

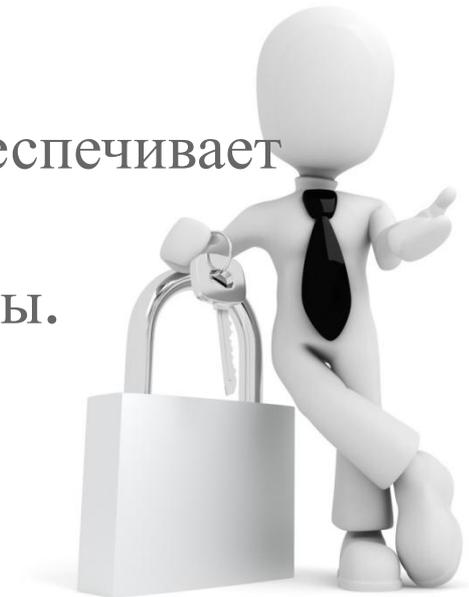
Коммерческая тайна

Презентацию подготовила
студентка: Заводовская Н.И.
Группа : ЭМЭ-42

Коммерческая тайна

Коммерческая тайна — это преднамеренно скрываемые по коммерческим соображениям экономические интересы и сведения о различных сторонах и сферах деятельности фирмы.

- Защищаемая информация обеспечивает ряд преимуществ компании для эффективной конкурентной борьбы.



Признаки коммерческой тайны

1. Информация должна иметь действительную или потенциальную коммерческую ценность.
2. К информации, составляющей коммерческую тайну, не должно быть свободного доступа на законном основании.
3. Для того, чтобы информация считалась коммерческой тайной, требуется, чтобы обладатель такой информации принимал меры к охране ее конфиденциальности.

Только при соблюдении этих трех условий у предпринимателя есть возможность защитить свои права в судебном порядке.

Срок охраны коммерческой тайны не ограничен.

Примеры коммерческих тайн

- Производственные процессы (данные о способах производства, схемы, чертежи)
- (Химические) формулы: напитки, пища, косметика, лекарства, и т.д.
- Программное обеспечение
- Проекты и модели
- Процедуры испытания
- Маркетинг, развитие и исследование, стратегические планы
- Отрицательная информация (процессы, которые не работали, и т.д.)
- Списки клиентов и информация о клиентах
- Деловые переговоры
- Новые идеи, методы, понятия и т.д.



Не относятся к коммерческой тайне

:

- учредительные документы (Устав)
- разрешительные документы (свидетельство о регистрации, лицензии, сертификаты)
- документация, подтверждающая уплату налогов и обязательных платежей;
- данные о составе, численности работающих, их условиях труда, зарплате;
- документы о платежеспособности;
- сведения о реализации продукции, причиняющей вред здоровью населения;
- сведения о загрязнении окружающей среды, состояния противопожарной безопасности, эпидемиологической обстановке и т. д.

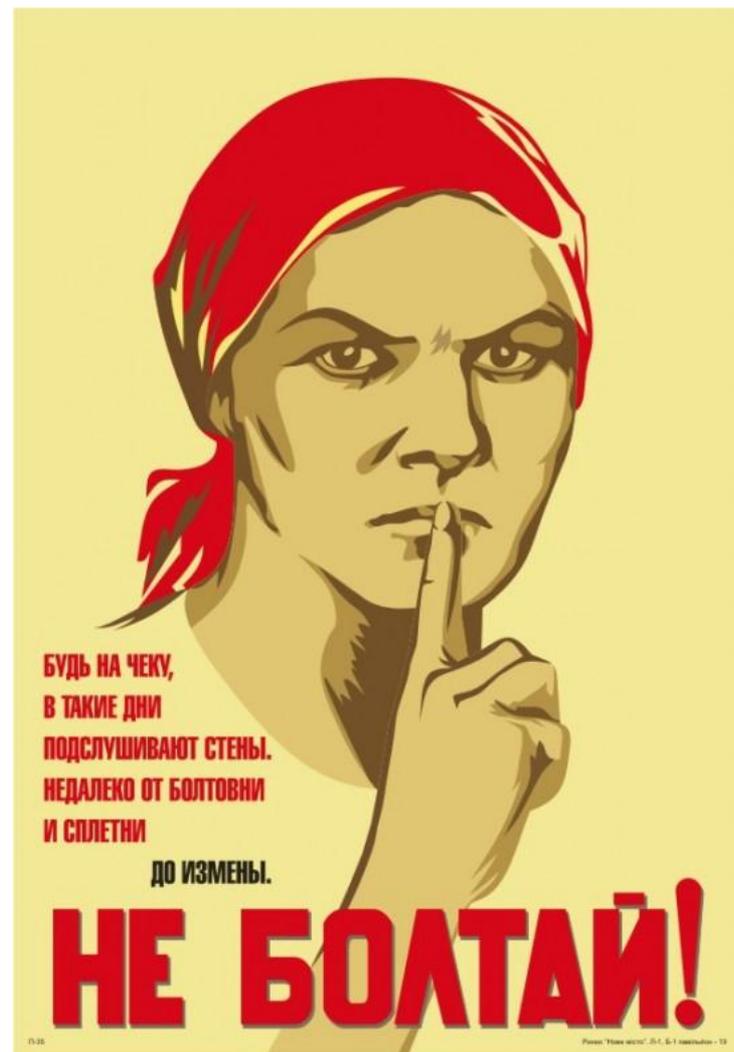
Введение режима охраны коммерческой тайны



1. определение перечня информации, составляющей коммерческую тайну;
2. ограничение доступа к информации (установления порядка обращений с этой информацией и контроля за соблюдением порядка);
3. учет лиц, получивших доступ к информации;
4. регулирование отношений по использованию информации работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
5. нанесение на материальные носители (документы) грифа «конфиденциально», «строго конфиденциально» и др.

Режим коммерческой тайны

В целях охраны конфиденциальности информации предприятие обязано ознакомить с установленным режимом коммерческой тайны под расписку всех работников, с которых берется подписка о неразглашении коммерческой тайны.



Закон «О коммерческой тайне»

Обладатель информации, составляющей коммерческую тайну, имеет право защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами информации, составляющей коммерческую тайну, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

Законом «О коммерческой тайне» предусматривается, что его нарушение влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность.

Причины утечки информации:

- Несовершенное состояние организации управления на предприятии, недостатки подбора, оснащения и обучения специалистов службы безопасности.
- Недостатки в организации обеспечения режима секретности, факты неудовлетворительной постановки учета и отчетности, не проводятся регулярные проверки и инвентаризации, недостаточный контроль выполнения инструкций и правил, низкое финансирование работ, связанных с режимом секретности.

Каналами утечки информации могут быть:

- Каналы связи, включая телефон, радиосвязь, телеграф, Интернет и переписку;
- Человеческий фактор — при приеме и увольнении сотрудников компании;
- Материальные потоки — включают транспортировку секретных изделий, документов, доставку специальной почты;
- Реклама, интервью для СМИ, публикации в печати.
- Совместная деятельность с прочими организациями;
- Переманивание ценных кадров конкурентов, чтобы получить их знания и информацию;
- Данные на компьютере: копирование программной информации с носителей, чтение распечаток, хищение носителей информации и пр.

