УДК 681.3.06

Цитування:
Цілина М. М. Сучасні технології захисту й опрацювання конфіденційної документної інформації в організаціях і установах різних форм власності. *Бібліотекознавство. Документознавство. Інформологія.* 2021. № 4. С. 15–23.

Tsilyna M. (2021). Modern technologies of protection and processing of confidential documentary information in organizations and institutions of different forms of ownership. Library science. Record Studies. Informology. 4, 15–23 [in Ukrainian].

Цілина Марина Миколаївна,
кандидат філологічних наук, доцент,
доцент кафедри документознавства та
інформаційно-аналітичної діяльності
Київського національного університету
культури і мистецтв
macilin@ukr.net
https://orcid.org/0000-0001-5339-5147

СУЧАСНІ ТЕХНОЛОГІЇ ЗАХИСТУ Й ОПРАЦЮВАННЯ КОНФІДЕНЦІЙНОЇ ДОКУМЕТНОЇ ІНФОРМАЦІЇ В ОРГАНІЗАЦІЯХ І УСТАНОВАХ РІЗНИХ ФОРМ ВЛАСНОСТІ

Мета наукової роботи *– установлення особливостей і видів сучасної документної інформації, що має інтелектуальну цінність; з'ясування принципів, за якими варто будувати захищений документообіг; характеристика основних технологічних етапів і процедур виконання конфіденційних документів; визначення загроз, що можуть виникати під час цього процесу.* ***Методологію дослідження*** *склала сукупність загальнонаукових, спеціальнонаукових та специфічних методів студіювання проблематики, застосування яких дає змогу досягти поставленої мети. Наукова розвідка ґрунтувалася на принципах об'єктивності та цілісності. Використання комплексу наукових методів дало змогу дослідити специфіку цінної документної інформації, з'ясувати основні канали витоку інформації, простежити етапи документообігу таких ділових паперів.* ***Наукова новизна****. Досліджено новітні міжнародні практики роботи з конфіденційними документами. Установлено особливості і види документної інформації, що має інтелектуальну цінність для підприємця. Сформульовано принципи, за якими варто будувати захищений документообіг. Окреслено основні технологічні етапи і процедури виконання конфіденційних документів. З'ясовано основні загрози, що можуть виникати під час цього процесу.* ***Висновки****. Конфіденційна інформація дає змогу будь-якому підприємству вести успішну діяльність завдяки захищеності інформації. Важливість такої інформації зумовлює ризик її втрати. Аби уникнути незручностей, що пов'язані з утратою чи розкраданням інформації, в установах потрібно створювати відповідні служби, представники яких стежать за конфіденційною інформацією, за обігом документів, створюють бази даних для комп'ютерів і картотеки для паперових носіїв, знищують чернетки конфіденційного документа, зберігають та знищують документи, що є цінними, за установленим порядком.*

Ключові слова*: виконання конфіденційного документа, гриф таємності, захист інформації, технологічна комплексність, цінність документної інформації.*

Tsilyna Maryna,
Candidate of Philological Sciences (PhD.),
Associate professor of the Department of Document Science,
Information and Analytical Activities of the
Kyiv National University of Culture and Arts

MODERN TECHNOLOGIES OF PROTECTION AND PROCESSING OF CONFIDENTIAL DOCUMENTARY INFORMATION IN ORGANIZATIONS AND INSTITUTIONS OF DIFFERENT FORMS OF OWNERSHIP

The purpose of the article *is to establish the features and types of modern documentary information that has intellectual value; finding out the principles on which to build a secure document flow; characteristics of the main technological stages and procedures for the implementation of confidential documents; identifying threats that may arise during this process.* ***The methodology*** *consisted of a set of general scientific, special scientific and specific methods of studying the problem, the application of which allows to achieve the goal. Scientific intelligence was based on the principles of objectivity and integrity. The use of a set of scientific methods made it possible to study the specifics of valuable documentary information, to find out the main channels of information leakage, to trace the stages of document circulation of such business papers.* ***Scientific novelty****. The latest international practices of working with confidential documents are studied. Features and types of documentary information that has intellectual value for the entrepreneur are established. The principles on which it is necessary to build a secure document flow are formulated. The main technological stages and procedures of execution of confidential documents are outlined. The main threats that may arise during this process have been identified.* ***Conclusions****. Confidential information allows any company to operate successfully due to the security of information. The importance of such information determines the risk of its loss. In order to avoid inconveniences related to the loss or theft of information, the institutions should create appropriate services, whose representatives monitor confidential information, document circulation, create databases for computers and files for paper media, destroy drafts of confidential documents, store and destroy documents that are valuable in the prescribed manner.*

Keywords: *execution of a confidential document, secrecy stamp, information protection, technological complexity, value of documentary information.*

Актуальність теми дослідження. Реалії сьогодення вимагають від державних службовців, підприємців та керівників інших фірм та установ цілісності створеної ними організаційної структури, що є безперечною умовою економічної, політичної і навіть національної безпеки їхньої діяльності. Інформаційна безпека у цьому контексті стає пріоритетною складовою, котру дуже складно зберегти.

Захист інформації щороку все важче забезпечити ще й з огляду на стрімкий розвиток інноваційних технологій. Окрім цього, ускладнює цей процес і зацікавленість конкурентів витоком інформації з фірми чи установи. Саме тому створюються служби з контролю за документами конфіденційного характеру, їх пересуванням і зберіганням в організації.

Зловмисники можуть створити потенційну або реальну загрозу несанкціонованого доступу до документів, використовуючи організаційні і технічні канали, і як результат відбувається розкрадання і неправомірне використання, модифікація, підміна, фальсифікація, знищення цінної документної інформації. Зловмисниками можуть бути як недобросовісні конкуренти, так і особи, що діють в інтересах конкурента, супротивника чи в особистих корисливих інтересах (агенти іноземних спецслужб, промислового й економічного шпигунства, кримінальних структур, окремі злочинні елементи, психічно хворі особи та ін.).

Чимало таких осіб і серед співробітників організацій, що не мають права доступу до приміщень, конкретних документів, баз даних тощо. Також зловмисниками є і сторонні особи, тобто будь-хто, що не має безпосереднього відношення до діяльності фірми, наприклад працівники комунальних служб, екстремальної допомоги, перехожі чи відвідувачі установ і організацій.

Мета наукової роботи – установлення особливостей і видів документної інформації, що має інтелектуальну цінність для підприємця; з'ясування принципів, за якими варто будувати захищений документообіг; характеристика основних технологічних етапів і процедур виконання конфіденційних документів; визначення загроз, що можуть виникати під час цього процесу.

Аналіз досліджень і публікацій. Питання захисту інформації завжди було, є і буде одним із найважливіших для функціонування будь-якої організації, установи чи фірми. Особливо актуальним для подальших досліджень є аспект захисту документної інформації, що розкритий у низці наукових розвідок. Технологічні основи опрацювання конфіденційних документів ґрунтовно розглянуто М. В. Гуцалюком, захист інформації в системі електронного урядування став об'єктом вивчення О. Б. Кукаріна, А. І. Семенченка, В. М. Дрешпака, О. М. Хошаби. Систему захисту інформації приватного підприємства й організацію служби захисту приватного підприємства охарактеризовано В. Василюком. Міжнародний досвід роботи з конфіденційними документами простудійовано у статтях Ю. М. Данілова, Д. Волкера, Дж. Карбо, Е. Уакініна. Законодавчо-правий аспекти роботи з інформацією з обмеженим доступом та із персональними даними визначено низкою нормативно-правових актів, а саме: Законом України «Про доступ до публічної інформації», Законом України «Про інформацію», Законом України «Про захист персональних даних» та ін.

Виклад основного матеріалу. Документна інформація, яка використовується в управлінні підприємством, організацією, банком, компанією чи іншою структурою, є приватною інформацією, зокрема інтелектуальною власністю.

Цінність інформації може бути вартісною категорією, що характеризує конкретний розмір прибутку під час її використання чи розмір збитків при її втраті. Інформація часто стає цінною ще й з огляду на її правове значення для фірми або розвитку бізнесу, приміром в установчих документах, програмах та планах, договорах із партнерами та посередниками. Цінність інформації може також відображати її перспективне наукове, технічне чи технологічне значення.

Інформація, що має інтелектуальну цінність для підприємця, буває:

1)технічною, технологічною (методи виготовлення продукції, програмне забезпечення, виробничі показники, хімічні формули, результати випробувань дослідних зразків, дані контролю якості);

2)діловою: вартісні показники, результати дослідження ринку, списки клієнтів, економічні прогнози, стратегія дій на ринку.

Основною частиною захисту інформації стає виявлення та регламентація реального складу інформації, що представляє цінність. Склад цінної інформації фіксується в спеціальному переліку, який визначає термін і рівень її конфіденційності, список співробітників, котрим надано право використовувати ці відомості під час роботи. Такий перелік являє собою класифікований список типової і конкретної цінної інформації про проведені роботи, вироблену продукцію, наукові й ділові ідеї, технологічні нововведення тощо. Додатково може складатися перелік документів, де ці відомості документуються. До переліку включено й документи, що представляють цінність для фірми і підлягають охороні.

Кожна організація чи фірма індивідуально формують перелік, із урахуванням рекомендацій спеціальної комісії. Затверджує цей документ керівник установи. Комісія регулярно вносить поточні зміни до переліків відповідно до динаміки виконання конкретних робіт.

Комерційна цінність інформації, як правило, недовговічна і визначається часом, необхідним конкуренту для вироблення тієї ж ідеї чи її викрадення і відтворення, опублікування та переходу інформації в категорію загальновідомих. Ступінь цінності інформації і надійність її захисту є взаємозалежними.

Документи, що містять цінну інформацію, входять до складу інформаційних ресурсів установи і можуть бути:

- відкритими, тобто доступними для роботи персоналу без спеціального дозволу;
- обмеженими для доступу до них персоналу, зокрема зарахованими до державної або недержавної таємниці. Документи, що містять відомості, які становлять недержавну

таємницю (службову, комерційну, банківську та ін.), чи містять персональні дані, є конфіденційними.

Відповідно до Закону України «Про доступ до публічної інформації» «Конфіденційна інформація – 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» [7].

Конфіденційність асоціюється із секретністю, термін широко використовується виключно для позначення інформаційних ресурсів обмеженого доступу. Ідеться про обмеження, яке відповідно до закону накладає власник інформації на доступ до неї інших осіб. Водночас до конфіденційних документів не належать установчі документи, статути підприємницьких структур, фінансова документація, відомості про заробітну плату персоналу та інша документна інформація, необхідна правоохоронним і податковим державним органам.

Конфіденційний документ існує як необхідним чином оформлений носій документної інформації, що містить відомості, які належать до недержавної таємниці і складають інтелектуальну власність юридичної або фізичної особи. Основна ознака конфіденційного документа – це наявність у ньому інформації, що підлягає захисту. До конфіденційних належать такі документи [4]:

● у державних структурах – документи, проєкти документів і додаткові матеріали, що є службовою інформацію обмеженого поширення (це документи службового користування), що містять відомості, зараховані до службової таємниці, мають робочий характер і не підлягають опублікуванню у відкритій пресі;

● у підприємницьких структурах і напрямах подібної діяльності – документи, що містять відомості, які їх власник або власник відповідно до законодавства має право зарахувати до комерційної (підприємницької) таємниці, таємниці організації;

● незалежно від приналежності – документи і бази даних, що фіксують будь-які персональні (особисті) дані про громадян, а також містять професійну таємницю, технічні та технологічні нововведення (до їх патентування), таємницю підприємств зв'язку, сфери обслуговування та ін.

Називати конфіденційні документи секретними або ставити на них гриф секретності не допускається. Особливістю конфіденційного документа є те, що він одночасно є масовим носієм цінної інформації, що захищається, основним джерелом накопичення та об'єктивного поширення цієї інформації, а також її неправомірного розголошення або витоку та обов'язковим об'єктом захисту.

Конфіденційність документів завжди пов'язана із відтермінуванням щодо обмеження вільного доступу до них персоналу установи чи організації. Часові рамки такого обмеження можуть охоплювати від декількох годин до багатьох років. Варто також мати на увазі, що основна маса конфіденційних документів після закінчення їх виконання або роботи з ними втрачає свою цінність і конфіденційність. Наприклад, листування до укладення контракту може мати гриф конфіденційності, але після його підписання цей гриф із письмового дозволу першого керівника установи знімається.

Конфіденційні виконані документи, що зберігають цінність для діяльності організації, формуються у справи відповідно до номенклатури справ. Цінність документної інформації зумовлює період перебування конфіденційних документів у справах, що може бути короткочасним або тривалим. Специфіка діяльності організації також має значення під час укладання переліків конфіденційних відомостей та визначення періоду конфіденційності. Так виробничі, науково-дослідні установи володіють більш цінними документами, ніж торговельні, посередницькі та ін.

Якщо документи довготривалого періоду конфіденційності, то вони мають ускладнений варіант обробки і зберігання, що у свою чергу дає змогу гарантувати безпеку інформації та її носія. Такими документами, зокрема, можуть бути програми і плани розвитку бізнесу, технологічна документація ноу-хау, винаходи до їх патентування та ін.

Якщо документи мають короткочасний період конфіденційності і, відповідно, оперативне значення для діяльності фірми, то вони

обробляються і зберігаються за спрощеною схемою і можуть не виділятися з технологічної системи обробки відкритих документів, за умови наявності у такій системі мінімальних захисних, контрольних та аналітичних елементів.

Конфіденційні документи знаходяться в постійному русі в часі і просторі, що відображає їх об'єктивну сутність як носія інформації, необхідної керівникам і співробітникам фірми для виконання функціональних обов'язків й ухвалення рішень. Технологічний аспект документообігу являє собою процес руху паперових і електронних документів за встановленими пунктами їх обліку, розгляду, виконання і зберігання для виконання різних процедур і операцій, зокрема творчих, формально-логічних і технічних. Переміщення конфіденційних документів значною кількістю ієрархічних рівнів системи управління створює серйозні передумови для втрати цінної інформації, вимагає здійснення захисних заходів щодо документопотоків і документообігу в цілому.

Розглядаючи документообіг як об'єкт захисту, можна сказати, що цей процес є упорядкованою сукупністю каналів об'єктивного, санкціонованого поширення конфіденційної документної інформації у ході управлінської та виробничої діяльності користувачів (споживачів) цієї інформації. Технологічна комплексність – основна характеристика руху інформації. Ідеться про об'єднання завдань, що забезпечують управлінські, діловодні й поштові функції. Документообіг відображає безпосередньо повний «життєвий цикл» документа.

Під час використання будь-якої технологічної системи обробки і зберігання документів принципи та напрямки руху конфіденційних традиційних та електронних документів в апараті управління установи залишаються єдиними. Технологічний взаємозв'язок документообігу із процесом управління зберігається, незважаючи на зміну методів роботи з документами.

У процесі переміщення конфіденційних документів різними інстанціями збільшується кількість джерел інформації (працівників, баз даних, робочих матеріалів), що володіють цінними відомостями, і неминучою стає втрата конфіденційної інформації, її розголошення персоналом, витік технічними каналами або ж зникає носій цієї інформації. Каналами втрати конфіденційної документної інформації можуть бути [4]:

1. Крадіжка документа чи окремих його частин, носія чорнового варіанту документа або робочих записів.

2. Несанкціоноване копіювання паперових і електронних документів, баз даних, фото-, відео- і аудіодокументів, запам'ятовування тексту документа.

3. Таємне чи дозволене ознайомлення працівника установи з документом і передавання інформації зловмиснику особисто чи лініями зв'язку, із використанням телефона або переговорного пристрою та ін.

4. Підміна документів, носіїв та їх частин задля фальсифікації чи приховування фактів утрати і крадіжки.

5. Дистанційний перегляд документів та зображень монітора з використанням технічних засобів візуальної розвідки.

6. Помилкові дії працівників під час роботи з документами, зокрема порушення системи дозволу доступу, правил і технологій обробки і зберігання документів.

7. Випадкове або умисне знищення цінних ділових паперів і баз даних, недозволене перетворення та перекручення елементів тексту, реквізитів.

8. Зчитування даних у чужих масивах за рахунок використання залишкової інформації на копіювальній стрічці, папері, дисках.

9. Витік інформації технічними каналами у процесі обговорення і диктування тексту документа, роботи з комп'ютером та іншою офісною технікою.

10. Зникнення документів через різні екстремальні ситуації.

Утрата конфіденційної інформації в електронних документах особливо небезпечна, оскільки крадіжку інформації дуже складно виявити.

Чинники, що призводять до втрати конфіденційної комп'ютерної інформації, бувають різними^ від ненавмисних помилок користувачів, операторів, референтів, співробітників служби конфіденційної документації, системних адміністраторів – до крадіжки і підробок

інформації, загроз, котрі трапляються від стихійних лих чи вірусів.

Аби уникнути і послабити ці загрози, ставляться завдання захисту інформації в документопотоках.

Основний напрям захисту документної інформації від можливих ризиків – це формування безпечного документообігу, зокрема використання у процесі опрацювання та зберігання документів спеціалізованої технологічної системи, що гарантуватиме безпеку інформації на будь-якому типі носія.

Захищений документообіг (документопотік) – це контрольований рух конфіденційної документної інформації регламентованими пунктами приймання, розгляду, виконання, використання і зберігання в умовах організаційного та технологічного гарантування безпеки інформаційних ресурсів і самої інформації.

Захищений документообіг ґрунтується на низці додаткових принципів, а саме [4]:

● обмеження доступу працівників до документів, справ і баз даних ділової, службової або виробничої необхідності;

● персональна відповідальність керівників за видачу дозволів на доступ працівників до конфіденційних відомостей та документів;

● персональна відповідальність кожного співробітника за збереження довіреного йому носія та конфіденційність інформації;

● сувора регламентація порядку роботи з документною інформацією для всіх категорій персоналу, зокрема і керівників.

Під час доставки і використання конфіденційної інформації в захищеному документообігу задіяний також принцип вибірковості, що полягає в існуванні чинної для певної установи дозвільної (розмежувальної) системи доступу персоналу до конфіденційної інформації, документів та баз даних. Вибірковість дає змогу забезпечити оперативність доставки документної інформації споживачеві. Проте відбувається доставлення тільки тієї інформації, робота з котрою дозволена відповідно до функціональних обов'язків певної посадової особи. Така вибірковість безпосередньо поширюється як на вхідні документи, так і на документи, що укладено персоналом на робочих місцях чи із якими працівники щойно ознайомлені.

Захищеність документопотоків може забезпечуватись:

● одночасним використанням режимних (дозвільних, обмежувальних) заходів і технологічних прийомів, які входять у систему обробки і зберігання конфіденційних документів;

● нанесенням відмітної позначки (грифа) на чистий носій конфіденційної інформації або документ, зокрема супровідний. Це дає змогу виділити їх у загальному потоці документів;

● формуванням самостійних, ізольованих потоків конфіденційних документів і (часто) додаткового їх поділу на підпотоки за рівнем конфіденційності переміщення документів;

● використанням незалежної технологічної системи опрацювання та зберігання конфіденційних документів, яка не натрапляє на систему опрацювання відкритих документів.

Виконання конфіденційного документа – це процес документування управлінських рішень і дій, результатів виконання керівниками і працівниками організацій певних завдань чи доручень та реалізація функцій, що закріплені за ними в посадових інструкціях. Ініціювати процес виконання можуть такі чинники [4]:

● отримання керівником, співробітником (виконавцем) вхідного документа;

● письмова чи усна вказівка керівника вищої інстанції;

● усний запит на інформацію або ухвалення рішення від інших організацій, установ і окремих осіб;

● завдання і доручення, включені в робочі плани, графіки роботи, посадові інструкції та інші організаційні та планові документи;

● необхідна інформація, отримана із реферативних та інформаційних збірників або рекламних видань.

Використання документа полягає у включенні його до інформаційно-документаційної системи, що забезпечить виконання інших документів, а також управлінських дій і рішень. Процес ознайомлення з конфіденційним документом – це повідомлення працівників організацій або інших зацікавлених осіб, що здійснюється відповідно до резолюції повноважного керівника на конфіденційному документі, про прийняте цією посадовою особою рішення.

У процесі виконання конфіденційних документів можуть виникати такі основні загрози:

● втрата (розголошення, витік) цінної інформації через її документування на випадковому носії, який не входить у сферу контролю служби конфіденційних документів;

● підготовка до видання документа без ділової необхідності або дозволу;

● введення в документ надлишкових конфіденційних відомостей, що є рівнозначним розголошенню таємниці установи;

● випадкове або навмисне заниження грифу конфіденційності відомостей, включених у документ;

● підготовка документа в умовах, котрі не гарантують збереження носія, конфіденційності інформації;

● втрата оригіналу, чернетки, варіанта чи редакції документа, його частини, додатка, замовчування цього факту і спроба підміни втрачених матеріалів;

● повідомлення плану проєкту конфіденційного або відкритого документа сторонній особі, недозволене копіювання документа чи його частини;

● витік інформації технічними каналами;

● неправильні дії співробітників, зокрема порушення дозвільної системи доступу до документів.

Варто зауважити, що виконання конфіденційних документів пов'язане з такими технологічними етапами і процедурами:

● установлення рівня грифу конфіденційності відомостей, котрі підлягають включенню до майбутнього документа;

● оформлення й облік носія для документування певного комплексу конфіденційної інформації;

● складання і виготовлення конфіденційного документа;

● видання конфіденційного документа.

Ці етапи характеризуються не лише регламентованою технологією, а й жорсткими вимогами до роботи виконавців із конфіденційною інформацією.

Найбільшу безпеку має конфіденційна інформація, яка не фіксується на будь-якому носії; цінна інформація швидко набуває загроз під час виникнення необхідності її документування.

Саме тому система захисту конфіденційної інформації має функціонувати не після видання (підписання) конфіденційного документа, а ще до створення майбутнього документа. Перед створенням документа, необхідно встановити, чи є ця інформація конфіденційною і який рівень грифу конфіденційності їй призначено у випадку позитивної відповіді.

Вчасне установлення грифу конфіденційності інформації, яка підлягає включенню в майбутній документ, – основний елемент її захисту. Це дає змогу гарантувати надійну безпеку таємниці установи.

Гриф конфіденційності присвоюється документу за наявності: переліку конфіденційних відомостей організації, вимог партнерів та переліку конфіденційних документів установи. Проте система грифування документів не гарантує збереження інформації, хоча дає змогу чітко організувати роботу з документами, тобто сформувати систему доступу до документів співробітників.

Гриф конфіденційності, або гриф обмеження доступу до традиційного, паперового чи електронного документа – це реквізит (елемент, службова відмітка, позначка) формуляра документа, що засвідчує конфіденційність відомостей, котрі містяться в документі, і проставляється на самому документі і (чи) супровідному листі до нього.

Необхідність присвоєння документу грифу «Для службового користування» вирішується виконавцем або посадовою особою, яка підписує документ, відповідно до переліку відомостей, що становлять службову інформацію та з дотриманням вимог частини другої статті 6 та статті 9 Закону України «Про доступ до публічної інформації» [7].

В інших випадках питання щодо необхідності присвоєння документу грифу «Для службового користування» може розглядатися комісією з питань роботи із службовою інформацією за поданням посадової особи, яка підписуватиме документ.

На документах, що містять службову інформацію з:

– мобілізаційних питань, додатково проставляється відмітка із літерою «М»;

– питань криптографічного захисту службової інформації – відмітка літерою «К»;

– питань спеціальної інформації – відмітка «СІ» [10].

Документна інформація, що є загалом конфіденційною, наприклад, документація служби персоналу, служби безпеки, документи, зараховані до професійної таємниці, зазвичай не маркуються, оскільки сповна володіють жорстким обмеженням доступу.

Цінні, проте неконфіденційні документи можуть мати відмітки, написи, штампи, що звертають особливу увагу до збереження таких ділових паперів: «Власна інформація фірми», «Інформація особливої уваги», «Копії не знімати», «Зберігати в сейфі» та ін. Аби швидко візуально виділити і проконтролювати використання під час роботи співробітників, також використовуються додаткові кольорові ідентифікатори цінних і конфіденційних документів.

Наукова новизна. Досліджено новітні міжнародні практики роботи з конфіденційними документами. Установлено особливості і види документної інформації, що має інтелектуальну цінність для підприємця. Сформульовано принципи, за якими варто будувати захищений документообіг. Окреслено основні технологічні етапи і процедури виконання конфіденційних документів. З'ясовано основні загрози, що можуть виникати під час цього процесу.

Висновки. Інформація є одним із ресурсів фірми, без котрого не буде чіткої і злагодженої роботи. Конфіденційна ж інформація дає змогу будь-якому підприємству вести успішну діяльність завдяки захищеності інформації. Важливості такої інформації зумовлює ризик її втрати. Задля уникнення незручностей, що пов'язані з утратою чи розкраданням інформації, в установах створюються відповідні служби, представники яких стежать за конфіденційною інформацією, за обігом документів, створюють бази даних для комп'ютерів і картотеки для паперових носіїв, знищують чернетки конфіденційного документа, зберігають та знищують документи, що є цінними, за установленим порядком.

Як відомо, захист документної інформації забезпечується системою різних заходів, зокрема режимного, технологічного, аналітичного і контрольного характеру. Переміщення документа під час виконання кожної стадії, опрацювання або виконання неодмінно супроводжується низкою облікових операцій, а також передбачає закріплення документа за конкретним працівником та його персональною відповідальністю.

Технологічний процес обліку конфіденційних документів пов'язаний із низкою процедур, обов'язкових для будь-якого виду обліку та обробки і зберігання таких ділових паперів. Під час обліку, розподілу, розгляду, передачі документів, котрі надійшли виконавцям, та повернення документів виконується комплекс технологічних і обмежувальних операцій, що дають змогу забезпечити фізичну схоронність документа, а також запобігти розголошенню й витоку документної інформації.

Список використаних джерел

1. Василюк В. Система захисту інформації приватного підприємства. Організація служби захисту приватного підприємства // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2007. Вип. 1 (14), С. 45–51.

2. Вимоги до роботи з конфіденційною інформацією установи // Баланс-Бюджет. 2020. № 51. URL: https://balance.ua/news/post/trebovaniya-k-rabote-s-konfidencialnoy-informaciey-uchrezhdeniya (дата звернення: 23.10.2021).

3. Гуцалюк М. В. Організація захисту інформації. Навчальний посібник. 2-е вид., перероб. та допов. Київ : Альтерпрес, 2011. 308 с.

4. Данилов Ю. М. Защита и обработка конфиденциальных документов. Делопроизводство. 2008. №1. URL: https://www.top-personal.ru/officeworkissue.html?23 (дата звернення: 22.09.2021).

5. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А. І. Семенченка, В. М. Дрешпака. Київ. 2017. Частина 13: Захист інформації в системах електронного урядування / [О.М. Хошаба]. Київ : ФОП Москаленко О. М., 2017. 72 с.

6. Закон України «Про доступ до публічної інформації» від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 22.09.2020).

7. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 22.09.2020).

8. Закон України «Про інформацію» від 02.10.1992 № 2657- XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 22.09.2020).

9. Кукарін О. Б. Електронний документообіг та захист інформації: навч. посіб. / За заг. ред. д.держ. упр., професора Н. В. Грицяк. Київ : НАДУ, 2015. 84 с.

10. Особливості роботи з документами з грифом «Для службового користування» // Юридична газета online. URL: https://yur-gazeta.com/publications/practice/sudova-praktika/osoblivosti-roboti-z-dokumentami-z-grifom-dlya-sluzhbovogo-koristuvannya.html (дата звернення: 22.10.2020).

11. Carbo D. Don't Just Rely On Data Privacy Laws to Protect Information URL: https://www.securitymagazine.com/articles/91775-dont-just-rely-on-data-privacy-laws-to-protect-information (дата звернення: 15.09.2020).

12. Ouaknine E. The importance of document security and how to make sure you are working safely. URL: https://www.upslide.net/en/the-importance-of-document-security-and-how-to-make-sure-you-are-working-safely/ (дата звернення: 15.09.2020).

13. Wolker D. The DNA of NDA's – Are confidentiality agreements worth the paper they are written on? URL: http://www.gridlaw.com/are-confidentiality-agreements-worth-the-paper-they-are-written-on/ (дата звернення: 15.09.2020).

References

1. Vasilyuk, V. (2007). Information protection system of a private enterprise. Organization of private enterprise protection service. Legal, normative and metrological support of information protection system in Ukraine. Vol. 1 (14). pp. 45-51 [in Ukrainian].

2. Requirements for working with confidential information of the institution. Balance-Budget. 2020. № 51. URL: https://balance.ua/news/post/trebovaniya-k-rabote-s-konfidencialnoy-informaciey-uchrezhdeniya [in Ukrainian].

3. Gutsalyuk, M. V. (2011). Organization of information protection. Tutorial. 2nd ed., Reworked. and add. Kyiv: Alterpress. p. 308. [in Ukrainian].

4. Danilov, Y. M. (2008). Protection and processing of confidential documents. Deloproizvodstvo. №1. URL: https://www.top-personal.ru/officeworkissue.html?23 [in Russian].

5. Dreshpak, V. M. (2017). E-government and e-democracy: textbook. aid.: at 15 Parts. A. I. Semenchenko, Kyiv. Part 13: Information protection in e-government systems. O. M. Hoshaba (Ed.). Kyiv: FOP Moskalenko O. M. 2017. 72 p. [in Ukrainian].

6. Law of Ukraine «On Access to Public Information» from 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text [in Ukrainian].

7. Law of Ukraine «On Personal Data Protection» from 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text [in Ukrainian].

8. Law of Ukraine «On Information» from 02.10.1992 № 2657- XII . URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text [in Ukrainian].

9. Kukarin, O. B. (2015). Electronic document management and information protection: textbook. aid. N.V. Hrytsiak (Ed.). Kyiv: NADU. 84 p. [in Ukrainian].

10. Features of working with documents marked «For official use» // Legal newspaper online. URL: https://yur-gazeta.com/publications/practice/sudova-praktika/osoblivosti-roboti-z-dokumentami-z-grifom-dlya-sluzhbovogo-koristuvannya.html [in Ukrainian].

11. Carbo, D. Don't Just Rely On Data Privacy Laws to Protect Information URL: https://www.securitymagazine.com/articles/91775-dont-just-rely-on-data-privacy-laws-to-protect-information [in English].

12. Ouaknine, E. (n.d). The importance of document security and how to make sure you are working safely. URL: https://www.upslide.net/en/the-importance-of-document-security-and-how-to-make-sure-you-are-working-safely/ [in English].

13. Wolker, D. (n.d). The DNA of NDA's – Are confidentiality agreements worth the paper they are written on? URL: http://www.gridlaw.com/are-confidentiality-agreements-worth-the-paper-they-are-written-on/ [in English].

Стаття надійшла до редакції 08.08.2021
Отримано після доопрацювання 29.09.2021
Прийнято до друку 15.11.2021