Коммерческая тайна. Способы защиты.

ОИБ 2017 Кудряшов Дмитрий Бис-21

Понятие коммерческой тайны и порядок отнесения информации к коммерческой тайне.

Коммерческая тайна – преднамеренно скрываемые экономические интересы и информация о различных сторонах производственной, управленческой, научно-технической, финансовой деятельности предприятия, охрана которых обусловлена интересами конкуренции и возможной угрозой экономической безопасности предприятия.

Коммерческая тайна предприятия – сведения, связанные с производством, управлением, финансовой деятельностью предприятия, разглашение которых может привести к ущербу его интересов.

Информация, составляющая коммерческую тайну, должна соответствовать следующим требованиям:

- иметь действительную или потенциальную ценность для предприятия по коммерческим признакам.
- не является общеизвестной и общедоступной.
- должна быть соответствующим образом помечена (совершенно секретно, для служебного пользования и др.)
- не должна являться государственным секретом и защищаться авторским или патентным правом.
- не должна касаться негативной деятельности предприятия.

Положении о коммерческой тайне определена информация, которая не может быть отнесена к коммерческой тайне :

- учредительные документы, лицензии.
- сведения по установленным формам отчетности предприятия.
- документы о платежеспособности.
- данные ля проверки правильности уплаты налогов и других обязательных платежей.
- сведения о численности, составе работающих, их заработной плате, условиях труда.

Каждое предприятие…

имеет специфику, поэтому перечень сведений, составляющих коммерческую тайну, определяет специально созданная группа экспертов из числа экономистов, маркетологов, коммерсантов. К коммерческой тайне могут быть отнесены:

- Деловая информация : финансовые сведения, технология, деловые планы и планы производства новой продукции, стратегия предприятия, списки клиентов, соглашения и предложения, контракты и договоры, информация о деловых качествах сотрудников и др.
- Научно-техническая информация: научно-исследовательские проекты, конструкторские разработки, технические параметры новой продукции, заявки на патенты, дизайн новой продукции, технические возможности производственного оборудования, программное обеспечение ПЭВМ, информационные технологии и др.

Со стороны закона.

Статья 1. Цели и сфера действия настоящего Федерального закона
Статья 3. Основные понятия, используемые в настоящем Федеральном законе
Статья 4. Право на отнесение информации к информации, составляющей коммерческую тайну, и способы получения такой информации
Статья 5. Сведения, которые не могут составлять коммерческую тайну
Статья 10. Охрана конфиденциальности информации
Статья 11. Охрана конфиденциальности информации, составляющей коммерческую тайну, в рамках трудовых отношений
Статья 14. Ответственность за нарушение настоящего Федерального закона

Не указанные или пропущенные статьи либо утратили силу, либо не касаются темы.

Статья 10. Охрана конфиденциальности информации.

1. Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

- 1) определение перечня информации, составляющей коммерческую тайну;
- 2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
- 3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;
- 4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
- 5) нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа "Коммерческая тайна" с указанием обладателя такой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства) (пункт в редакции, введенной в действие с 26 июля 2011 года Федеральным законом от 11 июля 2011 года N 200-ФЗ.

2. Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер, указанных в части 1 настоящей статьи.

3. Индивидуальный предприниматель, являющийся обладателем информации, составляющей коммерческую тайну, и не имеющий работников, с которыми заключены трудовые договоры, принимает меры по охране конфиденциальности информации, указанные в части 1 настоящей статьи, за исключением пунктов 1 и 2, а также положений пункта 4, касающихся регулирования трудовых отношений.

4. Наряду с мерами, указанными в части 1 настоящей статьи, обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству Российской Федерации меры.

5. Меры по охране конфиденциальности информации признаются разумно достаточными, если:

- 1) исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;

- 2) обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

6. Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Статья 11. Охрана конфиденциальности информации, составляющей коммерческую тайну, в рамках трудовых отношений

1. В целях охраны конфиденциальности информации, составляющей коммерческую тайну, работодатель обязан:

- 1) ознакомить под расписку работника, доступ которого к этой информации, обладателями которой являются работодатель и его контрагенты, необходим для исполнения данным работником своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну;
- 2) ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;
- 3) создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

2. Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями.

3. В целях охраны конфиденциальности информации, составляющей коммерческую тайну, работник обязан:

- 1) выполнять установленный работодателем режим коммерческой тайны;
- 2) не разглашать эту информацию, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях в течение всего срока действия режима коммерческой тайны, в том числе после прекращения действия трудового договора;
- 3) возместить причиненные работодателю убытки, если работник виновен в разглашении информации, составляющей коммерческую тайну и ставшей ему известной в связи с исполнением им трудовых обязанностей;
- 4) передать работодателю при прекращении или расторжении трудового договора материальные носители информации, имеющиеся в пользовании работника и содержащие информацию, составляющую коммерческую тайну.

4. Работодатель вправе потребовать возмещения убытков, причиненных ему разглашением информации, составляющей коммерческую тайну, от лица, получившего доступ к этой информации в связи с исполнением трудовых обязанностей, но прекратившего трудовые отношения с работодателем, если эта информация разглашена в течение срока действия режима коммерческой тайны.

5. Причиненные работником или прекратившим трудовые отношения с работодателем лицом убытки не возмещаются, если разглашение информации, составляющей коммерческую тайну, произошло вследствие несоблюдения работодателем мер по обеспечению режима коммерческой тайны, действий третьих лиц или непреодолимой силы.

6. Трудовым договором с руководителем организации должны предусматриваться его обязанности по обеспечению охраны конфиденциальности составляющей коммерческую тайну информации, обладателем которой являются организация и ее контрагенты, и ответственность за обеспечение охраны конфиденциальности этой информации.

- 7. Руководитель организации возмещает организации убытки, причиненные его виновными действиями в связи с нарушением законодательства Российской Федерации о коммерческой тайне. При этом убытки определяются в соответствии с гражданским законодательством.

- 8. Работник имеет право обжаловать в судебном порядке незаконное установление режима коммерческой тайны в отношении информации, к которой он получил доступ в связи с исполнением трудовых обязанностей.

Статья 14. Ответственность за нарушение настоящего Федерального закона

1. Нарушение настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. Работник, который в связи с исполнением трудовых обязанностей, получил доступ к информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет дисциплинарную ответственность в соответствии с законодательством Российской Федерации.

3. Органы государственной власти, иные государственные органы, органы местного самоуправления, получившие доступ к информации, составляющей коммерческую тайну, несут перед обладателем информации, составляющей коммерческую тайну, гражданско-правовую ответственность за разглашение или незаконное использование этой информации их должностными лицами, государственными или муниципальными служащими указанных органов, которым она стала известна в связи с выполнением ими должностных (служебных) обязанностей.

4. Лицо, которое использовало информацию, составляющую коммерческую тайну, и не имело достаточных оснований считать использование данной информации незаконным, в том числе получило доступ к ней в результате случайности или ошибки, не может в соответствии с настоящим Федеральным законом быть привлечено к ответственности.

5. По требованию обладателя информации, составляющей коммерческую тайну, лицо, указанное в части 4 настоящей статьи, обязано принять меры по охране конфиденциальности информации. При отказе такого лица принять указанные меры обладатель информации, составляющей коммерческую тайну, вправе требовать в судебном порядке защиты своих прав.

Наказание за Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну

Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом — наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо исправительными работами на срок до одного года, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, — наказываются штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до трех лет, либо лишением свободы на тот же срок.

Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, — наказываются штрафом в размере до одного миллиона пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия, — наказываются принудительными работами на срок до пяти лет либо лишением свободы на срок до семи лет.

Порядок действий для наказания сотрудника.

Для того чтобы обвинить сотрудника в разглашении коммерческой тайны и наказать его за это, должны выполняться два условия:

1.На предприятии должен быть введен режим коммерческой тайны, то есть, обеспечены мероприятия по ее защите и ограничению к ней доступа третьих лиц.

2.Работодатель должен доказать факт разглашения данных конкретным сотрудником, причем доказательства должны быть весомыми.

процедура наказания сотрудника

1.Установление работодателем факта разглашения (может происходить на основании как прямых, так и косвенных доказательств).
2.Проведение внутреннего расследования на предприятии с изучением всех обстоятельств дела.
3.Отправка подозреваемому в разглашении сотруднику письменного запроса с требованиями объяснить установленный факт нарушения. В запросе должны быть описаны обстоятельства и причины, при помощи которых работодатель сделал выводы о разглашении. После ознакомления с документом сотрудник должен подтвердить это своей подписью.
4.Ожидание письменного объяснения от работника относительно выдвигаемого ему обвинения. На составление этого документа отводится два дня. Если сотрудник игнорирует запрос и ничего не объясняет, работодатель должен составить соответствующий акт.
5.Создание специальной комиссии, которая займется анализом и оценкой обнаруженных обстоятельств, после чего примет решение об ответственности, которую понесет работник. В конце всех этих действий составляется протокол.
6.Издание приказа о применении к работнику ответственности (например, штрафа или увольнения).
7.Непосредственное выполнение изданного приказа и наказание работника.

Соблюдение законной процедуры и выполнение всех вышеуказанных действий – важное требование, поскольку без него наказание может быть засчитано как неправомерное.

Если в качестве способа воздействия к сотруднику применяется материальная ответственность, то размер компенсации также должна рассчитывать специальная комиссия.

Во внимание при этом принимаются только реальные, а не потенциальные убытки.

Разглашение коммерческой тайны является серьезным нарушением со стороны сотрудника, ведь это может принести предприятию большие убытки.

В зависимости от вида разглашения и степени его тяжести сотрудник может быть наказан штрафом, необходимостью возмещать ущерб компании и даже увольнением.

Главное при этом – доказать нарушение со стороны сотрудника, ведь действия работодателя могут быть оспорены в суде. К ответственности за разглашение могут быть привлечены не только сотрудники, работающие в компании, но также и уволенные ранее.

Мероприятия по защите коммерческой тайны.

Каналы утечки информации о коммерческой тайне :

- 1)Неформальные : выставки, семинары, конференции, презентации, средства массовой информации.
- 2)Формальные : деловые встречи, переговоры, обмен технической документацией, персонал фирмы, государственные органы и страховые компании.

Большой ущерб предприятию может нанести промышленный шпионаж – незаконный сбор сведений, составляющих коммерческую тайну. Основную роль в сохранении коммерческой тайны играют сами организации, которые должны проводить организационные, технические, правовые мероприятия.

К организационным мерам можно отнести :

- Создание служб безопасности предприятия.
- Руководитель организации утверждает Положение по защите коммерческой тайны, с которым под личную подпись должны быть ознакомлены лица, имеющие к ней доступ. Руководитель приказом издает перечень сведений, составляющих коммерческую тайну с определением степени секретности : строго секретно, конфиденциально, не подлежит огласке.
- Маркировка на документах в правом углу : «КТ», «строго конфиденциально» или «конфиденциально». Указание количества экземпляров документа и кому они направляются.

- Работа с персоналом, от которой на 80 % зависит сохранность коммерческой тайны.

Руководитель проводит беседы с работниками при приеме на работу и увольнении, заключает с работниками Соглашение о неразглашении коммерческой тайны, проводит инструктаж с обучением методам сохранности конфиденциальной информации.

- Комплексный анализ по выявлению каналов утечки информации, контроль работы подразделений и отдельных лиц.

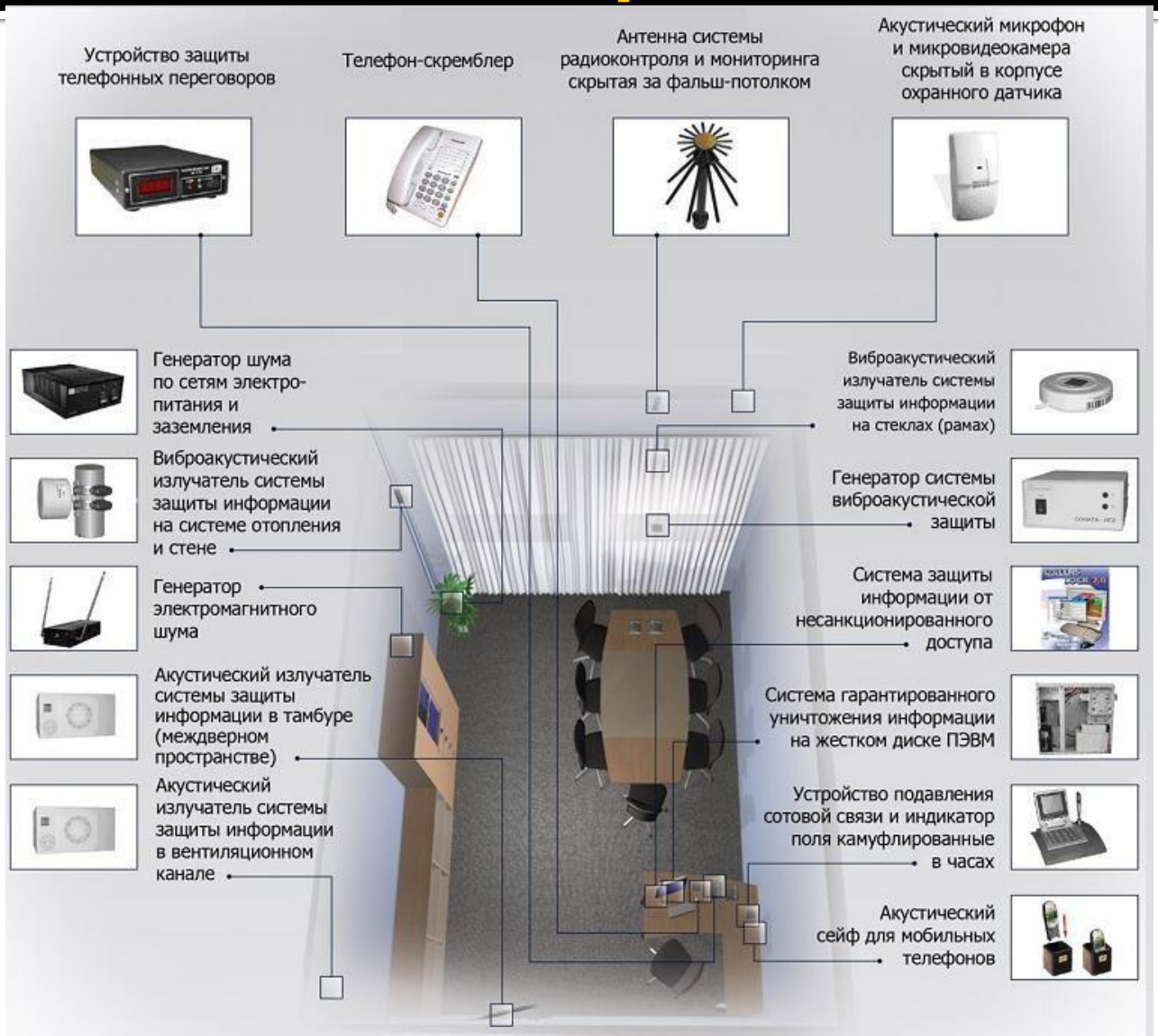
К техническим мероприятиям относят :

- Ограничить посещение посторонних лиц, выдача пропусков.
- Установление дополнительных дверей, запоров, сигнализации.
- Наличие специальных приборов, обнаруживающих любые подслушивающие устройства.
- Зашумление телефонной сети.
- Охрана фото- и копировального оборудования.
- Защита электронной информации.
- Хранение заключенных договоров и контрактов, других документов в сейфе.

К специальным мероприятиям можно отнести :

- Предусматривать в тексте заключаемых договоров ответственность сторон за несанкционированное разглашение коммерческой тайны.
- Работник должен иметь доступ лишь к информации, необходимой ему по службе.
- Разработка должностных инструкций специалистов с обязанностями по сохранению коммерческой тайны. Указание в трудовом договоре деловой информации, представляющей тайну.

Схема расположения устройств для защиты коммерческой тайны.



Процесс предотвращения утечек информации.

Чем опасна утечка коммерческой информации.

Если же, информация подобного характера, попадет в руки конкурентам, то компании может быть причинен огромный материальный ущерб, который чреват не только потерями прибыли, но и рынков сбыта, крупнейших партнеров или даже постоянных клиентов. Так, например если у компании была украдена информация, содержащая базу данных всех партнеров и постоянных клиентов, то конкурирующее предприятие может переманить к себе ведущих поставщиков, создать условия, отвечающие требованиям клиентов компании и тем самым лишить ее существенной части прибыли. Более того, если конкурирующая компания получит данные о направлениях расширения бизнеса или новых рынках сбыта продукции, то она может первой занять новую нишу или пустующий сектор на рынке. Следовательно, конкурирующие фирмы очень заинтересованы в получении определенной секретной информации компании, чтобы лишить ее конкурентного преимущества и препятствовать ее расширению и укреплению на рынке. В тоже время компания должна надежно охранять информацию от несанкционированного доступа и всячески препятствовать ее распространению.

Кого именно опасаться?

В связи с повсеместно распространившейся автоматизацией и информатизацией в сфере торговли, вся информация, включая и секретную, хранится в электронном виде. При этом секретные данные зачастую имеют мощную систему защиты, чтобы предотвратить несанкционированный доступ к ней. Однако какой бы качественной не была система защиты данных, стопроцентной гарантии от взлома быть не может. Дело в том, что если какой-то человек смог создать эту систему защиты, значит, какой-нибудь другой человек сможет ее взломать, а найти хакера сегодня трудности не составит.

И, тем не менее, стоит отметить, что взломы системы хакерами это не самый распространенный способ получения секретных данных компании, гораздо чаще используется другой, более надежный способ – внедрение своего «шпиона» или подкуп служащих компании. Гораздо проще подкупить сотрудника имеющего официальный доступ к системе с тем, чтобы тот передал всю необходимую информацию. А притом, что сотрудники редко бывают полностью удовлетворенными своей заработной платой и условиями работы, «соблазнить» на кражу обычно не составляет большого труда. Тут действует еще и тот факт, что не всегда сотрудники понимают всю серьезность своего поступка, и оправдываются тем, что они ведь ничего не украли материального, а, следовательно, и наказания серьезного за это быть не может.

Понятно, что доступ к коммерческой тайне имеют далеко не все сотрудники компании, а лишь те, кто должен ее использовать в процессе своей деятельности – то есть руководители отделов продаж, работы с клиентами, маркетинга и т.п. А на эти должности зачастую назначают не первых встречных людей и уж они то точно знают, чем чревата потеря такой информации. Однако по долгу службы доступ к коммерческой тайне получают и менее ответственные сотрудники, например секретари отделов, обрабатывающие эту информацию, помощники руководителей, которые работают над ее составлением и, конечно же, системные администраторы, которые устанавливают систему защиты на секретные данные и следят за исправностью работы всей системы. Вот эти работники, которые зачастую не обладают фундаментальными знаниями в области менеджмента и маркетинга являются наиболее слабыми звеньями для компании и самыми подходящими кандидатами для конкурентов.

Подробнее о том как защититься

Для того чтобы защитить коммерческую тайну от кражи и распространения необходимо проводить комплексную работу в области обеспечения безопасности. То есть необходимо постоянное совершенствование систем автоматизированной защиты, в сочетании с непрерывной работой над персоналом. Совершенствование средств защиты позволит минимизировать возможность доступа к базам данных сторонними пользователями, то есть хакерами. Не стоит жалеть денег на разработку индивидуальных решений, внедрение новейших технологий или оплату услуг высококлассного IT-специалиста. Поскольку расходы на совершенствование систем безопасности всегда оправданы. Защитить информацию от взлома сторонними лицами порой оказывается даже проще чем сохранить ее от кражи собственным персоналом. Ситуация осложняется еще и тем, что никогда не знаешь откуда ждать удара, то есть сложно угадать, кто окажется предателем – руководитель отдела, озлобленный на директора, или секретарь, подработавший таким способом на стороне.

Для того, что бы предотвратить кражу коммерческой тайны со стороны доверенных лиц, необходимо, прежде всего, четко очертить границы этого понятия для конкретного предприятия. Более того, необходимо поставить в известность весь персонал, имеющий доступ к этой информации, какие конкретно данные относятся к коммерческой тайне и не должны подвергаться разглашению. Это необходимо для того, чтобы потом работники не могли сказать, что они не знали о секретности информации или не догадывались о том, что ее нельзя выдавать конкурентам. Кроме того, важно донести до сотрудников насколько опасно разглашение коммерческой тайны для общего благополучия компании, и что в связи с этим нарушители понесут строгое наказание. При этом важно убедить работников, что наказание за кражу секретной информации действительно последует, и что оно будет заключаться в возмещении материального ущерба и выплате штрафов компании, которая пострадала из-за распространения секретной информации.

При этом преступление будет передано на рассмотрение в правоохранительные органы, что означает неотвратимость наказания за совершение противоправного деяния. Так же важно убедить персонал в том, что такие преступления доказуемы, для этого можно составить отдельный документ с перечнем всех составляющих коммерческой тайны предприятия и ответственностью персонала за ее разглашение. После этого каждый работник должен подписать данное соглашение, в знак того, что он ознакомлен со всеми требованиями компании.

Еще одним направлением для совершенствования системы безопасности предприятия является стимулирование и мотивация персонала, чтобы выработать у них лояльность к фирме и ощущение удовлетворенности работой. Поскольку, работников, которые ценят свою компанию и заботятся об ее благополучии гораздо сложнее «соблазнить» на предательство.

Подводя итог, можно отметить, что кража или разглашение коммерческой тайны может значительно отразиться на благополучии компании и формировании прибыли. Поэтому необходимо постоянное совершенствование мер защиты информационных ценностей, а, кроме того, ведение эффективной кадровой политики, особенно в отношении лиц, имеющих доступ к коммерческой тайне.

История

- В 1817 году в Великобритании, а в 1837 году в США впервые на судебных процессах обсуждалась коммерческая тайна, а решения этих судов стали важными прецедентами. Первым в мире законом, охраняющим коммерческую тайну, стал закон, подписанный в 1844 году французским королём Луи-Филиппом. В 1845 г. российский император Николай I ввел наказание за разглашение коммерческой тайны в «Уложении о наказаниях общего определения». К началу XX века во всех европейских странах защищалась коммерческая тайна.

Однако, в XX веке почти все развитые государства отошли от защиты коммерческой тайны. В одних случаях это было связано с введением антитрестовского законодательства, в других — с борьбой с коррупцией. Во многих государствах были даже введены законы, принуждающие акционерные общества раскрывать определённую информацию. В России, а в дальнейшем — в СССР и странах Восточной Европы, коммерческая тайна была отменена как пережиток капитализма.

Тем не менее, как правило, во всех западных странах предприниматели сохранили право уволить работника за промышленный шпионаж. Швейцария была одним из немногих государств, где законодательство об охране коммерческой тайны не переставало действовать в течение всего XX века.

Во второй половине XX века стал популярным довод о том, что введение коммерческой тайны в области технологий ускорит научно-технический прогресс, поощряя предпринимателей создавать оригинальные разработки вместо копирования чужих. В 1974 году Верховный суд США разрешил штатам принимать свои законы об охране коммерческой тайны. В 1996 году в США был принят Закон об экономическом шпионаже, криминализирующий (объявлявший преступлением) кражу технологических секретов в пользу иностранных государств (§ 1831 Кодекса Соединённых Штатов) и кражу технологических секретов в коммерческих целях (§ 1832). В течение 1990-х годов законы о коммерческой тайне вновь (а иногда — впервые) появились в России, Германии, Чехии, Венгрии, Таиланде, Японии, Китае. В одних государствах (например, в Японии, Франции) наказание ограничивается штрафом или возмещением ущерба, в других (например, в Германии) возможна и уголовная ответственность, если информация, составляющая коммерческую тайну, была получена с помощью незаконных действий.

В России защита коммерческой тайны законодательно регламентирована достаточно жёстко (ст. 183 УК РФ и ст.15 Федерального закона от 20 февраля 1995 г. «Об информации, информатизации и защите информации») и подразумевает выполнение организацией, защищающей свою информацию, целого ряда требований

«Инсайдер»

Инсайдерская информация (англ. *Insider information*) — существенная, публично не раскрытая служебная информация компании, которая в случае её раскрытия способна повлиять на рыночную стоимость ценных бумаг компании. Сюда можно отнести: информацию о готовящейся смене руководства и новой стратегии, о подготовке к выпуску нового продукта и к внедрению новой технологии, об успешных переговорах о слиянии компаний или идущей скупке контрольного пакета акций; материалы финансовой отчётности, прогнозы, свидетельствующие о трудностях компании; информация о тендерном предложении (на торгах) до его раскрытия публике, список аффилированных лиц и т. д.

В более широком смысле — любая информация, известная неопределенному кругу лиц, близких к её источнику.

В Законе от 27.07.2010 N 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» говорится, что «*под инсайдерской информацией понимается точная и конкретная информация, которая не была распространена или предоставлена (в том числе сведения, составляющие коммерческую, служебную, банковскую тайну, тайну связи (в части информации о почтовых переводах денежных средств) и иную охраняемую законом тайну), распространение или предоставление которой может оказать существенное влияние на цены финансовых инструментов, иностранной валюты и (или) товаров (в том числе сведения, касающиеся одного или нескольких эмитентов эмиссионных ценных бумаг (далее - эмитент), одной или нескольких управляющих компаний инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов)*».

- Руководство предприятия, как правило, владеет инсайдерской информацией. Другие сотрудники компании также владеют ею. Другие лица, с которыми компания может в процессе работы обмениваться соответствующими сведениями, тоже становятся инсайдерами. Такими лицами могут быть, например, адвокаты, финансовые консультанты, аудиторы, банкиры и пр.

- В большинстве стран законы о ценных бумагах содержат нормы, направленные против использования инсайдерской информации в целях дестабилизации рынка и получения ограниченным кругом лиц, имеющих к ней доступ, несправедливой прибыли. В России в Федеральном законе «О рынке ценных бумаг» (1996) используется понятие «служебная информация».

Подводя итоги.

Чтобы защитить секреты компании, придется провести большую предварительную работу.

Купите сейф и в нем храните важные документы и прочие носители, например, флешки. Доступы к компьютеру и локальной корпоративной сети выполнять только по персональному логину и паролю. Если коммерческие данные вашей компании все же украли, то минимизировать именно эти потери будет уже сложно, однако стоит предусмотреть меры, чтобы предупредить подобные проблемы в будущем.

Потери уже никак не минимизировать — вы уже их понесли. Что делать? Уволить службу безопасности, учесть ошибки и создать что-то новое, новый продукт, новое позиционирование. Обязательно сформировать новую структуру системы безопасности, потому что просто кадровые перестановки ничего не дадут. Порой причины „лежат" совсем в другой области, например, в неправильном менеджменте или самообмане собственника.

Если секреты компании были похищены, то вы имеете полное право обратиться в полицию и суд за защитой своих законных интересов.

КОНЕЦ