**Захист документів та інформаційні технології підтримки документообігу**

***Правова охорона документів***.

Особи, відповідальні за роботу з документами, зобов’язані забезпечувати збереження документів, що створюються на підприємствах, в установах, організаціях. Справи з моменту їх заведення і до здачі до архіву установи зберігаються в робочих кімнатах чи в спеціально відведених приміщеннях. Ці приміщення мають відповідати вимогам пожежної безпеки, мати певний температурний режим.

Справи поміщують в шафи канцелярського типу, які обов’язково закриваються. Це допомагає вберегти документи від попадання пилу, впливу сонячного світла та інших чинників. Документи підшиваються в тверді обкладинки чи в папки-реєстратори. Папки встановлюють на полицях шафи в тій послідовності, в якій вони вказані в номенклатурі справ, досить щільно притискаючи одну до одної. Папки встановлюють вертикально, корінцем назовні. При такому зберіганні основний тиск направлений на корінець, а аркуші документів всередині папки тиску не відчувають. Це зручно як для зберігання документів, так і для користування ними.

Якщо довідки підшиті в папки з м’якими обкладинками, ставити їх вертикально не можна, бо від цього псуються нижні краї аркушів документів. Такі довідки зберігаються горизонтально. Забезпеченню фізичного збереження документів сприяє також і правильна підшивка аркушів документів у справі. При підшивці необхідно слідкувати за тим, щоб нижні краї документів були на одному рівні, вище від краю папки приблизно на 1 см.

Вилучення і видача будь-яких документів зі справ постійного збереження не дозволяється. У виняткових випадках (наприклад, на вимогу судово-слідчих органів) таке вилучення робиться з дозволу керівника установи з обов’язковою постановою у справі точно завіреної копії вилученого документу і вкладанням акту про причину вилучення оригіналу.

Протягом справочинного року на видану по службовій необхідності справу заповнюється картка, в якій вказуються структурний підрозділ, номер справи, дата видачі, її заголовок, кому справа видана, дата повернення; передбачаються глави для розписок про отримання і прийом справи.

***Захист документів, які містять інформацію, що не підлягає розголошенню.***

Інформацією, що не підлягає розголошенню, є службова та ділова інформація, яка має тактичну чи потенційну цінність для організації. Ця інформація може містити державну таємницю, знаходитися у власності держави, бути комерційно вигідною для недобросовісних конкурентівтощо. Втрата державної та комерційної таємниці може завдати шкоди державі, збитків організації або навіть привести підприємство до банкрутства.

З метою захисту державної таємниці прийнято відповідний закон, що регламентує роботу з документами, які містять державну таємницю. Крім того існує відповідний закон щодо охорони документів, що містять інформацію, яка є власністю держави, і не підлягають розголошенню.

Методами захисту важливої інформації є правовий захист та організаційні міри захисту. Правовий захист здійснюється методом закріплення прав і порядку захисту комерційної таємниці в нормативних і статутних актах. Ці міри можуть бути закріплені у статуті підприємства, трудових угодах (контрактах) із співробітниками підприємства, наказах, правилах внутрішнього розпорядку підприємства тощо. Організаційні міри захисту передбачають:

* організацію конфіденційного справочинства. «Грифи» і порядок функціонування цього справочинства затверджуються керівництвом підприємства;
* розмежування доступу до інформації: кожен співробітник підприємства може користуватись тільки тими відомостями, які необхідні йому для виконання службових обов’язків. Дозвіл на доступ до такої інформації видається керівником підприємства, при цьому співробітник несе відповідальність за розголошення отриманих відомостей;
* встановлення такого порядку використання технічних засобів і приміщень, який виключав би витік відомостей. Наприклад, при роботі з копіювальними засобами необхідно забезпечити суворо регламентоване копіювання тих документів, на які поширюється режим конфіденційності;
* встановлення порядку ведення переговорів з відвідувачами. Переговори мають сприяти, по-перше, недопущенню витоку інформації, по-друге, — отриманню найбільш повних відомостей про наміри відвідувачів;
* навчання співробітників підприємства заходам захисту комерційної таємниці, підвищення їх відповідальності за її розголошення.

**Захист за допомогою технічних засобів.**

Використання технічних засобів для забезпечення збереження інформації створює додаткові гарантії того, що документи та інші носії інформації будуть надійно захищені. Технічні засоби захисту можуть бути розділені на наступні види:

* засоби охорони території підприємства, засоби захисту комунікацій;
* засоби захисту комп’ютерних систем і баз даних від несанкціонованого доступу.

Засоби охорони території — це різноманітні типи обмежень і контролюючих систем (системи телевізійного контролю території, різноманітні електронно-оптичні та інші засоби охорони).

У наш час джерелом витоку інформації у більшості випадків є процеси опрацювання, передачі і збереження інформації, пов’язані з використанням електронних, електромеханічних та електротехнічних засобів. Досить просто використати інформацію, яка зберігається в ЕОМ, аудіо- та відеозаписуючій апаратурі, якщо попередньо не було вжито спеціальних засобів для її захисту.

Основні засоби захисту інформації при використанні технічних засобів:

* забезпечення закритої передачі інформації телефоно-телеграфними каналами шляхом її шифрування;
* спеціальний захист апаратури від опромінення за допомогою захисних балонів;
* використання спеціальних засобів захисту комп’ютерних систем і баз даних;
* створення штучних перешкод перехвату електронних чи акустичних сигналів.

Заходи щодо захисту комерційної таємниці при використанні комп’ютерних систем і баз даних можна поділити на такі групи:

* кодування документів на магнітних носіях, тобто доповнення тексту документів ознакою авторства, що при нормальному прослуховуванні не читається;
* шифрування всього документа чи його частин на машинних носіях, що робить цей документ недоступним для розуміння особам, які не володіють кодом для розшифровки.

Використання комп’ютерів у бізнесі призвело до того, що великі обсяги ділової інформації передаються і отримуються комп’ютерними мережами, які охопили майже увесь світ. Саме через комп’ютерні мережі здійснюється більшість викрадень інформації.

Іншою проблемою є захист інформації, що передається, від підробок та перекручень. З такою метою використовується програма під назвою «електронний підпис». Вона дозволяє засвідчити належність документа, що передається мережею, але його текст при цьому залишається незахищеним.

Щоб захистити всю інформацію, що передається, її краще зашифровувати. Зручніше зробити це за допомогою апаратних засобів, підключивши до комп’ютера додаткову електронну плату.

Просто та ефективно захищають дані в комп’ютері від копіювання механічні або електромеханічні ключі, що входять до комплекту. Поворот ключа, який легко носити з собою, надійно блокує роботу комп’ютера.

Серед безлічі варіантів захисту і збереження інформації головне — правильно підібрати носій та якомога найкращий вид захисту. В такому разі інформація буде належати тільки своєму власникові.

**Що таке конфіденційна інформація та комерційна таємниця?**

Правовий режим конфіденційної інформації в Україні регулюється Законом України «Про інформацію» (далі – Закон). Визначення цього поняття можна знайти у ст. 21 Закону, де зазначено, що *конфіденційною є*інформаціяпро фізичну особу, а також інформація, доступ до якої обмежений фізичною або юридичною особою, крім суб’єктів владних повноважень.

Визначення *комерційної таємниці*міститься в Цивільному та Господарському кодексах України. Зокрема, це інформація, яка є секретною в тому розумінні, що вона загалом чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які зазвичай мають справу з видом інформації, до якого вона належить, у зв’язку з цим має комерційну цінність та була предметом адекватних наявним обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Конкретного переліку інформації, яка може бути конфіденційною чи комерційною таємницею, чинне законодавство України не визначає. Натомість ч. 4 ст. 21 Закону 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 того ж важливо пам’ятати, що поняття «конфіденційна інформація» є ширшим ніж поняття «комерційна таємниця», тому можна зробити висновок, що *вся комерційна таємниця є конфіденційною інформацією, але не вся конфіденційна інформація є комерційною таємницею*. Отже, якщо розмір заробітної плати не може бути комерційною таємницею, то ніхто не забороняє віднести цю інформацію до конфіденційної.

Постає питання про те, які відомості можна обмежити у доступі? Комерційною таємницею можуть бути відомості організаційного, технічного, комерційного, виробничого та іншого характеру. Керівник/засновник підприємства в кожному випадку самостійно визначає обсяг інформації, яка становить комерційну таємницю та/або є конфіденційною. Зазвичай це інформація про собівартість товару, дані про клієнтів, стратегії розвитку, маркетингові плани, умови договорів тощо.

*Верховний суд (КГС)*у Постанові від 23.11.2020 р. у справі [№910/1759/19](https://reyestr.court.gov.ua/Review/93149537?fbclid=IwAR23q9oqRn-rsi78-To4J9KG9a_OrGY-qbQZXT8OE-bnH6OsxU79Ix5sgfw) зазначив, що*інформація щодо повного переліку постачальників та клієнтів (покупців) ТОВ (який містить контактні дані їх представників), розміру торговельної націнки, знижок на закупівлю продукції, обсягів закупівлі та постачання продукції є інформацією, що має комерційний характер.* Тож будь-яка інформація, яка має комерційну цінність, може бути віднесена до комерційної таємниці та/або конфіденційної інформації, за винятком тих відомостей, які відповідно до вимог законодавства не можуть бути обмежені у доступі.

**Як охороняти інформацію в компанії?**

На переконання мою думку, захищати інформацію мають усі: від салонів краси до заводів-виробників. Адже ніколи не знаєш, в який момент твій колега може стати твоїм конкурентом.

З аналізу чинного законодавства України та Постанови Верховного Суду у справі [№910/1759/19](https://reyestr.court.gov.ua/Review/93149537?fbclid=IwAR23q9oqRn-rsi78-To4J9KG9a_OrGY-qbQZXT8OE-bnH6OsxU79Ix5sgfw) можна дійти висновку, що для охорони інформації необхідно **здійснити певні дії** з метою збереження її конфіденційності. Можна обирати різні шляхи охорони інформації на підприємстві від розголошення та/або неправомірного використання. Пропоную такі:

1. *Розробити внутрішній документ* (положення, інструкція тощо) про комерційну таємницю та конфіденційну інформацію в компанії. Оскільки законодавство чітко не регулює це питання, такий документ буде внутрішньою нормативною підставою та основою для охорони секретної інформації. В ньому визначається перелік відомостей, доступ до яких обмежується, порядок зберігання, використання та поширення інформації, що становить комерційну таємницю/є конфіденційною, а також відповідальність працівників за її розголошення або неправомірне використання. Вказаний документ затверджується наказом керівника та доводиться до відома працівників під розписку.
2. *Укласти з працівниками договори про нерозголошення інформації* (Non-disclosure agreement, або NDA). Оскільки Кодекс законів про працю України не встановлює обов’язку працівників зберігати робочу інформацію в секреті, варто укладати окремі договори про нерозголошення з кожним працівником. До того ж, щоб мати можливість притягнути працівників за неправомірне поводження з інформацією до дисциплінарної відповідальності, слід додати умову про нерозголошення до посадових інструкцій та довести їх до відома працівників під розписку.
3. *Включити в господарські договори з контрагентами умови про конфіденційність.*Якщо ви укладаєте договори про надання послуг чи будь-які інші господарські договори, варто узгодити з контрагентами питання конфіденційності. Ці питання можна визначити в окремому розділі господарського договору або укласти договір про нерозголошення.
4. *Провести тренінг працівникам.*Саме собою визначення статусу комерційної таємниці та конфіденційності й підписання документів ще не гарантує, що працівники усвідомили свої обов’язки з інформаційної безпеки. Адже достатньо часто працівники можуть підписати угоду, але так і не зрозуміти, про що можна говорити, а про що ні. Тому варто провести тренінг-консультацію для працівників та пояснити, що саме вони підписують та про які «робочі питання» не варто говорити вдома за вечерею.

**Судова практика**

Слід звернути вашу увагу на той факт, що українські суди дедалі частіше почали розглядати справи щодо захисту конфіденційної інформації та пов’язані з цим спори.

Наприклад,Угода про нерозголошення – самостійний договір**.**У Постанові Західного апеляційного господарського суду від 28.02.2019 р. у справі [№907/258/18](https://reyestr.court.gov.ua/Review/80396820) зазначено, що укладений між сторонами договір (мається на увазі про нерозголошення конфіденційної інформації) є обов’язковим до виконання сторонами протягом строку його дії. Тому висновок суду першої інстанції на те, що спірний договір укладений у зв’язку та для забезпечення виконання контракту, тобто прямо пов’язаний з контрактом та є похідним від нього, вважається помилковим та суперечливим. Оспорюваний договір не містить вказівки на те, що укладається на виконання договору (контракту), натомість сторони врегулювали зазначене питання шляхом встановлення п. 4.7 договору, відповідно до положень якого зобов’язання сторін, визначені цим договором, залишаються чинними в межах строку дії цього договору, незалежно від припинення дії будь-яких інших договорів (контрактів), укладених між сторонами.

Ще один приклад – незаконне використання комерційної таємниці потребує доведення.ТОВ (позивач) звернувся до суду і вказав, що його співробітниця, з якою був підписаний договір про нерозголошення відомостей, у період перебування на лікарняному здійснила несанкціонований доступ через корпоративну поштову систему до інформації, що містить комерційну таємницю, з подальшим розголошенням такої інформації компанії-конкуренту, з яким відповідач вступив у трудові відносини. При цьому позивач доводив вину співробітниці, посилаючись на результати службового розслідування. Працівниця стверджувала, що інформацію не розголошувала, а в систему зайшла через цікавість. Суди всіх інстанцій, в тому числі Верховний суд у Постанові від 28.12.2019 р. у справі [№752/5775/16-ц](https://reyestr.court.gov.ua/Review/80304725), погодилися з тим, що факт входження в корпоративну систему відповідача зі свого домашнього комп’ютера за допомогою власного пароля ще не свідчить про використання комерційної таємниці та про будь-які порушення прав позивача.

**Як висновок,** варто зазначити, що захищати інформацію чи ні – це вибір кожного. Однак якщо ви хочете, щоб ваш бізнес був у безпеці, якщо ви хочете зберегти унікальність та конкурентоспроможність, то необхідно потурбуватися про те, щоб всі ваші секрети залишалися такими.