Як правильно захистити комерційну таємницю: практичний алгоритм для бізнесу

Клієнтська база, ціни та система знижок, технології, алгоритми роботи, фінансові моделі, бізнес-плани, внутрішня аналітика, умови співпраці з постачальниками можуть мати для бізнесу значно більшу цінність, ніж матеріальні активи.

Проте самого рішення керівника назвати певну інформацію «комерційною таємницею» недостатньо.

Для реального юридичного захисту бізнес має не лише визначити, **яка саме інформація є секретною**, а й запровадити систему її охорони та бути здатним довести, що така система фактично працювала.

Що вважається комерційною таємницею

Стаття 505 Цивільного кодексу України пов’язує статус комерційної таємниці з одночасною наявністю ключових ознак: інформація є секретною, не є легкодоступною для осіб, які зазвичай мають справу з відповідним видом інформації, має комерційну цінність саме через свою секретність та була предметом адекватних заходів щодо збереження секретності.

Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, крім інформації, яка відповідно до закону не може бути віднесена до комерційної таємниці.

Комерційна таємниця виникає не лише тому, що компанія назвала інформацію таємною. Необхідно фактично забезпечити режим її секретності.

Що бізнес може захищати

Залежно від специфіки діяльності до комерційної таємниці можуть бути віднесені, наприклад:

- клієнтські та партнерські бази;
- індивідуальні комерційні умови;
- закупівельні та продажні ціни;
- система знижок і бонусів;
- бізнес-плани та стратегії;
- бюджети і внутрішня фінансова аналітика;
- технології та виробничі процеси;
- формули, рецептури, креслення;
- програмні рішення та внутрішні алгоритми;
- маркетингові стратегії;
- результати внутрішніх досліджень;
- інформація про переговори та майбутні проєкти;
- внутрішні методики організації бізнес-процесів.

Перелік має формуватися індивідуально для конкретної компанії. Надмірно загальне формулювання на кшталт «усі відомості про діяльність підприємства є комерційною таємницею» саме по собі не створює ефективної системи захисту.

Що не можна просто оголосити комерційною таємницею

Постанова Кабінету Міністрів України від 09.08.1993 № 611 встановлює перелік відомостей, що не становлять комерційної таємниці.

До них, зокрема, віднесено установчі документи, документи, що дозволяють здійснювати господарську діяльність та її окремі види, інформацію за встановленими формами державної звітності, дані, необхідні для перевірки обчислення і сплати податків та інших обов’язкових платежів, документи про їх сплату, документи про платоспроможність та інші визначені постановою

відомості.

Тому перед затвердженням внутрішнього переліку комерційної таємниці потрібно перевірити, чи законодавство не встановлює для відповідної інформації інший режим.

NDA недостатньо

Одна з типових помилок бізнесу: укласти з працівником або контрагентом NDA і вважати питання захисту інформації закритим.

NDA є важливим елементом системи, але не замінює її.

Якщо компанія заявляє, що певна база клієнтів є комерційною таємницею, але одночасно:

- доступ до неї мають практично всі працівники;
- файли зберігаються без обмежень;
- працівники пересилають їх на особисту пошту;
- документи не маркуються;
- доступ колишніх працівників своєчасно не припиняється;
- не ведеться журналювання дій користувачів,

у судовому спорі закономірно виникне питання: **які саме адекватні заходи компанія вживала для збереження секретності цієї інформації?**

Як побудувати систему захисту

1. Провести аудит інформації

Спочатку необхідно визначити, яка інформація дійсно має економічну цінність для бізнесу і розголошення якої може завдати шкоди.

Не потрібно намагатися засекретити все.

Чим точніше визначено об’єкт захисту, тим простіше встановити

правила доступу та в майбутньому довести порушення.

2. Затвердити перелік комерційної таємниці

Доцільно оформити внутрішній документ, у якому визначити конкретні категорії інформації, що становлять комерційну таємницю.

Працівники, які працюють з такими даними, повинні розуміти, **які саме відомості вони зобов’язані не розголошувати**.

3. Запровадити Положення про комерційну таємницю

Це один із базових документів системи.

У ньому доцільно визначити:

- поняття та категорії захищеної інформації;
- перелік осіб, які можуть отримувати доступ;
- порядок надання та припинення доступу;
- правила копіювання та передачі інформації;
- правила використання корпоративної та особистої електронної пошти;
- порядок роботи з паперовими документами;
- правила зберігання електронних файлів;
- порядок роботи з інформацією поза офісом;
- процедуру повернення або знищення носіїв;
- порядок дій при виявленні витоку;
- відповідальних за організацію режиму конфіденційності.

4. Укласти NDA та передбачити конфіденційність у договорах

Зобов’язання щодо нерозголошення доцільно встановлювати не лише для штатних працівників.

Вони можуть бути необхідними у відносинах із:

- підрядниками;
- консультантами;
- бухгалтерами;
- IT-фахівцями;
- маркетинговими агентствами;
- потенційними інвесторами;
- постачальниками;
- дистриб’юторами;
- іншими особами, які отримують доступ до чутливої інформації.

У договорі важливо не обмежуватися фразою «сторона зобов’язується не розголошувати конфіденційну інформацію».

Необхідно визначити, **яка інформація охороняється, як її можна використовувати, кому дозволено її передавати, протягом якого строку діють відповідні обмеження та які наслідки матиме порушення**.

5. Обмежити доступ за принципом «необхідно для роботи»

Менеджеру з продажу не обов’язково мати доступ до всієї фінансової інформації підприємства, а бухгалтеру до технологічної документації виробництва.

Доцільно застосовувати принцип мінімально необхідного доступу: працівник отримує тільки ті дані, які потрібні йому для виконання конкретних функцій.

Це одночасно зменшує ризик витоку та полегшує встановлення джерела інциденту.

6. Забезпечити технічний захист

Юридичні документи повинні доповнюватися IT-заходами.

Залежно від масштабів бізнесу це можуть бути:

- персоналізовані облікові записи;
- багатофакторна автентифікація;
- розмежування прав доступу;
- шифрування;
- журналювання операцій;
- резервне копіювання;
- контроль зовнішніх носіїв;
- обмеження можливості завантаження або копіювання файлів;
- корпоративні системи обміну інформацією;
- моніторинг аномальної активності.

7. Встановити процедуру звільнення працівників

Окремою зоною ризику є припинення трудових або договірних відносин.

У день припинення доступу до інформації варто забезпечити:

- блокування корпоративних облікових записів;
- зміну необхідних паролів;
- відкликання прав доступу;
- повернення ноутбуків, телефонів, накопичувачів та документів;
- перевірку корпоративних сховищ;
- документальне підтвердження повернення майна та носіїв;
- нагадування про збереження чинних зобов’язань щодо конфіденційності.

Що робити, якщо витік уже стався

Перші дії компанії можуть визначити результат майбутнього судового спору.

Насамперед потрібно **зафіксувати докази**, а не просто видалити файл, заблокувати користувача чи провести усну розмову з

працівником.

Доцільний алгоритм:

1. **Локалізувати інцидент.**
   Обмежити подальший несанкціонований доступ та поширення інформації.
2. **Зафіксувати цифрові докази.**
   Зберегти журнали доступу, електронне листування, файли, історію завантажень, інформацію про користувачів, резервні копії та інші цифрові сліди.
3. **Провести внутрішнє розслідування.**
   Встановити, хто мав доступ до інформації, коли відбулося копіювання чи передача та кому могла бути передана інформація.
4. **Оцінити шкоду.**
   Необхідно встановити не лише факт витоку, але й його економічні наслідки.
5. **Визначити правовий механізм реагування.**
   Це може бути договірна претензія, судовий захист або, залежно від характеру порушення, звернення до компетентних державних органів.

Судова практика: наявність NDA ще не означає перемогу в суді

Показовою є постанова Верховного Суду від 28.02.2019 у справі № 752/5775/16-ц.

ТОВ «Смайл-Експо» звернулося до суду у зв’язку з можливим неправомірним використанням комерційної таємниці працівницею.

При цьому в компанії існував наказ про віднесення певних відомостей до комерційної таємниці, а працівниця підписала угоду про нерозголошення. Під час службового розслідування було також зафіксовано її доступ до корпоративної системи Redmine.

Однак цього виявилося недостатньо.

Верховний Суд погодився з висновком про відмову в позові, оскільки позивач не надав належних та допустимих доказів неправомірного використання працівницею комерційної таємниці.

Сам факт входу працівника до корпоративної системи не доводив факту розголошення комерційної таємниці.

Практичний висновок із цієї справи

Для судового захисту недостатньо показати:

> ***«Працівник мав доступ до секретної інформації».***

Потрібно сформувати доказовий ланцюг:

яка конкретно інформація була комерційною таємницею → який режим захисту щодо неї діяв → хто отримав доступ → які конкретні дії ця особа вчинила → у чому полягає порушення прав компанії → які наслідки воно спричинило.

Саме доказова база часто стає слабким місцем компанії у спорі.

Чекліст для бізнесу

Перевірте, чи має ваша компанія:

- затверджений перелік відомостей, що становлять комерційну таємницю;
- внутрішнє положення про порядок роботи з такою інформацією;
- визначене коло осіб із доступом;
- NDA та умови про конфіденційність у договорах;
- підтвердження ознайомлення працівників із правилами;
- технічне розмежування прав доступу;
- журналювання дій користувачів;
- правила передачі та копіювання інформації;
- процедуру припинення доступу при звільненні;

- порядок реагування на витоки;
- процедуру збереження електронних доказів.

Якщо частина цих елементів відсутня, режим захисту комерційної таємниці варто переглянути **до виникнення інциденту**, а не після нього.

Головний висновок

Ефективний захист комерційної таємниці складається щонайменше з трьох рівнів:

- **юридичного**: внутрішні документи, NDA, договори та визначення режиму інформації;
- **організаційного**: обмеження доступу, навчання персоналу, процедури прийняття і звільнення працівників, внутрішній контроль;
- **технічного**: управління доступом, журналювання, шифрування, резервування та інші засоби інформаційної безпеки.

І лише їх поєднання дозволяє компанії не просто назвати інформацію комерційною таємницею, а створити реальний механізм її захисту.

Компанія «Вікторія» може допомогти провести юридичний аудит системи захисту конфіденційної інформації, розробити Положення про комерційну таємницю, NDA, договірні положення про конфіденційність та алгоритм дій на випадок витоку інформації.

Детальніше про юридичний супровід:

Ваше ім'я (обов'язково)

Ваш email (обов'язково)

Ваш номер телефону (обов'язково)

Ваше повідомлення

Відправити

Приєднуйтесь до нашого ТГ каналу: Компанія Вікторія – юридичні та бухгалтерські рішення для бізнесу в Україні та за кордоном.
 victorija.ua

Політика конфіденційності

1. Загальні положення

Ця Політика конфіденційності розроблена відповідно до Закону України від 01 червня 2010 року № 2297-VI «Про захист персональних даних» (надалі – «Закон»). Під “персональними даними” розуміються відомості або сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Ми поважаємо конфіденційність наших клієнтів і осіб, які користуються нашими послугами. Згідно з цією Політикою конфіденційності, під “особистою інформацією” розуміється будь-яка інформація, що дозволяє ідентифікувати особу, зокрема ім’я, прізвище, контактні дані (адреса електронної пошти, номер телефону), а також інші відомості, надані Вами добровільно. Ми збираємо ці дані безпосередньо від Вас під час реєстрації на нашому сайті або під час взаємодії з нами.

2. Мета збору та використання персональних даних

Ми збираємо Ваші персональні дані для надання наших послуг

відповідно до Ваших потреб, для виконання договірних зобов’язань, а також для відповідей на Ваші запитання. Ваші контактні дані можуть використовуватися для інформування Вас про нові послуги, акції чи інші новини.

Зберігання персональних даних здійснюється стільки, скільки це необхідно для виконання мети, визначеної цією Політикою, або протягом строку, встановленого чинним законодавством України.

3. Передача даних третім особам

Ми не передаємо персональні дані третім особам без Вашої згоди, за винятком випадків, передбачених законодавством України або для запобігання правопорушенням.

4. Захист інформації

Ми впроваджуємо всі необхідні технічні та організаційні заходи для захисту Ваших даних від несанкціонованого доступу, втрати, зміни чи розголошення. До цих заходів належать шифрування, контроль доступу, а також фізичний захист серверів і баз даних.

5. Зміна Політики конфіденційності

Ми можемо періодично вносити зміни до цієї Політики конфіденційності. Оновлена версія буде доступна на нашому сайті, і ми повідомимо Вас про всі істотні зміни.

Якщо у Вас виникли питання або Ви хочете видалити свої персональні дані, будь ласка, зв’яжіться з нами за електронною адресою: office@vg.ua