної діяльності
від _____ 2024 р.
Завідувачка кафедри проф. Гаврилюк С. В._____

Луцьк–2024

АНОТАЦІЯ

Красьоха О. П. Конфіденційна інформація в організаційних документах: стратегії та методи захисту. Кваліфікаційна робота на правах рукопису на здобуття освітнього ступеня «Бакалавр». Волинський національний університет імені Лесі Українки, Луцьк, 2024.

У роботі розкривається поняття конфіденційної інформації, аналізуються суть і види конфіденційної інформації в організаційних документах. Увага звертається на особливості документообігу конфіденційної інформації в установах і організаціях, правила документообігу конфіденційної документації, прийняті в організаціях. Детально висвітлюються технології і методи захисту конфіденційної інформації від несанкціонованого доступу, наводяться приклади і окремі рекомендації щодо захисту конфіденційної інформації в організаційних документах. Проводиться теза, що створення умов для збереження конфіденційних документів і запобігання витоку інформації – це основа конфіденційного діловодства в будь-якій організації.

Зроблено висновок, що розуміння і впровадження комплексного підходу до захисту документів в умовах сучасного інформаційного суспільства, дотримання законодавчих вимог та використання передових технологій для забезпечення безпеки і конфіденційності інформації є основним підґрунтям функціонування установ і організацій різних форм власності для забезпечення розвитку держави в усіх сферах діяльності.

Ключові слова: конфіденційна інформація, документообіг, організаційні документи, комерційна таємниця, захист документної інформації, несанкціонований доступ до інформації.

ЗМІСТ

ВСТУП

Актуальність дослідження. Упродовж усіх історичних епох одним із завдань, яке вирішувалося на державному рівні, був захист конфіденційної інформації. 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 [50]. Розпорядники інформації, визначені частиною першою ст. 13 Закону України «Про доступ до публічної 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. Відповідно до ст. 21 Закону України «Про інформацію» конфіденційна інформація разом із службовою та таємною інформацією належить до інформації з обмеженим доступом [56].

У XXI ст. атаки на корпоративні та господарські системи для отримання несанкціонованого доступу до документів та конфіденційної інформації стають все досконалішими. З розвитком сучасних новітніх технологій збільшується кількість цінних документів, які зберігаються в електронному вигляді. Це стосується банківських даних, медичних записів, інформації, що містить державну таємницю тощо. Захист цих даних від несанкціонованого доступу стає критичним завданням як органів державної влади, так і установ та організацій різних форм власності. Тим більше, що у наш час все активніше впроваджуються цифрові технології та відбувається обробка значних обсягів документів для покращення ефективності роботи і прийняття певних рішень. Усе це актуалізує завдання захисту конфіденційнї інформації, яка наявна в організаційних документах і використовуються в управлінських процесах.

Актуальність такого дослідження підсилюється важливістю збереження конфіденційної інформації, яка є об'єктом уваги як держави, так і комерційних структур. З кожним роком внаслідок глобальних подій у світі набуває

популярності робота з віддаленим доступом, тобто онлайн, що призводить до збільшення кількості працівників, які мають доступ до корпоративних документів за межами організацій. Це підвищує ризики несанкціонованого доступу та вимагає додаткових зусиль для захисту секретної інформації. Розголошення конфіденційної інформації може призвести до серйозних наслідків, включаючи матеріальні збитки. Тому чітка правова політика та правильне ведення документації, що містить конфіденційну інформацію, державну або комерційну таємницю, стають важливими завданнями.Усі вказані фактори підсилюють актуальність досліджуваної теми, пов'язаної із методами і шляхами захисту конфіденційної інформації в організаційних документах, а також сприяють розвитку технологій та методів ефективного регулювання безпеки даних та конфіденційності документів.

Метою кваліфікаційної роботи є аналіз чинного законодавства України з питань захисту конфіденційної інформації, дослідження теоретичних і практичних аспектів документообігу конфіденційної документації, технологій і методів її захисту від несанкціонованого доступу, а також формулювання пропозицій щодо подальшого вдосконалення нормативної бази в цій сфері. Відповідно до мети сформульовано наступні **завдання дослідження:**

- розглянути поняття конфіденційної інформації та захищеного документообігу;
- охарактеризувати законодавчі акти з питань захисту документів з конфіденційною інформацією в Україні;
- висвітлити критерії віднесення інформації в організаційних документах до конфіденційної;
- дослідити особливості документообігу конфіденційної документації в установах та організаціях;
- проаналізувати сучасні технології і методи захисту конфіденційної інформації в організаційних документах.

Об'єктом дослідження є документаційне забезпечення управління.

Предметом дослідження є стратегії та комплекс організаційних, методичних і практичних заходів, спрямованих на захист конфіденційної інформації в організаційних документах від несанкціонованого доступу.

Методи дослідження. Методологічними засадами дослідження є принципи наукової об'єктивності, системності при висвітленні досліджених фактів; соціально-комунікаційно-інформаційний і діяльнісний підходи до процесу захисту документів. При аналізі поняття «захищений документообіг» використовувався порівняльний метод. Для вирішення конкретних завдань застосовувалися методи історіографічного і термінологічного аналізу та синтезу, інтерпретації та узагальнення; бібліографічний, моделювання.

Стан наукової розробки проблеми. Загалом проблема захисту конфіденційної документної інформації є актуальною упродовж останніх трьох десятиліть. Загальні питання поняття документа та діловодства порушували у своїх працях С. Гонгало [15], С. Савченко, Л. Ткач, К. Прокоф'єва, В. Вітер [59], С. Сельченкова [60]. Такі вчені, як І. Горбенко, Т. Гриненко [16], М. Гуцалюк [18], А. Чунарьова, А. Чунарьов [70], О. Матвієнко, М. Цивін [40] вивчали проблему інформаційної безпеки та захисту інформації. Окремі питання теми, зокрема, конфіденційного діловодства, висвітлюються в підручниках і навчальних посібниках [7; 45; 5; 12; 47; 13; 14; 61].

Чимало дослідників звертаються до вивчення питань захисту комерційної таємниці, державної таємниці як складників конфіденційної інформації [8; 42; 11; 1; 38; 19; 29]. Тут виділяються статті О. Кравченка, у яких піднімаються проблеми методів охорони комерційної таємниці від сучасних загроз, удосконалення законодавства України щодо охорони комерційної таємниці суб'єктів господарювання тощо [36; 35; 37; 34]. Дослідники О. Архипов та В. Ворожко присвятили монографію системним аспектам оцінювання рівня важливості секретної інформації [2]. Особливий інтерес викликають статті С. Князєва, присвячені питанням захисту комерційної таємниці в Україні, а також правовим основам використання «ноу-хау» в Україні під час здійснення комерційної діяльності [28; 27].

Значна увага приділяється дослідженню розвитку електронного документообігу. Тут особливої уваги заслуговує науковий доробок Л. Філіпової [65], дві статті колективу авторів у журналі «Захист інформації» за 2005 р. [9; 10], тези авторів Дмитренко Т., Деркач Т. та Воронюк Н. [20].

При підготовці кваліфікаційної роботи використовувались також праці Л. Ковальської, К. Котова [30], М. Назаркевича, Я. Возного [43], І. Розломій, Г. Косенюк [58], М. Цілиної [66], в яких викладені результати наукової роботи з основних методів та технологій захисту документообігу від несанкціонованого доступу. Серед технологій захисту документної інформації автори В. Чередниченко В. [67], Ю. Зінковський і Д. Танцюра [26], А. Чунарьова [69] виділяють електронний цифровий підпис як один з найнадійніших методів захищеності документів в електронній формі. З розвитком новітніх технологій питання захищеного документообігу потребують постійного вивчення для створення нових методів та технологій захисту.

Важливі також довідкові видання, які допомагають розібратися у понятійно-категоріальному апараті теми [63; 32].

Отже, досліджувана тема знайшла достатнє висвітлення у науковій літературі. Однак наявні праці більше стосуються правових, економічних питань, проблем державного управління і менше – питань, пов’язаних із документаційним забезпеченням управління. Тому цей аспект ще більше посилює актуальність роботи.

Джерельна база дослідження. Основна робота під час підготовки кваліфікаційного дослідження була зосереджена на опрацюванні джерел, зокрема, Конституції України [31], відповідних Законів України [56; 57; 49; 54; 52; 55; 51], нормативно-правових актів виконавчих органів влади з питань інформаційної безпеки документообігу [53; 48], технічних правил і рекомендацій, підготовлених відповідними органами, які відповідають за захист інформації [24; 25; 46], вимог до роботи з конфіденційною інформацією установи [3], ін. Також дослідження проводилось на основі аналізу офіційних

сайтів Служби Безпеки України [62] та Міністерства цифрової трансформації України [41].

Практичне значення роботи полягає в тому, що вона може сприяти покращенню організації роботи з питань захисту документної інформації в організаціях та установах різних форм власності, а також бути використана в навчально-методичній діяльності при викладанніі відповідних нормативних і вибіркових освітніх компонентів, науково-дослідній роботі. Результати дослідження можна використовувати в діловодній справі, зокрема, у державних установах, приватних підприємствах, при роботі з документами, що містять державну і комерційну таємницю, конфіденційну інформацію.

Апробація роботи здійснювалася шляхом участі у наукових заходах факультету історії, політології та національної безпеки Волинського національного університету імені Лесі Українки, виступу на засіданні кафедри музеєзнавства, пам’яткознавства та інформаційно-аналітичної діяльності, де обговорювалися питання стану готовності кваліфікаційних робіт, під час проходження навчальних і виробничих практик.

Структура роботи. Кваліфікаційна робота містить титульний аркуш, анотацію, зміст, вступ, два розділи, поділені на підрозділи, висновки, список використаних джерел.

РОЗДІЛ 1

СУТЬ ТА ВИДИ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В ОГАНІЗАЦІЙНИХ ДОКУМЕНТАХ

1.1. Поняття конфіденційної інформації

Конфіденційна інформація, як уже зазначалося – це інформація, доступ до якої обмежено фізичною або юридичною особою та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов [54]. 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.

Правовий режим конфіденційної інформації в Україні регулюється Законом України «Про інформацію». Визначення цього поняття можна знайти у ст. 21 Закону, де зазначено, що *конфіденційною є* інформація про фізичну особу, а також інформація, доступ до якої обмежений фізичною або юридичною особою, крім суб'єктів владних повноважень. Відповідно до ст. 21 Закону України «Про інформацію» конфіденційна інформація разом із службовою та таємною інформацією належить до інформації з обмеженим доступом [60].

Конкретного переліку інформації, яка може бути конфіденційною чи комерційною таємницею, чинне законодавство України не визначає. Натомість ч. 4 ст. 21 згаданого Закону України містить перелік відомостей, *доступ до яких не може бути обмежений* (зокрема, це інформація про стан довкілля, якість харчових продуктів, аварії, катастрофи та надзвичайні ситуації, стан здоров'я населення). Постанова Кабінету Міністрів України «Про перелік відомостей, що не становлять комерційної таємниці» №611 від 09.08.1993 р. визначає

перелік відомостей, що не можуть бути віднесені до комерційної таємниці (зокрема, відомості про чисельність і склад працівників, їхню заробітну плату, наявність вільних робочих місць, документи про сплату податків та обов'язкових платежів).

До конфіденційних належать відомості, які становлять особисту або сімейну таємницю особи, наприклад, інформація про сімейний стан, стан здоров'я, майновий стан, відомості про дату народження тощо, а також будь-які інші відомості, які особа бажає зберегти в таємниці [54].

Конфіденційна інформація пов'язана із комерційною таємницею, яка стосується різних аспектів виробництва, технологій, управління, фінансів та іншої діяльності підприємства, розголошення якої може завдати шкоди інтересам цього підприємства [34, с. 35–36]. Рух документів в рамках відкритого діловодства починається з моменту їх отримання, але до їх реєстрації проходять певні етапи підготовки та обробки. У конфіденційному діловодстві робота з документами, що надійшли, також починається з моменту їх отримання, але враховується перед початком руху. Таким чином, рух конфіденційних документів настає після їх обліку. Метою і відкритого, і конфіденційного документообігу є забезпечення виконання та застосування документів, але в конфіденційному документообігу особливу увагу приділяють захисту документів від несанкціонованого доступу для запобігання витоку конфіденційної інформації.

Отже, підходи до організації конфіденційного документообігу базуються на кількох принципах. По-перше, це створення системи доступу до конфіденційних документів. Другий принцип - запобігання несанкціонованому доступу до таких документів. Третій – регулювання руху цих документів. Четвертий принцип передбачає обмеження проходження та обробки конфіденційних документів, які не відповідають характеру чи порядку виконання. П'ятий – фіксація передачі конфіденційних документів. Шостий - забезпечення своєчасного та якісного виконання таких документів. Сьомий - особиста і обов'язкова відповідальність за видання неправомірних дозволів на

ознайомлення з конфіденційними документами та їх відправлення. Конфіденційне діловодство охоплює документування конфіденційної інформації, організацію роботи з конфіденційними документами та захист інформації, яка вони містять.

Відтік конфіденційної інформації – це незаконне поширення такої інформації за межі зони її захищеності або встановленого кола осіб, які мають право доступу до неї [32, с. 355–356]. Це може статися, якщо ця інформація потрапить до осіб, які не мають до неї дозволу, незалежно від їхньої зайнятості чи минулої роботи в відповідному закладі. Уразливість інформації – це її можливість стати об’єктом дестабілізації, тобто процесів, що порушують її статус. Це може включати фізичну безпеку, логічну структуру, доступність для правозастосовних користувачів, а також конфіденційність. Уразливість інформації має різні форми, такі як крадіжка, втрата, руйнування, спотворення, блокування та розголошення інформації. Ці форми можуть виникнути як навмисне, так і випадкове впливи на інформацію через різні джерела, такі як люди, технічні засоби та природні явища.

Способами впливу на інформацію можуть бути копіювання, записування, передача, зараження вірусом програм обробки, порушення технології обробки та зберігання, а також фізичний вплив на інформацію.

Вразливість документованої інформації може призвести до втрати або витоку інформації. Втрата може відбутися через розкрадання або втрату носіїв інформації, несанкціоноване знищення носіїв, спотворення або блокування інформації. Витік конфіденційної інформації може статися через її розголошення. Терміни «витік» і «розголошення» не повинні бути використані як синоніми, оскільки витік відбувається при несанкціонованому розголошенні, а також внаслідок втрати або розкрадання носія інформації.

Розкрадання конфіденційної інформації завжди пов’язане з отриманням нею особами, які мають до неї доступ. Були випадки, коли розкрадання носіїв такої інформації вчинялося колегами по роботі з метою шкоди. Зазвичай такі носії знищувалися зловмисниками. Це може створювати ризик витоку

інформації. Тому розголошення, розкрадання і втрата можуть призвести до витоку конфіденційної інформації. Однак часто важко визначити, чи сталася розкрадання чи розголошення, і чи потрапила інформація до сторонніх осіб.

Необхідно приділяти однакову увагу запобіганню як втраті, так і витоку документованої інформації, що підлягає захисту, оскільки в будь-якому випадку завдання носію інформації завдається шкода. Захист конфіденційної документованої інформації від втрати та витоку частково реалізується через першу та другу складові конфіденційного діловодства, оскільки вони взаємопов'язані: документування конфіденційної інформації та управління конфіденційними документами повинні відбуватися з урахуванням забезпечення їх захисту, і багато заходів захисту вирішуються під час здійснення регулярних операцій з обліку та обробки документів. Проте заходи захисту включають як самі документи, так і інші об'єкти, пов'язані з документами, що підлягають захисту (приміщення, технічні засоби обробки та передачі інформації та інші).

Інформація, яка може вважатися комерційною таємницею підприємства, згідно з рішенням керівництва, повинна відповідати таким критеріям: відсутність державної таємниці; непосягання на інтереси суспільства; стосування до виробничої діяльності підприємства; наявність реальної або потенційної комерційної цінності та створення переваг у конкурентній боротьбі; обмеження доступу.

Для державних організацій, які не займаються комерційною діяльністю, необхідність дотримання режиму конфіденційності інформації може стосуватися тих відомостей, поширення яких відповідно до чинних законодавчих актів організації вважають небажаним на користь забезпечення своєї діяльності. У комерційних організацій прагнення охорони інформаційних ресурсів і збереження їх конфіденційності найчастіше зумовлено умовами конкуренційної боротьби. Пов’язано це з тим, що на сьогоднішній день інформація є своєрідним товаром, що підпорядковується законам товарно-грошових відносин [28].

Реальний механізм, який може забезпечити захист документованої конфіденційної інформації – це створення в організації системи конфіденційного діловодства або, як мінімум, застосування у відкритому діловодстві засобів та методів, які використовуються під час роботи із закритими документами. Однак для цього необхідно дотримання цілого ряду принципів. Насамперед необхідно зазначити, що на відміну від відкритого діловодства, мета якого полягає у створенні довідково-інформаційної системи, мета обліку конфіденційних документів полягає у збереженні документів та фіксуванні їхнього місцезнаходження [27, с. 62–63].

Внаслідок цього система обробки та захисту конфіденційних документів включає низку заходів, не властивих відкритому діловодству. Серед них:

• жорстке регламентування складу документів, що видаються, і контроль процесів документування починаючи зі стадії підготовки чернеток і проектів документів;

• створення дозвільної системи доступу до документів та справ, що забезпечує правомірне та санкціоноване ознайомлення з ними;

• обов'язковий поекземплярний та полистовий облік усіх без винятку документів, проектів та чернеток;

• облік та забезпечення безпеки не тільки всіх документів, а й облікових форм;

• фіксація проходження та місцезнаходження кожного документа, у тому числі письмове фіксування всіх звернень персоналу до документів;

• контроль копіювання та розмноження документів;

• регламентація обов'язків співробітників, у тому числі запровадження персональної відповідальності, щодо роботи з документами та захисту довіреної конфіденційної інформації;

• проведення систематичних перевірок наявності конфіденційних документів, їх збереження та цілісності;

• проведення постійної інформаційно-аналітичної роботи, спрямованої на виявлення потенційних загроз, визначення найбільш оптимальних заходів, що

сприяють зміцненню та оновленню системи захисту документованої інформації відповідно до змінних внутрішніх і зовнішніх обставин [1, с. 104–106].

Отже, конфіденційне діловодство ширше відкритого і за своїм завданням, оскільки завдання відкритого діловодства полягає у документаційному забезпеченні управлінської діяльності. Зазначимо, що метою конфіденційного діловодства, крім того, є і захист документованих відомостей, що утворюються в процесі конфіденційної діяльності, а також інших об'єктів, так чи інакше пов'язаних із документами, що захищаються.

Конфіденційні документи повинні створюватися лише за дійсної необхідності в письмовому посвідченні їх наявності та змісту. При цьому вирішення завдань конфіденційної діяльності має забезпечуватись мінімальною кількістю документів за збереження повноти необхідних відомостей.

Конфіденційною інформацією є інформація, яка потребує захисту. Технології конфіденційного (захищеного) електронного документообігу – це процеси, методи пошуку, збирання, зберігання, обробки, надання, розповсюдження інформації та способи здійснення відповідних процесів та методів. Технології обробки, зберігання, передачі та захисту інформації входять до Переліку технологій, що мають велике соціально-економічне значення, та відіграють важливу роль у забезпеченні оборони країни та безпеки держави (критичні технології) [1, с. 14].

Проблеми захисту стали ще складнішими і значимими у зв’язку з переходом життєвого циклу документованої інформації на безпаперову, електронну основу з одночасним застосуванням як «паперових» технологій діловодства і документообігу, так і електронних з допомогою автоматизованих інформаційних систем (АІС). Технології конфіденційного діловодства та документообігу багато в чому збігаються з технологіями організації роботи з документованою інформацією обмеженого доступу, яка становить державну таємницю [6, с. 289].

Особливість конфіденційних документів у тому, що є масовим носієм цінної інформації, основним джерелом накопичення та поширення цієї

інформації, і навіть обов'язковим об'єктом захисту. Роль конфіденційної інформації у діяльності будь-якої організації дуже висока. Підприємства, установи, інші організації використовують конфіденційну інформацію для того, щоб зберегти секрет секрет виробництва; приховати службові дані; не оприлюднювати відомості про особисте життя своїх співробітників; приховати фінансовий бік діяльності [11].

Завдяки конфіденційній інформації можна створити гідний бізнес. Справжня чи потенційна комерційна цінність інформації багато в чому носить суб'єктивний характері і дозволяє підприємцю обмежувати доступом до практично будь-яким відомостям, які у підприємницької діяльності, крім відомостей, визначених нормативно-правовими актами.

Перелік конфіденційної документованої інформації організації є основою організації конфіденційного діловодства та залежить від компетенції та функцій організації, характеру її діяльності, взаємозв'язків з іншими підприємствами та організаціями, порядку вирішення питань. У свою чергу, якість складання цього переліку впливає на якість відповідної сфери діяльності, організацію, надійність обробки та захисту документованої інформації. Перелік також є підставою для створення класифікатора автоматизованої інформаційної системи та обмеженої доступу, що циркулює в системі інформації, або, іншими словами, системи захищеного електронного документообігу [12, с. 91].

При складанні переліку необхідно виходити із трьох основних принципів: законності, обґрунтованості та своєчасності надання документованої інформації статусу конфіденційності. Термін «конфіденційність» використовується виключно для позначення інформаційних ресурсів обмеженого доступу, які не віднесені до державної таємниці. Обов'язковою ознакою конфіденційного документа є наявність у ньому інформації, що підлягає захисту. Називати конфіденційні документи секретними чи ставити ними гриф секретності забороняється.

Ефективність роботи будь-якої організації залежить від того, наскільки раціонально та чітко в ній збудовані основні бізнес-процеси, у тому числі в

галузі документаційного забезпечення. Але успіх організації може бути стабільним, якщо у ній відсутня система захисту конфіденційної інформації. Одним із основних елементів цієї системи є конфіденційне діловодство. Порядок роботи з конфіденційними документами має особливості. Як і загальному діловодстві, всі етапи роботи з документами обмеженого доступу мають бути регламентовані.

Основним документом, в якому визначено вимоги до всіх стадій проходження документа з грифом обмеженого доступу з моменту його створення до направлення у справу або знищення, є інструкція з конфіденційного діловодства [18, с. 84]. Інструкція з конфіденційного діловодства має розділи, аналогічні інструкції із загального діловодства, але в ній знаходять своє відображення особливості роботи з конфіденційними документами. Основою організації конфіденційного діловодства є облік конфіденційної документованої інформації кожному етапі її проходження. Наказом керівника підприємства призначається посадова особа, відповідальна за облік, зберігання та використання документів, які містять конфіденційні відомості. Це може бути співробітник, для якого робота з документами, що містять комерційну таємницю, є основним службовим обов'язком або секретар-референт підприємства. Ці особи несуть персональну відповідальність за втрату чи витік конфіденційної інформації. Сукупність технологічних стадій (функціональних елементів), що супроводжують потоки конфіденційних документів, відрізняється від сукупності, властивої відкритим документам [18, с. 84–87].

Таким чином, сам термін «конфіденційна інформація» і використання цієї інформації в організаційних документах має свої особливості. Технології обробки, зберігання, передачі та захисту інформації входять до Переліку технологій, що мають велике соціально-економічне значення, та відіграють важливу роль у забезпеченні оборони країни та безпеки держави (критичні технології). Організація роботи з конфіденційними документами схожа на роботу з відкритими документами, але різниця полягає в тому, що

конфіденційні документи містять інформацію обмеженого доступу. Тому конфіденційне діловодство визначається як діяльність, що забезпечує документування, організацію роботи з конфіденційними документами та захист інформації, що міститься в них. Стадії обробки конфіденційних документів характеризують сукупність методів та засобів, що становлять певну технологічну систему обробки та зберігання даних документів.

1.2. Основні види конфіденційної інформації в організаційних документах

При передачі конфіденційних документів за межі відділу конфіденційної інформації їх безпека значно падає через можливе ознайомлення з ними багатьма працівниками компанії. Тому важливо правильно організувати роботу персоналу з цими документами. Особливо велика загроза виникає для електронних документів через можливість доступу до них багатьох працівників і складнощів у виявленні факту крадіжки інформації [17; 18].

Керівники та виконавці повинні: переглядати лише ті конфіденційні документи, до яких отримали дозвіл у зв'язку з посадовими обов'язками; пред'являти свої документи співробітникам служби конфіденційної інформації для перевірки їх наявності та повноти; вести облік документів, що знаходяться у них; щоденно після закінчення робочого дня перевіряти наявність документів, здавати їх для зберігання у службу конфіденційної інформації; негайно повідомляти безпосередньому керівнику та службі конфіденційної інформації про втрату або недостачу документів, виявлення зайвих або пропущених документів, окремих листів; здавати всі документи згідно інструкцій у службу конфіденційної інформації при звільненні, виході у відпустку або відрядженні [12; 11].

Керівники, проводячи процедуру розгляду документів, вирішують наступні завдання забезпечення інформаційної безпеки: визначення

правильного складу виконавців, які мають доступ до документу; виключення можливості ознайомлення з документом осіб, які не мають до нього доступу; запобігання можливості крадіжки або копіювання документів сторонніми особами; уникнення витоку інформації через технічні канали. При цьому важливо пам’ятати, що сторонніми особами вважаються всі, хто не має права доступу до даного документа, включаючи інших керівників і фахівців компанії.

Працівник служби конфіденційної документації, який видає документи виконавцям для роботи, повинен: уникати видачі документа особі, яка не має права доступу до нього; зафіксувати факт передачі документа виконавцю; забезпечити безпечне зберігання документа та його частин; дати доступ виконавцю лише до частини документа, призначеної для нього; уникнути можливості ознайомлення сторонньої особи з документом під час його видачі та повернення; вести облік документів, що знаходяться у виконавців [7, с. 132].

Відповідальність за збереження конфіденційних документів і запобігання витоку інформації в підрозділах компанії покладається на їхніх керівників. Друкування конфіденційних документів на паперовому носії проводиться працівником служби конфіденційної документації на друкарській машинці або за допомогою ПЕОМ. Виготовлення документів може провадити сам працівник на своєму робочому місці, але лише за умови збереження конфіденційності фірми. На кожному екземплярі документа обов’язково зазначається кількість надрукованих копій, їх призначення, прізвище та контактний номер виконавця, а також прізвище оператора, який друкував документ, та дата [7, с. 132].

При виготовленні документів не допускається використання нових фарбувальних стрічок або копіювального паперу, а також додавання додаткових аркушів паперу від валика пишучого пристрою. Документи не мають бути записані на диктофон. Вікна у приміщенні рекомендується затемнювати або заслонювати, а екран дисплея повинен бути обернутий від вікон та вхідних дверей. Розповсюдження конфіденційних документів та копіювання їх дозволяється лише за письмовим дозволом керівника підрозділу, де працює виконавець [12].

Додаткові копії враховуються в службі конфіденційної інформації за номером оригіналу в тій же системі обліку. Виписки з конфіденційних документів робляться лише за згодою керівника підрозділу та враховуються під новими номерами в картках обліку. Необхідно строго контролювати використання копіювальної техніки співробітниками компанії. Копіювальні апарати можуть розміщуватися у спеціальних приміщеннях служби конфіденційної інформації або у кабінетах керівників за необхідності. Після закінчення робочого дня ці приміщення повинні бути зачинені, опечатані та під охороною. Робота з електронними конфіденційними документами супроводжується додатковими вимогами до системи безпеки.

Для персоналу розробляється ієрархічна система ідентифікаційних засобів для забезпечення обмеження доступу до інформації. Ця система затверджується наказом керівника і розподіляється індивідуально до кожного співробітника під розпис. Необхідно постійно оновлювати систему, особливо у випадку частої зміни персоналу. Будь-яке використання інформації, яке дозволено або не дозволено, повинно бути зареєстроване. Рекомендується регулярно перевіряти використовуване програмне забезпечення для виявлення незвичайних програм. Заборонено використовувати незареєстровані захисні заходи. Якщо сталася несанкціонована спроба доступу до конфіденційного файлу, інформація в ньому має бути негайно видалена автоматично [13, с. 111].

Після завершення роботи на ПЕОМ співробітник повинен: перенести конфіденційну інформацію на гнучкі носії (дискети, диски); видалити конфіденційну інформацію з ПЕОМ і записати шумову інформацію для захисту; перевірити та здати гнучкі носії службі конфіденційної документації; заблокувати ПЕОМ та відключити його від електроживлення; зачинити і опечатати приміщення й передати його під охорону. Після друкування конфіденційного документа і, за потреби, перенесення тексту на дискету, інформація на ПЕОМ також повинна бути видалена з магнітного носія [3].

При обробці конфіденційних документів керівники та виконавці повинні мати стабільне робоче місце, особистий сейф або кейс для зберігання

документів та особисту металеву печатку. Ключі та металева печатка зберігаються у керівника або виконавця, а дублікати ключів - у службі конфіденційної документації. Робоче місце повинно бути розташоване таким чином, щоб уникнути можливості погляду на конфіденційні документи особами, які не мають до них відношення. Вікна в приміщенні мають бути захищені від шпигунства, а робочий стіл завжди повинен містити лише той конфіденційний документ, яким працює співробітник в даний момент [3].

Класифікація документів використовується для підвищення ефективності управління та відповідальності виконавців. У поточній роботі класифікація проводиться на рівні груп та у справі, де документи поділяються на роди, види, підвиди і різновиди. Вид – це другий рівень розподілу. Відповідно до цього, поняття «документ» розділяється на видові категорії, або види документів. Наступним рівнем є підвид, а потім – різновид, щоб визначити конкретне місце кожного документа у класифікації. Ієрархія відображає розташування документів від більш загального до менш загального. Класифікація документів виконується залежно від різних критеріїв поділу, що відповідають різним аспектам аналізу документів. Кожен аспект аналізу визначає певний аспект класифікації, тобто список документів з урахуванням певної ознаки. Класифікація документів може бути багатоаспектною фасетною.

Отже, класифікація будь-чого включає в себе встановлення зв’язку між елементами, вираженими у їхньому розміщенні в певному послідовному порядку або системі відповідно до загальних принципів. У нашому випадку, предметом класифікації є документ як матеріальна форма збирання, зберігання, використання та поширення інформації. Документи можуть бути класифіковані за різними критеріями, такими як: письмові, графічні, фото- та кінодокументи, фонодокументи, в залежності від способу фіксації інформації.

РОЗДІЛ 2

ПРАВИЛА ДОКУМЕНТООБІГУ КОНФІДЕНЦІЙНОЇ ДОКУМЕНТАЦІЇ В УСТАНОВІ ТА ОСОБЛИВОСТІ ЇЇ ЗАХИСТУ

2.1. Основи документообігу конфіденційної документації

Для функціонування та розвитку будь-якої організації чи установи важливою є організація безпечного та захищеного документообігу. Документообіг – це рух усіх документів в установі чи організації. Іншими словами його називають повним «життєвим циклом» документів. Документообіг може бути і паперовим, і електронним [60, с. 17–23]. Закон України «Про електронні документи та електронний документообіг» дає чітке визначення поняття «електронний документообіг». Під електронним документообігом розуміється сукупність процесів, через які проходять електронні документи, та які перевіряють на цілісність і підтверджують факт одержання таких документів. Це процеси створення, обробки, відправлення, передачі, одержання, зберігання, використання і знищення документів, тобто увесь рух електронного документу від початку існування до передачі в архів або знищення [52].

Варто зазначити, що не всі документи, які є в тій чи іншій установі, потребують захисту. Публічні документи, тобто матеріальні носії публічної (відкритої) інформації, є у відкритому доступі для будь-кого, оскільки там зазначається загальні відомості, що відповідно до Закону України «Про доступ до публічної інформації», не заборонені у використанні суспільством [50].

Захисту потребують документи, які в діловодстві прийнято називати конфіденційними, тобто містять закриту для широкого загалу інформацію. Закон України «Про доступ до публічної інформації» дає визначення поняттю «конфіденційна інформація», як інформації, яка обмежена в доступі фізичною

чи юридичною особою, крім тих суб'єктів, які мають владні повноваження стосовно даної інформації. Така інформація може поширюватись на певну аудиторію у визначеному порядку лише за особливих передбачених суб'єктами умов. Головною ознакою конфіденційного документа є наявність даних, що потребують захисту. Такі документи в сукупності формують захищений документообіг [50]. Отже, захищений документообіг – це система організації та обробки документів з метою забезпечення їх конфіденційності, цілісності та доступності. Основна мета полягає в уникненні несанкціонованого доступу до інформації, її втрати чи пошкодження, що може завдати шкоди діяльності організації.

При зберіганні документів у компанії дотримуються певних правил. Документи розділяються на три категорії в залежності від їх важливості, для кожної категорії встановлені власні вимоги до організації зберігання [16].

Перша категорія включає документи, які надзвичайно важливі для ведення справ компанії або для ознайомлення з її минулим. Втрата таких документів може негативно вплинути на фінансове становище компанії, її репутацію, відносини зі стейкхолдерами, юридичні питання тощо. Друга категорія включає документи, які мають обмежений термін зберігання і є важливими для щоденних операцій. Ці документи можуть бути конфіденційними. Третя категорія охоплює документи, які не потребують спеціального зберігання і не мають великого значення для компанії. Вони не впливають на роботу компанії, не мають конфіденційного характеру та не є необхідними для щоденних операцій [5].

Найвищі вимоги до організації зберігання застосовуються до документів першої категорії. Щоб успішно вести справи, документи мають створюватися, використовуватися і знищуватися відповідно до вимог Статуту компанії. Знищення документів є необхідним і має бути проведене розумно, відповідно до всіх нормативних вимог. Недбале знищення документів може призвести до розголошення конфіденційної інформації. Організація контролю за виконанням службових документів базується на таких принципах: пунктуальності,

об’єктивності, відкритості, систематичності та індивідуального підходу. Ігнорування цих принципів може призвести до зниження результатів роботи підприємства.

Проекти конфіденційних документів можна створювати рукописним способом або за допомогою ЕОМ. Друкування таких документів здійснюється у спеціально відведених для цього приміщеннях. Засоби для друкування, що використовуються, повинні бути захищені від перехоплення, тобто повинні відповідати вимогам безпеки [5, с. 34].

Якщо документ друкується з чернетки, на чернетці має бути написано скільки копій має бути зроблено. Наприклад, створюємо один і після цього знищуємо чернетку. При прийомі чернетки від виконавця співробітник відділу конфіденційного діловодства зобов’язаний: якщо створюється чернетка у спецблокноті, прорахувати кількість аркушів чернетки, та вилучити їх із блокнота, вшити в окрему справу тощо, щоб наступного разу коли візьмуть спецблокнот, щоб не було там інформації; при складанні чернетки на окремих аркушах прорахувати кількість його аркушів; при складанні чернетки у робочих зошитах перевірити відповідність наявності аркушів зошита зазначеній кількості [17].

Журнал обліку виданих документів із грифом «Комерційна таємниця» має 16 стовпів. Це: обліковий номер та гриф конфіденційності; дата документа (коли видано); вид (заголовок) документа; прізвище та ініціали виконавця; обліковий номер чернеток та кількість аркушів; кількість надрукованих екземплярів; кількість аркушів у кожному екземплярі (примірник 1 - 12 аркушів, і так далі); підпис за отримання чернетки, надрукованих документів та дата; відмітка про знищення зіпсованих листів; відмітка про отримання та знищення чернетки; підпис за повернення надрукованого документа та дата; номери примірників (кількість у значенні); куди відправлено документ (або співробітнику чи іншу організацію); з яким документом (за яким номером) надіслано (номер, дата); місцезнаходження (у якій справі знаходиться (його

номер) та номери аркушів; місцезнаходження (номер обліку виділеного зберігання) [27, с. 62–64].

Важливою складовою документообігу конфіденційної інформації в організації є отримання або надсилання конфіденційних документів та їх облік. Усі документи конфіденційного характеру підлягають обліку. Відповідний журнал зберігається в логанізації чи установі протягом календарного року. Супровідний документ відправляється назад відправнику після проставки на ньому підпису про отримання конфіденційного листа [23].

Послідовність роботи з документами, які містять конфіденційну інформацію: отримання пакета, перевірка та облік (згідно з вищезгаданими пунктами) Якщо лист не відповідає запиту – повернення листа назад адресату (помилкова адреса, порушена цілісність пакета), але облік все одно ведеться; розкриття пакета, перевірка та облік вмісту Складання акта про виявлені порушення, якщо виявляються порушення (не той документ, не той гриф тощо); вивчити вміст документа (отримання резолюції від керівника) [5, с. 175].

Підготовка та відправлення документа (з поміщенням останнього екземпляра у справу) (мається на увазі відповідь, зазвичай з тим самим грифом, другий екземпляр залишається і підшивається). Далі знімається з контролю. Або виконання документа (ознайомлення з ним) з наступним поміщенням у справу. На документі може стояти резолюція «на контроль». У такому разі такий документ підлягає особливій увазі, зоркрема, щодо якості і термінів виконання.

Підготовка та відправлення документа (з поміщенням останнього екземпляра у справу) (мається на увазі відповідь, зазвичай з тим самим грифом, другий екземпляр залишається і підшивається). Далі знімається з контролю. Або виконання документа (ознайомлення з ним) із наступним поміщенням у справу. Далі знімається з контролю.

Журнал обліку документів, що надійшли (конфіденційних), включає наступні графи: дата надходження документа чи пакету; номер реєстру або підпис особи, яка передала пакет; звідки поступив відповідний документ

(організація); номер і гриф документа, що надійшов, дата видання; вхідний номер документа (номер екземпляра, гриф конфіденційності) присвоюємо самі; вид та заголовок документа; кількість аркушів документа; кількість аркушів додатка до документа (скільки аркушів, а не скільки додатків); кому видано документ; кількість виданих листів; підпис за отримання, дата; підпис за повернення та дата; місцезнаходження документа (номер справи, в якому він знаходиться та номери аркушів); номер з обліку виділеного зберігання, кількість аркушів; примітка (позначка повернення документа) (назад відправнику зазвичай) [23].

Якщо на пакеті інший адресат, то такий пакет не розкривається, не приймається. Пакет із позначкою «особисто для» розкривається або цією особою, або відділом конфідеційного діловодства. При отриманні такого документа заповнюються перші три графи у журналі обліку. Якщо прийшов зайвий документ, повертаємо назад. Також вказуємо причину повернення (наприклад, як зайвий або як помилково надісланий) з номером таким-то від такої-то дати. Якщо документ, що надійшов, підлягає передачі на виділене зберігання, то без присвоєння вхідного облікового номера присвоюється черговий порядковий номер журналу обліку документів виділеного зберігання. Документи (надані) повинні потрапляти до посадової особи в день отримання або не пізніше наступного робочого дня.

Вирізняється також врахування конфіденційних документів виділеного зберігання. Наприклад, документ не можу бути підшитим у справу, оскільки розміщений на флешці, або жорсткому диску тощо. Відрізняє ці документи від простих «інвентарний номер або буква В, номер та ДСП». Журнал обліку конфідеційних документів виділеного зберігання включає: обліковий (інвентарний) номер та гриф конфіденційності; дата реєстрації; вид та заголовок документа; звідки надійшов (ким розроблено); з якого облікового номера (обліковий номер з якого документа надійшов); номери екземплярів; кількість листів в екземплярі; місцезнаходження; відмітка про картотеку (у якій

картотеці знаходиться); відмітка про відправку; відмітка про повернення; відмітка про зняття з обліку виділеного зберігання; відмітка про знищення.

Зазвичай копіювання таких документів відбувається у відділі конфіденційного діловодства. Копіювання конфіденційних документів не повинно проводитись разом з копіюванням звичайних документів. Під час копіювання доступ сторонніх осіб до приміщення заборонений. Список осіб, які мають право на копіювання документів з конфіденційною інформацією, повинен бути зафіксований у положенні про комерційну таємницю.

Якщо потрібно скопіювати документи, які прийшли з іншої компанії (організації, установи), необхідно отримати дозвіл у керівника цієї компанії. Надруковані копії підлягають обліку, а в деяких випадках – засвідчення як копія. Дозвіл на виготовлення додаткових екземплярів конфіденційного документа оформляється на звороті останнього екземпляра, з якого проводиться копіювання. Цей екземпляр не повинен відправлятися в жодні організації, а повинен підшиватися у справу і зберігатися у відділі конфіденційного діловодства.

Копіювання документа, який містить конфіденційну інформацію, реєструється у журналі копіювання конфіденційних документів. Цей журнал включає: обліковий номер, гриф конфіденційності та дата документа; кількість або номери сторінок; дата копіювання; кількість знятих копій (аркушів або екземплярів); облікові номери, присвоєні копіям або екземплярам (такі ж самі номери, як і для оригіналів); підпис за отримання та дата.

Проекти конфіденційних документів друкуються або з чернетки, або з тексту, нанесеного на інший носій інформації, або без використання того й іншого. Найпоширенішими носіями документованої конфіденційної інформації є машинні та паперові носії [22]. Серед машинних носіїв: жорсткі магнітні диски; гнучкі магнітні диски (дискети); магнітні стрічки; магнітооптичні диски; оптичні диски.

Паперові носії – це для текстових документів – спецблокноти, окремі аркуші паперу, типові форми документів, стенографічні та робочі зошити; для креслярсько-графічних документів – ватман, калька, міліметровий папір.

На обкладинках спецблокнотів співробітник підрозділу конфіденційного діловодства пише або проставляє штампом слово «Спецблокнот» та у правому верхньому кутку ставить гриф конфіденційності. Якщо листи спецблокнота не пронумеровані друкарським способом, то вони нумеруються співробітником підрозділу конфіденційного діловодства.

Обсяг та характер створюваних документів впливають на організацію роботи із захисту інформації. Тому документування конфіденційної інформації є найважливішою складовою конфіденційного діловодства, оскільки від кількості, складу та правильності оформлення документів залежить якість та ефективність управлінської та виробничої діяльності, достовірність та юридична сила документів, трудомісткість їх обробки та якість організації.

Працівники підприємства, допущені до конфіденційних відомостей та документів, перш ніж отримати доступ до них, повинні пройти інструктаж та ознайомитися з пам’яткою про збереження комерційної таємниці підприємства. Пам’ятка складається службою безпеки з урахуванням специфіки конкретного підприємства, підписується заступником директора та затверджується директором підприємства [24]. Ведення діловодства, що забезпечує облік та збереження документів, що містять конфіденційну інформацію, передбачає виконання низки рекомендацій.

Наказом керівника підприємства призначається посадова особа, відповідальна за облік, зберігання та використання документів, які містять конфіденційні відомості. Це може бути співробітник, для якого робота з конфіденційними документами є основним службовим обов'язком або секретар-референт підприємства. Ці особи несуть персональну відповідальність за втрату або витік інформації з них. Знову прийняті на роботу співробітники попереджаються про можливу кримінальну, адміністративну та іншу відповідальність відповідно до законодавства [25].

Усі документи, що містять конфіденційну інформацію, підлягають обліку та спеціальному позначенню. На документі проставляють гриф обмеження доступу із зазначенням номера екземпляра, який має цю інформацію. Гриф конфіденційності або гриф обмеження доступу до традиційного, машиночитаного або електронного документа являє собою реквізит (елемент, службову позначку) формуляра документа, що свідчить про конфіденційність відомостей, які містяться в документі [26].

Облік (частіше використовується термін «реєстрація») відкритих документів насамперед має на меті включення документа до довідково-інформаційної системи для цілей довідкової та пошукової роботи з документів та контролю виконання доручень та завдань, що містяться в документі [25]. Облік конфіденційних документів має на меті збереження документів та фіксування їх місцезнаходження. Облік конфіденційних документів має забезпечувати:

• фіксування факту надходження пакета з документами, окремого паперового чи машиночитаного документа, або документа, що надходить електронною або факсимильною поштою (лініями зв'язку);

• фіксування факту реєстрації вихідних відомостей про документ та включення його до довідково-інформаційного банку даних за документами;

• фіксування факту перенесення інформації з паперового документа на машинний носій, факту включення документа в електронну базу даних та факту розміщення паперового документа у відповідній справі;

• фіксування факту переміщення документа (всіх звернень персоналу до документа) у процесі його розгляду, виконання та повернення до служби КД (реєстрація робочих відомостей);

• фіксування місцезнаходження документа (у менеджера, референта, у справі, файлі, на машинному носії поза ЕОМ тощо) у будь-який момент часу в період виконання документа та за його архівного зберігання;

• фіксування факту реєстрації вихідних відомостей про підготовлений документ;

• фіксування факту початку та закінчення складання, виготовлення та видання документа;

• фіксування факту подальшої роботи над виданим документом або надсилання його адресату (реєстрація робочих відомостей);

• фіксування факту оформлення спеціально підготовлених носіїв для складання конфіденційних документів;

• забезпечення пошукової, довідкової та контрольної роботи за конфіденційними документами;

• фіксування регулярних контрольних операцій другого працівника служби КД щодо перевірки правильності виконання працівником служби всіх технологічних операцій та перевірки наявності документів [25].

При передачі документів, що містять конфіденційну інформацію, до органів державної влади та органів місцевого самоврядування, гриф «Конфіденційно» проставляється в обов'язковому порядку [23]. Друк документів з грифом «Конфіденційно» проводиться централізовано, у спеціально відведеному приміщенні, яке виключає доступ сторонніх осіб.

Призначені для розмноження документів технічні засоби (копіювально-розмножувальне обладнання, комп'ютери, друкарські машинки) повинні бути захищені від можливого перехоплення електромагнітних випромінювань, що виникають при роботі. Розмноження конфіденційних документів не повинно проводитися вперемішку із розмноженням відкритих документів. Під час розмноження конфіденційних документів все, що має відношення до їх розмноження, повинно бути прибрано з робочих місць, що використовуються при розмноженні, доступ сторонніх осіб до приміщення, в якому відбувається робота з копіювання конфіденційної інформації, не дозволяється.

При значному обсязі документів можуть бути заведені журнали окремо для вхідних, вихідних та внутрішніх документів підприємства, що містять гриф «Конфіденційно». Усі аркуші журналів, що враховують такі документи, нумеруються, прошиваються та опечатуються. Наприкінці журналу в засвідчувальному аркуші вказується загальна їх кількість. Усі документи з

грифом «Конфіденційно» приймаються та розкриваються спеціально призначеною посадовою особою або секретарем-референтом, якщо їй надано таке право. При надходженні обов'язково перевіряється цілісність кореспонденції, кількість аркушів та екземплярів основного документа та додатків до нього. У разі відсутності або недостачі в конвертах документів з грифом «Конфіденційно» складається акт у двох примірниках, один із яких надсилається відправнику. Документи, які мають гриф «Конфіденційно», формуються окремо. На обкладинці у верхньому правому куті ставиться гриф «Конфіденційно». На внутрішній стороні обкладинки пишеться список працівників, які мають право користування цією справою. Всі аркуші справи нумеруються простим олівцем у верхньому правому кутку. На початку справи підшивається внутрішній опис документів, які у ній. Зберігаються такі справи в сейфі, який опечатується посадовцем, відповідальним за збереження документів із грифом «Конфіденційно». Інші працівники не повинні мати доступу до цього сейфа [35; 36].

Терміни зберігання документів визначаються внаслідок експертизи цінності документів як наукової, і практичної. У ході експертизи проводиться відбір документів на зберігання та встановлюються терміни їх зберігання. Комісія має право призначити такі терміни зберігання документів: короткочасні терміни зберігання – менше 10 років (наприклад, 1рік, 3 роки або 5 років); довготривалі терміни зберігання – понад 10 років, включаючи постійне зберігання (наприклад, 10 років, 30 років, 75 років тощо); ряд документів не зберігають – вони підлягають знищенню [35].

2.2. Склад конфіденційної інформації в організаційних документах

Комерційні відомості (таємниця) – це прихована від стороннього та загальнодоступного користування інформація, що дозволяє особі-власнику за рахунок її використання збільшувати власні доходи, отримувати та зберігати

найбільш вигідне становище на ринку, отримувати будь-яку іншу економічну вигоду. Розмірковуючи на тему комерційних відомостей, не можна не відзначити, що постійного, зафіксованого переліку документів, які б у ста відсотках випадків мали подібний зміст, немає [27].

Однак є ряд певних відомостей, здатних перетворити будь-який акт організації на носій конфіденційної інформації. До них відносяться: дані про комерційну діяльність організації, розголошення яких може призвести до значних фінансових втрат; особливо конфіденційні відомості про стратегічні плани компанії, у тому числі подальші плани розвитку, виробничої діяльності; розмір доходу, одержуваного компанією внаслідок реалізованої продукції / виконання певного роду робіт, послуг; відомості про найбільш ефективні та прибуткові способи ведення фінансової діяльності в галузі купівлі-продажу акцій, облігацій та інших цінних паперів; технології, рецептури, креслення, схеми, обладнання, програмне забезпечення виробничої електронно-обчислювальної техніки тощо, які використовуються у виробництві і розкриття інформації про які здатне призвести до суттєвих збитків та зниження конкурентоспроможності організації в рамках ринкової економіки загалом [19, с. 77–78].

Без сумніву, комерційні відомості та конфіденційність деякої інформації мають колосальне значення для будь-якої компанії, тому необхідно забезпечити правильну послідовність роботи з такою документацією [35]. Насамперед потрібно підготувати й видати наказ, що визначає відомості, що саме становить комерційну таємницю у конкретній компанії. Тоді варто сформувати склад комісії, відповідальної за комерційні відомості, що функціонуватиме на постійній основі, та розробити критерії категорії співробітників, яким надається право на попереднє визначення конфіденційної інформації: юристи, економісти, наукові співробітники, менеджери [11].

На основі оцінки комісії, за комерційними даними, спроектувати можливі збитки від витоку внутрішньої, таємної інформації. Скоординувати, а потім і застосувати перелік заходів щодо збереження, безпеки комерційної таємниці.

Розробити порядок доступу та процедуру роботи з подібними відомостями. Визначити коло осіб, які відповідають за забезпечення безпеки даних, що, зазвичай, перебуває у компетенції керівника організації. Необхіднр також здійснити маркування носіїв вузько доступної інформації із запобіганням несанкціонованому доступу. Як правило, на документи наносяться грифи: «Секретно», «Конфіденційно», «Комерційна таємниця», «Для внутрішнього користування», ін. [19].

Друк усіх паперових носіїв інформації з маркуванням «Конфіденційно» проводиться централізовано у спеціальному приміщенні, позбавленому загального доступу, особою, яка за розпорядженням керівника організації отримала дозвіл на роботу та інші операції з комерційними документами. Реєстрація документів, що містять комерційні відомості, здійснюється відокремлено від решти документообігу в «Журналі обліку вихідних документів» із грифом «Комерційна таємниця». Передача документів іншим співробітникам організації, які мають доступ до комерційних даних, здійснюється виключно через секретаря та його запис в обліковому журналі.

Конфіденційна інформація містить дані, включаючи комерційну таємницю, які належать підприємству (організації, установі), ним використовуються, зберігаються та розповсюджуються відповідно до встановлених положень цього підприємства, організації або установи. До цієї документації відносять документи про фінансову стабільність; відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, об’єднаннях та інших організаціях, які займаються підприємницькою діяльністю; ін. При цьому керівники підприємств, установ та організацій зобовязані надавати вказані відомості органам державної виконавчої влади, контролюючим та правоохоронним органам, іншим юридичним особам згідно з чинним законодавством, за їх вимогою [23, с. 44–46].

Комерційна таємниця може включати різні види інформації, такі як організаційна, комерційна, технічна, виробнича та інша. Визначення переліку відомостей, які можуть бути визнані комерційною таємницею підприємства,

повинне враховувати такі критерії: відсутність державної таємниці; відсутність шкоди для інтересів суспільства; відношення до виробничої діяльності підприємства; наявність ефективної або потенційної комерційної цінності і створення конкурентних переваг. Для встановлення такого переліку призначається експертна комісія, до складу якої залучають фахівців, що володіють інформацією щодо фінансових питань, ринкових умов та інформацією про діяльність конкуруючих фірм, а також мають досвід укладання договорів та контрактів. ЕК повинна керуватися такими критеріями при оформленні переліку відомостей, що становлять комерційну таємницю: виокремлення інформації, що належить до державної таємниці; розподіл інформації на науково-технічну (технологічну) та службову (ділову) інформацію [34].

Документи, що надсилаються до інших підприємств, установ і організацій, слід вкладати у конверти або упаковувати так, щоб унеможливити доступ до них. При цьому конверти повинні бути світлонепроникними, а пакети щільно заклеєними. На конвертах або інших упаковках обов'язково зазначають: назву і адресу підприємства-одержувача; назву і адресу підприємства-відправника; номери вкладених документів із зазначенням відповідної відмітки «ДСК», «Конф.» або «КТ». Варто звернути увагу на те, що на конвертах забороняється зазначати прізвища й посади працівників – виконавців документів, а також назви структурних підрозділів.

Документи, що містять комерційну таємницю, формують у справу. Порядок їх формування відповідає порядку формування справ у загальному діловодстві й здійснюється на підставі номенклатури справ підприємства. При цьому до номенклатури справ включають усі документи з грифами обмеженого доступу, а також довідкові й реєстраційні картотеки й журнали до них [34].

Документи, що містять конфіденційну інформацію, можуть бути зібрані у спеціальні справи залежно від потреб у виробництві та іншій довідковій інформації. Однак, якщо на підприємстві формується значна кількість документів однакового типу з обмеженим доступом, цілком логічно розглянути

можливість їхнього упорядкування у відповідні справи. У цьому випадку в номенклатурі справ має бути відповідний індекс для документів з комерційною таємницею, наприклад, «03-11-КТ».

Якщо у справі формується документ з обмеженим доступом разом з несекретними документами, на обкладинці справи ставиться відмітка про обмежений доступ, наприклад, «ДСК», і номенклатура справи змінюється відповідно. Якщо створюється лише декілька документів з комерційною таємницею, то може бути встановлена лише одна справа з відповідною відміткою. Тривалість зберігання такої справи не визначається і позначається відміткою «ЕК» у відповідному розділі номенклатури справи.

Після завершення робочого року справа переглядається експертною комісією і при необхідності приймається рішення щодо переформування документів. Таким чином, документи, які потрібно зберігати постійно, формуються в окремі справи з відповідною номенклатурою, а тимчасові документи залишаються у попередній розформованій справі. Якщо у справі з обмеженим доступом є лише тимчасові документи, то переформування її не обов'язкове. Тривалість зберігання такої справи встановлюється відповідно до найбільшого терміну зберігання документів, що в ній містяться, і відмічається відповідно в номенклатурі [39. С. 359–360].

Відділ канцелярії несе повну відповідальність за те, щоб виконавці своєчасно реагували на документи. Якщо виконавець не відповів на документ і не звернувся із запитом щодо продовження терміну виконання, то керівник канцелярії складає службову записку на ім'я директора, вказуючи на порушення. Доручення вважається виконаним, якщо інформація про виконані завдання прийнята і не надано додаткових вказівок. Після цього доручення знімається з контролю посадовою особою, що його дала. Відмітка про виконання також робиться в журналі, а контроль знімається [11].

Після завершення ревізії організації обліку конфіденційних документів для завершення переведення їх реєстрації в СЕД були підготовлені методичні рекомендації, які вдосконалюють порядок реєстрації таких документів.

Нововведення дозволять виключити некоректне використання бланків документів при їх створенні, неправильну реєстрацію внутрішніх конфіденційних документів, застосовувати метадані для зберігання відомостей про електронний примірник документа, стандартизувати та спростити записи про підвиди конфіденційних документів з використанням одноманітних літерних позначень в одній колонці журналу; ефективніше будувати аналітичні звіти за видами та підвидами конфіденційних документів, вірогідніше розраховувати документообіг конфіденційних документів та загальний документообіг філії [59].

Деякі дослідники відстоюють думку, що конфіденційне діловодство суттєво відрізняється від відкритого, є самостійним видом діяльності, мотивуючи це тим, що воно: поширюється як у управлінську, і на виробничу діяльність; включає у собе як роботу з документами, так і з їх проектами, чернетками тощо; вирішує два завдання: документаційне забезпечення всіх видів конфіденційної діяльності та захист інформації під час роботи з конфіденційними документами [17].

Запропонований у таких роботах підхід до конфіденційного діловодства призводить до розробки не завжди вдалих технологій. Якщо дотримуватися рекомендацій авторів окремих посібників, секретар-референт одні документи повинен реєструвати, інші - враховувати, складати кілька номенклатур, формувати у різні справи документи з одного питання. Така схема не завжди застосовується на практиці. Не слід також вважати, що документ обмеженого доступу за визначенням є більш цінним, ніж загальнодоступний.

Неопрацьованість змісту понять «конфіденційна інформація», «конфіденційний документ», «конфіденційне діловодство» та визначення його як самостійного, відмінного від відкритого діловодства напряму, впливає на сферу їх поширення і, що особливо важливо, на розробку технологічних процедур [32, с. 355–356]. У зв’язку з цим, на нашу думку, під конфіденційною документованою інформацією, конфіденційним документом слід розуміти узагальнююче поняття зафіксованої на матеріальному носії інформації, що

містить комерційну або службову таємницю, з реквізитами, що дозволяють її ідентифікувати та забезпечувати захист, доступ до якого обмежується. також її власником [3].

Щоб зрозуміти, як захистити інформацію, критично важливу для організації, необхідно розглянути основні причини витоків, із якими найчастіше стикаються підприємці [16; 17]. Умовно їх можна розділити на дві категорії: зовнішні та внутрішні. До зовнішніх загроз можна віднести такі:

Фізична крадіжка. Корпоративні дані можуть бути вкрадені третіми особами за допомогою різних способів. Одним із найпоширеніших способів є фішинг разом із соціальною інженерією.

Зламування IT-інфраструктури. Зловмисники можуть оволодіти даними методом кібератак на основний корпоративний сервер чи мережу. Часто хакери використовують метод DDoS-атак, які передбачають створення великої кількості "сміттєвого" трафіку, що перевантажує мережу та сервер.

Комерційний шпигунство. Часто конкуренти використовують звані чорні методи конкурентної боротьби і збирають інформацію нетрадиційним способом, використовуючи підставних клієнтів та агентів під прикриттям. Крім того, популярними методами шпигунства є прослуховування, злом акаунтів та серверів.

Внутрішні загрози можуть виникати від:

співробітників, які розкривають інформацію випадковим чином або внаслідок проведення зовнішніх ділових операцій;

колишніх співробітників, які залишилися незадоволені ставленням до компанії. Вони можуть намір передати секретні дані конкурентам з метою завдати шкоди своїм колишнім колегам та роботодавцям;

невдалих переговорів з іншими компаніями. Часто в процесі ділових переговорів з потенційними партнерами необхідно відкрити завісу конфіденційності та поділитися будь-якими даними або напрацюваннями. У разі зриву переговорів інформація залишається в іншої сторони, яка може

вчинити з нею несумлінно і використовувати її на шкоду своєму потенційному партнеру.

Щоб уникнути негативних наслідків, рекомендується розробити рівні захисту інформації. Це означає, що секретні дані мають бути розподілені за пріоритетністю. Інформація з найвищим пріоритетом таємності має бути доступна лише декільком високопоставленим особам компанії, наприклад, власнику та бухгалтеру. У міру зменшення пріоритету доступ до даних можуть отримувати співробітники різних відділів. Конфіденційна інформація – це один із видів інформації, тому доцільним є розглянути спочатку категорію «інформація» як родове поняття стосовно категорії «конфіденційна інформація» [16].

Поняття інформації (лат. Informatio – роз'яснення, виклад, тлумачення, подання, повідомлення) – приблизно до 40-х рр. XX ст. було синонімом поняттям «дані», «відомості», «повідомлення», «сукупність знань про навколишній світ». Водночас з початку 1950-х рр. воно стало активно розвиватися і збагачуватися і поступово перетворилося на загальнонаукову категорію, що надає методологічний вплив на розвиток різних наук. Ряд вчених вважає, що поняття інформації як таке використовується у тих випадках, коли воно пов'язується з можливістю передачі (отримання) відомостей про осіб, предмети або, навпаки, із забороною на її передачу (отримання) третім особам (третіми особами) [32].

На етапі розвитку нашого суспільства та держави виникла нагальна необхідність правового регулювання особливого роду відносин, об'єктом яких виступає інформація. Визнання особливої ролі інформації призвело до того, що багато вчених почали висловлюватися за виділення особливої комплексної галузі інформаційного права та прийняття Інформаційного кодексу. У зв'язку з виконанням трудових функцій працівник може отримати доступ до найрізноманітнішої інформації роботодавця, зокрема складової його комерційної таємниці або комерційної таємниці його контрагентів. У цьому випадку стосовно працівника ця секретна інформація виступатиме і в ролі

трудової (службової) таємниці і працівник буде зобов'язаний дотримуватися режиму конфіденційності.

Щоб зрозуміти природу трудових відносин щодо комерційної таємниці або конфіденційної інформації, необхідно досліджувати їх сутність. Складність дослідження полягає в тому, що інформація, що становить комерційну таємницю, позначається різними термінами: «комерційна таємниця», «службова таємниця», «секрети виробництва», «торговельні секрети», «таємна бізнес-інформація», «технічні секрети», «виробничі секрети», «конфіденційна комерційна інформація», «ноу-хау», «промислова таємниця», «секрети промислу» тощо [27].

Комерційна таємниця може розглядатися як правовий інститут, що представляє собою сукупність правових норм, що регулюють суспільні відносини з приводу інформації, що представляє реальну або потенційну комерційну цінність через її невідомість третім особам, до якої надається доступ на законній підставі та власник якої вживає заходів до охорони її конфіденційності. Крім того, комерційна таємниця може розглядатися як інформація, тобто як об'єкт цивільних прав [28, с. 13–15].

Комерційна таємниця – це інформація і їй притаманні всі властивості інформації як об'єкта права. Визначаючи властивості, характер самої комерційної таємниці як об'єкта, варто насамперед відзначити, що комерційна таємниця – це інформація. І саме тому їй притаманні всі риси, властиві нематеріальному об'єкту, зміст якого складають відомості: можливість одночасного використання необмеженим колом осіб, відсутність фізичного зношування, можливість «морального зношування»; легкість та простота тиражування та перетворення форм фіксації; неможливість відчуження від людини, яка зробила інформацію або в користуванні якої вона опинилася, тощо. Процес контролю над поширенням інформації вкрай утруднений [28].

Комерційна таємниця це не просто інформація, а один із видів конфіденційної інформації, і тому їй властиві загальні ознаки конфіденційної інформації, такі як секретність, невідомість широкому колу осіб; вжиття

власником інформації заходів, спрямованих на охорону інформації від розголошення; довірчий характер, який пояснює суворо цільове її використання за наявності згоди правовласника; можливість порушення прав та законних інтересів власників інформації та суспільства, а також заподіяння збитків у разі розголошення відповідних конфіденційних відомостей. Однак досі серед дослідників точаться суперечки з приводу того, що слід розглядати як комерційну таємницю. В основі розбіжності лежать різні тлумачення та підходи до визначення поняття «таємниця», що використовується для позначення досліджуваного правового явища [28].

Виявлення та регламентація реального складу інформації, що становить цінність для підприємства – основні частини системи захисту інформації. Склад цінної інформації фіксується у спеціальному переліку, що визначає період та рівень її конфіденційності, список співробітників підприємства чи фірми, яким надано право використовувати ці відомості у роботі. Перелік, основу якого становить типовий склад відомостей підприємств даного профілю, що захищаються, є постійним робочим матеріалом керівництва підприємства, служби безпеки та підрозділу конфіденційного діловодства. Він являє собою класифікований список типової і конкретної цінної інформації про роботи, виробленої продукції, наукових і ділових ідеях, технологічних нововведеннях.

Крім того, до переліку включається службова інформація, інформація персонального характеру тощо. Може бути окремо сформульований перелік відомостей, що становлять конфіденційну інформацію організації, підприємства, фірми. Переліки формуються індивідуально кожним підприємством відповідно до рекомендацій спеціальної комісії та затверджуються керівником підприємства. Ця ж комісія регулярно вносить поточні зміни до переліків відповідно до динаміки виконання конкретних робіт. Додатково може складатися перелік документів, у яких ці відомості відображаються (документуються).

Захист галузевої конфіденційної інформації (службової та комерційної) регламентується нормативними документами та переліками, що діють у галузі.

Для роботи зі складання Переліку має залучатися широке коло експертів та посадових осіб відділів, служб організації для того, щоб жоден з можливих напрямів її діяльності не був упущений під час його розробки. Керівництво роботою з формування Переліку, як правило, покладається на начальника служби безпеки (заступника за режимом) підприємства [35? С. 373–376].

Для безпосереднього формування Переліку на підприємстві повинна створюватися експертна комісія (далі – ЕК), що комплектується найбільш кваліфікованими співробітниками та фахівцями зі структурних підрозділів. ЕК має здійснювати аналіз усіх сторін діяльності підприємства в цілому та підпорядкованих йому підрозділів окремо, а також координувати питання, що стосуються їх спільних дій щодо формування Переліку, шляхом узагальнення пропозицій, що надходять.

Робота з формування Переліку та визначення відомостей, що становлять службову або комерційну таємницю, повинна складатися з наступних етапів: • складання попереднього переліку відомостей, що містять службову чи комерційну таємницю, для структурних підрозділів (відділів, служб) підприємства; • визначення можливої шкоди, що настає внаслідок несанкціонованого поширення відомостей, що включаються до Переліку; • визначення переваг відкритого використання даних у порівнянні з закритим; • визначення витрат на захист даних; • складання узагальненого Переліку та розгляд його на засіданні ЕК; • оформлення результатів роботи з формування Переліку.

Експертна комісія має визначити види можливої шкоди, які можуть бути завдані інтересам діяльності організації у разі несанкціонованого розповсюдження відомостей, що включаються до узагальненого Переліку [35]. Можливі збитки повинні оцінюватися з використанням якісних або кількісних показників, що впливають на стан захисту відомостей, що охороняються, і виключають можливість нанесення організації моральної, матеріальної, виробничої, фінансової та іншої шкоди. Ці показники повинні оцінюватися шляхом реального визначення розмірів збитків, які можуть виникнути

внаслідок несанкціонованого поширення відомостей, що включаються до остаточного варіанта Переліку [35].

Отже, склад конфіденційної інформації в організаційних документах може бути складником економічної безпеки держави чи окремого підприєстваю. Безпека такої інформції досягається за рахунок використання комплексу систем, методів та засобів захисту інформації від можливих зловмисних дій конкурентів та з метою збереження її цілісності та конфіденційності.

2.3. Технології і методи захисту конфіденційної інформації в організаційних документах

Сучасні технології захисту конфіденційної інформації в організаціях включають широкий спектр рішень, орієнтованих на ефективність, конфіденційність, цілісність та доступність інформації. Для паперових документів характерна традиційна технологія захисту документів, яка характеризується низкою завдань роботи:

– захист від несанкціонованого доступу до документів сторонніх осіб;

– безпечне збереження документів, що підлягають захисту;

– забезпечення збереження таємниці організації, що представлена у захищеному документообігу [66, с. 16].

Захищеність паперового документообігу починається з моменту отримання чи створення документа. Тут використовуються прийоми і методи роботи з документами. Також на документі, що потребує захисту, проставляють спеціальну відмітку (гриф). Це дає можливість відрізняти документи загальні від захищених. Документи відповідно до грифу поділяють на окремі групи що формують документні потоки за рівнем їх захищеності [39, с. 359]. Важливо визначити чи документ є публічним чи захищеним та вчасно проставити

відповідний гриф, який виступає головним елементом захисту. Гриф захищеності забезпечує надійність збереження таємниці певної установи чи організації, незалежно від того чи таємниця стосується лише приватного підприємства чи це інформація, що належить до державної таємниці [44, с. 62].

Варто звернути увагу на те, що гриф конфіденційності сам по собі не захищає документ. Він виступає рушієм для правильної організації роботи з документами та вимагає розробити схему доступу до документів посадових осіб, що мають право доступу до захищеної інформації.

Уся службова документація поділяється на види відповідно до сфери використання. Тому на кожному виді документа проставляється різна відмітка грифу конфіденційності. Так, на документах, що відносяться до питань мобілізації додатково проставляється відмітка «М». Документи, що потребують криптографічного захисту інформації містять відмітку «К». Відмітка «СІ» відповідно ставиться на документах, що містять спеціальну інформацію. Гриф конфіденційності дає можливість не тільки захищати документообіг під час його обробки та використання чи передачі, а й під час архівного зберігання. Документи з обмеженим доступом, у дому числі з конфіденційною інформацією, відносять до документів, що потребують особливих умов зберігання. Відповідно до відміток документи формують у справи, які у свою чергу у архівні фонди та зберігають в спеціальних сейфах, шафах та кімнатах архіву, які закриваються на ключ та потребують захисту з використанням систем спостереження та сигналізації [46].

Сучасними технологіями захисту документної інформації є латентні елементи захисту, блокчейн-технології, гільйошні захисні сітки, а також криптографічні водяні знаки. Розглянемо кожну технологію захисту детальніше. Дослідники вважають, що використання латентних елементів в контексті багатовимірного аналізу документів чи тексту може служити для створення «пасивного» захисту, який ускладнює зрозуміння змісту документів. Моделі автоенкодерів, наприклад, можуть вивчати латентні представлення, що ускладнює витягнення інформації з документа без відповідного декодування.

Латентні елементи, отримані в результаті роботи алгоритмів аналізу документів, можуть використовуватися як ключі для шифрування. Такий підхід дозволяє забезпечити конфіденційність інформації, зберігаючи секретні латентні параметри [43, с. 32–34]. Латентні елементи також можуть бути використані для створення ідентифікаторів чи «цифрових відбитків» документів, які потім використовуються для контролю доступу. Наприклад, при використанні в контексті блокчейн-технологій, латентні елементи можуть бути використані для генерації унікальних хеш-кодів для документів. Важливо відзначити, що конкретний підхід до використання латентних елементів для захисту документів буде залежати від конкретних вимог і контексту застосування. Також, при використанні технологій, пов’язаних з латентним аналізом, слід враховувати етичні та правові питання, пов’язані з обробкою та зберіганням даних.

Наступною технологією захисту конфіденційної інформації в документообігу є блокчейн-технології. Застосування блокчейн-технологій для захисту документів надає ряд переваг у забезпеченні безпеки, цілісності та автентифікації інформації [30, с. 155]. Наведемо кілька способів, які можуть використовуватися для захисту документів за допомогою блокчейн-технологій. Першим способом є неможливість фальсифікації документів. Тобто блокчейн працює таким чином, щоб забезпечити невіддільність блоків, що включають інформацію, і підписується за допомогою криптографічних хеш-функцій. Це робить надмірно складним зміну документа чи внесення будь-яких фальсифікацій. Документна інформація в блокчейні зберігається на різних комп’ютерах у мережі. Це ускладнює можливість атаки на централізовані ресурси і зменшує ризик втрати документів чи доступу до них внаслідок атак на систему. **С**март-контракти – це програмні коди, що виконуються автоматично при виконанні певних умов. Вони можуть використовуватися для автоматизації процесів, таких як підписання документів чи здійснення транзакцій, що робить процес більш безпечним і ефективним.

Як і інші технології захисту, блокчейн у процесі своєї роботи використовує криптографічні методи для забезпечення безпеки та конфіденційності. Кожен блок підписується приватним ключем, і ці підписи важко підробити. Кожен процес передачі документів в блокчейні залишає слід, і інформацію можна трасувати від початку до кінця. Це полегшує аудит та визначення, хто, коли і як вносив зміни до документів чи транзакцій.

Блокчейн-технологія передбачає використання цифрових підписи для ідентифікації користувачів мережі та підтвердження їх прав доступу. Це забезпечує аутентифікацію та авторизацію. Застосування блокчейн-технологій для захисту документів дозволяє створити довірену та безпечну інфраструктуру для обміну даними та ведення електронних записів. Однак важливо ретельно розглядати конкретні вимоги та вибрати ефективні блокчейн-рішення для потреб тої чи іншої структури [4].

Ще однією технологією захисту документів з обмеженим доступом є криптографічні водяні знаки. Такі водяні знаки представляють собою технологію, яка використовує криптографічні методи для вбудовування унікальної інформації в документ з метою захисту від підробок. Криптографічні водяні знаки можуть бути вбудовані в документ шляхом генерації унікального хеша або цифрового підпису. Ці дані можуть бути засекречені і важкодоступні для підробки. Якщо документ змінюється, це стає відомим під час перевірки криптографічного водяного знака [20; 58].

Використання криптографічних водяних знаків може включати секретну інформацію в саму структуру документа, яка може бути важкодоступною для зміни або видалення. Наприклад, це може бути спеціально форматований текст чи код, який може виглядати як частина документа, але при цьому містити приховану криптографічну інформацію. Водяні знаки можуть бути вбудовані також у графічний матеріал документа, наприклад, у зображення чи фотографії. Це може включати в себе криптографічно підписані або зашифровані елементи, які можуть бути візуально непомітними для звичайного спостереження. Варто відмітити, що використання для захисту документів конкретних

криптографічних алгоритмів для вбудовування водяних знаків може додатково забезпечити безпеку. Наприклад, електронні цифрові підписи або алгоритми стеганографії можуть бути використані для більшої захищеності інформації в документах. Загалом, криптографічні водяні знаки можуть використовуватися для захисту документів шляхом вбудовування унікальної інформації, яка важко підробити, змінити або видалити без виявлення [58, с. 230].

Гільйош – технологія, що використовується для додавання захисту та елемента важкодоступності до документа. Спеціально виготовлені гільйоши можуть бути вбудовані в папір або інший матеріал документа для створення водяного знака. Цей знак може бути видимим або невидимим і використовувати особливості гільйошу для додаткового захисту від підробок. Гільйоши можуть бути використані як захисні елементи, які вбудовуються в сам документ чи його пакет. Це може включати гільйоши з унікальними номерами, кодами чи іншими ідентифікаторами, які можна використовувати для валідації або трасування [22].

Гільйоши можуть також виступати як елементи аутентифікації, які підтверджують валідність документа. Такі вони можуть бути дуже складними для відтворення і дозволяють легко визначити оригінал від підробки. Вони можуть використовуватися для захисту від незаконного копіювання чи відсканування документа. Унікальні або складні гільйоши можуть ускладнити спроби створити вірний дублікат. Спеціальні або унікальні гільйоши можуть служити як маркери часу для визначення моменту виготовлення документа. Це може бути важливим для визначення часового підпису або інших справжніх даних. Гільйоши можуть додавати фізичний та візуальний елемент захисту, що ускладнює підробку та надає можливості для валідації аутентифікованого документа. Тому їх роль в захисті документа є дуже значною в установі.

Однією з найважливіших технологій захисту документної інформації є впровадження електронного документообігу. Як і на паперових носіях, електронні документи потребують особливого захисту від несанкціонованого

доступу. Захист документної інформації тут здійснюється за допомогою програмних та апаратних засобів захисту [20].

Програмні засоби забезпечують захист від редагування. За допомогою встановлення індивідуальних паролів до входу в програму, де зберігається той чи інший документ, лише автор документу може внести зміни в документ. Користувачі можуть лише знайомитись з текстом документа без права їх редагування.

Апаратні засоби захисту включають в себе спеціальні ключі захисту. Це можуть бути спеціальні пристрої чи картки, в яких вмонтовано програму доступу до захищеного комп'ютера чи системи, де є конфіденційні документи. До апаратних засобів також відносять біометричні технології захисту. Суть таких технологій полягає у ідентифікації посадової особи, що має права доступу до документів з обмеженим доступом. Ідентифікація проводиться відповідно до ознак людини – голосу, відбитку пальця, розпізнавання обличчя тощо [20].

Важливе значення для захищеності документообігу має електронний цифровий підпис. Електронний цифровий підпис (ЕЦП) – це технологія, яка використовується для забезпечення аутентифікації, цілісності та невідмінності електронних документів чи повідомлень. Він використовує криптографічні методи для створення унікального «підпису», який може бути перевірений іншими сторонами для підтвердження того, що документ не був змінений і що він походить від певного власника. Для більш глибшого вивчення системи роботи ЕЦП, слід розглянути його основні властивості [26, с. 156]. Першою ознакою ЕЦП є аутентифікація особи. Вона полягає в тому, що ЕЦП дозволяє ідентифікувати особу, яка створює підпис, забезпечуючи впевненість в тому, що тільки правомірний власник ключа використовує його для підпису. Це дозволяє захистити документну інформацію від несанкціонованого доступу в межах установи чи організації.

Цілісність документа – наступна властивість ЕЦП. Підпис дозволяє перевірити, чи був документ змінений після того, як був підписаний. Якщо

документ зазнав змін, його підпис вже не буде вірогідним. Це дає змогу виявити хто змінив документ та як відбувся витік інформації з обмеженим доступом. Ще однією ознакою ЕЦП є невідмінність. Підпис не може бути переданий або підроблений без знання особи, яка володіє відповідними приватними ключами. Тобто для кожного працівника створюється ключ до ЕЦП, за допомогою якого лише вона може передати іншим працівникам на доопрацювання документ. І дані посадові особи повинні бути наділені спеціальними повноваженнями для можливості роботи з захищеними документами [20].

Криптографічна безпека в ЕЦП є також важливою складовою в захищеності документообігу. Використовуючи алгоритми криптографії, такі як RSA чи ECDSA, електронний цифровий підпис забезпечує високий рівень безпеки і стійкість до різних атак. Зміст даних алгоритмів полягає в тому , що в криптографії використовується пара ключів: публічний та приватний. Публічний ключ може бути розданий будь-якому, хто хоче надіслати вам зашифроване повідомлення або перевірити ваш цифровий підпис. Приватний ключ потрібно держати в секреті, і він використовується для розшифрування повідомлень або створення цифрових підписів. Ці алгоритми використовуються в різних криптографічних протоколах і системах зберігання інформації для забезпечення її конфіденційності, цілісності та аутентифікації у системах електронного документообігу [69].

Наступна ознака – зручність та ефективність. ЕЦП забезпечує процес підписування та перевірки підпису електронних документів швидким та зручним, що особливо важливо в сучасному цифровому середовищі. Це скорочує терміни виконання документів та спрощує роботу з документами. Правовий статус ЕЦП. Багато країн надають юридичну силу електронним цифровим підписам, роблячи їх юридично визнаними для різних електронних та правових транзакцій. В Україні ЕЦП має таку ж юридичну силу, як і особистий підпис. Порядок та вимоги до роботи з ЕЦП регламентовані в Законах України «Про електронні документи та електронний документообіг» та

«Про електронні довірчі послуги». Тобто, ЕЦП має свої гарантії захисту на державному рівні [69]. Загалом можна зазначити, що електронний цифровий підпис є ефективним і надійним засобом захисту документів у цифровому середовищі, забезпечуючи безпеку та вірогідність інформації.

Отже, використання технологій захисту дає змогу зберегти цінність документів в установі, що дає можливість безпечному її функціонуванню.

Основні методи забезпечення інформаційної безпеки для сталого захисту даних фізичних осіб, організацій, устапнов чи держави загалом поділяються на:

1. *Базові засоби захисту електронної інформації*. До них відносять програми антивірусного захисту, системи захисту електронної пошти співробітників, які автоматично видаляють небажані та підозрілі листи з поштових скриньок. Також потрібно забезпечити роботу обмеженого списку осіб, які мають право систематично змінювати паролі та шифри [20].

2. *Фізичні засоби захисту*. У цьому випадку йдеться про територіальний захист всієї організації та окремих зон, що особливо охороняються, всередині приміщення. До них відносять контрольно-пропускні пункти на в'їзд, ідентифікаційні дозволи на вхід до особливо секретних приміщень, які ретельно охороняються, у тому числі шляхом встановлення перепон новітніх інформаційних обмежень. Тобто, за такої системи є певний перелік осіб, яким дозволено увійти до приміщення, а сторонні особи легально увійти всередину не зможуть. Часто для такого контролю використовують карти HID.

3. *Резервне копіювання даних*. У цьому способі головний сенс у тому, що для того, щоб у разі витоку інформації не втратити її повністю та мати можливість подальшого функціонування організації, необхідно зберігати інформацію не тільки безпосередньо на комп'ютері, але й на зовнішніх носіях або на сервері. У разі конфіскації документації або інших важливих інформатизованих даних організація чи устанва зможе не припиняти роботу та мати доступ до всіх своїх документів. Найбільш зручним є зберігання інформації в «хмарі». З її допомогою користувач має можливість у будь-який

час і в будь-якому місці скористатися своїми даними без фактичного знаходження в приміщенні з автоматизованою системою [10, с. 107–111].

4. *Анти-DDoS.* Тут необхідно розуміти, що найповніший захист від DDoSатак можуть забезпечити лише розробники програмного забезпечення шляхом вшивання цієї послуги безпосередньо у ПЗ. Ця послуга самостійно розпізнає та блокує всі небезпечні операції, що надходять ззовні. Самостійний захист від такого виду атак неможливий, оскільки користувач розуміє, що DDoS-атаки відбуваються лише після отримання несприятливої події. Головна перевага такого захисту полягає в тому, що всі процеси в організації проходять безперешкодно і без збоїв. Ця послуга буде працювати аж до того моменту, поки користувач не змінить програмне забезпечення.

5. *Шифрування даних електронної інформації*. В цьому випадку для засекречування інформації, що передається користувачам, необхідно користуватися відповідними програмами, які дозволяють підтвердити певну особистість і справжність інформації при передачі або зберіганні, яка передається по каналах зв'язку і при цьому захищена від нелегального доступу [20].

6. *Аварійне відновлення даних*. Необхідно завжди мати план дій у разі втрати даних чи доступу до них. Це насамперед для того, щоб уникнути простою виробництва чи діяльності організації. Цей метод може забезпечити організації скорочення часу очікування на відновлення доступу до інформації [21].

Таким чином, захист інформації повинен працювати безперебійно, постійно підлаштовуючись під зміни систем, а також у комплексі та взаємов'язку усіх елементів, які працюють на недопущення несанкціонованого використання конфіденційної інформації. Для того, щоб керівнику установи зробити максимально стійкий та безпечний стан на ринку, необхідно використовувати всі перераховані вище методи. Фахівець з компєютерної чи інформаційної безпеки – це професіонал у галузі IT-технологій, який забезпечує цілісність та конфіденційність інформації шляхом тестування системи на

предмет уразливостей, а також детально опрацьовуэ всі виявлені проблеми за допомогою захисних програм [20]. Для забезпечення інформаційної безпеки компаній та держави всередині організаційної структури створюються окремі департаменти чи комітети захисту інформації, де працюють фахівці з відповідною освітою. Серед них:

1. Пентестери. Їх ще називають «етичними» хакерами. Такі фахівці на законних підставах зламують систему замовника і таким чином шукають уразливості, які згодом разом із розробниками усувають.

2. Фахівці із розробки. Вони беруть участь у процесі створення програм та додатків, працюють тільки з готовими кодами та шукають у них помилки і можливі канали витоку інформації.

3. Фахівці з мереж. Вони займаються пошуком можливих та відомих уразливостей в обладнанні та мережевих системах. Простіше кажучи, вони знають, як злочинець може потрапити на ваш комп’ютер за допомогою Windows, Linux або інших систем і встановити необхідне програмне забезпечення. Такі фахівці можуть знайти слабкі місця відповідної програми, встановити причину несанкціонованого проникнення у програму, створити систему, в яку буде складно проникнути.

Різними способами провідні країни світук досить ефективно реалізують національну політику інформаційної безпеки. Найсучасніші та найнадійніші системи захисту інформації діють у Сполучених Штатах Америки, Ізраїлі, Німеччині, Великій Британії та Китаї. Ці країни постійно перебувають під сильним зовнішнім інформаційним впливом і тому змушені створювати національні системи захисту. Останні мають досить активну складову, завдяки якій можна проводити інформаційні та психологічні заходи та кібер-атаки проти країн-противників. Система інформаційної безпеки Сполучених Штатів Америки є особливо ефективною. Її система має достатню широку основу, яка охоплює всі сфери життєдіяльності, через що вона досить багатовимірна, і водночас контрольована відповідними органами [27, с. 62–63].

Країни європейського континенту, які мають досить високий рівень життя, також приділяють багато уваги розвиткові інформаційної безпеки, ґрунтуючись на власній національній політиці та принципах захисту населення від неминучих у сучасному інформаційному суспільстві загроз і небезпек.

Так, у Франції сфера забезпечення інформаційної безпеки разом із інформаційним сектором є дуже важливою сферою життя разом із економікою, політикою та культурою. У цій державі інформаційна сфера має такий же високий рівень захисту, як і інші сфери життєдіяльності. Звідси можна дійти висновку, що саме тут концепція сучасної багатовекторної геостратегії французької правлячої еліти відбиває новий елемент, що безпосередньо впливає на оперативне прийняття рішень державних чи недержавних організацій, ЗМІ, і навіть національних спеціальних служб, що беруть участь у процесі впровадження державних програм і стратегій. Інформаційний простір Франції вважається одним із пріоритетних об’єктів захисту, що забезпечуються всіма можливими законодавчими, організаційними, адміністративними, владними та інформаційними технологіями. Уряд Китайської Народної Республіки у цьому питанні менш демократичний, ніж правлячі структури США та Франції [33; 38].

В інформаційній політиці КНР переважають принципи впровадження досить моноцентричних, оборонних та наступальних доктрин. Стратегія Китаю здебільшого спрямована на інтеграцію у світову спільноту сфери інформаційної безпеки, приймаючи політику, що має демократичну орієнтацію як фактор модернізації політичної системи КНР та її потенційного лідерства на регіональному та міжнародному рівні. Проект під назвою «Велика китайська інформаційна стіна» на даний момент прийнято та діє в Китаї. Він спрямований на фільтрацію всієї інформації, що проходить технічними каналами та соціальними мережами країни.

Китайська Народна Республіка демонструє відносно успішні результати всередині своєї державної стратегії, охоплюючи весь практичний масив інформації як усередині країни, так і спрямованої за кордон. Враховуючи, що у

Китаю своя власна, ні на які інші не схожа модель стратегії, то країна поступово досягає успіху, виконуючи завдання з виходу на провідні позиції серед великих гравців світової арени у сфері інформаційної безпеки, створюючи конкуренцію навіть Сполученим Штатам Америки. Питання захисту персональних даних, регульовані в багатьох країнах, заслуговують на особливу увагу у сфері правового забезпечення інформаційної безпеки [21].

Таким чином, у світі є країни з різними традиціями державного управління, які ефективно реалізують національну політику інформаційної безпеки у різний спосіб: від створення систематизованої нормативної бази до використання різних матеріальних ресурсів. Вивчаючи успішний досвід провідних країн світу, можна отримати висновки і досвід, які позитивно можуть вплинути на вирішення багатьох проблем, які існують сьогодні у сфері безпеки інформаційного простору України. Україна встановила загальнодержавну систему заходів, які охоплюють організаційно-правові, інженерно-технічні, криптографічні та оперативні аспекти, спрямовані на запобігання порушенням захисту інформації. Розгляд цієї системи з організаційно-правового погляду можливий у науково-практичному вимірі, враховуючи закономірності та положення науки соціального управління.

ВИСНОВКИ

Відповідно до поставлених у кваліфікаційній роботі завдань можна зробити наступні висновки.

Проблема захисту документної інформації від несанкціонованого доступу є актуальною у світі, що швидко розвивається, і де вірогідність кіберзагроз та порушення безпеки даних значно зростає. Державне регулювання захисту документообігу визначається законодавчими актами та стандартами, які встановлюють вимоги до збереження, обробки та передачі інформації. Державні органи виступають в ролі контролерів і забезпечують виконання встановлених норм. Варто звернути особливу увагу на створення потужних державних цифрових систем та платформ роботи з документами та персональними даними, що прискорює процес документообігу та реалізує захищену інформаційну державу.

Законодавча база України включає ряд актів, таких як Закони «Про інформацію», «Про захист персональних даних», «Про державну таємницю», «Про електронний документ та електронний документообіг» тощо. Ці акти встановлюють правила та вимоги для забезпечення захисту інформації, що задокументована на матеріальному носії. Варто зазначити, що органи державної влади у сфері інформаційної безпеки створюють, удосконалюють різні стратегії та програми захисту документів в електронній формі, а також розробляють нормативно-правову базу для контролю за захистом інформації.

Створення умов для збереження конфіденційних документів і запобігання витоку інформації – це основа конфіденційного діловодства в будь-якій організації. Цей процес включає в себе ряд заходів: створення відділу, що відповідає за обробку та зберігання конфіденційної інформації, встановлення його структури, кадрового складу та функцій; розробка правил та інструкцій для працівників; надання відповідних робочих умов; підготовка та навчання персоналу. Цей підрозділ може бути частиною служби безпеки або іншого відділу, що відповідає за захист інформації. Назва, структура та функції

підрозділу конфіденційного діловодства визначаються керівником організації з урахуванням обсягу робіт з документами та загальної структури компанії. Кількість працівників у цьому підрозділі повинна бути достатньою для ефективного виконання завдань.

Основні завдання та функції підрозділу конфіденційного діловодства, а також права та обов'язки його керівника мають бути визначені у положенні про цей підрозділ, а права та обов'язки співробітників – у посадових інструкціях, які розробляються для кожної посади. У посадових інструкціях можуть також встановлюватися кваліфікаційні вимоги до співробітників.

Положення про підрозділ конфіденційного діловодства та посадові інструкції є документами, що регламентують діяльність цього підрозділу та його співробітників. При визначенні завдань та функцій підрозділу конфіденційного діловодства необхідно враховувати його участь у всіх заходах щодо запобігання втраті та витоку конфіденційної інформації, а також навчання виконавців та користувачів правилам роботи з конфіденційними документами. При розробці посадових інструкцій слід враховувати спеціалізацію співробітників та нормативи часу на роботи, а також встановлювати відповідальність за збереження конфіденційних документів та інформації.

Підрозділ, що відповідає за конфіденційне діловодство, повинен мати відповідне приміщення для зберігання документів і роботи персоналу, а також для виконавців, якщо їхня робота з конфіденційними документами не може відбуватися в їхніх основних робочих приміщеннях. Це приміщення повинно мати належні умови для праці, щоб забезпечити продуктивність роботи та здоров'я працівників.

Захищений документообіг – це система організаційних та технічних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації в процесі обігу документів. Вона включає в себе контроль доступу, шифрування, аутентифікацію та інші заходи для запобігання несанкціонованому доступу. Захисту потребують документи на різних матеріальних носіях, що містять особливо цінну інформацію.

Для збереження та захисту конфіденційних документів повинні застосовуватися всі необхідні заходи, такі як друкування, облік, зберігання, передача, відправлення, систематизація, перевірка наявності та утилізація документів. Функції виконавців та користувачів конфіденційних документів обмежуються підготовкою документів та їх обробкою.

Сучасні технології захисту є досить надійними та включають в себе електронні цифрові підписи, криптографічні водяні знаки, захищені з'єднання, блокчейн-технології та системи контролю доступу. Ці технології дозволяють ефективно захищати документи в електронному вигляді. Проте з розвитком новітніх технологій методи та засоби захисту документів з обмеженим доступом потребують оновлення, удосконалення, замінb, створення нових технологій, які б протистояли загрозам інформаційної безпеки та допомогли зберегти цінність та важливість захищеної інформації. Загалом, розуміння і впровадження комплексного підходу до захисту документів в умовах сучасного інформаційного суспільства, дотримання законодавчих вимог та використання передових технологій для забезпечення безпеки і конфіденційності інформації є основним підґрунтям для діяльності та функціонування установ та організацій різних форм власності для забезпечення розвитку держави в усіх сферах діяльності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Актуальні проблеми забезпечення інформаційної безпеки держави: матеріали наук.-практ. конф., Київ, 20 березня 2009 р. / Упоряд. В. П. Мікулін. Київ : Національна академія Служби Безпеки України, 2009. 200 с.
2. Архипов О. Е., Ворожко В. П. Системні аспекти оцінювання рівня важливості секретної інформації : монографія. Київ : Юстініан, 2007. 152 с.
3. Вимоги до роботи з конфіденційною інформацією установи. *Баланс-Бюджет.* 2020. № 51. Режим доступу: https://balance.ua/news/post/trebovaniya. (дата звернення: 23.04.2024).
4. Ворса Р. В. Система забезпечення цілісності електронних документів на основі технології блокчейн. 2021 р. Режим доступу: : https://dspace.nau.edu.ua/bitstream/NAU/55899/1/ (дата звернення: 23.04.2024).
5. Габович А. Г., Головань С. М., Жлобін С. І., Хорошко В. О. Організація конфіденційного діловодства : підруч. Київ : ДУІУТ, 2005. 376 с.
6. Глухівський Л. Державна таємниця та охорона прав на винаходи. *Інтелектуальна власність*. 2005. № 9. С. 289.
7. Глущик С. В. Сучасні ділові папери. Навч. посібник для сер. спец. навч. закладів. 3-тє видання, пер. і доп. Київ : А.С.К., 2002. 400 с.
8. Головань С. М. Загальне діловодство та ведення документів, що містять інформацію з грифом «Для службового користування». Навч.-метод. посіб. Київ : НАУ, 2003. 92 с.
9. Головань С. М., Мелешко О. О., Щербак Л. М. Концепція створення системи електронних документів. *Захист інформації*. 2005. № 2. С. 63-67.
10. Головань С. М., Давиденко А. М., Щербак Л. М. Процеси оцінки безпеки електронного документообігу. *Захист інформації*. 2005. № 4. С. 107-111.
11. Головань С. М., Давиденко . М., Хорошенко В. О., Щербак Л. М. Організація роботи підрозділу захисту інформації з обмеженим доступом. *Захист*

інформації. 2006. № 1. С. 79-82.

12. Головань С. М., Поповський В. В., Хорошко В. О. Конфіденційний документообіг : навч. посіб. Київ : ДУІКТ, 2007. 264 с.
13. Голубенко О. Л., Хорошко В. О., Петров О. С., Головань С. М. Конфіденційне діловодство : підручник. Луганськ : СНУ ім. В. Даля, 2009. 208 с.
14. Голубенко О. Л., Хорошко В. О., Петров О. С., Головань С. М. Конфіденційне діловодство. Практикум : навч. посіб. Луганськ : СНУ ім. В. Даля, 2010. 180 с.
15. Гонгало С. Й. Поняття документів, їх види, способи розпізнання та захисту. *Наукові записки*: *Серія «Право»*. 2006. № 7. Острог : Видавництво НаУ «Острозька академія», 2006. С. 153–159.
16. Горбенко І. Д., Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах. Навч. посіб. Ч.1. Криптографічний захист інформації. Харків : ХНУРЕ, 2004. 368 с.
17. Григоренко О. Г., Голуб О. С. Конфіденційність даних в інфокомунікаційних мережах і засоби їх забезпечення. Перспективи телекомунікацій. Київ : КПІ ім. Ігоря Сікорського, 2021. Режим доступу: https://its.kpi.ua/sites/default/files/NDI%20TK%202021.
18. Гуцалюк М. В. Організація захисту інформації. Навчальний посібник. 2-е вид., перероб. та допов. Київ : Альтерпрес, 2011. 308 с.
19. Дідук А. Г., Смірнов О. Г. Захист комерційної таємниці за допомогою законодавства про недобросовісну конкуренцію. *Сучасне право в епоху соціальних змін. Матеріали XI Міжнародної наук.-практ. конф.* (Київ, 26 лютого 2021 р). Тернопіль : Вектор, 2021. С. 77–81.
20. Дмитренко Т. А., Деркач Т. М., Воронюк Н. П. Впровадження системи електронного документообігу як засіб підвищення інформаційної безпеки підприємства. *Тези 70-ої наукової конференції професорів, викладачів, наукових працівників, аспірантів та студентів університету*, (Полтава, 23 квіт. – 18 трав. 2018 р.). Полтава : ПолтНТУ, 2018. Т. 2. С. 235–236.

21. Дрейс Ю. О. Підхід до аналізу і оцінки ризиків захисту персональних даних в державних автоматизованих системах. *Зб. тез 68-ї науково-технічної конференції,* 4-6 грудня 2013. Одеса : ОНАЗ ім. Попова, 2013. С. 114–120.
22. Дурняк Б. В., Музика Д. В., Сабат В. І. Стеганографічні методи захисту документів. 2014. Режим доступу: http://elar.nung.edu.ua/bitstream/123456789/5123/1/6664s. (дата звернення: 04.04. 2024).
23. Загорецька О. Особливості роботи з документами, що містять комерційну таємницю підприємства. *Довідник кадровика*. 2011. № 9 (111). С. 40–46.
24. Захист інформації. Технічний захист інформації. Основні положення : ДСТУ 3396.0-96. Київ : Держкомстандарт України, 1996. 26 с.
25. Захист інформації. Технічний захист інформації. Порядок проведення робіт: ДСТУ 3396.1-96. Київ: Держкомстандарт України, 1996. 18 с.
26. Зінковський Ю. Ф., Танцюра Д. В. Надійність захисту інформації системи електронного цифрового підпису. *Вісник НТУУ КПІ. Серія Радіотехніка. Радіоапаратуробудування.* 2007. № 34. С. 156–163.
27. Князєв С. Правові основи використання «ноу-хау» в Україні під час здійснення комерційної діяльності. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2008. Вип. 1(16). Режим доступу: https://ela.kpi.ua. (дата звернення: 30.04.2024).
28. Князєв С. О. Комерційна таємниця в Україні: особливості організаційно-правового впровадження. *Юридичний журнал*. 2006. № 5. С. 13–17.
29. Коваленко О. О. Парадокс правового регулювання охорони комерційної таємниці у трудових відносинах. *Сучасний стан забезпечення трудових прав і прав у сфері соціального забезпечення та перспективи його поліпшення : матеріали IX Всеукр. наук.-практ. конф.,* Харків, 4 черв. 2021 р. / Харків. нац. ун-т внутр. справ ; за заг. ред. К. Ю. Мельника. Харків : ХНУВС , 2021. С.99–103.

30. Ковальська Л. А., Котов К. Р. Блокчейн-технології і безпека цифрового документообігу. *Інформація та соціум.* 2023. Вип. 23. С. 153–157.
31. Конституція України. *Відомості Верховної Ради України*. 1996. № 30. Режим доступу: https://zakon.rada.gov.ua/laws/show. (дата звернення: 30.03.2024).
32. Конфіденційна інформація. *Термінологічний словник з питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму, фінансуванню розповсюдження зброї масового знищення та корупції* /Чубенко А. Г., Лошицький М. В., Павлов Д. М., Бичкова С. С., Юнін О. С. Київ : Ваіте, 2018. С. 355–356.
33. Коц Д. В. Теоретико-правові засади інформації з обмеженим доступом. *Вісник Національного технічного університету «Київський технічний інститут імені Ігоря Сікорського». Політологія. Соціологія. Право*. 2019. №2 (42). С. 107–111.
34. Кравченко О. М. Дистинкція між конфіденційною інформацією та комерційною таємницею. *Право та закон: теорія, методологія, практика : збірник матеріалів Міжнародної юридичної науково-практичної конференції «Актуальна юриспруденція»*. 15 квітня 2021 р. Київ : Центр учбової літератури, 2021. С. 35–38.
35. Кравченко О. М. Охорона комерційної таємниці від сучасних загроз. *Юридична практика в країнах ЄС та в Україні на сучасному етапі : матеріали міжнародної юридичної науково-практичної конференції*. Университет ім. Васіле Голдеш, 25-26 січня 2019 р.,м. Арад, Румунія, 2019. С. 373–376.
36. Кравченко О. М. Проблеми правової природи комерційної таємниці як окремого виду таємної інформації в Україні. *Вісник Академії праці, соціальних відносин і туризму*. 2015. № 1–2. С. 59–65.
37. Кравченко О. М. Удосконалення законодавства України в сфері охорони комерційної таємниці суб'єктів господарювання. *Євроінтеграція: польський досвід і українські перспективи : матеріали міжнар. юридичної науково-практичної конференції*. Одеса, Міжнародний гуманітарний університет. 29

квітня 2019 року. Одеса, 2019. С. 54–59.

38. Курман О.В. Відомості, що становлять комерційну таємницю, як предмет злочинного посягання. *Право і суспільство*. 2015. №5-2. Част. 2. С. 177–181.

39. Маслюк Д. В. Захист документної інформації від несанкціонованого доступу. *Актуальні проблеми розвитку природничих та гуманітарних наук* : збірник матеріалів VII Міжнар. наук. практ. конф. (10 листопада 2023 р.) / відп. ред. Голуб Г. С., Зінченко М. О. Луцьк, 2023. С. 359–360.

40. Матвієнко О., Цивін М. Інформаційна безпека та документознавча освіта: фахівці із захисту інформації з обмеженим доступом. *Вісник Книжкової палати.* 2023. № 7. С. 23–29.

41. Міністерство цифрової трансформації України : офіційний сайт. Режим доступу : https://thedigital.gov.ua/ (дата звернення 01.04.2024).

42. Мірошник Ю. Державна таємниця як складова забезпечення національної безпеки. *Право України*. 2004. № 9. С. 32–34.

43. Назаркевич М., Возний Я. Метод захисту матеріальних носіїв інформації латентними елементами. *Кібербезпека: освіта, наука, техніка.* 2019. № 33. С. 27–41.

44. Назаркевич М., Троян О. Аналіз сучасних методів та видів графічного захисту друкованих документів. *Вісник Національного університету «Львівська політехніка». Комп'ютерні науки та інформаційні технології*. 2014. № 8. С. 61–65.

45. Основи інформаційного права України. Навч. посіб. / За ред. Швеця М. Я., Калюжного Р. А., Мельника П. В. Київ : Знання, 2004. 274 с.

46. Особливості роботи з документами з грифом «Для службового користування». *Юридична газета online.* Режим доступу: https://yur-gazeta.com/publications/practice/sudova-praktika/osoblivosti-roboti-zdokumentami. (дата звернення: 01.04.2024).

47. Марущак А. І. Правові основи захисту інформації з обмеженим доступом :

Курс лекцій. Київ : Вид-во КНТ, 2007. 208 с.

48. Правила організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях / Мін-во юстиції України, Держ. архів. служба України. Київ : Держкомвидав, 2015. 248 с.
49. Про державну таємницю: Закон України від 21.01.1994 № 3856-XII. *Відомості Верховної Ради України.* 1994. № 16. Ст. 93. Режим доступу : https://zakon.rada.gov.ua/laws/show/3855-12/ (дата звернення: 07.04.2024).
50. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. *Відомості Верховної Ради України*. 2011. № 32. Ст. 314. Режим доступу : https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 05.04.2024).
51. Про електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII. *Відомості Верховної Ради України.* 2017. № 45. Ст. 400. Режим доступу : https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 20.04.2024).
52. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV. *Відомості Верховної Ради України*. 2003. № 36. Ст. 275. Режим доступу : https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 20.04.2024).
53. Про затвердження Інструкції з діловодства за зверненнями громадян в органах державної влади і місцевого самоврядування, об'єднаннях громадян, на підприємствах, в установах, організаціях незалежно від форм власності, в засобах масової інформації : Постанова Кабінету Міністрів України від 14.04.1997 р. № 348. Режим доступу: https://zakon.rada.gov.ua/laws/show/348-97-%D0%BF#Text (дата звернення: 30.04.2024).
54. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 2130-IX. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286. URL : https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 20.04.2024).

55. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. *Відомості Верховної Ради України.* 2010. № 34. Ст. 481. Режим доступу : https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 04.04.2024).
56. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. *Відомості Верховної Ради України.* 1992. № 48. Ст. 650. Режим доступу: http://zakon4.rada.gov.ua/laws/show/2657-12 (дата звернення: 04.04.2024).
57. Про Службу безпеки України: Закон України від 25.03.1992 р. № 2229-XII. *Відомості Верховної Ради України.* 1992. № 27. Ст. 382. Режим доступу: https://zakon.rada.gov.ua/laws/show/2229-12#Text (дата звернення: 04.04.2024).
58. Розломій, І. О. Косенюк, Г. В. Спосіб формування цифрового водяного знаку для електронних документів на основі операцій матричного криптографічного перетворення. *Вісник Хмельницького національного університету. Технічні науки.* 2017. № 4. С. 229–233.
59. Савченко С. В., Ткач Л. М., Прокоф'єва К. А., Вітер В. О. Дослідження діловодства та документообігу в установі: етапи, принципи, методи. *Вісник Придніпровської державної академії будівництва та архітектури.* 2015. № 3. С. 66–73.
60. Сельченкова С. В. Діловодство: Практичний посібник. Київ : Видавництво «Інкунабула», 2008. 480 с.
61. Сенів М. М. Безпека програм та даних: навч. посібник. Львів : Вид-во Львів. політехніки, 2015. 256 с.
62. Служба безпеки України : офіційний сайт. URL : https://ssu.gov.ua/ (дата звернення 04.04.2024).
63. Сучасне діловодство: зразки документів, діловий етикет. Довідник / Уклад. В. Бріцин. Київ : Довіра, 2010. 687 с.
64. Татарин І. І. Передумови та процес створення системи економічної безпеки на підприємствах. *Вісник Хмельницького національного університету*. 2008. №3. С. 386–389.

65. Філіпова Л. Системи управління електронним документообігом: загальні поняття термінології, організації, технології (зарубіжний досвід). *Вісник Книжкової палати.* 2001. № 4. С. 15–18.
66. Цілина М. Сучасні технології захисту й опрацювання конфіденційної документної інформації в організаціях і установах різних форм власності. *Бібліотекознавство. Документознавство. Інформологія.* 2021. № 4. С. 15–23.
67. Чередниченко В. Б. Електронний цифровий підпис у правовому полі України. Режим доступу : http://www.nbuv.gov.ua/portal/natural/soi/2009_7 (дата звернення: 04.04.2024).
68. Чикін С., Черненко В. Комерційна таємниця як об'єкт управління на підприємстві: дії правового характеру. *Теорія і практика інтелектуальної власності.* 2011. № 5 (61). С. 56–64.
69. Чунарьова А. Практичні схеми реалізації алгоритмів електронного цифрового підпису. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.* Київ: Національний авіаційний університет. 2013. №1(25). С. 81–88.
70. Чунарьова А. В., Чунарьов А. В. Принципи організації захисту інформації в сучасних інформаційно-комунікаційних системах і мережах: монографія. Київ : КНЕУ, 2010. 358 с.