**Введение**

Предпринимательская деятельность во всех сферах неразрывно связана с получением и использованием различного рода информации. Причем в современных условиях информация представляет собой особого рода товар, имеющий определенную ценность. Для предпринимателя зачастую наиболее ценной является информация, которую он использует для достижения целей фирмы и разглашение которой может лишить его возможностей реализовать эти цели, то есть создает угрозы безопасности предпринимательской деятельности. Конечно, не вся информация может, в случае ее разглашения, создавать эти угрозы, однако существует определенная ее часть, которая нуждается в защите.

Информация, используемая в предпринимательской деятельности весьма разнообразна. Ее можно разделить на два вида: промышленная и коммерческая(1). К промышленной относится информация о технологии и способе производства, технических открытиях и изобретениях, «ноу-хау», конструкторская документация, программное обеспечение и т.п. Коммерческая информация – о финансово-экономическом положении предприятия (бухгалтерская отчетность), кредитах и банковских операциях, о заключаемых договорах и контрагентах, структуре капиталов и планах инвестиций, стратегических планах маркетинга, анализе конкурентоспособности собственной продукции, клиентах, планах производственного развития, деловой переписке и пр.

Вся эта информация представляет различную ценность для самого предпринимателя и, соответственно, ее разглашение может привести (либо не привести) к угрозам экономической безопасности различной степени тяжести. Поэтому информацию необходимо разделить на три группы:

* информация для открытого пользования любым потребителем в любой форме;
* информация ограниченного доступа – только для органов, имеющих соответствующие законодательно установленные права (милиция, налоговая полиция, прокуратура);
* информация только для работников (либо руководителей) фирмы.

Информация относящаяся ко второй и третьей группам является конфиденциальной и имеет ограничения в распространении. ***Конфиденциальная информация*** – это документированная (то есть зафиксированная на материальном носителе и с реквизитами, позволяющими ее идентифицировать) информация, доступ к которой ограничивается в соответствии с законодательством РФ. Часть этой коммерческой информации составляет особый блок и может быть отнесена к коммерческой тайне.

**Коммерческая тайна и ее содержание**

Коммерческая тайна, в соответствии с гражданским законодательством РФ, это информация которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель принимает меры к охране ее конфиденциальности. Следовательно, коммерческая тайна не может быть общеизвестной и общедоступной информацией, открытое ее использование несет угрозу экономической безопасности предпринимательской деятельности, в связи с чем предприниматель осуществляет меры по сохранению ее конфиденциальности и защите от незаконного использования.

Однако не вся информация, которой располагает предприниматель, может быть отнесена к категории коммерческой тайны. Существует официально утвержденный перечень сведений, которые не могут составлять коммерческую тайну в РФ. К ним относятся:

* учредительные документы (устав, учредительный договор);
* документы, дающие право заниматься предпринимательской деятельностью (регистрационное удостоверение, свидетельство о регистрации, лицензии, сертификаты, патенты);
* сведения по установленным формам отчетности о финансово-хозяйственной деятельности, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему РФ);
* документы о платежеспособности;
* сведения о численности работающих, их составе, заработной плате, наличии свободных рабочих мест;
* документы об уплате налогов и обязательных платежей;
* сведения о соблюдении установленных правил охраны труда;
* сведения о соблюдении установленных норм охраны окружающей среды;
* сведения о нарушении антимонопольного законодательства;
* сведения о реализации продукции, причинившей вред здоровью населения;
* сведения об участии должностных лиц предприятия в кооперативах, малых предприятиях, акционерных обществах и других организациях, занимающихся предпринимательской деятельностью.

Но и эти сведения не предназначаются для открытого доступа – всем желающим. Например, сведения о заработной плате работников предприятия, финансовая отчетность могут быть предоставлены только по требованию органов власти, управления, контролирующих и правоохранительных органов, а также других юридических лиц, имеющих на это право в соответствии с действующим законодательством РФ. В то же самое время клиенты фирмы вправе ознакомиться с ее уставом, свидетельством о регистрации, лицензией, сертификатами, патентами.

**Содержание коммерческой тайны**

Как уже отмечалось, предприниматель в своей деятельности имеет дело с самой разнообразной информацией. Однако он не может всю информацию, которой обладает, сделать закрытой для внешних пользователей. Предприниматель в плане защиты наиболее важной информации решает сложную проблему. С одной стороны, он должен предоставить максимум информации о своей деятельности потребителям, контрагентам, кредиторам и т.п. для того, они сделали выбор в его пользу. Реклама привлекает покупателей, деловые связи, патенты и лицензии, «ноу-хау» – контрагентов, финансовое положение – инвесторов. С другой стороны, предприниматель должен оградить названные группы лиц, а также своих конкурентов от информации, утечка или разглашение которой может представлять угрозу его экономической безопасности. В выборе «золотой середины», то есть определении того оптимального количества информации, которого будет достаточно для внешних пользователей и оно не будет представлять угроз экономической безопасности, и состоит первый шаг предпринимателя в процессе защиты информации, составляющей коммерческую тайну.

Получить информацию о деятельности фирмы можно двумя способами: законным и незаконным. Законный способ – это получение информации из средств массовой информации, рекламных проспектов фирмы, статей о фирме, с выставок, пресс-конференций. Эта информация специально готовится работниками фирмы для открытого пользования всеми заинтересованными лицами. Незаконный способ – это получение информации, не предназначенной для внешних пользователей, без согласия руководства фирмы, с нарушением действующего законодательства и приводящее к прямым экономическим потерям для фирмы, либо к упущенной выгоде.

Наиболее ценной в этом плане является информация, представляющая коммерческую тайну. Она важна, прежде всего, для конкурентов данной фирмы, а также для криминальных структур. Интересно, что в мировой практике в течении последних нескольких десятков лет 80–90% информации, интересующей конкурентов, получается последними из открытых источников – из газет, специальных журналов, на выставках и пр. Для этого многие фирмы даже используют специалистов, изучающих всю открытую информацию, «просеивающих» ее и выбирающих нужные сведения.

Вообще существует большое количество способов получения информации. Так, американский журнал «Chemical engineering» опубликовал такой перечень из 16 источников получения информации.

1. сбор информации, содержащейся в средствах массовой информации, включая официальные документы, например, судебные отчеты;
2. использование сведений, распространяемых служащими конкурирующих фирм;
3. биржевые документы и отчеты консультантов; финансовые отчеты и документы, находящиеся в распоряжении маклеров; выставочные экспонаты и проспекты, брошюры конкурирующих фирм; отчеты коммивояжеров своей фирмы;
4. изучение продукции конкурирующих фирм; использование данных, полученных во время бесед со служащими конкурирующих фирм (без нарушения законов);
5. замаскированные опросы и «выуживание» информации у служащих конкурирующих фирм на научно-технических конгрессах (конференциях, симпозиумах);
6. непосредственное наблюдение, осуществляемое скрытно;
7. беседы о найме на работу со служащими конкурирующих фирм (хотя опрашивающий вовсе не намерен принимать данного человека в свою фирму);
8. так называемые «ложные» переговоры с фирмой-конкурентом относительно приобретения лицензии;
9. наем на работу служащего конкурирующей фирмы для получения требуемой информации;
10. подкуп служащего конкурирующей фирмы или лица, занимающегося ее снабжением;
11. использование агента для получения информации на основе платежной ведомости фирмы-конкурента;
12. подслушивание переговоров, ведущихся в фирмах-конкурентах;
13. перехват телеграфных сообщений;
14. подслушивание телефонных разговоров;
15. кража чертежей, образцов, документации;
16. шантаж и вымогательство.

В связи с этим необходимо определить – какая информация должна быть отнесена к коммерческой тайне и требует защиты, каков срок ее «хранения» в качестве тайны, какие ее части наиболее важны. Важность информации определяется ее ценностью для предпринимателя, которая, по мнению ряда специалистов(5), должна включать полезность (создание субъекту выгодных условий для принятия оперативного решения и получения эффективного результата), своевременность, достоверность и полноту.

Прежде чем приступить к определению информации, относящейся к категории коммерческой тайны, предприниматель должен учесть, что вся имеющаяся информация по степени конфиденциальности, утрата которой может вызвать различные по тяжести последствия, может быть распределена по следующим группам:

1. Высшая степень конфиденциальности. Данная информация является ключевой в деятельности фирмы, основой ее нормального функционирования. Утрата или разглашение этой информации нанесет непоправимый ущерб деятельности фирмы. Это – угроза высокой степени тяжести, последствия реализации которой могут ликвидировать саму фирму.
2. Строго конфиденциальная информация. Утечка этой информации может вызвать значительные по тяжести последствия. Это информация о стратегических планах фирмы, о перспективных соглашениях и т.п.
3. Конфиденциальная информация – ее разглашение наносит фирме ущерб, сопоставимый с текущими затратами фирмы, ущерб может быть преодолен в сравнительно короткие сроки.
4. Информация ограниченного доступа – ее утечка оказывает незначительное негативное воздействие на экономическое положение фирмы (должностные инструкции, структура управления).
5. Открытая информация. Ее распространение не представляет угроз экономической безопасности фирмы. Наоборот, отсутствие данной информации может оказать негативное воздействие на экономическое положение фирмы.

Каким же образом можно осуществить разграничение информации открытой и той, которая нуждается в защите? Для этого следует использовать следующие критерии.

Во-первых, это вероятность угрозы экономической безопасности фирмы. В случае получения этой информации конкурентами фирма понесет экономический ущерб. Так, широко известный напиток «кока-кола» производится на основе секретной формулы, являющейся коммерческой тайной, и обеспечивает процветание фирмы. В случае разглашения этой информации фирму ожидают серьезные экономические трудности.

Во-вторых, это возможность защиты информации. Если, например, информация не входит в обязательный перечень открытого характера, то следует определить – существует ли возможность ее защиты с помощью общих, либо специальных мер защиты.

В-третьих, это экономическая целесообразность защиты информации. Только в том случае, если разглашение или утечка информации может нанести существенный экономический ущерб фирме, следует организовывать ее защиту.

По функционально-целевому признаку выделяются следующие составляющие коммерческой тайны:

1. Деловая информация:

* сведения о контрагентах;
* сведения о конкурентах;
* сведения о потребителях;
* сведения о деловых переговорах;
* коммерческая переписка;
* сведения о заключенных и планируемых контрактах.

2. Научно-техническая информация:

* содержание и планы научно-исследовательских работ;
* содержание «ноу-хау», рационализаторских предложений;
* планы внедрения новых технологий и видов продукции;

3. Производственная информация:

* технология;
* планы выпуска продукции;
* объем незавершенного производства и запасов;
* планы инвестиционной деятельности.

4. Организационно-управленческая информация:

* сведения о структуре управления фирмой не содержащиеся в уставе;
* оригинальные методы организации управления;
* система организации труда.

5. Маркетинговая информация:

* рыночная стратегия;
* планы рекламной деятельности;
* планы обеспечения конкурентных преимуществ по сравнению с продукцией других фирм;
* методы работы на рынках;
* планы сбыта продукции;
* анализ конкурентоспособности выпускаемой продукции.

6. Финансовая информация:

* планирование прибыли, себестоимости;
* ценообразование – методы расчета, структура цен, скидки;
* возможные источники финансирования;
* финансовые прогнозы.

7. Информация о персонале фирмы:

* личные дела сотрудников;
* планы увеличения (сокращения) персонала;
* содержание тестов для проверки вновь принимаемых на работу.

8. Программное обеспечение:

* программы;
* пароли, коды доступа к конфиденциальной информации, расположенной на электронных носителях.

Как правило, именно перечисленная выше информация в наибольшей степени интересует конкурентов, партнеров, банки, криминальные структуры.

Информация, составляющая коммерческую тайну, может существовать в бумажной форме, на дискетах и лазерных дисках, на «жестком» диске компьютера, в памяти сотрудников.

Регулирование отношений, связанных с использованием конфиденциальной информацией должно начинаться с основного документа – устава, в котором дается понятие коммерческой тайны и устанавливается ответственность за ее несоблюдение.

Для более эффективной организации работы по защите коммерческой информации весьма целесообразно разработать и утвердить ***Положение о коммерческой тайне на предприятии (фирме).*** Этот документ основывается на действующем законодательстве и отражает специфику данного субъекта предпринимательства. Он включает перечень сведений, составляющих коммерческую тайну, степень конфиденциальности информации, порядок доступа к информации и круг работников предприятия, допущенных к информации той или иной степени конфиденциальности.

**Банковская тайна**

Одной из специфических разновидностей коммерческой тайны является банковская тайна. ***Банковская тайна*** – это информация, доступ к которой банк, в соответствии с законом, имеет право ограничивать. Банки, как правило, работают с многочисленными клиентами, вкладчиками, корреспондентами, интересы которых могут пострадать при разглашении информации об их операциях, сделках, счетах и пр. Причем угрозы могут исходить как от конкурентов, так и от преступных сообществ. В связи с этим возникает необходимость в защите информации, которой обладают банки, в том числе и информации о деятельности лиц, пользующихся разнообразными услугами банков.

Особенность правового режима банковской тайны заключается в том, что перечень сведений, включаемых в нее, устанавливается не только законодательно, но и самими банками. Причем, в Российской Федерации пока нет отдельного закона о банковской тайне, а законодательное регулирование осуществляется в основном Гражданским кодексом РФ (ст. 857) и Федеральным законом «О банках и банковской деятельности» (ст. 26). В этих законодательных актах предусмотрено, что банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиентах и корреспондентах. Кроме того, банки сами могут относить часть информации, которой они владеют к категории банковской тайны (если это не противоречит федеральному закону). Служащие банка обязаны хранить банковскую тайну.

Сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям. Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и в порядке, предусмотренных законом. Закон же предусматривает, что справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются кредитной организацией им самим, судам и арбитражным судам (судьям), Счетной палате Российской Федерации, органам государственной налоговой службы и налоговой полиции, таможенным органам Российской Федерации в случаях, предусмотренных законодательными актами об их деятельности, а при наличии согласия прокурора – органам предварительного следствия по делам, находящимся в их производстве. Справки по счетам и вкладам в случае смерти их владельцев выдаются кредитной организацией лицам, указанным владельцем счета или вклада в сделанном кредитной организации завещательном распоряжении, нотариальным конторам по находящимся в их производстве наследственным делам о вкладах умерших вкладчиков, а в отношении счетов иностранных граждан – иностранным консульским учреждениям.

Коммерческие банки тесно связаны с Банком России, который получает от них большое количество информации. Законодательно установлено, что Банк России не вправе разглашать информацию о счетах, вкладах, конкретных сделках и об операциях из отчетов кредитных организаций, полученных им в результате исполнения лицензионных, надзорных и контрольных функций, за исключением случаев, предусмотренных федеральными законами.

Кроме того, аудиторские организации, осуществляющие обязательные ежегодные проверки кредитных организаций, также не вправе раскрывать третьим лицам сведения об операциях, о счетах и вкладах кредитных организаций, их клиентов и корреспондентов, полученные в ходе проводимых ими проверок, за исключением случаев, предусмотренных федеральными законами.

За разглашение банковской тайны Банк России, кредитные, аудиторские и иные организации, а также их должностные лица и работники несут ответственность, включая возмещение нанесенного ущерба, в порядке, установленном федеральным законом. Гражданско-правовая ответственность выражается в применении способов защиты гражданских прав, предусмотренных ст. 12 ГК РФ. В случае разглашения банком сведений, составляющих банковскую тайну, клиент, права которого нарушены, вправе потребовать от банка возмещения причиненных ему убытков.

Несмотря на наличие ряда общих законодательных норм, гарантирующих сохранение банковской тайны, в российском законодательстве отсутствует разъяснение того, что понимается под этой гарантией, какие условия должны при этом выполняться, каковы критерии обеспечения защиты информации, составляющей банковскую тайну и т.п. В связи с этим, реальное обеспечение защиты банковской тайны в современных условиях сопряжено со значительными трудностями.

В нынешних условиях угрозы банковской тайны зачастую исходят не только от конкурентов и преступных группировок, но и от правоохранительных органов, например, налоговой полиции. Злоупотребления в этом случае могут иметь форму:

* изъятия конфиденциальных документов без надлежащего правового оформления (протокола выемки);
* проведения обыска без санкции прокурора;
* использования спецсредств («жучков») в собственных корыстных целях.

**Коммерческая тайна и персонал**

В деле защиты предпринимательской деятельности от различного вида угроз значительное место занимает персонал предприятия, который может стать как объектом, так и субъектом таких угроз. Это процесс предполагает проведение превентивных и текущих мер, направленных на работу с кадрами. Важность работы с персоналом определяется тем, что в случае желания сотрудника разгласить сведения (в силу корыстных или других мотивов), являющиеся коммерческой тайной, воспрепятствовать этому не смогут никакие, даже дорогостоящие средства защиты. Западные специалисты по обеспечению экономической безопасности считают, что сохранность конфиденциальной информации на 80% зависит от правильного подбора, расстановки и воспитания персонала.

Угрозы экономической безопасности фирмы со стороны, например, конкурентов, реализуемые через ее персонал, могут принимать такие формы как:

* переманивание сотрудников, владеющих конфиденциальной информацией;
* ложные предложения работы сотрудникам конкурентов с целью выведывания информации;
* выведывание конфиденциальных сведений у сотрудников в такой форме, что последние не догадываются о цели вопросов;
* прямой подкуп сотрудников фирм-конкурентов;
* засылка агентов к конкурентам;
* тайное наблюдение за сотрудниками конкурентов.

Организация эффективной защиты экономической безопасности фирмы со стороны персонала включает три основных этапа работы с сотрудниками, допущенными к конфиденциальной информации:

1. предварительный (в период предшествующий приему на работу);
2. текущий (в период работы сотрудника);
3. заключительный (во время увольнения сотрудника).

Предварительный этап является наиболее ответственным и, соответственно, более сложным. В случае возникновения необходимости принять нового сотрудника на работу, связанную с допуском к конфиденциальной информации, целесообразнее всего соблюсти следующую технологию приема.

Прежде всего, на основании должностной инструкции и особенностей деятельности разрабатываются ***требования к кандидату на должность***. Они включают не только формальные требования – пол, возраст, образование, опыт работы, но и ряд морально-психологических качеств, которыми должен обладать кандидат. Это позволяет уточнить – какой работник необходим фирме, а самому кандидату – сопоставить собственные качества с требующимися.

Затем производится ***подбор*** кандидатов на вакантную должность. Методы подбора кандидатом могут быть разнообразными. Предпочтение следует отдавать тем методам, которые минимизируют возможность проникновения недобросовестных людей, либо представляющих интересы конкурентов или криминальных структур. К ним относятся:

* обращение в службы занятости, агентства по найму рабочей силы и прочие аналогичные организации;
* поиск кандидатов среди студентов и выпускников высших учебных заведений;
* подбор кандидатов по рекомендациям фирм-партнеров;
* подбор кандидатов по рекомендациям надежных сотрудников фирмы.

Подбор, основанный на случайном обращении кандидатов непосредственно в фирму, может представлять угрозу ее экономической безопасности в будущем.

Целесообразно, особенно при случайном подборе кандидата, произвести запрос на предыдущее место работы с целью получения характеристики его морально-деловых качеств, а также данных о погашенных судимостях.

Для более полного ознакомления с личностью кандидата имеется возможность воспользоваться услугами органов внутренних дел. Последние могут оказывать такого рода платные услуги в соответствии с приказом МВД РФ №319 от 1994 г. Органы внутренних дел предоставляют сведения о наличии (отсутствии) судимости кандидата и о лицах, находящихся в розыске

После ознакомления с документами кандидата (личными документами, об образовании, прежней должности и стаже работы, характеристиками и рекомендациями), а последнего – с требованиями к нему и признания обоюдного соответствия, производится собеседование работника кадровой службы фирмы с кандидатом. Кандидат заполняет анкету, отвечает на вопросы, в том числе вопросы профессиональных и психологических тестов. Следует отметить, что психологические качества кандидата не менее важны, чем профессиональные. Психологический отбор позволяет не только выяснить морально-этические качества кандидата, его слабости, устойчивость психики, но и его возможные преступные наклонности, умение хранить секреты.

В случае успешного прохождения кандидатом проверки и признания его соответствующим должности, осуществляется заключение (подписание) двух документов:

* трудового договора (контракта). Контракт обязательно должен содержать пункт об обязанности работника не разглашать конфиденциальную информацию (коммерческую тайну) и соблюдать меры безопасности;
* договора (обязательства) о неразглашении конфиденциальной информации (коммерческой тайны), представляющего собой правовой документ, в котором кандидат на вакантную должность дает обещание не разглашать те сведения, которые ему будут известны в период его работы в фирме. а также об ответственности за их разглашение или несоблюдение правил безопасности (расторжение контракта и судебное разбирательство). Пример договора – см. Приложение №16.

Непосредственная деятельность вновь принятого работника, в целях проверки его соответствия занимаемой должности и соблюдения правил работы с конфиденциальной информацией, должна начинаться с испытательного срока, в конце которого принимается окончательное решение о приеме кандидата на постоянную работу.

В процессе постоянной работы необходимо определение порядка доступа сотрудников к конфиденциальной информации (коммерческой тайне). Все работники фирмы (предприятия), имеющие дело с конфиденциальной информацией, имеют право знакомиться с последней только в том объеме, который предусмотрен их должностными обязанностями и требуется для работы. В связи с этим каждая должность должна предусматривать право получения определенного объема конфиденциальной информации, выход за который будет считаться нарушением обязанностей, и представлять определенную угрозу безопасности фирмы. Размер этого перечня определяется руководителем фирмы, либо специальной комиссией. В соответствии с ним каждый работник получает допуск к конфиденциальной информации определенного уровня.

Эффективным способом защиты информации, особенно если фирма имеет ряд производств (цехов, подразделений, участков), является ограничение физического доступа (перемещения) персонала в другие зоны, не связанные с функциональными обязанностями работников. Посещение же «закрытых» территорий производится только с разрешения руководства.

Оригинальным приемом защиты информации, используемым некоторыми фирмами, является разбиение однородной информации на отдельные самостоятельные блоки и ознакомление сотрудников только с одним из них, что не позволяет работникам представить общее положение дел в данной сфере.

Третий этап – увольнение работника, имевшего дело с конфиденциальной информацией, также может представлять угрозу экономической безопасности. Уволившийся работник, не имея обязанностей перед фирмой, может поделиться ценными сведениями с конкурентами, криминальными структурами. Для снижения опасности таких последствий при увольнении работник предупреждается о запрещении использования сведений в своих интересах или интересах других лиц и дает подписку о неразглашении конфиденциальной информации (коммерческой тайны) после увольнения в течение определенного срока. В противном случае все убытки, которые будут причинены предпринимателю вследствие разглашения информации, могут быть взысканы в судебном порядке.

**Работа с конфиденциальными документами**

Конфиденциальная информация, в том числе коммерческая тайна, как правило, содержится в виде каких-либо документов – традиционных, бумажных, либо электронных. Эти источники информации могут являться объектами неправомерных посягательств и, следовательно, нуждаются в защите. Конфиденциальная информация на крупных предприятиях, предприятиях имеющих нескольких собственников представляет собой более сложный объект защиты.

Все документы в фирме делятся на три категории: входящие, исходяшие и внутренние. Первым шагом в обеспечении защиты информации является выявление из общей массы документов, содержащих ценную для фирмы коммерческую информацию. Составляется перечень конфиденциальных документов. Затем вводятся степени конфиденциальности информации (или ***грифы ограничения доступа*** к документам) и каждому документу присваивается соответствующий гриф. Данный перечень составляется специальной комиссией (в крупных фирмах), либо секретарем-референтом фирмы (специальным сотрудником). Потом он согласовывается с начальниками отделов, служб и утверждается руководителем фирмы. В перечне документов указываются категории работников, которые по должности могут пользоваться этими документами. Гриф ограничения доступа к документу устанавливается на определенный срок. Каждый документ, отнесенный к той или иной степени конфиденциальности должен на титульном (первом) листе иметь в правом верхнем углу пометку о грифе.

Порядок работы с документами, составляющими коммерческую тайну, регламентируется специальной инструкцией по закрытому делопроизводству, которая регулирует порядок документирования и организации работы с конфиденциальными документами, включающей следующие разделы: «Общие положения» – на основе действующего законодательства и нормативно-методических документов определяется понятие коммерческой тайны, устанавливаются цели данной инструкции, определяются люди или подразделения, ответственные за работу с документами, составляющими коммерческую тайну; «Документирование деятельности фирмы, составляющей коммерческую тайну» – определяются виды конфиденциальных документов, порядок их подготовки и оформления, присваиваемые грифы ограничения доступа к документам; «Организация работы с документами» – устанавливается порядок присвоения грифов и правила работы с документами, содержащими коммерческую тайну (подробнее см.: Шатина Н.В. Как работать с документами, составляющими коммерческую тайну // Предпринимательское право, 1997, №9, с. 19).

Процесс обеспечения сохранности информации в документах содержащих коммерческую тайну осуществляется в соответствии с основными стадиями «жизненного» цикла документа. Этими стадиями являются:

1. Получение (отправка) документа. Документ, поступающий в фирму и содержащий гриф конфиденциальной информации, должен быть передан только секретарю-референту или инспектору закрытого делопроизводства и зарегистрирован. Далее, он передается руководителю, а последний определяет непосредственного исполнителя по данному документу, имеющему допуск к этой категории документов, и адресует документ ему. Аналогичный порядок при отправлении документа – подготовка документа, подпись руководителя, регистрация в специальном журнале секретарем-референтом и отправка.
2. Хранение документа. Все документы, содержащие конфиденциальную информацию, должны храниться в специально отведенных, закрывающихся помещениях, в запертых шкафах, столах или ящиках. Документы же составляющие коммерческую тайну – только в металлических сейфах, оборудованных сигнализацией. Все помещения должны опечатываться. Следует иметь в виду, что при определении степени конфиденциальности документа производится также определение срока в течение которого она действует По истечении срока возможны различные действия: 1) гриф может быть продлен, 2) гриф может быть снят и документ становится открытым, 3) документ уничтожается.
3. Использование документа. Система доступа сотрудников, не имеющих соответствующих прав по должности, к конфиденциальным документам должна иметь разрешительный характер. Каждая выдача таких документов регистрируется (расписываются оба сотрудника – и тот кто берет документ и тот кто его выдает) и проверяется порядок работы с ними (например, нарушением считается оставление данных документов на столе во время обеда, передача другим лицам, вынос за пределы служебных помещений).
4. Уничтожение документа. Конфиденциальные документы, утратившие практическое значение и не имеющие какой-либо правовой, исторической или научной ценности, срок хранения которых истек (либо не истек), подлежат уничтожению. Для этого создается комиссия (не менее 3 человек) в присутствии которой производится уничтожение. Затем члены комиссии подписывают акт об уничтожении. Бумажные документы уничтожаются путем сожжения, дробления, превращения в бесформенную массу, а магнитные и фотографические носители уничтожаются сожжением, дроблением, расплавлением и др.

Контроль за соблюдением правил хранения и использования документов, содержащих конфиденциальную информацию, осуществляется с помощью проверок. Они могут быть как регулярными (еженедельными, ежемесячными, ежегодными), так нерегулярными (выборочными, случайными). В случае обнаружения нарушений составляется акт и принимаются меры, позволяющие в будущем предотвратить нарушения такого рода.

Следует контролировать не только документы, содержащие конфиденциальную информацию, но и бумаги с печатями, штампами, бланки. Бланк – лист бумаги с оттиском углового или центрального штампа, либо с напечатанным любым способом текстом (или рисунком), используемый для составления документа. Особое внимание следует уделять охране так называемых бланков строгой отчетности, содержащих номер (серию), зарегистрированных одним из установленных способов и имеющих специальный режим использования.

**Компьютерная безопасность и коммерческий шпионаж**

В системе обеспечения безопасности предпринимательской деятельности все большее значение приобретает обеспечение компьютерной безопасности. Это связано с возрастающим объемом поступающей информации, совершенствованием средств ее хранения, передачи и обработки. Перевод значительной части информации в электронную форму, использование локальных и глобальных сетей создают качественно новые угрозы конфиденциальной информации.

Компьютерные преступления в этом аспекте можно охарактеризовать как противоправные посягательства на экономическую безопасность предпринимательства, в которых объектом, либо орудием преступления является компьютер.

Источник данного вида угроз может быть внутренним (собственные работники), внешним (например, конкуренты), смешанным (заказчики – внешние, а исполнитель – работник фирмы). Как показывает практика, подавляющее большинство таких преступлений совершается самими работниками фирм.

Что же является непосредственным объектом компьютерных преступлений? Им может являться как информация (данные), так и сами компьютерные программы(7).

Преступник получает доступ к охраняемой информации без разрешения ее собственника или владельца, либо с нарушением установленного порядка доступа. Способы такого неправомерного доступа к компьютерной информации могут быть различными – кража носителя информации, нарушение средств защиты информации, использование чужого имени, изменение кода или адреса технического устройства, представление фиктивных документов на право доступа к информации, установка аппаратуры записи, подключаемой к каналам передачи данных. Причем доступ может быть осуществлен в помещениях фирмы, где хранятся носители, из компьютера на рабочем месте, из локальной сети, из глобальной сети.

Все угрозы на объекты информационной безопасности по способу воздействия могут быть объединены в пять групп: собственно информационные, физические, организационно-правовые, программно-математические, радиоэлектронные.

Последствия совершенных противоправных действий могут быть различными:

* копирование информации (оригинал при этом сохраняется);
* изменение содержания информации по сравнению с той, которая была ранее;
* блокирование информации – невозможность ее использования при сохранении информации;
* уничтожение информации без возможности ее восстановления;
* нарушение работы ЭВМ, системы ЭВМ или их сети.

Большую опасность представляют также компьютерные вирусы, то есть программы, которые могут приводить к несанкционированному воздействию на информацию, либо ЭВМ (системы ЭВМ и их сети), с теми же последствиями

Правовое обеспечение безопасности предпринимательской деятельности от компьютерных преступлений основывается на том, что по российскому законодательству защите подлежит любая документированная информация, неправомерное обращение к которой может нанести ущерб ее собственнику, владельцу, пользователю. Защита осуществляется в целях утечки, хищения, утраты, искажения, подделки информации, а также предотвращения несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращения других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечения правового режима документированной информации как объекта собственности. Кроме того, за перечисленные выше противоправные действия предусмотрена уголовная ответственность. И это представляется не случайным, поскольку угрозы компьютерным системам могут привести не только к значительным финансовым потерям, но и к необратимым последствиям – ликвидации самого субъекта предпринимательства.

Угрозы компьютерным системам и компьютерной информации могут быть со стороны следующих субъектов:

* работники фирмы, использующие свое служебное положение (когда законные права по должности используются для незаконных операций с информацией);
* работники фирмы, не имеющие права в силу своих служебных обязанностей, но, тем не менее, осуществившими несанкционированный доступ к конфиденциальной информации;
* лица, не связанные с фирмой трудовым соглашением (контрактом).

В процессе своей деятельности предприниматели, неоднократно испытывающие неправомерные действия других субъектов, не всегда обращаются в правоохранительные органы, либо вообще стараются не разглашать случаи посягательств на их компьютерные системы. Это связано с тем, что фирмы, коммерческие банки не хотят «отпугнуть» клиентов, потребителей тем фактом, что их компьютерные системы (а значит и вся информация, содержащаяся в них) недостаточно хорошо защищены. Латентная по своему характеру преступность приносит наибольший вред, поскольку безнаказанность преступников позволяет им продолжать и расширять свою преступную деятельность.

Обеспечение безопасности предпринимательской деятельности со стороны компьютерных систем представляет собой один из блоков проблемы безопасности вообще. Защита от компьютерных преступлений должна начинаться с разработки концепции информационной безопасности фирмы. На основе вышеназванных принципов – вероятности угрозы, возможности защиты и экономической целесообразности защиты информации разрабатываются конкретные способы защиты.

Способы защиты можно разделить на две группы – организационные и технические. Организационные способы защиты связаны с ограничением возможного несанкционированного физического доступа к компьютерным системам. Технические способы защиты предполагают использование средств программно-технического характера, направленных, прежде всего, на ограничение доступа пользователя, работающего с компьютерными системами фирмы, к той информации, обращаться к которой он не имеет права (подробнее о программно-технических и технических средствах обеспечения информационной безопасности см. Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. Справочник. – М.: Новый Юрист, 1998, с. 189–238).

Специалисты-практики выделяют, например, такие основные направления технической защиты компьютерной системы:

* защита информационных ресурсов от несанкционированного доступа и использования – используются средства контроля включения питания и загрузки программного обеспечения, а также методы парольной защиты при входе в систему;
* защита от утечки по побочным каналам электромагнитных излучений и наводок – с помощью экранирования аппаратуры, помещений, применением маскирующих генераторов шумов, дополнительной проверкой аппаратуры на наличие компрометирующих излучений;
* защита информации в каналах связи и узлах коммутации – используются процедуры аутентификации абонентов и сообщений, шифрование и специальные протоколы связи;
* защита юридической значимости электронных документов – при доверительных отношениях двух субъектов предпринимательской деятельности и когда возникает необходимость передачи документов (платежных поручений, контрактов) по компьютерным сетям – для определения истинности отправителя документ дополняется «цифровой подписью» – специальной меткой, неразрывно логически связанной с текстом и формируемой с помощью секретного криптографического ключа;
* защита автоматизированных систем от компьютерных вирусов и незаконной модификации – применяются иммуностойкие программы и механизмы модификации фактов программного обеспечения.

Действенным способом ограничения несанкционированного доступа к компьютерным системам является также регулярная смена паролей, особенно при увольнении работников, обладающих информацией о способах защиты.

**Коммерческий шпионаж**

Одним из наиболее опасных для нормального осуществления предпринимательства видов незаконной деятельности является коммерческий шпионаж. Коммерческий шпионаж – это действия лиц, направленные на незаконное получение коммерческой информации, находящейся под защитой. Коммерческий шпионаж включает в себя промышленный шпионаж, производственный, научно-технический и т.п. Объектом коммерческого шпионажа является информация, составляющая коммерческую тайну. Как уже отмечалось, к ней относится информация: деловая, научно-техническая, производственная, организационно-управленческая, маркетинговая, финансовая, о персонале фирмы, программное обеспечение. Утечка этой информации может привести к реальным потерям для фирмы, либо к упущенной выгоде или к обоим последствиям сразу.

Чаще всего коммерческий шпионаж осуществляется:

* конкурентами,
* криминальными структурами,
* лицами, стремящимися получить доход от перепродажи полученных незаконным путем сведений.

Конкуренты, получив информацию о секретах производства («ноу-хау»), новейших научных разработках, планах других фирм, могут использовать ее для получения преимуществ в конкурентной борьбе, выпуска аналогичной продукции, либо для непосредственного воздействия на успех деятельности своих «противников» (срыв сделок, недопущение объединения конкурентов и пр.). Криминальные структуры чаще всего используют информацию для шантажа в целях получения незаконных доходов.

В условиях острой конкурентной борьбы каждая фирма, действующая на рынке, неизбежно сталкивается с необходимостью решения двух проблем.

Первая связана с получением информации о деятельности конкурентов, причем как можно более полной, точной и своевременной. Без наличия такой информации невозможно строить производственную, научно-техническую, финансовую, рыночную стратегии и тактику поведения фирмы. Особенно важна информация, составляющая коммерческую тайну. Зачастую получение такой информации позволяет фирме экономить огромные суммы на научно-исследовательских работах и опытно-конструкторских разработках. Если способы получения информации выходят за разрешенные законом рамки (например, с помощью подкупа сотрудников, незаконного доступа к компьютерной системе), то эта деятельность может считаться коммерческим шпионажем.

Вторая проблема – защита конфиденциальной информации. Как сама фирма стремится узнать секреты других, так и ее конкуренты делают то же самое. Следовательно, каждая фирма может являться одновременно как объектом, так и субъектом коммерческого шпионажа, или, если использовать более «мягкий» термин – экономической разведки.

Субъектом коммерческого шпионажа в развитых странах все чаще становятся не сами фирмы-конкуренты, а специализированные коммерческие организации, основной целью деятельности которых как раз и является изъятие или защита конфиденциальной информации. В этих странах даже государственные спецслужбы вынуждены обеспечивать защиту наиболее важной коммерческой информации частных фирм от международного экономического шпионажа, поскольку потери от утраты информации такого рода достигают сотен миллиардов долларов.

Объектом преступных посягательств являются люди (персонал фирмы), документы, технические средства. Непосредственным носителем информации могут быть бумажные документы, планы, отчеты, финансовые документы, чертежи, техническая документация, дискеты, кассеты.

Наряду с названными выше используются технические средства коммерческого шпионажа. К ним относятся: направленные микрофоны, минирадиозакладки («жучки»), звукозаписывающая аппаратура, специальные системы наблюдения, фотоаппаратура, приборы для съема информации с телефонных аппаратов, приборы для съема информации через стекло здания.

Борьба с угрозами данного вида может быть эффективной, как правило, на основе:

во-первых, соблюдения общих требований режима безопасности,

во-вторых, создания собственной службы безопасности,

в-третьих, обращения предпринимателей в соответствующие специализированные фирмы, агентства, оказывающие услуги по охране информации,

в-четвертых, своевременного информирования правоохранительных органов.

**Заключение**

коммерческий банковский тайна конфиденциальный

Защита коммерческой информации как часть деятельности по обеспечению безопасности предпринимательства в целом, предполагает, что возможные противоправные посягательства на коммерческую информацию могут идти по различным направлениям. В связи с этим эффективная защита информации должна предусматривать целую систему направлений деятельности, каждому из которых соответствует свой способ защиты.

Кроме того, следует учитывать мировой опыт по защите коммерческой информации. В разных странах существуют различные приоритетные направления защиты коммерческой информации (коммерческой тайны). Так, в Германии преобладают законодательные меры, в США и Франции, наряду с ними, предпочтение отдается организации собственных служб безопасности фирм, для Японии характерен корпоративный дух и долгосрочная занятость в фирме, в Великобритании защита обеспечивается договорными обязательствами. Принимая во внимание российскую специфику, выделяются следующие основные способы защиты информации, которые могут использоваться предпринимателями:

1. Законодательный. Основан на соблюдении тех прав предпринимателя на конфиденциальную информацию, которые содержатся в российском законодательстве. При обнаружении нарушения прав предпринимателя как собственника, владельца или пользователя информации должно быть обращение в соответствующие органы (МВД, ФСБ, прокуратуру, суд) для восстановления нарушенных прав, возмещения убытков и т.п.
2. Физическая защита – охрана, пропускной режим, специальные карточки для посторонних, использование закрывающихся помещений, сейфов, шкафов и пр.
3. Организационный. Он включает:

- введение должности или создания службы, ответственной за отнесением определенной информации к категории конфиденциальной, соблюдением правил доступа и пользования этой информацией;

- разделение информации по степени конфиденциальности и организация допуска к конфиденциальной информации только в соответствии с должностью или с разрешения руководства;

- соблюдение правил пользования информацией (не выносить за пределы служебных помещений, не оставлять без присмотра во время обеда, включить сигнализацию при уходе);

- наличие постоянно действующей системы контроля за соблюдением правил доступа и пользования информацией (контроль может быть визуальный, документальный и др.).

1. Технический. Используются такие средства контроля и защиты как сигнализирующие устройства, видеокамеры, микрофоны, средства идентификации, а также программные средства защиты компьютерных систем от несанкционированного доступа.
2. Работа с кадрами. Предполагает активную работу кадровых служб фирмы по набору, проверке, обучению, расстановке, продвижению, стимулированию персонала. Следует регулярно проводить инструктажи персонала о необходимости соблюдения правил пользования конфиденциальной информацией и об ответственности за нарушения.

Часть этих способов предполагает значительные финансовые расходы, в связи с чем использование всех способов одновременно по средствам только достаточно крупным и платежеспособным фирмам

**Список литературы**

1. Афанасьев В.Г. Системность и общество. – М.: Политиздат, 1980, с. 24.

2. Альбрехт У., Венц Дж., Уильямс Т. Мошенничество. – СПб: Питер Пресс, 1996, с. 398–404.

3. Ларичев В.Д. Как уберечься от мошенничества в сфере бизнеса. – М.: Юристъ, 1996, с. 118–120.

4. Ольшаный А.И. Банковское кредитование: российский и зарубежный опыт. – М.: Русская Деловая Литература, 1998, с. 288.

5. Ярочкин В.И. Секьюритология – наука о безопасности жизнедеятельности. – М.: «Ось-89», 2000, с. 151.