Практические советы

УДК 65.01

Яновский А. М.

СОХРАНЕНИЕ КОРПОРАТИВНЫХ СЕКРЕТОВ

Усиление конкуренции на современных товарных рынках порождает спрос на коммерческие секреты конкурентов. А раз есть спрос, то есть и предложение. Услуги подобного рода предлагают специализированные агентства, для которых охота за чужими секретами — основной бизнес. Кроме того, многие фирмы создают в своей структуре службы, в обязанность которых входит как охота за чужими коммерческими секретами (коммерческий шпионаж), так и охрана секретов своей фирмы от утечки. Сохранность коммерческих секретов — головная боль многих преуспевающих субъектов бизнеса.

Одной из проблем, с которыми человечество постоянно сталкивается и которые вряд ли когда-нибудь исчезнут, является экономический шпионаж. Естественно, изменяются формы, методы и его приёмы. Но неизменной остаётся цель — незаконное получение корпоративных секретов конкурента (технологии, ноу-хау и т. п.) и их использование для получения прибыли и иных конкурентных преимуществ.

Основная опасность — в управлении человеческим фактором как главной возможности утечки корпоративных секретов.

Выдать коммерческую тайну фирмы практически может любой её сотрудник. Его к этому могут принудить различные причины и обстоятельства. Статистика утверждает, что даже в хорошо управляемой фирме и при наличии нормальной корпоративной культуры всегда существует примерно 80% так называемых «ситуативно» благополучных сотрудников, которые при определённых условиях готовы организовать (а иногда даже принять непосредственное участие) утечку секретной информации и документов. При наличии устойчивого спроса на секреты конкурентов уберечься от разглашения коммерческой тайны весьма сложно, и удаётся это только единицам.

Существует много специальных приёмов, позволяющих минимизировать риск и ущерб. Ведь если утечка секретной информации будет обнаружена в кратчайшие сроки, — это уже возможность принять экстренные меры для минимизации возможного ущерба.

Сохранить корпоративные секреты очень сложно (практически невозможно), если в фирме не налажен и строго не соблюдается режим доступа к корпоративным секретам. Отсутствие документов, чётко регламентирующих, что́ относится к корпоративным секретам и кто персонально из сотрудников в силу выполнения служебных обязанностей имеет доступ к определённым секретам, затрудняет технологию сохранения коммерческих секретов фирмы. Формирование режима секретности и охраны коммерческих тайн — в компетенции руководства фирмы.

Такой режим обязательно регламентирует процесс набора новых сотрудников в постоянный штат работников фирмы после их проверки на «устойчивость» сохранения конфиденциальной информации, подписание с ними особых документов, предусматривающих персональную ответственность за разглашение коммерческих корпоративных секретов и особые преференции за их сохранение, а также перечень того, что можно делать в определённых производственных условиях, а чего делать не следует (например, поведение сотрудников фирмы при различного рода контактах с посторонними лицами). Кроме того, сотрудники подписывают обязательство соблюдать требования внутреннего распорядка межличностных взаимоотношений между сотрудниками фирмы и различными её службами, а также обязательство о сохранении секретов фирмы в течение определённого времени (например, в течение трёх лет) после увольнения из фирмы независимо от причины увольнения. Естественно, в качестве компенсации им предлагаются различные льготы, которые фирма в состоянии им предоставить. Естественно, болтливых сотрудников руководство фирмы имеет возможность своевременно уволить.

В практике, однако, фирмы не ограничиваются выстраиванием юридических и бюрократических барьеров в вопросах информационной безопасности, связанных с человеческим фактором. Существуют различные технические средства, как для несанкционированного съёма информации, так и для защиты от подобных действий. Средства эти постоянно совершенствуются, и следить за этим процессом следует очень внимательно, чтобы вовремя использовать их новые возможности.

Модели внутрифирменной информационной безопасности

Всё разнообразие мер внутрифирменной информационной безопасности должно вписываться в определённую модель безопасности. Таких моделей может быть несколько. Назовём основные из них. Итак:

1. Система непрерывного и тотального контроля над поведением персонала (прослушивание, видеонаблюдение, мониторинг личных контактов и т. п.).

Возможные варианты:

— негласный для сотрудников;

— гласный (с личной ответственностью за допущенные нарушения общепринятых норм); в этом случае модель должна быть соответствующим образом документирована и юридически определена.

2. Построение бюрократических и административных барьеров

Основной аспект построения различных барьеров:

— строгое регламентирование работы с конфиденциальной информацией строго в рамках служебной целесообразности;

— продуманная система допуска сотрудников к различным аспектам корпоративных секретов (предусмотрение допусков к секретной информации различных категорий);

— введение мер психологического характера и ограничений, предусмотренных внутренним распорядком ;

— построение системы внутрифирменной коммуникации (например, порядок использования средств ЭВМ и компьютеров и других средств передачи информации). Предупредить утечку важной информации легче, когда сотрудники фирмы хорошо осведомлены о всех требованиях режима секретности.

В украинском законодательстве чётко определенью какие сведения не подпадают под понятие секретной информации и засекречиванию не подлежат (Постановление Кабмина Украины № 611 от 9 августа 1993 года). К таковым относятся:

— учредительные документы фирмы;

— информация по всем формам государственной отчётности;

— данные о численности и составе работающих;

— данные о зарплате работников;

— сведения о наличии свободных рабочих мест.

Недопустимо, чтобы к корпоративной тайне относилась информация, связанная с теневыми бизнес-схемами.

3. Формирование лояльности персонала к бизнес-деятельности фирмы

Важнейшие пункты: целенаправленное формирование корпоративной культуры и внутрифирменного климата взаимоотношений сотрудников, способствующих воспитанию патриотов фирмы, которые ни при каких обстоятельствах не нанесут фирме вреда.

Практика показывает, что опасность для фирмы может исходить не только от её рядовых сотрудников, но и от высокопоставленных работников, и это опасно серьёзными нежелательными последствиями. Подтверждающий пример: попытка рассекретить одним из руководящих работников фирмы «Сока-Кола» секрета этого напитка. Величину возможного ущерба трудно себе представить.

4. Недопущение утечки секретной информации с уходом сотрудника из фирмы

Потеря сотрудника фирмой путём его увольнения, как по инициативе руководства фирмы, так и по его собственному желанию, ситуация тривиальная. За время работы в фирме сотрудник приобретает объём знаний о фирме, который хранит в своей памяти и который у него стереть из памяти при увольнении не представляется возможным. И, хотя такая информация не является его собственностью с юридической точки зрения, он ею фактически располагает. А уволившись из фирмы и, скажем, перейдя на работу к конкуренту, он уже фактически не обязан быть лояльным к своей прежней фирме. А значит, может распорядиться имеющейся у него информацией, как ему будет угодно или выгодно.

Учитывая такую возможность, фирма, которую покидает сотрудник, старается обеспечить неразглашение им своих секретов.

Возможные варианты решения проблемы:

1. Подписание сотрудником (например, в момент его приёма на работу) обязательства о неразглашении им известных ему корпоративных секретов ни в период его работы в фирме, ни после увольнения в течение определённого времени, получая за это определённые льготы.

2. Заключение соглашения с конкурентами о недопустимости переманивания сотрудников с целью овладевания с их помощью корпоративными секретами конкурента для коммерческого использования.

3. Привлечение на законных основаниях бывших сотрудников к ответственности за разглашение ими корпоративных секретов (как это делается, например, в некоторых странах Европы и в США). Пока сделать это в Украине невозможно, т. к . такая мера не предусмотрена законодательством. Но лоббировать её включение в действующее законодательство, безусловно, следует.

4. Следует строго следить за тем, чтобы, покидая фирму, сотрудник не имел возможности унести с собой документы, содержащие корпоративную тайну. Стараться уволить сотрудника таким образом, чтобы он не сохранил чувство обиды к покидаемой фирме, и не стремился отомстить ей, путём нанесения вреда доступным ему способом.

Шпионаж как основа конкурентного преимущества

Практически каждая фирма старается овладеть коммерческими секретами конкурентов. И одновременно страдает от аналогичных действий с их стороны. Службы экономической разведки фирм стараются овладеть информацией о рыночной конъюнктуре, финансовом положении конкурентов, об их реальных планах и возможностях обновления рыночного ассортимента.

Эти службы также способствуют выявлению уязвимых мест в системе безопасности конкурентов.

Деятельность этих служб должна находиться под контролем руководства фирм и строиться по трём основным направлениям: внутренней оценки деятельности, внешней оценки и анализа полученных данных. Внутренняя оценка руководствуется исключением утечки секретной информации о своей фирме. Внешняя — определяется сбором экономической разведывательной информации о конкурентах, а анализ полученной информации — полученными сведениями и документами по разным сторонам деятельности конкурентов.

В заключение следует отметить, что разработка режима сохранения секретности, как и его строгое соблюдение, — это внутреннее дело конкретного предприятия. Научиться этому необходимо. Это позволит избежать в дальнейшем многих неприятностей, больших и малых.

Об авторе:

ЯНОВСКИЙ Александр Михайлович — маркетолог, руководитель информационно-аналитической службы ОАО «НИИСЛ» (г. Одесса). Область деятельности: новые бизнестехнологии; организация успешной деятельности предприятия; кадровый, инновационный и технический менеджмент. краткая информация об авторе в свободной форме.