Організація захисту комерційної таємниці

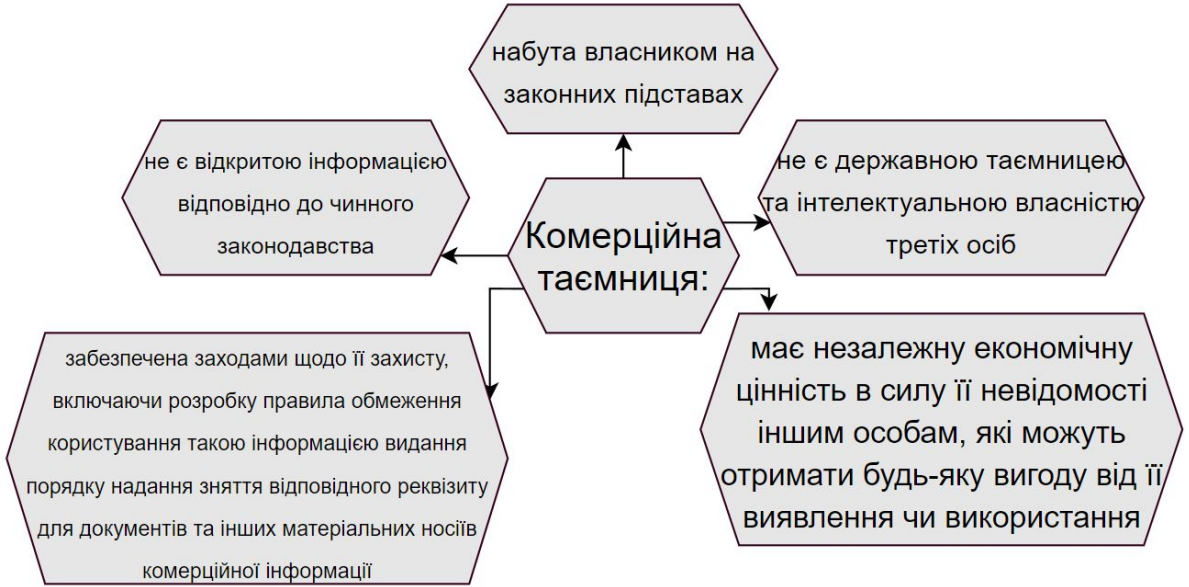
Виконав студент групи ФІТ 12-4 Ліщук Олег

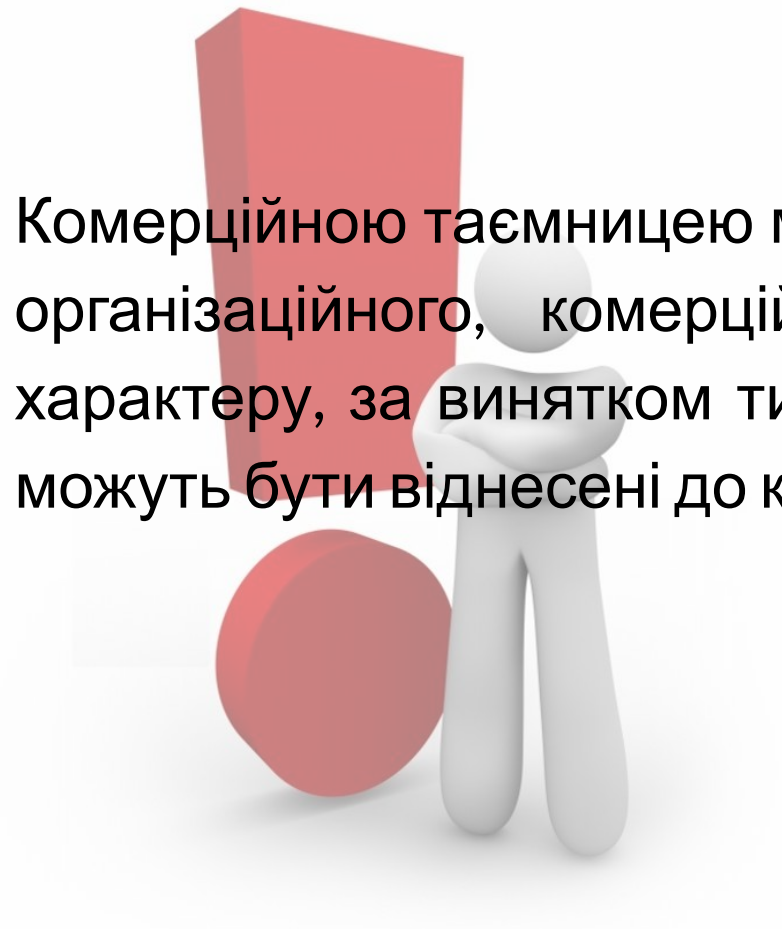
Комерційна таємниця

Поняття комерційної таємниці

Комерційна таємни́ця — інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Ознаки інформації, що відноситься до комерційної таємниці



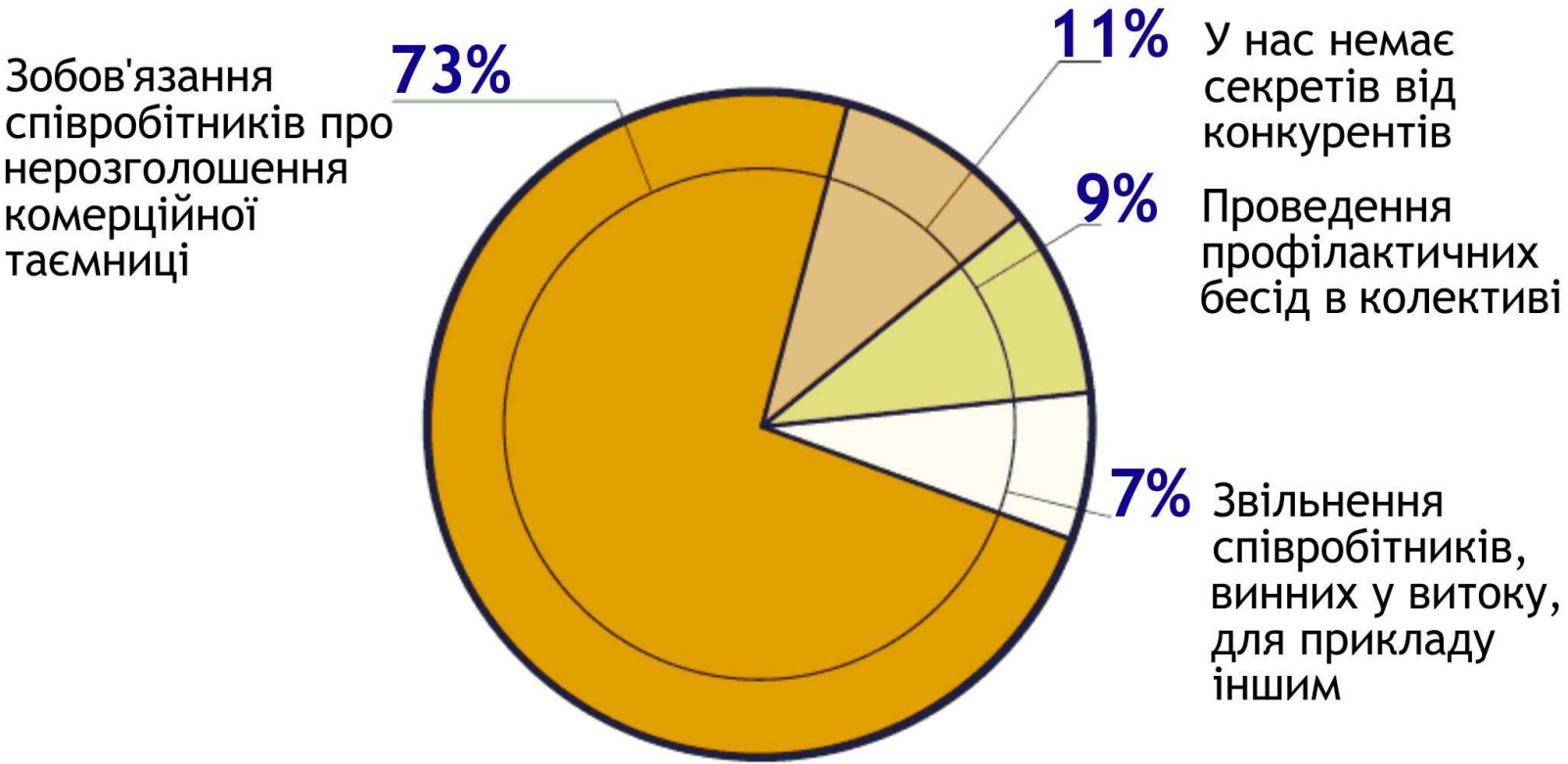


Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, **які відповідно до закону** не можуть бути віднесені до комерційної таємниці.

Конфіденційна інформація і комерційна таємниця - тотожність чи відмінність

Захист комерційної таємниці

Як захищати комерційну інформацію?



Що робити з початку?

Перш за все, компанії повинні почати з належних процедур реєстрації.

Всі співробітники повинні підписати контракт з положеннями про нерозголошення, коли вони погоджуються не розголошувати конфіденційну інформацію.

Додатково

Іншим пунктом, який може бути включений в контракт, є пункт, який не допускає конкуренції, який забороняє співробітникам працювати на аналогічній посаді в фірмі-конкуренті або починати бізнес з конфіденційною інформацією підприємства.

Ці угоди завжди пов'язані обмеженнями в часі і географічними кордонами. Саме тому компаніям необхідно вжити додаткових заходів для захисту комерційної таємниці.

По-перше

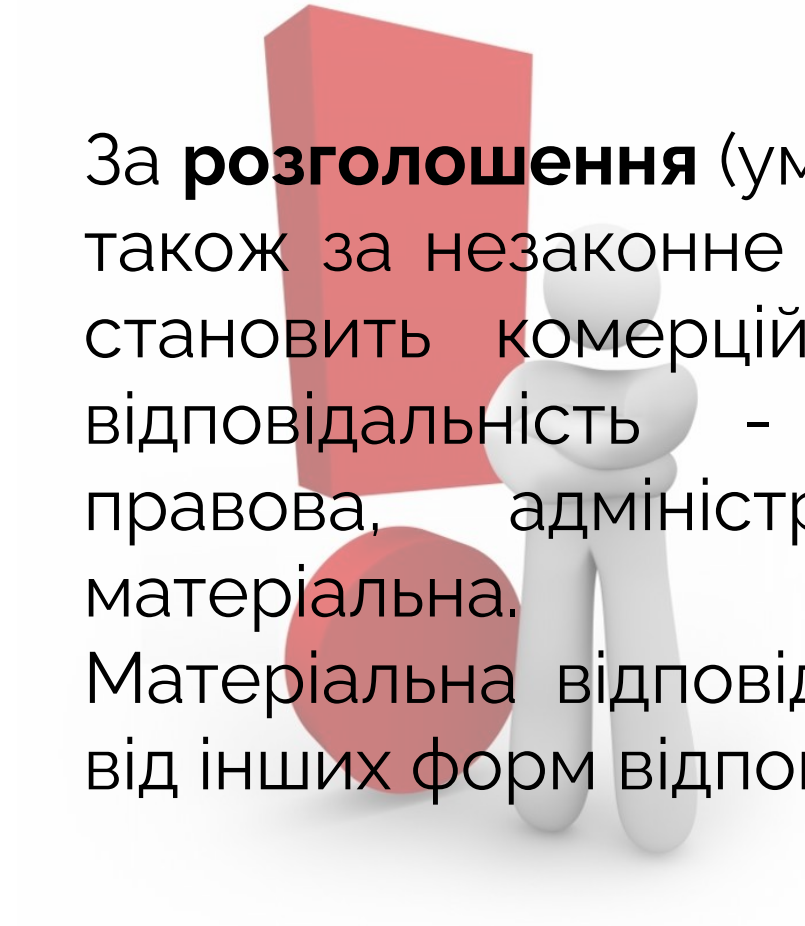
Роботодавці повинні постійно відслідковувати електронну пошту співробітників і роботу, яку вони виконують на пристроях компанії.

Крім того, повинна існувати політика, яка зобов'язує співробітників виконувати всі свої обов'язки на пристроях компанії, а не на особистих пристроях. Проте, весь цей моніторинг повинен проводитися з обмеженнями, конфіденційність співробітників повинна дотримуватися, в іншому випадку це може стати загрозою для лояльності співробітників.

По-друге

Слід проводити заключні співбесіди з усіма звільняються співробітниками, нагадуючи їм про зобов'язання після закінчення трудової діяльності щодо нерозголошення комерційної таємниці.

Весь інвентар та носії конфіденційної інформації, надані працівникові, повинні бути повернуті назад.



За **розголошення** (умисне або з необережності), а також за незаконне використання інформації, що становить комерційну таємницю, передбачена відповідальність - дисциплінарна, цивільно-правова, адміністративна, кримінальна та матеріальна.

Матеріальна відповідальність **настає незалежно** від інших форм відповідальності.

Комп'ютерне шпигунство

Адміністрації слід насторожитися в наступних випадках

- без серйозних на те причин проводиться перезапис баз даних
- дані не обновлюються
- на ключових документах з'являються підроблені підписи
- виникають фальшиві записи

А також

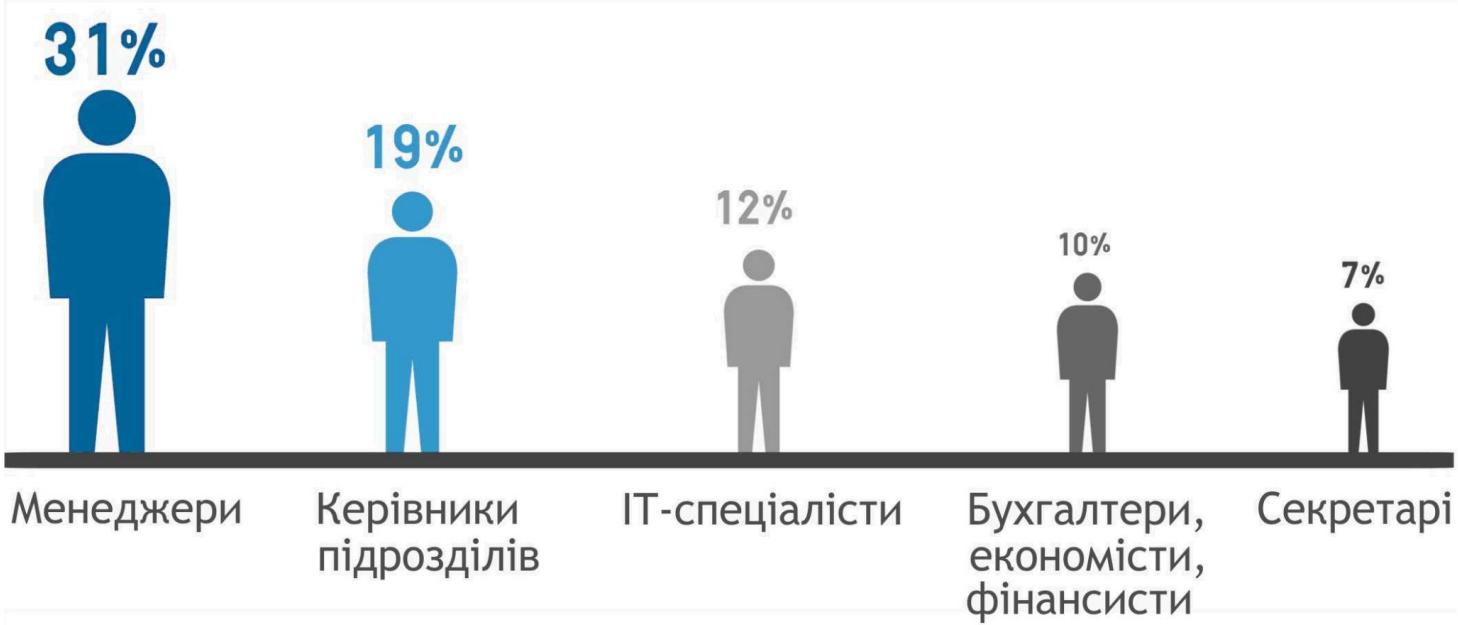
- персонал системи без видимих підстав починає працювати надурочно
- персонал заперечує проти контролю над записом даних
- співробітники, що мають справу з комп'ютерами, неадекватно реагують на рутинні питання

Запобігання витоку інформації

Будьте пильні!

Нещодавні дослідження показують, які категорії співробітників частіше за інших "зливають" комерційні таємниці.

Звідки витікає інформація?



Інструкція про проведення копіювальних робіт

Каналом витоку інформації можуть стати копіювання та розмноження документації, тому на підприємстві повинна бути розроблена інструкція, що встановлює:

- порядок обліку документів що поступають на копіювання, реєстрації підстав для їхнього копіювання та особи, яка санкціонувала копіювання;
- перелік осіб, безпосередньо відповідальних за копіювання, видачу підготовлених документів виконавцеві, облік чернеток, бракованих екземплярів та їх знищення.

Контроль над пересиланням і передачею інформації

При розробці правил пересилання документальних і магнітних носіїв інформації необхідно виходити з того, що після відправлення носіїв підприємство фактично втрачає над ними контроль.

Ця обставина змушує **максимально** звузити коло осіб, яким дозволено санкціонувати пересилання носіїв комерційної таємниці.

Захист переданої інформації

При використанні каналів зв'язку для передачі конфіденційної інформації слід мати на увазі, що більшість із них уразливі для несанкціонованого знімання даних.

Для захисту переданої інформації можуть використовуватися ліцензійні криптографічні засоби захисту, фельдзв'язок і спецзв'язок, відправлення рекомендованих листів і т.п.

Постановка діловодства

В охороні комерційної таємниці важлива постановка діловодства на підприємстві, введення єдиного порядку обліку, руху й зберігання документів, що визначає:

- порядок встановлення ступеня конфіденційності підготовлених матеріалів, їхні печатки, оформлення, адресування, відправлення вихідних і реєстрації вхідних документів

Постановка діловодства

- особливості роботи з розпорядними документами (наказами, циркулярами й т.п.)
- порядок формування справ, їх зберігання й передачі в архіви, у тому числі державні
- порядок перевірки наявності документів. Перевірку схоронності необхідно проводити періодично й обов'язково фіксувати її результати.

Створення служби безпеки

Охорона комерційних таємниць

У промислово розвинених країнах охороною комерційних таємниць підприємства займаються як окремі особи, так і внутрішні підрозділи (власник підприємства, члени правління, заступники керівника із загальних питань, кадрові служби, спеціально створені підрозділи, режимно-секретні органи підприємства й т. п.).

Служба безпеки

Конкретна структура внутрішньої системи захисту комерційної таємниці визначається фінансовими й технічними можливостями підприємства, його розмірами й розміщенням, номенклатурою продукції, що випускається, системою внутрішнього документообігу, обсягом і видом інформації, що захищається, і т.п. При виборі варіантів побудови доцільно враховувати можливості конкурентів.

Найдоцільніше **обмежити** число осіб, що допускаються до секретної інформації, розробити заходи персональної матеріальної й правової відповідальності за збереженість комерційної таємниці.

Контроль над персоналом

При прийомі на роботу

При прийомі менеджера в контракті необхідно вказати форми й розміри його **персональної відповідальності** за схоронність інформації, обговорити конкретні обов'язки, заборонити використання інформації на шкоду підприємству, визначити умови **розірвання** контракту при невиконанні вимог конфіденційності.

Трудовий договір

У трудовому договорі, що укладається між адміністрацією підприємства (підприємцем) і працівником, **необхідно** доцільно відображати індивідуальні зобов'язання останнього за схоронність комерційної таємниці.

Цей документ буде юридичною основою для застосування санкцій до працівників, **винних** у витоку конфіденційної інформації.

Список використаної літератури

- Незаконні дії щодо комерційної або банківської таємниці // Велика українська юридична енциклопедія. У 20 т. Т. 17. Кримінальне право / В. Я. Тацій (відп. ред.) та ін. — 2017. — С. 592.
- Комерційна таємниця // Термінологічний словник з питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму, фінансуванню розповсюдження зброї масового знищення та корупції / А. Г. Чубенко, М. В. Лошицький, Д. М. Павлов, С. С. Бичкова, О. С. Юнін. — Київ : Ваіте, 2018. — С. 342.
- КОМЕРЦІЙНА ТАЄМНИЦЯ //Юридична енциклопедія : [у 6 т.] / ред. кол. Ю. С. Шемшученко (відп. ред.) [та ін.]. — К. : Українська енциклопедія ім. М. П. Бажана, 1998—2004.
- Розголошення комерційної таємниці // Юридична енциклопедія : [у 6 т.] / ред. кол. Ю. С. Шемшученко (відп. ред.) [та ін.]. — К. : Українська енциклопедія ім. М. П. Бажана, 2003. — Т. 5 : П — С. — 736 с.

Дякую за увагу!