В.И. Ярочкин
Я.В. Бузанова

ОСНОВЫ БЕЗОПАСНОСТИ БИЗНЕСА И ПРЕДПРИНИМАТЕЛЬСТВА

Москва
Академический Проект
2005

Москва
Фонд «Мир»
2005

УДК 65
ББК 65.290
Я 76

ФЕДЕРАЛЬНАЯ ПРОГРАММА «КУЛЬТУРА РОССИИ»
(ПОДПРОГРАММА «ПОДДЕРЖКА ПОЛИГРАФИИ
И КНИГОИЗДАНИЯ РОССИИ»)

Ярочкин В.И., Бузанова Я.В.
Я 76 Основы безопасности бизнеса и предпринимательства. М.: Академический Проект: Фонд «Мир», 2005. 208 с. — («Технологии безопасности»).

ISBN 5-8291-0490-3 (Академический проект)
ISBN 5-902357-21 -7 (Фонд «Мир»)

В книге рассматриваются особенности обеспечения безопасности предпринимательства в различных сферах деятельности, правовые, организационные и инженерно-технические мероприятия по защите интересов бизнеса.

Книга предназначена для студентов средних специальных и высших учебных заведений, сотрудников и руководителей охранных структур, предпринимателей.

УДК 65
ББК 65.290

ISBN 5-8291-0490-3
ISBN 5-902357-21 -7

ВВЕДЕНИЕ

В настоящее время положение дел в вопросах обеспечения безопасности и устойчивого функционирования хозяйственно-финансовых процессов в сфере предпринимательства, действующего в зоне повышенного риска, весьма и весьма сложное. Отставание в разработке законодательства, регулирующего область развивающегося предпринимательства, неразбериха в сфере правоприменения и абсолютная рассогласованность действий различных государственных институтов сопровождаются ростом коррупции и криминала. К сожалению, стало правдой утверждение, что Россия выходит на ведущие позиции в мире по размаху преступности. Криминальный прессинг на частное предпринимательство со стороны организованных преступных группировок характеризуется как мощный и все более усиливающийся. Растет число предпринимателей — жертв преступных посягательств. Три четверти представителей торгового бизнеса регулярно выплачивает «дань» криминальным структурам на долгосрочной основе либо вынуждаются последними вести дела с посредниками на заведомо невыгодных условиях. Охрана подконтрольных фирм сочетается с подавлением конкурентов. Множатся такие противоправные действия как промышленный шпионаж, хищение информации, прослушивание линий связи, установка в офисах подслушивающих устройств и пр. Ни в одной другой стране, ни в какую эпоху не получило столь широкого распространения такое явление как «заказные убийства» .

За уголовным террором в отношении предпринимателей просматриваются экономические интересы организованной преступности. Опираясь на коррумпированные связи в органах государственной власти и управления, она сегодня не только претендует на лидерство в ряде секторов экономики, но и вторгается в политику, не без результата лоббирует свои интересы во властных структурах всех уровней.

В этих условиях криминализируется и сама предпринимательская деятельность. Ее цель — извлечение прибыли с использованием незаконных методов и средств. Применительно к трем основным сферам предпринимательства (торговля, финансы, производство) общими для них негативными проявлениями являются уклонение от налогов, недобросовестная конкуренция, обман партнеров и клиентов и другие.

Сложившаяся ситуация в сфере предпринимательства и особенно в сфере малого бизнеса остро ставит проблему обеспечения безопасности и защиты интересов предпринимательства. Так как государство не может обеспечить безопасность личности и предпринимательства остается один путь: «Спасение утопающих — дело рук самих утопающих». Проблеме безопасности предпринимательства и посвящается эта книга.

ГЛАВА

ОПАСНОСТИ И УГРОЗЫ ПРЕДПРИНИМАТЕЛЬСТВУ

«Угроза — потенциально или реально существующая опасность нарушения безопасности»

В мире реального бизнеса предпринимателей подстерегают самые различные опасности и угрозы, т. к. в конкурентной борьбе слову «конкурировать» больше соответствует понятие «уничтожить конкурента любой ценой»». Конкуренция — это жестокая борьба. Она ставит конкурентов в такие жесткие условия, что они вынуждены поступать по принципу «победителей не судят», «цель выше средств». Вопрос в бизнесе ставится однозначно: или ты, или тебя пустят по миру.

Угрозами в сфере предпринимательства являются опасности экономического, социального, правового, организационного, информационного, экологического, технического и криминального характера, снижающие эффективность и надежность функционирования предприятий, а в отдельных случаях, приводящие к прекращению его деятельности.

Угрозы безопасности предпринимательству проявляются в следующих основных сферах.

Экономические угрозы. К группе угроз безопасности и преступлений, совершаемых в сфере экономики, относятся: хищения, совершенные путем присвоения, растраты, злоупотребления служебным положением; кражи; взяточничество; корыстные злоупотребления властью или служебным положением; контрабанда; нарушение правил валютных операций и пр. Анализ преступности на протяжении многих лет говорит о высокой системности данного явления — тенденции одних эко-

номических преступлений взаимосвязаны, а частью и взаимообусловлены изменениями других.

В структуре экономической преступности одну треть занимают хищения государственного и общественного имущества, совершаемые путем присвоения, растраты либо злоупотребления служебным положением.

Высокую общественную опасность представляют должностные преступления и прежде всего взяточничество, поразившее практически все звенья управленческих, хозяйственных и коммерческих структур.

Социальные угрозы. Социальные угрозы связаны с повышающимся уровнем безработицы, расширяющейся зоной нищеты, увеличивающимся разрывом в уровнях доходов между бедными и богатыми, с нарастающей региональной дифференциацией. Сюда же можно отнести дискриминационное положение женщин в бизнесе, инвалидов, военнослужащих и т. д.

Информационные угрозы. К группе информационных угроз относятся действия, приводящие к ознакомлению с конфиденциальной информацией, к ее модификации (т. е. изменению содержания и структуры в интересах злоумышленника) и к уничтожению, а также действия, приводящие к неправомерному обладанию охраняемыми сведениями, к которым относится разглашение, утечка по техническим каналам и несанкционированный доступ со стороны злоумышленников.

1.1. Экономические угрозы

Экономическая безопасность предпринимательства определяется современным характером, ориентацией и направленностью воздействующих на него (предпринимательство) внешних и внутренних угроз.

К **внешним** угрозам относятся:

1. Разведывательная деятельность иностранных спецслужб и организаций по:
   - — добыванию материалов, связанных с созданием в России новейших образцов техники и технологий, результатов фундаментальных и прикладных научных исследований, опережающих мировой опыт;
   - — сбору конфиденциальных сведений экономического характера, обладание которыми наносит или может нанести ущерб оборонно-экономическому потенциалу, стратегическим позициям России на мировом рынке.

2. Деятельность иностранных организаций, фирм, компаний, направленная в ущерб национальным интересам и безопасности России:
   — ослабление или даже свертывание российских производств с конкурентоспособной продукцией, в частности в ходе приватизации (через приобретение части капитала) и конверсии этих предприятий;
   — стимулирование утечки «мозгов», вывоза из России капиталов и стратегически важных научно-технических разработок и стратегических сырьевых товаров;
   — попытки поставить нашу страну в зависимость от импорта за счет продажи специфического оборудования.
3. Проникновение в нашу экономику международных преступных формирований и их капитала, различного рода авантюристов и мошенников из числа иностранных граждан.

К **внутренним** угрозам относятся:

1. Постоянное расширение масштабов коррупции в органах государственной власти, проникновение в них преступных элементов, что, в свою очередь, влияет на развитие негативных тенденций в сферах приватизации, финансово-банковской деятельности в сфере внешнеэкономических связей.
2. Рост экономической преступности, включая контрабанду и незаконный экспорт капиталов, валюты, стратегического сырья, преступления в финансовой сфере, фальшивомонетничество и незаконные операции с ценными бумагами, по привлечению вкладов.
3. Организованная преступная деятельность в экономике, проникновение криминального капитала в важнейшие и наиболее доходные сферы легального бизнеса.

Наряду с макроэкономической существует и микроэкономическая трактовка угроз предпринимательству. По отношению к отдельному предприятию или отдельной коммерческой структуре можно привести следующие виды **внешних** угроз:

1. Недобросовестная конкуренция.
2. Преступные действия: криминальное насилие, посягательства на коммерческую тайну.
3. Противозаконные действия отдельных лиц и организаций административного аппарата, в том числе и налоговых служб.
4. Нарушение установленного регламента сбора, обработки и передачи информации.
5. Промышленный шпионаж.

Внутренние угрозы можно классифицировать следующим образом:

1. преднамеренные преступные действия (продажность) собственного персонала из-за низкого профессионализма и недобросовестности;
2. непреднамеренные действия и ошибки сотрудников;
3. отказ оборудования и технических средств;
4. сбои программного обеспечения средств обработки информации.

Соотношение между внутренними и внешними угрозами может быть охарактеризовано следующими показателями:

- 81,7% угроз совершается либо самими сотрудниками организации, либо при их прямом или опосредованном участии (внутренние угрозы);
- 17,3% угроз — внешние угрозы или преступные действия; 1,0% угроз — угрозы со стороны случайных лиц.

Объектами различных угроз предпринимательству выступают:

1. люди (персонал, сотрудники, компаньоны и др.);
2. материальные ценности;
3. финансовые ресурсы;
4. информационные ресурсы, включая патенты, незавершенные проектно-конструкторские разработки, «ноу-хау», программные продукты, массивы бухгалтерской и статистической информации и пр.

Угрозами **персоналу** являются моральные и физические страдания, выражающиеся в:

- убийствах;
- похищениях и угрозах похищения сотрудников, членов их семей и близких родственников;
- психологический террор, угрозы, запугивание, шантаж, вымогательство и т. д.

Угрозы персоналу, как правило, сопровождаются и крупными экономическими издержками — утрата ценных работников, затраты на возмещение работникам и членам их семей понесенного ими материального и морального урона, включая утрату здоровья и пр.

Угрозы **материальным ценностям** проявляются в:

- краже продукции, в повреждении зданий, помещений, квартир, дач, гаражей и другого недвижимого имущества;
- выводе из строя средств связи и систем коммунального обслуживания;
- краже, угоне и уничтожении транспортных средств.

Эта категория угроз продуцирует наиболее явный и наиболее значительный экономический урон.

Вот показательный пример, приведенный «Московским комсомольцем» 28.01.1998 г.

> Одно из самых удачных разбойных нападений прошлого года — налет на обменный пункт банка «Российский кредит» на улице Панфилова — удалось раскрыть сотрудникам милиции. Арестованы 8 человек, так или иначе причастных к этому дерзкому преступлению.
>
> 28 августа к обменному пункту уверенной походкой приблизились двое мужчин. Охранникам на входе они предъявили удостоверения работников службы безопасности «Российского кредита», сказали, что пришли с инспекцией, и проследовали внутрь. В помещении поведение «инспекторов» изменилось как по волшебству. Один из гангстеров достал пистолет, наставил его на секьюрити и кассиршу, а другой схватил увесистый мешок с приготовленными к инкассации деньгами (всего примерно 500 тысяч долларов и 173 миллиона рублей). После этого бандиты заковали сотрудников «экс-чейнч» в кандалы, опять же по удостоверению прошли мимо наружной охраны и умчались на поджидавшей их машине.
>
> Сыщики сразу обратили внимание, как тщательно спланирован налет. Все объяснилось в ходе следствия: банде помогал... один из работников службы безопасности банка, кстати, бывший милиционер. Он помог сделать фальшивые ксивы, рассказал, куда и когда приезжать. Преступники руководили действиями «коллег» по . рации..
>
> В течение четырех последних дней сотрудники ОВД «Сокол», 4-го отдела МУРа, угрозыска и следственного отдела по борьбе с оргпреступностью Северного округа арестовали грабителей. На вырученные от налета деньги друзья, члены одной из столичных преступных группировок, купили оружие, машины, одежду... Задержан и наводчик, который, кстати, получив свой гонорар, уволился из банка.

Наиболее опасным источником угроз малым предприятиям выступают их собственные сотрудники, значительная часть которых работает по совместительству. Нынешнее удручаю-

щее состояние российского законодательства по финансовым и налогово-бюджетным вопросам делает различные формы негативного «давления» на финансовые ресурсы предпринимательства одной из наиболее распространенных форм экономических угроз предпринимательству.

Анализ преступных действий, предпринятых, в частности, против предпринимательства, показал следующие их соотношения:

Таблица 1

1.	Преступления против личности	4,3%
2.	Хулиганские действия	7,2%
3.	Кражи	49,9%
4.	Грабежи и разбойные нападения	7,0%
5.	Присвоение вверенного имущества	1,3%
6.	Мошенничество в финансовой сфере	2,5%
7.	Иные преступления	28,3%

Анализ общей ситуации в российской экономике показывает, что новая система хозяйствования и хозяйственных отношений складывается в аморальных, а то и криминальных условиях вообще и в малом предпринимательстве, в частности. Внутренние и внешние угрозы предпринимательства тесно взаимодействуют. Например, общая тенденция криминализации хозяйственной деятельности ведет к снижению морально-этических норм работников всех рангов, что часто толкает их на действия, наносящие урон «собственной» фирме. Мотивами внутренних угроз в этом случае являются безответственность, некомпетентность (низкая квалификация), личные побуждения (самоутверждение, корыстные интересы).

Можно привести экспертные характеристики и некоторых других действий, приводящих к возникновению угроз предпринимательству (см. таблицу 2).

Комментарий: угрозы со стороны административного аппарата распределились так: со стороны налоговой инспекции — 20%; со стороны таможни — 6%; со стороны администрации — 31 %; и выражались в предвзятом отношении,

в пассивности в поддержке, в вымогательстве, в пособничестве конкурентам.

Таблица 2

1.	Участие госструктур власти и управление в коммерческой деятельности, в том числе для подавления конкурентов	31%
2	Использование криминальных структур для подавления конкурентов	25%
3.	Отсутствие необходимого законодательства, позволяющего эффективно противодействовать недобросовестной конкуренции	20%
4.	Экономический и информационный шпионаж	20%
5.	Отсутствие необходимых условий и культуры ведения бизнеса, неуважение партнеров, невыполнение обязательств, срыв договорных условий	6%

В условиях сохраняющейся высокой степени монополизации российской экономики огромную опасность в плане продуцирования экономических угроз предпринимательству, особенно малому, представляет практика **недобросовестной конкуренции.**

Под недобросовестной конкуренцией понимают действия, направленные на приобретение преимуществ в предпринимательской деятельности хозяйствующих субъектов, которые противоречат положениям действующего законодательства, обычаям делового оборота, требованиям добропорядочности, разумности и справедливости и могут причинить убытки другим хозяйствующим субъектам — конкурентам либо нанести ущерб их деловой репутации.

Так гласит закон:

Закон РФ «О конкуренции и ограничении монополистической деятельности на товарных рынках».

Раздел III. Недобросовестная конкуренция.

Статья 10. Формы недобросовестной конкуренции.

Не допускается недобросовестная конкуренция, в том числе:

• распространение ложных, неточных или искаженных сведений, способных причинить убытки другому хозяйствующему субъекту, либо нанести ущерб его деловой репутации;

• введение потребителей в заблуждение относительно характера, способа и места изготовления, потребительских свойств, качества товара;

•некорректное сравнение хозяйствующим субъектом в процессе его рекламной деятельности производимых или реализуемых им товаров с товарами других хозяйствующих субъектов;

• самовольное использование товарного знака, фирменного наименования или маркировки товара, а также копирование формы, упаковки, внешнего оформления товара другого хозяйствующего субъекта;

'получение, использование, разглашение научно-технической, производственной или торговой информации, в том числе, коммерческой тайны, без согласия ее владельца.

В более широком плане недобросовестная конкуренция — это любые направленные на приобретение преимуществ в предпринимательской деятельности действия хозяйствующих субъектов, которые противоречат положениям действующего законодательства, способные причинить ущерб субъектам рынка.

Основной принцип недобросовестной конкуренции заключается в стремлении укрепить свое положение на рынке за счет ослабления позиций конкурентов или обмана потребителей. Для этого на конкурирующие фирмы оказывается соответствующее давление, которое может осуществляться в прямом или косвенном виде.

К числу таких действий относятся:

- использование своего экономического потенциала для продажи продукции по ценам ниже себестоимости (демпинг) с целью подрыва позиций конкурента и последующего вытеснения его с рынка;
- злоупотребление господствующим положением на рынке (монополия);
- установление дискриминационных коммерческих условий;
- тайный сговор на торгах и неофициальное создание тайных картелей;
- выпуск продукции с характеристиками, не соответствующими рекламе;
- подделка и производство оригинальных изделий, выпускаемых конкурентами;
- незаконное использование товарных знаков для маркировки своей продукции.

Какие же формы и методы недобросовестной конкуренции находят сегодня большее распространение? Их можно охарактеризовать следующими данными:

Таблица 3

1	*Экономическое подавление:*	
	• срыв сделок и иных соглашений;	48%
	• парализация деятельности фирм с использованием полномочий госорганов, средств массовой информации;	31% 11%
	• компрометация деятельности фирм за счет недобросовестной рекламы;	10%
	• шантаж, компрометация руководителей и отдельных сотрудников	
2	*Физическое подавление:*	
	• ограбления и разбойные нападения на офисы, склады:	73%
	• угрозы физических расправ	22%
3	*Промышленный шпионаж::*	
	• подкуп сотрудников;	43%
	• передача документов и разработок;	10%
	• копирование программ и данных;	24%
	• проникновение в ПЭВМ;	18%
	• подслушивание переговоров	5%

Значительную угрозу предпринимательству наносит МОШЕННИЧЕСТВО — завладение имуществом или приобретение права на имущество путем обмана либо злоупотребления доверием. Способы завладения имуществом при мошенничестве своеобразны: преступник прибегает к обману лиц, во владении или ведении которых оно находится, в результате чего они, будучи введенными в заблуждение, добровольно передают имущество преступнику, полагая, что последний имеет право его получать.

При совершении мошенничества обман выступает в качестве одного из элементов способа совершения преступления, является необходимым признаком, обуславливающим неправомерный переход имущества из владения правомочного лица в незаконное владение преступника.

Цель мошеннического обмана — ввести в заблуждение владельца имущества и добиться добровольной передачи его в распоряжение преступника.

Так гласит закон:

Статья 159 УК РФ «Мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием».

Формы обманных действий могут быть самыми разнообразными:

- *дезинформационные;*
- *подложные документы;*
- *ложное предпринимательство и др.*

Способом преступного завладения имуществом может быть и злоупотребление доверием, когда преступник или использует для получения имущества в целях обращения его в свою пользу определенные гражданско-правовые (договорные) отношения, основанные главным образом на доверии сторон, или пользуется тем, что имущество передается ему лицами, во владении которых оно находилось, без соответствующих предосторожностей и оформления, а преступник, воспользовавшись этим, присваивает его.

Пример. (Российская газета 29.01.98)

Гербовая печать в кармане мошенников

Оригинальный способ бизнеса нашли на Кубани мошенники-гастролеры из Ставрополья. Они разъезжали по всему краю, выдавая себя за инспекторов краевой налоговой службы. Пользуясь доверчивостью предпринимателей, мошенники проводили «проверки» применения контрольно-кассовых аппаратов, составляли акты, а за их уничтожение требовали взятки от провинившихся в размере от одного до шести миллионов рублей. При себе они имели фальшивые удостоверения и гербовые печати.

Владимир Удачин, соб. корр.

К типичным видам мошенничества относятся:

1. Воровство наличности из кассы:
   воровство чеков;
   использование наличности не по назначению;
   - фальсификация кассовых книг;
   фальсификация сумм на банковских счетах;
   подделка чеков;

- использование поступлений в пенсионные фонды не по назначению;
  оплата личных счетов чеками фирмы.

2. Представление фальсифицированные счетов:
   - фальсификация транспортных накладных;
   - завышенное фактурирование.
3. Кражи инвентаря:
   - сговор с клиентами или поставщиками;
     получение «благодарности» за определенные услуги (взятки);
     использование подставных поставщиков;
   - завышение цен.
4. Выдача фальшивых векселей.
5. Использование имущества фирмы в личных целях:
   предоставление заказов за взятки;
   мошенничество с кредитными карточками.
6. Фальсификация записей в бухгалтерских книгах:
   - для улучшения отчетности;
   - для покрытия недостач.
7. Несанкционированная продажа имущества фирмы: инвентаря, оборудования, отходов производства.
8. Мошенничество с выплатой заработной платы:
   - обналичивание невостребованных чеков;
     оплата труда работников-«подснежников» (мертвые души).
9. Компьютерные преступления.

Основные элементы, определяющие мотивацию и возможности для совершения мошенничества:

- давление внешних обстоятельств;
  возможность совершить и некоторое время скрывать акт мошенничества;
- личные моральные факторы, оправдывающие преступные действия.

1. Давление внешних обстоятельств проявляется в финансовой сфере. Примерно 95% от всех случаев мошенничества вызваны или финансовыми обстоятельствами или человеческими пороками. К ним можно отнести:
   - жадность;
     жизнь не по средствам;
     большие долги;
   - большие счета за покупки и другие виды обслуживания;

- отсутствие денег;
- неожиданная потребность в деньгах.

2. Давление пороков и пагубных привычек тесно связано с финансовыми обстоятельствами. К ним относятся азартные игры, наркотики, алкоголь, сексуальные удовольствия. Надо отметить, что пороки и пристрастия относятся к худшим из факторов мошенничества, так как носят долговременный и постоянный характер, часто хронический, неизлечимый.
3. Давление обстоятельств, связанных с работой, приводит к мошенничеству лишь ради того, чтобы свести счеты со своими начальниками или еще кем-то на работе. Мотивы: кажущаяся недооценка своих успехов, чувство неудовлетворенности от работы, боязнь ее потерять, невыдача премиальных, ощущение, что тебе платят меньше, чем ты того заслуживаешь.

Статистика дает такое распределение побудительных мотивов совершения мошеннических действий и преступных деяний (таблица 4).

Таблица 4

№	Причины	% соотношений
1.	Алкоголь и наркотики	67
2.	Проблемы эмоционального характера	63
3.	Семейные проблемы (бытовые)	57
4.	Азартные игры	38
5.	Финансовые трудности	37
6.	Прочие проблемы	32

По честности можно так классифицировать сотрудников фирмы:

честные — 40%;
- относительно честные — 30%;
- нечестные — 30%.

Широкое распространение получило лжепредпринимательство — создание предпринимательских организаций без намерения осуществлять уставную деятельность с целью получения ссуд, кредитов, снижения налогообложения или иного извлечения имущественной выгоды противозаконным путем. Особо широкое распространение приобрело уклонение от уплаты налогов с предприятий и организаций как в виде действий

по сокрытию и занижению прибыли, так и иным путем со стороны должностного лица хозяйствующего субъекта.

Заметно растет количество злоупотреблений в финансово-кредитной сфере, среди которых получение кредита обманным путем, выпуск и распространение необеспеченных ценных бумаг, а также нарушение порядка их эмиссии, незаконные операции по переводу за границу значительных денежных сумм, подделка банковских чеков и кредитных карточек.

Значительную общественную опасность стало представлять ложное и злостное банкротство — заведомо ложное заявление предпринимателя о невозможности исполнения обязательств перед кредиторами с корыстными целями, а также умышленное сокрытие предпринимателем-должником своей устойчивой неплатежеспособности путем предоставлений, не соответствующих действительности.

Какова вероятность наступления опасных действий или условий их определяющих?

Определить вероятность наступления угрозы можно несколькими путями или способами. Наиболее практичным является метод математической статистики. На основе статистической обработки данных приводятся такие показатели вероятности наступления угрожающих событий.

Таблица 5

№	Виды угроз	(опрошенных)	R (вероятность)
1	Стихийные бедствия	25	0,4
2	Перерывы электропитания и связи	50	0.5
3	Проникновение в информационные системы извне	3	0.03
4	Внутренние нарушения работы информационных систем	70-75	0.7-0.75
5	Злонамеренные действия обиженных сотрудников	10	0,1
6	Корыстные побуждения персонала	10	0,1
7	Неумышленные ошибки	50-55	0.5-0,55

Что генерирует сегодня нарастание названных выше угроз предпринимательству и связанные с ними формы экономической преступности? Прежде всего, это — характер общей ситуации в экономике.

Говоря об экономической безопасности, надо установить взаимосвязь угроз со стороны конкурентов и злоумышленников и рисков в процессе функционирования предприятия во времени и в пространстве угроз. Пространство угроз охватывает объект защиты — персонал коммерческой структуры, имущество, денежные средства и сведения, составляющие коммерческую или служебную тайну. Каждая угроза влечет за собой определенный ущерб — моральный или материальный, а противодействие призвано снизить его величину, в идеале — полностью, реально — значительно или хотя бы частично. Хотя и это удается далеко не всегда.

Можно утверждать, что **РИСК есть стоимостное выражение вероятности наступления события, ведущего к каким-либо потерям или ущербу.** Понятие риска является естественным для всякой коммерческой деятельности, осуществления инвестиционных проектов и не обязательно продуцируется именно факторами, нарушающими экономическую безопасность различных видов предпринимательства. Например, коммерческие банки опасаются повышения рисков при финансировании малых предприятий. Чтобы снизить возможный невозврат кредитов, ЦБ России разработал норматив риска на одного клиента. Превышение этого норматива может привести к решению ЦБ об изъятии у банка лицензии. Поскольку наиболее рискованным является кредитование именно малых предприятий, соблюдение этого норматива служит формальным поводом для отказа в выдаче кредитов предпринимателям.

Как экономическая категория РИСК представляет собой событие, которое может произойти или не произойти. Следовательно, риском можно управлять, используя различные меры, позволяющие в определенной степени прогнозировать наступление рискового события и принимать меры к снижению его величины.

Риски, непосредственно связанные с предпринимательской деятельностью, можно подразделить на такие категории как коммерческие, инвестиционные, валютно-финансовые.

1. **Коммерческие риски** представляют собой возможность потерь (ущерба) в процессе хозяйственной деятельности. Они означают неопределенность результатов конкретной коммерческой сделки. Коммерческие риски могут быть декомпозированы на имущественные, производственные, торговые и транспортные.

- Имущественные риски связаны с вероятностью потерь имущества в результате краж, грабежей, уничтожения по различным причинам и условиям.
- Производственные риски являются результатом нарушения производственного процесса по различным причинам: недопоставка комплектующих, повреждение или уничтожение основных и оборотных фондов (оборудование, транспорт, сырье), нарушение технологии производства (неопытность, браки др.).
- Торговые риски приводят к убыткам в результате задержки платежей, недобросовестной конкуренции на товарных рынках.
- Транспортные риски связаны с перевозкой грузов различными видами транспорта.

2. Инвестиционные риски подразделяются на упущенную выгоду, снижение доходности и прямые финансовые потери.

- Упущенная выгода — это финансовый ущерб в виде неполучения дохода (прибыли) в результате срыва какого-либо мероприятия или сделки, например, срыва контракта на приобретение кем-то товаров или услуг.
- Снижение доходности может возникнуть в результате уменьшения размера процентов и дивидендов по вкладам и кредитам.
- Риски прямых финансовых потерь — это биржевые риски, риски банкротства, селективные риски, а также кредитные риски:
  - — биржевые риски — это потери от биржевых сделок. Они представляют собой риск неплатежа по коммерческим сделкам или неплатежи комиссионного вознаграждения брокерской фирмы и т. п.;
  - — селективные риски — это риски неправильного выбора видов вложения капитала, вида ценных бумаг для инвестирования в сравнении с другими ценными бумагами при формировании инвестиционного портфеля;
  - — риски банкротства представляют собой опасность в результате неправильного вложения капитала, полной потери предпринимателем собственного капитала и неспособности рассчитываться по взятым на себя обязательствам.

3. Валютно-финансовые риски. Это риски, связанные с вероятностью потерь финансовых ресурсов. Сюда относятся

риски, связанные с покупательной способностью денег, и риски, связанные с вложением капитала.

- К рискам, связанным с покупательной способностью денег, относятся инфляционные и дефляционные риски, валютные риски и риски ликвидности:
  — инфляционный риск приводит к обесцениванию покупательской способности, а дифляционный — к снижению доходов при падении уровня цен;
  — валютные риски представляют собой опасность валютных потерь, связанных с изменением курса иностранной валюты;
  — риски ликвидности — это риски, связанные с возможностью потерь при реализации ценных бумаг или других товаров из-за изменения оценки их качества и потребительской стоимости.

Помимо предпринимательских рисков существуют природно-естественные риски, политические риски, экологические и другие, характер действий которых мало зависит от социально-политической сферы и создают как бы определенный «опасный» фон. Очевидно, что каждый отдельный предприниматель не в силах влиять на эти факторы непосредственно, но учитывать возможность их появления он должен.

1.2. Социальные угрозы

Социальные угрозы предпринимательству вызваны в значительной степени сохраняющейся в стране экономической и политической нестабильностью, что порождает безработицу, нищету, социально-экономическое расслоение общества в связи с разрывом в уровнях доходов и в еще большей мере — в располагаемых имущественных и финансовых ресурсах. Применительно к предпринимательству эти обстоятельства затрудняют вхождение в бизнес широких слоев населения. Нестабильность функционирования предприятий малого и среднего бизнеса приводит к разорению, банкротству многих из них, что также дополнительно порождает безработицу. Особенно трудно пробиться в самостоятельном бизнесе наиболее социально незащищенным слоям населения: инвалидам, многодетным матерям, беженцам, вынужденным переселенцам, в т. ч. из зон бедствия. Затрудненность и неравная доступность «вхождения в бизнес» для различных социальных групп населения порождает дополнительную социальную напряженность

в обществе, генерирует негативное, а часто и криминальное отношение ко всей предпринимательской среде.

Угрозы предпринимателям, относящимся к действию названных выше факторов усиливаются в связи с тем, что часто «под крышей» различных общественных и благотворительных организаций и фондов, создающихся людьми, нуждающимися в защите и поддержке государства, рано или поздно оказываются представители криминально-предпринимательских кругов, легализующих таким образом свои капиталы и более того — получающие дополнительную выгоду за счет представленных данным организациям и фондам налоговых и иных льгот.

Социальные угрозы также можно классифицировать по некоторым признакам:

- по направленности против социальных интересов предпринимателей;

по масштабам (местные, локальные, в масштабе фирмы, предприятия);

- по причинам (несправедливое распределение собственности, доходов, жизненных благ, власти и т.д.).

1.3. Информационные угрозы

Известно, что информация — это сведения о лицах, предметах, событиях, явлениях и процессах (независимо от формы их представления), отраженные на материальных носителях, используемые в целях получения знаний и практических решений. Информация выступает на сегодня как один из важнейших ресурсов, в том числе и предпринимательских. Информация выступает как собственность, она имеет потребительское и стоимостное содержание. В сфере предпринимательства установился такой афоризм: «Кто владеет информацией, тот владеет миром».

По отношению к информации, к информационным ресурсам можно представить следующие виды угроз:

- ознакомление с конфиденциальной информацией различными путями (подглядывания, копирования и т. д.);
- модификация информации в интересах злоумышленника;
- разрушение информации (факты вандализма, вредительства).

Осуществление этих угроз может быть реализовано:

- путем неофициального доступа к источникам конфиденциальной информации;

- путем подкупа сотрудников предприятия, непосредственно связанных с коммерческой тайной;
- путем перехвата информации, передаваемойсредствами связи или излучаемой различными техническими средствами;
- через переговорные процессы между представителями различных структур и др.

Угрозы информационного характера для предпринимательства можно также классифицировать на внутренние и внешние.

К **внутренним** угрозам относятся преднамеренные или случайные негативные воздействия на информационные ресурсы предпринимательских структур, выражающиеся в неправомерном ознакомлении со сведениями, составляющими коммерческие и иные секреты предпринимателей; изменение (фальсификация) состава и структуры информации (баз данных) в преступных целях или ее полное разрушение с целью нанесения предпринимательству морального и материального ущерба.

К внутренним угрозам относится и разглашение конфиденциальных сведений сотрудниками коммерческого предприятия, как по незнанию, так и по злому умыслу. К информационным угрозам относится также и утечка информации по техническим каналам, за счет которой существенно возрастает вероятность овладения коммерческими секретами данного предприятияконкурирующими структурами.

К **внешним** угрозам относится прежде всего недоступность или недостаточная доступность предпринимателей к официальной информации о новых законодательных и иных нормативных актах, в частности, в области лицензирования хозяйственной деятельности, налоговой политики, льгот и преимуществ для субъектов малого предпринимательства.

К внешним угрозам в области информации относится и недобросовестная конкуренция, проявляющаяся в форме промышленного шпионажа, распространения ложной информации о продукции конкурентов и их финансовом положении; в виде несанкционированного доступа к конфиденциальной информации предпринимателей-конкурентов различными легальными и нелегальными путями.

Как внутренние, так и внешние угрозы приносят предпринимателям те или иные виды ущерба в их производственно-коммерческой деятельности.

1.4. Коррупция, как фактор угроз предпринимательству

Масштабная коррупция на всех уровнях оказывает разлагающее влияние на все стороны жизни и деятельности страны, в том числе и на малый и средний бизнес.

Негативные последствия проявляются во всех сферах. Например, в экономической сфере это влияние проявляется в следующих видах.

1. Расширяется теневая экономика.
2. Нарушаются реальные конкурентные механизмы рынка.
3. Повышаются цены за счет коррупционных «накладных расходов».
4. Теряется доверие участников рынка к способности власти устанавливать и соблюдать честные правила рыночных отношений.
5. Расширяются масштабы коррупции в неправительственных структурах.

Экономические потери от коррупции в 1997 г. составили 49 триллионов (неденоминированных) рублей, что составило 20% бюджета [30].

По подсчетам экспертов общественной организации «Технологии — XXI век» малые предприниматели тратят во всей стране на взятки чиновникам минимум 500 миллионов долларов в месяц. В год это оборачивается суммой в 6 миллиардов долларов. Предварительный анализ показывает, что 10% всего дохода в малом и среднем бизнесе тратится на коррупционные сделки. При этом на начальном этапе (регистрация и др.) расходы существенно выше. «Вход в бизнесе» требует решений примерки 50 чиновников различного ранга. Если добавить к этому коррумпированность отношений внутри самих предприятий, то суммарные экономические потери от коррупции в нашей стране могут составить от 10 до 20 миллиардов долларов.

Пример. «Российская газета» от 21.2.98 г.

«Безнаказанно обворовать предпринимателя может каждый...» Под таким заголовком 12 ноября минувшего года была опубликована беседа с известным нижегородским предпринимателем и журналистом, генеральным директором Нижегородского торгово-промышленного дома Владимиром Носковым.

В ней мой собеседник рассказывал о том, как открыто правоохранительные органы грабят бизнесменов, занимающихся малым предпринимательством. В частности, в ав-

густе 1996 г. начальник отдела снабжения Нижегородского торгово-промышленного дома в районе города Петушки Владимирской области подверглась нападению. Было похищено 60 миллионов рублей. Однако все обращения в правоохранительные органы заканчивались ничем. Заявление пересылалось из одного отделения милиции в другое. В конечном итоге милиция вынесла вердикт: дело закрыть «за не доказанностью совершения факта ограбления».

(Юрий Шуков)

Состав и структура привлеченных к ответственности в 1997 г. коррумпированных лиц представлены в таблице 7.

Таблица 7

	Состав	*%*
1	Работники министерств, комитетов и структур на местах	41.1
2	Работники кредитно-финансовой системы	11.7
3	Сотрудники правоохранительных органов	26.5
4	Работники таможенной службы	3.2
5	Работники контролирующих органов	8.9
6	Депутаты	0.8
7	Прочие	7.8

Социальные последствия коррупции:

1. Закрепляется и увеличивается резкое имущественное неравенство, бедность большей части населения.
2. Коррумпированность правоохранительных органов способствует укреплению организованной преступности. Последняя сращивается с коррумпированными группами чиновников и предпринимателей, усиливается еще больше с помощью доступа к политической власти и возможностям для отмывания денег.
3. Увеличивается социальная напряженность, бьющая по экономике.

Политические последствия:

1. Уменьшается доверие к органам власти.
2. Растет угроза экономической и политической изоляции на международном рынке.
3. Увеличивает возможности властвования олигархических группировок др.

Можно утверждать, что коррупция, ее масштабы, специфика и динамика — следствие общих политических, социальных и экономических проблем страны.

1.5. Правовые угрозы

Угрозы правового характера вызваны прежде всего отсутствием устойчивого, исчерпывающего и непротиворечивого законодательства, прежде всего регулирующего процесс хозяйственной деятельности. Наличие «пробелов» в действующем законодательстве и других нормативных документах порождают различные «лазейки» для утаивания прибыли, реальных доходов, различных «обходных маневров» в хозяйственных и финансовых операциях, а также для прямого криминального давления на предпринимательство.

Массовый характер приобрели прямые нарушения местными органами власти законов о предпринимательской деятельности.

Основными видами нарушений являются:

- посягательства на имущество предпринимателей;
- ограничения на межрегиональное перемещение товаров;
- незаконное регулирование цен;
- взыскание не предусмотренных законодательством сборов;
- вмешательство во внутренние дела предприятий;
- попытки административного регулирования деятельности предприятий и др.

Определенные правовые угрозы (угрозы административного произвола) содержатся и в правовом регулировании практики лицензирования хозяйственной деятельности. Несмотря на Закон РФ «О лицензировании отдельных видов деятельности» от 1б сентября 1998 г., остаются значительные сферы административно-правовых угроз в области предпринимательства. По сути дела под видом лицензирования часто определяется сертификация помещения; в некоторых случаях лицензии выдавались и выдаются на месяц, на квартал, а в лучшем случае — на полгода. В связи с этим для продления лицензии предприниматель вновь вынужден обходить множество инстанций и везде платить как официальные, так и «неофициальные» сборы.

Кроме этого лицензирующие органы наделены правом приостанавливать действие лицензии. Пользуясь этим правом, данные органы могут прекратить действие лицензии, что приведет к остановке предпринимательской деятельности. В результате

могут возникнуть финансовые потери не только для самого предпринимателя, но и его партнеров. Дело может закончиться целой цепочкой банкротств.

В отдельных случаях нечеткость нормативно-правового обеспечения, дополненная низкой квалификацией служащих, приводит к конфликтным ситуациям (рисковым для предпринимателей), перерастающих иногда в криминальные действия. Подобная ситуация во многом характерна для взаимоотношений предпринимательства с органами налоговой инспекции. Для российского предпринимателя угрозы безопасности от существующей практики налогообложения возникают вследствие запутанности ныне действующего законодательства, его нестабильности, возможности, с одной стороны, разнообразных уклонений от налогообложения, а с другой — завышенности некоторых налоговых ставок и ненужности целого ряда налогов, а также неопределенности в налогово-бюджетных взаимоотношениях федерального Центра с регионами.

Нестабильность налогового законодательства создает ряд рисковых ситуаций и для зарубежных предпринимателей, о чем свидетельствуют результаты опроса российско-американской торговой палатой среди 47 иностранных фирм. Им был задан вопрос, какие проблемы они считают самыми серьезными для своего бизнеса в России. 42 фирмы ответили, что такой важнейшей проблемой является нестабильность и неясность налогового законодательства, 41 фирма также отметила проблемы, связанные с налогом на сверхнормативныйфонд оплаты труда. На третьем месте — 16 раз — отмечены проблемы налогов на добавленную стоимость, прежде всего по «межфирменным» ссудам.

1.6. Криминальные угрозы

По данным МВД России, «криминальные структуры» в государстве в настоящее время контролируют свыше 50% всех хозяйствующих субъектов. Нелегальные группировки оказывают силовое давление на коммерческую структуру до тех пор, пока она не соглашается платить регулярную дань. Взамен рэкетиры охраняют эту структуру, у которой не хватает собственных средств для защиты от мафии, и она вынуждена соглашаться. Такие структуры оказываются под давлением мафии и, как правило, оказываются не в состоянии преодолеть это давление собственными силами.

Криминальные угрозы генерируются также тем, что крупные суммы денег, добытые незаконным путем, вынуждают мафию искать способы их легализации. Мафия все чаще заставляет предпринимателей «принимать в оборот» свои теневые капиталы и отдавать мафии ту или иную меру контроля над предприятием. Последнее еще более усиливает воздействие криминальных структур на предпринимательство. По расчетам Аналитического центра РАН, 39% капитала и 80% «голосующих» акций перешло в руки криминального капитала посредством взимания дани с коммерческих структур, в том числе в виде части акционерного капитала. Однако основной формой легализации мафии является создание собственных коммерческих структур. В целом же в настоящее время в криминальные отношения вовлечены 40% предпринимателей и 60% всех коммерческих структур. Мафией установлен контроль над 35 тыс. хозяйствующих субъектов, среди которых 400 банков, 47 бирж, 1,5 тыс. предприятий государственного сектора.

В последнее время с развитием коммуникаций и электронных форм расчетов распространились проникновения в компьютерные сети для внедрения фиктивных платежных документов, хищения средств с использованием векселей, арбитражных приказов, акций и облигаций.

Распространение «электронных преступлений» объясняется и довольно низкой степенью защиты компьютерных сетей, и возросшей «квалификацией» мошенников.

Пример

Не так давно в Москве пресечена крупномасштабная попытка «электронного мошенничества» на сумму более 68 млрд. рублей.

Преступники действовали в сговоре с рядом коммерческих структур — клиентов восьми московских банков, в том числе крупных и известных, и намеревались провести ряд фиктивных платежей с использованием модемной связи. Сотрудники главного управления ЦБ отметили высокий уровень квалификации организаторов аферы в области программирования и в вопросах электронных расчетов между коммерческими банками и расчетно-кассовые центром. И лишь благодаря мерам, проводимым с целью защиты системы межбанковских платежей, удалось вовремя выявить и пресечь аферу.

Факторы, способствующие распространению криминальных угроз

Внешние:

- объективный рост террористических проявлений в странах ближнего и дальнего зарубежья;
- социально-политическая и экономическая нестабильность в сопредельных государствах, наличие вооруженных конфликтов в отдельных из них;
- стратегические установки некоторых иностранных спецслужб и зарубежных террористических организаций;
- «прозрачность» границ и отсутствие надежного контроля за режимом въезда-выезда;
- наличие каналов нелегального поступления в Россию из-за рубежа оружия, ВВ и других запрещенных для оборота вещей и предметов;
- образование российской «диаспоры» за пределами России.

Внутренние:

- наличие в стране значительного нелегального «рынка» оружия и относительная легкость его приобретения;
- наличие значительных контингентов лиц, прошедших школу войны и их недостаточная социальная адаптация в обществе;
- существенное ослабление ряда административных режимов;
- наличие и деятельность ряда экстремистских группировок;
- обостренное чувство социальной неустроенности и незащищенности;
- слабая работа правоохранительных органов и организаций по защите прав граждан.

Статистические показатели распространенности криминальных угроз по сферам и годам приведены в следующих таблицах (табл. 8, 9).

Таблица 8

Годы	Число преступлений с использованием физического и психического насилия	%
1986	30299	44
1990	89109	7,6
1991	107521	6,8
1995	161425	7,7

1.7. Хозяйственные преступления

Хозяйственные преступления разделяются на три основные группы в зависимости от защищаемых интересов:

№	Показатели/годы	1990	1991	1992	1993	1994	1995
1.	Убийства с покушениями	17124	17746	24448	31246	343024	31001
2.	Угрозы убийством, нанесение тяжких телес-ных повреждений, уничтожение имущества	8020	8114	9420	19375	45864	
3.	Умышленные тяжкие телесные повреждения	40962	41195	53286	66864	67706	61734
4.	Похищение людей				110	499	628
5.	Захваты заложников	1			3	51	118

а) преступления, причиняющие ущерб или создающие реальную возможность причинения ущерба путем непосредственного нарушения интересов государства или любого иного хозяйствующего субъекта, независимо от формы собственности;

б) преступления, причиняющие ущерб или создающие реальную возможность причинения ущерба путем нарушения интересов граждан, поскольку они соприкасаются с хозяйственной деятельностью учреждений и частных лиц;
в) преступления, которые могут причинить ущерб народному хозяйству в области *его* ведения и организации как путем непосредственного нарушения интересов государства или иного хозяйствующего субъекта, так и путем нарушения интересов граждан, поскольку они соприкасаются с хозяйственной деятельностью учреждений и частных лиц.

Хозяйственные преступления ориентированы на следующие сферы деятельности:
а) преступления в сфере предпринимательской деятельности;
б) преступления, связанные с нарушением антимонопольного законодательства и законов, запрещающих практику недобросовестной конкуренции;
в) преступления в сфере защиты прав потребителей;
г) преступления в налоговой сфере;
д) валютные преступления;
е) преступления в финансово-кредитной сфере;
ж) преступления в сфере осуществления внешнеэкономической деятельности и др.

1.8. Политические угрозы

Политические угрозы предпринимательству вызываются межнациональными конфликтами, их переходом в стадию высокой напряженности и конфронтации. В ряде случаев политическая нестабильность связана с конфликтами исполнительной и законодательной властей на местах, которые втягивают в сферу конфликта и предпринимательские круги. Политическая ситуация в регионе является одним из факторов, определяющих его инвестиционный климат, в зависимости от которого инвесторы, особенно иностранные, принимают решения в вложении своих капиталов в те или иные сферы региональной экономики.

1.9. Реальное состояние безопасности малого предпринимательства

Сложная социально-экономическая обстановка в стране, спад производства, развал социальной сферы, организованная

преступность, общая криминализация общества и коррумпированность органов управления накатываются огромной волной на всю сферу предпринимательства лавиной угроз и причиняет огромный урон безопасности бизнеса. Оценка реального состояния безопасности малого предпринимательства весьма затруднена из-за скудного характера и низкой достоверности сведений.

Нерегулярное отслеживание состояния безопасности малого предпринимательства, анкетирование по этим проблемам слушателей постоянно действующего семинара «Экономическая безопасность и защита информации» (Институт повышения квалификации информационных работников) и обработка результатов экспресс-опроса участников 1-го Всероссийского съезда представителей малых предприятий (февраль 1996 г.) показал следующее состояние безопасности малых предприятий.

На вопрос о том, какова оценка состояния безопасности в сфере предпринимательства, 2 из 3-х работающих в бизнесе респондентов ответили: «Неудовлетворительная». И только 3% дали хорошую оценку. Наиболее мрачная картина видится предпринимателям из торговой сферы (80% дали неудовлетворительную оценку). 45% предпринимателей в течение последнего года были жертвами краж, ограблений, мошенничества и других имущественных преступлений. В сфере торговли эта цифра доходит до 59%, а среди охранных фирм о насилии, примененном к сотрудникам, их родным и близким, заявили 55% опрошенных.

При этом степень выполнения требований по комплексному обеспечению безопасности оценивается как реализованное только на 1/6 предприятий. На остальных эти требования не реализованы.

В части отдельных направлений обеспечения безопасности по видам приводятся такие же результаты.

Как же обеспечивается безопасность?

1. Полномасштабные требования по безопасности предпринимательства закреплены в Уставе предприятия только у 20% опрошенных и совершенно не закреплены у 60%.
2. Требования по экономической безопасности и защите информации предусмотрены в Коллективном договоре только у 12% опрошенных, 88% их не имеют.
3. В правилах внутреннего трудового распорядка требования по безопасности предусмотрены только у 48% опрошенных.

4. Полномасштабные требования по безопасности имеются в трудовых соглашениях (контрактах) только у 13%. У 32% имеются отдельные требования. У 55% опрошенных в контрактах таких требований нет.
5. Значительная часть опрошенных показала полное отсутствие требований по безопасности в положениях о подразделениях и в функциональных обязанностях своих сотрудников.
6. Перечень сведений, составляющих коммерческую тайну предприятия имеют только 25%, остальные не имеют таких перечней даже в виде ограниченного списка.
7. На вопросы «Как организована защита информационных ресурсов» были получены такие ответы: организована надежная защита — 13%, посредственная — 6 %, совершенно не защищается — 81%.
8. Технические средства охраны имущества, материальных и финансовых ценностей используются достаточно широко у 20%, ограниченно — 6%, в отдельных зонах — 13%, не используются вообще — 71%.
9. Для защиты конфиденциальной информации технические средства используют только 20% опрошенных.

По итогам опроса можно сделать следующие выводы:

1. Общее состояние защищенности крайне слабое. Более 60% опрошенных вообще не защищены. Отдельные сферы безопасности большинства предприятий характеризуются ограниченными мерами и не ориентированы на комплексную защиту своих интересов.
2. Малые предприятия практически не имеют штатных структурных подразделений для обеспечения собственной безопасности.
3. Ограниченно используются технические средства охраны, безопасности и защиты информации.

Такое состояние безопасности и защиты коммерческих секретов можно объяснить только полным непониманием важности обеспечения безопасности предпринимательской деятельности, полным забвением правила «кто не защищен — тот теряет все!»

В заключении раздела можно утверждать, что уже четко выявились следующие аспекты угроз предпринимательству:

- угрозы безопасности самому предпринимателю;
- угрозы безопасности для потребителя услуг, продукции при недобросовестной деятельности предпринимателя;

- угрозы предпринимательской информации;
- угрозы безопасности обществу (государству, населению).

Главные источники угроз безопасности предпринимательства:

- рэкет со стороны частных лиц (на это указали 64 %. • опрошенных);
- реальная возможность физического насилия над сотрудниками фирм и членами их семей (54%);
- вымогательство со стороны представителей правоохранительных и контролирующих органов (49%), других государственных структур (40%);
- незаконные действия властей (39%).

Определены социальные аспекты безопасности:

- несправедливое распределение собственности, доходов, жизненных благ, власти;
- уничтожение важных социальных институтов;
- негибкий, антисоциальный характер политики реформ;
- проникновение иностранного капитала в сферу и овладение национальной инфраструктурой.

Угрозами экономической безопасности являются:

а) нарушение оптимального функционирования экономической системы:
   — развал производства в основных сферах;
   — утеря государственного управления экономикой, должного контроля за налогообложением, ценообразованием, внешней торговлей;
   — нарушение сбалансированности народного хозяйства;
   — нарушение функционирования денежной и финансово-кредитной системы;

б) бесконтрольное расхищение природных ресурсов;

в) установление контроля иностранного капитала за ключевыми отраслями национальной экономики;

г)утечка интеллектуального потенциала.

К внешним источникам угроз относятся:

- деятельность разведывательных и специальных служб иностранных государств;
- деятельность иностранных негосударственных структур и организаций, несовместимая с безопасностью и интересами страны;
- преступные действия иностранных государств и международных криминальных групп, структур и отдельных лиц.

К внутренним источникам угроз относятся:

- противозаконная деятельность юридических и физических лиц, а также иных субъектов в области формирования, использования и распространения информации, включая нарушения установленных регламентом сбора, обработки и использования информации;
- недобросовестная конкуренция и промышленный шпионаж с целью дискредитации конкурентов и производимой им продукции, вытеснения конкурентов с конкретных рынков нелегальными методами, монополизации рынков путем сговора о ценах, а также получения информации о составе, состоянии и деятельности конкурирующих предпринимательских структур.

В итоге вся совокупность угроз малому предпринимательству приводит к значительным затруднениям, осложнениям во всех направлениях деятельности в лучшем случае или к развалу, банкротству — в худшем, что вызывает органическую потребность в обеспечении безопасности предпринимательской деятельности.

ГЛАВА II

ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОММЕРЧЕСКОГО ПРЕДПРИЯТИЯ

Безопасность коммерческого предприятия достигается проведением единой политики в области обеспечения безопасности, системой мер правового, организационного и технического характера, адекватных угрозам жизненно важным интересам предприятия.

Для создания *и* поддержания необходимого уровня защищенности объектов коммерческого разрабатывается система правовых норм, регулирующих отношения сотрудников в сфере безопасности, определяются основные направления деятельности в данной области, формируются органы обеспечения безопасности и механизмы контроля и надзора за их деятельностью.

Основными принципами обеспечения безопасности являются законность, соблюдение баланса интересов личности и предприятия; взаимная ответственность персонала и руководства, взаимодействие с государственными структурами безопасности.

Основными направлениями обеспечения безопасности коммерческого предприятия как нормативно правовыми категориями, определяющими комплексные меры защиты его интересов, выступают правовая, организационная и инженерно-техническая защита.

2.1. Правовая защита

Правовые или законодательные основы обеспечения безопасности коммерческого предприятия составляют Конституту-

ция РФ, Законы РФ и другие нормативные акты РФ, регулирующие отношения в области безопасности.

Законодательные акты, защищающие интересы личности и материальные и финансовые ресурсы как собственность лица или предприятия не являются новыми для наших предпринимателей. На это направлены и Законы и Кодексы, в том числе и Уголовный Кодекс РФ, четко определяющий понятие, разновидности и состав преступлений против личности, предприятия и государства, различные действия и меры их пресечения.

В части коммерческой информации — сведений, связанных с производством, используемой технологией изготовления продукции, управлением, финансами и другой деятельностью предприятия формой обеспечение безопасности выступает понятие Коммерческая тайна. Коммерческая тайна — форма обеспечения безопасности наиболее важной, наиболее ценной коммерческой информации, составляющей объект охраны и предполагающей ограничения в ее распространении.

В зависимости от характера информации, ее доступности для заинтересованных потребителей, а также экономической целесообразности конкретных защитных мер, могут быть избраны следующие формы защиты информации:

- признание сведений коммерческой тайной;
- патентование;
- использование норм авторского права;
- применение норм обязательного права.

Создавая любые системы защиты информации необходимо четко понимать, что без создания правовых основ обеспечения безопасности любые последующие претензии с вашей стороны к недобросовестным сотрудникам, клиентам, конкурентам и должностным лицам окажутся просто беспочвенными.

Если перечень сведений, составляющий коммерческую тайну предприятия, остается в Вашей памяти, в записной книжке или даже в виде многочисленных устных указаний, то сотрудник, укравший важную информацию, скорее всего, разведет руками: мол, откуда ему было знать.

Для создания правовых основ защиты информации на коммерческом предприятии необходимо:

1. Внести в Устав предприятия следующие дополнения:
«предприятие имеет право: определять состав, объем и порядок защиты сведений, составляющих коммерческую тайну, требовать от сотрудников предприятия обеспечения ее сохранности»

«предприятие обязано: обеспечить сохранность коммерческой тайны».

Внесение этих дополнений дает право администрации предприятия:

- создавать организационные структуры по защите коммерческой тайны;
- издавать нормативные и распорядительные документы, определяющие порядок выделения сведений, составляющих коммерческую тайну, и механизмы их защиты;
- включать требования по защите коммерческой тайны в договора по всем видам хозяйственной деятельности;
- требовать защиты интересов предприятия перед государственными и судебными органами;
- распоряжаться информацией, являющейся собственностью предприятия, в целях извлечения выгоды и недопущения экономического ущерба коллективу предприятия и собственнику средств производства.

2. Разработать «Перечень сведений, составляющих коммерческую тайну предприятия». Перечень сведений, составляющих коммерческую тайну, может быть декомпозирован до каждого должностного лица и доведен до каждого сотрудника в рамках его функциональных обязанностей.

3. Дополнить «Коллективный договор» следующими требованиями:

Раздел: «Предмет договора»

а) Администрация предприятия (в том числе и администрация всех самостоятельных подразделений) **обязуется:** в целях недопущения нанесения экономического ущерба коллективу предприятия обеспечить разработку и осуществление мероприятий по определению и защите коммерческой тайны;

б) Трудовой коллектив принимает на себя обязательство по соблюдению установленных на предприятии требований по защите коммерческой тайны;

в) Администрации учесть требования защиты коммерческой тайны в правилах внутреннего трудового распорядка.

Раздел: «Кадры. Обеспечение дисциплины труда»

Администрация обязуется привлекать нарушителей требований по защите коммерческой тайны к административной и уголовной ответственности в соответствии с действующим законодательством.

4. Правила внутреннего трудового распорядка для рабочих и служащих предприятия дополнить:

Раздел: «Порядок приема и увольнения рабочих и служащих»

- При поступлении рабочего или служащего на работу или перевода его в установленном порядке на другую работу, связанную с коммерческой тайной предприятия, а также при увольнении, администрация обязана проинструктировать работника или служащего по правилам сохранения коммерческой тайны с оформлением письменного обязательства об ее неразглашении.
- Администрация предприятия вправе принимать решение об отстранении от работ, связанных с коммерческой тайной лиц, которые нарушают установленные требования по ее защите.

Раздел: «Основные обязанности рабочих и служащих»

Рабочие и служащие обязаны соблюдать требования по защите коммерческой тайны предприятия.

Раздел: «Основные обязанности администрации»

Администрация предприятия, руководители подразделений обязаны:

- обеспечить строгое сохранение коммерческой тайны, постоянно осуществлять организаторскую, экономическую и воспитательно-профилактическую работу, направленную на защиту коммерческой тайны предприятия;
- включать в должностные инструкции и положения обязанности по сохранению коммерческой тайны;
- неуклонно выполнять требования Устава, коллективного договора, трудовых договоров, правил внутреннего трудового распорядка и других хозяйственных и организационных документов в части обеспечения безопасности и сохранения коммерческой тайны.

5. Трудовой договор.

В соответствии с трудовым кодексом при заключении трудового договора трудящийся обязуется выполнять определенные требования, действующие на данном предприятии. Независимо от формы заключения договора (устная или письменная) подпись трудящегося на приказе о приеме на работу подтверждает его согласие с условиями договора.

Требования по защите коммерческой тайны могут быть оговорены в тексте договора, если договор заключается в письменной форме. Если же договор заключается в устной форме, то действует требование по защите коммерческой тайны, вытекающее из правил внутреннего трудового распорядка. Об

осведомлении в содержании правил внутреннего трудового распорядка лица, с которым заключается трудовой договор, делается отметка при ознакомлении его с приказом о приеме на работу. Это создает необходимый элемент включения данного лица в механизм обеспечения сохранности коммерческой тайны.

Один экземпляр договора должен быть обязательно вручен поступающему на работу сотруднику.

Использование договоров о неразглашение коммерческой тайны — вовсе не самостоятельная мера по ее защите. Не надо думать, что, подписав такое соглашение с новым сотрудником, коммерческая тайна сохранена. Это только предупреждение сотруднику, что в дело вступает система мероприятий по организационной и инженерно-технической защите информации. Это только правовая основа к тому, чтобы пресечь его первые действия. Дальше задача — не допустить разглашения коммерческой тайны.

2.2. Организационная защита

2.2.1. Общие положения

Организационная защита информации — это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что несанкционированный доступ к конфиденциальной информации становится невозможным или существенно затрудняется за счет проведения организационных мероприятий.

По мнению зарубежных специалистов организационные мероприятия играют большую роль в создании надежного механизма защиты информации, так как возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловливаются не техническими аспектами, а злоумышленными действиями, нерадивостью, небрежностью и халатностью пользователей или персонала системы защиты. Влияние этих аспектов практически невозможно исключить с помощью технических средств, программно-математических методов и физических мер. Для этого необходима совокупность организационно-правовых и организационно-технических мероприятий, которая исключала бы (или по крайней мере сводила к минимуму) возможность возникновения опасности утечки информации.

К организационным мероприятиям можно отнести:
мероприятия, осуществляющиеся при проектировании, строительстве и оборудовании служебных и производственных зданий и помещений, исключающих возможность тайного проникновения на территорию и в помещения; мероприятия для обеспечения удобства контроля прохода и перемещения людей, проезда транспорта и других средств передвижения; мероприятия по созданию отдельных производственных зон по типу конфиденциальности работ с самостоятельными системами доступа и т. п.;

- мероприятия, осуществляющиеся при подборе персонала, включающие ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;
- организация и поддержание надежного пропускного режима и контроля посетителей;
- организация надежной охраны помещений и территории.

Системы охранных мер должны предусматривать:

- многорубежность построения охраны (территории, здания, помещения) по нарастающей к наиболее ценной оберегаемой конкретности;
- комплексное применение современных технических средств охраны, обнаружения, наблюдения, сбора и обработки информации, обеспечивающих достоверное отображение и объективное документирование событий;
- надежную инженерно-техническую защиту вероятных путей несанкционированного вторжения в охраняемые пределы;
- устойчивую (дублированную) систему связи и управления всех взаимодействующих в охране структур;
- высокую подготовку и готовность основных и резервных сил охраны к оперативному противодействию нарушителю;
- самоохрану;
- организацию хранения и использования документов и носителей конфиденциальной информации, включая порядок учета, выдачи, исполнения и возвращения;
- организацию защиты информации, в том числе назначение ответственного за защиту информации в конкретных производственных коллективах, про ведение систематического контроля за работой персонала с конфиденциальной информацией, порядок учета, хранения и уничтожения документов и т. п.

В каждом конкретном случае организационные мероприятия носят специфическую для данной организации форму и содержание, направленные на обеспечение безопасности информации в конкретных условиях.

Очевидно, что организационные мероприятия охватывают самые различные источники информации и всевозможные каналы ее утечки, на которые возможно воздействовать организационными, а зачастую и организационно-техническими мерами.

Организационные мероприятия при работе с сотрудниками предприятия (организации, фирмы, СП и МП) в общем плане включают в себя:

- беседы при приеме на работу. В результате беседы устанавливается целесообразность приема кандидата на соответствующую вакансию. При приеме на работу возможно заключение между предприятием и сотрудником соглашения о частной информации, которая является собственностью организации и которое поступающий обязуется строго соблюдать;
- ознакомление с правилами и процедурами работы с конфиденциальной информацией в данной организации (предприятии). В подтверждение требований сохранения в тайне коммерческой информации поступающий на работу сотрудник дает подписку о сохранении коммерческой тайны предприятия, в которой обязуется не раскрывать секреты фирмы;
- обучение сотрудников правилам и процедурам работы с конфиденциальной информацией. Обучение сотрудников предполагает не только приобретение и систематическое поддержание на высоком уровне производственных навыков, но и психологическое их воспитание в плане глубокой убежденности в необходимости выполнения требований промышленной (производственной) секретности, информационной безопасности, защиты интеллектуальной собственности и коммерческой тайны. Систематическое обучение способствует развитию функциональной грамотности и повышению уровня компетентности руководства и сотрудников в защите коммерческих интересов своего предприятия.

Организуя регулярное обучение сотрудников необходимо учитывать, что:

- часто утечка информации происходит из-за невежества сотрудников в оценке важности той или иной информации для упрочения престижа и финансовой стабильности организации;

- процесс обучения персонала должен быть непрерывным, организованным, обеспеченным материально, а не иметь форму редких, часто необязательных и формальных собраний;
- лучше иметь специальную программу обучения. В этом случае следует учитывать:
  — что представляет из себя технология обработки и содержание деловой информации;
  — насколько серьезно ее необходимо защищать;
  — какие конкретно обязательства по обеспечению безопасности информации должен нести каждый конкретный сотрудник на конкретном участке работы;
  — какие меры ответственности действуют в рамках данной организации.

Беседы с увольняющимися имеют главной целью предотвратить утечку информации или ее неправильное использование. В ходе беседы следует особо подчеркнуть, что каждый увольняющийся сотрудник имеет твердые обязательства о неразглашении фирменных секретов и эти обязательства, как правило, подкрепляются подпиской о неразглашении известных сотруднику конфиденциальных сведений.

Одним из важных направлений организационных мероприятий является четкая организация системы делопроизводства и документооборота. Система делопроизводства способствует рационализации и унификации документальных процессов и обеспечивает порядок делопроизводства, порядок учета, обработки, хранения, уничтожения и контроля наличия и правильности исполнения документов.

При реализации системы особое внимание уделяется обеспечение безопасности документов и конфиденциальной информации. Организационные мероприятия, обеспечивающие защиту документной информации и информации, закрепленной на технических носителях.

Основными составными частями делопроизводства являются: документирование информации, учет документов, организация документооборота, обеспечение надежного хранения документов и своевременного их уничтожения, а также проверка их наличия; и контроль своевременности и правильности их исполнения.

Каждой составной части ставятся соответствующие целевые функции, отражающие задачи, формы и цели обеспечения безопасности. В свою очередь, каждая функция реализуется определенными способами, решающими задачу безопасности.

Организационные мероприятия при эксплуатации различных технических средств имеют целью:

- определить технические средства, которые могут быть каналами утечки конфиденциальной информации;
- обеспечить их защиту (или исключение их из практики работы);
- осуществлять периодический контроль надежности технических средств защиты информации.

Организационные мероприятия по защите предприятия предусматривают:

- обеспечение безопасности рабочих зданий и территории;
- обеспечение безопасности отдельных зон и конкретных помещений;
- организацию четкой системы контроля допуска и доступа на территорию (помещение), к определенной информации.

Одним из основных организационных мероприятий является разработка перечня охраняемых сведений.

2.2.2. Организационная защита коммерческой тайны

Под коммерческой тайной предприятия понимаются не являющиеся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью предприятия, разглашение (передача, утечка) которых может нанести ущерб его интересам.

Как следует из этого определения, коммерческая тайна, по существу, состоит из двух взаимосвязанных и в то же время самостоятельных предметов — предмета сделки и условий сделки.

К предмету сделки могут относиться изобретения, научные, технические, конструкторские, проектные и технологические решения, технология и технологический опыт, промышленные образцы, товарные знаки, оригинальные решения по управлению предприятием или производством.

К условиям сделки могут относиться расчеты цен и обоснования сделок, контрактная цена товара или услуг, размеры предоставленных скидок до и после контракта, кредитные условия и условия платежа, рыночная стратегия и конъюнктура, сведения о поставщиках и потребителях, организация и размеры оборота и т. п.

Часть сведений может составлять интеллектуальную собственность. Так, согласно ст. 2 Закона о собственности в РСФСР, «Объектами интеллектуальной собственности явля-

ются произведения науки, литературы, искусства и других видов творческой деятельности в сфере производства, в том числе открытия и изобретения, рационализаторские предложения, промышленные образцы, программы для ЭВМ, базы данных, экспертные системы, ноу-хау, торговые секреты, товарные знаки, фирменные наименования и знаки обслуживания».

Однако не всегда сведения, составляющие коммерческую тайну, могут явиться в чистом виде предметом практической реализации.

Исходя из такого подхода, очевидно, что коммерческую тайну могут составлять сведения, характеризующие довольно широкий круг вопросов деятельности предприятия, причем сведения, которые составляют коммерческую тайну, являются открытыми, несекретными.

Для их защиты на предприятии должен быть определен свой порядок защиты. Следует подчеркнуть, что под разглашением коммерческой тайны понимаются умышленные или неосторожные действия должностных или иных лиц, приведшие к преждевременному, не вызванному служебной необходимостью, открытому опубликованию сведений, составляющих коммерческую тайну, либо к утрате документов с такими сведениями или к бесконтрольному использованию и распространению этих сведений.

Вместе с тем следует иметь в виду, что защита технических, технологических, проектных и конструкторских решений, изобретений и т. п., появившихся в результате проведения работ по созданию вооружения и военной техники или связанных с разработкой новых материалов, новой техники и технологии, имеющих существенное значение для обороны и безопасности страны и являющихся по своему существу секретными, обеспечивается в соответствии с законодательством по защите секретной информации.

План мероприятий по защите коммерческих секретов предприятия

1. Определение целей плана по защите коммерческой тайны.

Ими могут быть:

- предотвращение кражи коммерческих секретов;
- предотвращение разглашения коммерческих секретов сотрудниками и утечки через технические каналы.

2. Анализ сведений, составляющих коммерческую тайну:

- определить, какие сведения предприятия (технологические и деловые) являются коммерческой тайной;
- установить места ее накопления и хранения;
- выявить потенциальные каналы утечки сведений; оценить возможности по перекрытию этих каналов;
- проанализировать соотношение затрат и доходов по использованию различных технологий, обеспечивающих защиту коммерческой тайны;
- назначить сотрудников, ответственных за каждый участок системы обеспечения безопасности.

3. Обеспечить реализацию деятельности системы по следующим направлениям:

- контроль сооружений и оборудования предприятия (обеспечение безопасности производственных и конторских помещений, охрана фото- и иного копировального оборудования, контроль посещений предприятия и т. п.);
- работа с персоналом предприятия, в том числе проведение бесед при приеме на работу, инструктаж вновь принятых на работу по правилам и процедурам защиты коммерческой тайны на предприятии; обучение сотрудников правилам сохранения коммерческих секретов; стимулирование соблюдения конфиденциальности, беседы с увольняющимися;
- организация работы с конфиденциальными документами (установление порядка и правил ведения делопроизводства, контроль за конфиденциальными документами, контроль за публикациями; контроль и учет технических носителей конфиденциальных сведений, рассекречивание и уничтожение конфиденциальных документов, охрана чужих секретов);
- работа с конфиденциальной информацией, циркулирующей в технических средствах и системах обеспечения производственной и трудовой деятельности (создание системы защиты информации через технические каналы утечки);
- работа с конфиденциальной информацией, накопленной в компьютерных системах (создание системы защиты электронной информации от несанкционированного доступа к ней; обеспечение контроля за использованием ЭВМ);
- защита коммерческой тайны предприятия в организационно-правовых документах, в процессе заключения контрактов и договоров с коллективом, сотрудниками, смежника-

ми, поставщиками и т. д. Здесь важно четко определить круг лиц, имеющих отношение к этой работе.

2.3. Инженерно-техническая защита

В настоящее время на вооружении промышленных шпионов находятся самые разнообразные средства проникновения на объекты криминальных интересов и получения различными способами конфиденциальной информации, разработанные на основе последних достижении науки и техники, с использованием новейших технологий в области миниатюризации в интересах скрытного (тайного) их использования против своих конкурентов. Противодействуя промышленному шпионажу, службы безопасности оснащаются необходимой им аппаратурой, не уступающей по надежности и функциональным возможностям аппаратуре шпионажа.

Инженерно-техническая защита — это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах обеспечения безопасности коммерческого предприятия. По функциональному назначению инженерно-техническая защита использует следующие средства:

- *физические средства защиты.* Они включают различные инженерные средства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие защиту персонала (личные средства безопасности), материальных средств и финансов, информации от противоправных воздействий;
- *аппаратные средства защиты.* Сюда входят приборы, устройства, приспособления и другие технические решения, используемые в интересах обеспечения безопасности коммерческого предприятия (КП). В практике деятельности КП находит широкое применение самая различная аппаратура от телефонного аппарата до совершенных автоматизированных информационных систем, обеспечивающих его производственную деятельность. Основная задача аппаратных средств — стойкая безопасность коммерческой деятельности;
- *программные средства защиты.* Это специальные программы, программные комплексы: и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных.

- *криптографические средства защиты* — это специальные математические и алгоритмические средства защиты информации, передаваемой по сетям связи, хранимой и обрабатываемой на ЭВМ с использованием методов шифрования.

Очевидно, что такое деление средств безопасности достаточно условно, так как на практике очень часто они и взаимодействуют и реализуются в комплексе в виде программно-аппаратных реализаций с широким использованием алгоритмов закрытия информации.

Тем не менее, такое рассмотрение в определенном смысле удобно с позиции методологии их изложения.

2.4. Универсальные меры обеспечения безопасности предприятия

Универсальные меры обеспечения безопасности предприятия — способы защиты, которые самостоятельно или в совокупности со средствами обеспечивают *один или несколько видов защиты.*

1. **Регламентация-** Состоит в том, что все защитные мероприятия должны быть подчинены строго установленным правилам, закрепленным в нормативной базе.
2. **Скрытие*** Состоит в том, чтобы сделать незаметным сам факт существования защищаемого объекта или проведение любых работ по его защите.
3. **Маркировка.** Состоит в том, чтобы скрыть истинное состояние деятельности объекта.
4. **Дезинформация.** Состоит в том, чтобы подать заведомо ложную, но весьма правдоподобную информацию об объекте защиты.
5. **Дробление (расчленение).** Состоит в том, чтобы разнести части защищаемого объекта и хранить их независимо друг от друга.
6. **Препятствие.** Состоит в том, чтобы создать полосы препятствий на пути проникновения противника к защищаемому объекту.

ГЛАВА III

ОБЩИЕ ПОЛОЖЕНИЯ КОНЦЕПЦИИ БЕЗОПАСНОСТИ КОММЕРЧЕСКОГО ЛРШРИЯТИЯ

Концепция выражает систему взглядов на проблему безопасности коммерческого предприятия (КП) на различных этапах и уровнях производственной деятельности, а также основные принципы, направления и этапы реализации мер безопасности.

Анализ состояния дел в области безопасности коммерческого предприятия показывает, что в ведущих странах мира сложилась вполне сформировавшаяся концепция и инфраструктура системы безопасности, основу которой составляют структурные компоненты; весьма развитый арсенал технических средств защиты, производимых на промышленной основе; значительное число фирм, специализирующихся на решении вопросов обеспечения безопасности; достаточно четко очерченная система концептуальных взглядов на эту проблему; наличие значительного практического опыта. И тем не менее, как свидетельствует зарубежная печать, злоумышленные действия по отношению к предпринимателям не только не уменьшаются, но и имеют достаточно устойчивую тенденцию к росту.

Опыт показывает, что для борьбы с этой тенденцией необходима стройная и целеустремленная организация процесса обеспечения безопасности. При чем в этом должны активно участвовать профессиональные специалисты, администрация коммерческого предприятия, сотрудники и пользователи, что и определяет повышенную значимость организационной стороны вопроса.

Зарубежный и отечественный опыт также показывает, что:

- обеспечение безопасности не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных форм, методов, способов и путей создания, совершенствования и развития системы безопасности, непрерывном управлении ею, контроле, выявлении ее узких и слабых мест и потенциально возможных угроз предприятию;
- безопасность может быть обеспечена лишь при комплексном использовании всего арсенала средств защиты во всех структурных элементах производственной системы и на всех этапах технологического цикла его деятельности. Наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый целостный механизм — СИСТЕМУ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ (СБП);
- никакая СБП не может обеспечить требуемый уровень безопасности без надлежащей подготовки персонала предприятия и пользователей и соблюдения ими всех установленных правил, направленных на обеспечение безопасности.

С учетом накопленного опыта систему безопасности предприятия можно определить как организованную совокупность специальных органов, средств, методов и мероприятий, обеспечивающих безопасность КП, под которой будем понимать состояние защищенности жизненно важных интересов предприятия от внутренних и внешних угроз. Согласно [15] под угрозой безопасности понимается совокупность условий и факторов, создающих опасность жизненно важным интересам КП. Реальная и потенциальная угроза объектам безопасности, исходящая от внутренних и внешних источников опасности, определяет содержание деятельности СБП.

С позиций системного подхода к безопасности предъявляются определенные требования.

Безопасность должна быть:

- *непрерывной.* Это требование проистекает из того, что злоумышленники только и ищут возможность, как бы обойти защиту и достичь своих противоправных целей;
- *плановой.* Планирование осуществляется путем разработки детальных планов действий по обеспечению защищенности предприятия всеми компонентами *его* структуры;
- *централизованной.* В рамках определенной структуры должно обеспечиваться организованно-функциональная самостоятельность процесса обеспечения безопасности КП;

- *целенаправленной*. Защищается то, что должно защищаться в интересах конкретной цели, а не все подряд;
- *конкретной*. Защите подлежат конкретные объекты, угрозы которым могут нанести ущерб КП;
- *активной*. Защитные меры претворяются в жизнь с достаточной степенью настойчивости;
- *надежной*. Методы, средства и формы защиты должны надежно перекрывать все пути проникновения и возможные каналы утечки информации. При этом надежность предполагает не только перекрытие, но и дублирование средств и мер безопасности;
- *универсальной*. Считается, что меры безопасности должны перекрывать пути угроз независимо от места их возможного воздействия;
- *комплексной*. Для обеспечения безопасности во всем многообразии структурных элементов, угроз и каналов несанкционированного доступа должны применяться все виды и формы защиты в полном объеме. Недопустимо применять отдельные формы или технические средства. Комплексный характер защиты проистекает из того, что это специфическое явление, представляющее собой сложную систему неразрывно взаимосвязанных и взаимозависимых процессов, каждый из которых, в свою очередь, имеет множество различных взаимообусловливающих друг друга сторон, свойств, тенденций.

Система безопасности предприятия, как и любая иная система, должна иметь определенные виды собственного обеспечения, опираясь на которые она будет способна выполнять свою целевую функцию. С учетом этого СБП должна иметь:

- *правовое обеспечение*. Сюда входят нормативные документы, определяющие ее статус, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы их действия;
- *организационное обеспечение*. Имеется в виду, что реализация защитных мер осуществляется определенными структурными единицами, такими как служба защиты информации и другие;
- *техническое обеспечение*. Предполагается широкое использование технических средств различного назначения, обеспечивающих реализацию защитных мероприятий. В том числе средства личной безопасности, технические средства охраны и другие;

- *информационное обеспечение.* Оно включает в себя сведения, данные, показатели, параметры, лежащие в основе решения задач, обеспечивающих функционирование системы. Сюда могут входить как показатели доступа, учета, хранения, так и системы информационного обеспечения расчетных задач различного характера, связанных с деятельностью службы безопасности;
- *программное обеспечение.* Имеются в виду различные информационные, учетные, статистические и расчетные программы для ЭВМ, обеспечивающие оценку наличия и опасности угроз безопасности предприятию;
- *нормативное обеспечение.* Сюда входят нормы и регламенты деятельности органов, служб, средств, методы, обеспечивающие деятельность сотрудников при выполнении своей работы в условиях жестких требований безопасности.

Система безопасности предприятия, как любая система, может быть охарактеризована рядом показателей, определяющих ее направленность, организационную и функциональную структуру, объекты и способы обеспечения своей деятельности и другие.

3.1. Цели и задачи системы безопасности

Основной целью системы безопасности является предотвращение ущерба интересам коммерческого предприятия за счет хищения финансовых и материально-технических средств, уничтожения имущества и ценностей, разглашения, утечки, искажения и уничтожения информации, нарушения работы технических средств обеспечения производственной деятельности, включая и средства информатизации, а также ущерба персоналу.

Целями системы безопасности являются:

- защита прав коммерческого предприятия, его структурных подразделений и сотрудников;
- сохранение и эффективное использование финансовых, материальных и информационных ресурсов;
- повышение имиджа и роста прибылей за счет обеспечения качества услуг и безопасности его клиентов.

Задачами системы безопасности являются:

- своевременное выявление и устранение угроз безопасности персоналу и ресурсам; причин и условий, способствующих нанесению финансового, материального и морального

ущерба его интересам, нарушению его нормального функционирования и развития;

- отнесение информации к категории ограниченного доступа (служебной и коммерческой тайнам, иной конфиденциальной информации, подлежащей защите от неправомерного использования), а других ресурсов — к различным уровням уязвимости (опасности) и подлежащих сохранению;
- создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций в функционировании предприятия;
- эффективное пресечение посягательств на ресурсы и угроз персоналу на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности;
- создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения безопасности на достижение стратегических целей КП.

3.2. Объекты защиты

К объектам, подлежащим защите от потенциальных угроз и противоправных посягательств, относятся:

- персонал (руководящие работники, производственный персонал, осведомленные в сведениях, составляющих коммерческую тайну, работники внешнеэкономических служб и другой «уязвимый» персонал);
- финансовые средства, валюта, драгоценности;
- материальные средства (здания, сооружения, хранилища, техническое оборудование, транспорт и иные средства);
- информационные ресурсы с ограниченным доступом, составляющие служебную и коммерческую тайну, а также иная конфиденциальная информация на бумажной , магнитной, оптической основе, информационные массивы и базы данных, программное обеспечение, информативные физические поля различного характера;
- средства и системы информатизации (автоматизированные системы и вычислительные сети различного уровня и назначения, линии телеграфной, телефонной, факсимильной, радио- и космической связи, технические средства передачи информации, средства размножения и отобра-

жения информации, вспомогательные технические средства и системы);
- технические средства и системы;
- технические средства и системы охраны и защиты материальных и информационных ресурсов.

3.3. Основные виды угроз интересам коммерческого предприятия

Ухудшение состояния криминогенной обстановки в стране, усиление межрегиональных связей организованных преступных групп, рост их финансовой мощи и технической оснащенности дает основание полагать, что тенденция к осложнению оперативной обстановки вокруг коммерческих предприятий в ближайшее будущее сохранится. Отсюда определение и прогнозирование возможных угроз и осознание их опасности необходимы для обоснования, выбора и реализации защитных мероприятий, адекватных угрозам.

В процессе выявления, анализа и прогнозирования потенциальных угроз в рамках концепции учитываются объективно существующие внешние и внутренние условия, влияющие на их опасность. Таковыми являются:
- нестабильная политическая, социально-экономическая и криминогенная ситуация;
- невыполнение законодательных актов, отсутствие ряда законов по жизненно важным вопросам;
- снижение моральной, психологической и производственной ответственности граждан.

На стадии концептуальной проработки вопросов безопасности коммерческого предприятия представляется возможным рассмотрение общего состава потенциальных угроз. Конкретные перечни, связанные со спецификой, требуют определенной детализации и характерны для этапа разработки конкретного проекта системы безопасности.

В общем плане к угрозам безопасности личности относятся:
- похищения и угрозы похищения сотрудников, членов их семей и близких родственников;
- убийства, сопровождаемые насилием, издевательствами и пытками;
- психологический террор, угрозы, запугивание, шантаж, вымогательство;

- грабежи с целью завладения денежными средствами, ценностями и документами.

Преступные посягательства в отношении продукции помещений (в том числе и жилых), зданий и персонала проявляются в виде:

- взрывов;
- обстрелов из огнестрельного оружия;
- минирования, в том числе с применением дистанционного управления;
- поджогов;
- нападения, вторжения, захватов, пикетирования, блокирования;
- повреждения входных дверей, решеток, ограждений, витрин, мебели, а также транспортных средств личных и служебных.

Цель подобных акций:

- откровенный террор в отношении коммерческого предприятия;
- нанесение серьезного морального и материального ущерба;
- срыв на длительное время нормального функционирования;
- вымогательство значительных сумм денег или каких-либо льгот перед лицом террористической угрозы.

Осуществление угроз информационным ресурсам может быть произведено:

- через имеющиеся агентурные источники в органах государственного управления, коммерческих структур, имеющих возможность получения конфиденциальной информации;
- путем подкупа лиц, непосредственно работающих на предприятии или в структурах, непосредственно связанных с его деятельностью;
- путем перехвата информации, циркулирующей в средствах и системах связи и вычислительной техники с помощью технических средств разведки и съема информации, несанкционированного доступа к информации и преднамеренных программно-математических воздействий на нее в процессе обработки и хранения;
- путем подслушивания конфиденциальных переговоров, ведущихся в служебных помещениях, служебном и личном автотранспорте, на квартирах и дачах;

- через переговорные процессы между фирмой и иностранными или отечественными фирмами, используя неосторожное обращение с информацией;
- через инициативников из числа сотрудников фирмы, которые хотят заработать деньги и улучшить свое благосостояние или проявляют инициативу по другим моральным или материальным причинам.

Реализация угроз препятствует нормальному выполнению фирмой своих основных функций.

3.4. Управление безопасностью

Действующие в настоящее время и разрабатываемые законодательные и иные нормативные акты предусматривают право КП на выработку собственной концепции системы безопасности и создания соответствующей службы, как системы исполнительных органов, реализующей эту концепцию.

Служба безопасности взаимодействует с подразделениями МВД Российской Федерации по обеспечению его безопасности.

Исходя из представленных в концепции задач, принципов организации и функционирования системы безопасности, основных угроз безопасности целесообразно выделить следующие основные направления деятельности по обеспечению его безопасности:

- информационно-аналитических исследований и прогнозных оценок безопасности;
- безопасности персонала;
- сохранности и физической защиты материальных и финансовых средств и объектов;
- безопасности информационных ресурсов.

Основными задачами информационно-аналитических исследований и прогнозных оценок безопасности являются:

- добывание и анализ информации о мировом и национальном рынках и прогнозирование их развития;
- организация работ по выявлению конфиденциальной информации, обоснованию уровня ее конфиденциальности и документальному оформлению в виде перечней сведений, подлежащих защите;
- сбор экономической и научно-технической информации для обеспечения эффективности деловых связей с зарубежны-

ми и отечественными партнерами, выявление в их числе некредитоспособных и ненадежных партнеров;

- выявление и прогнозирование реальных и потенциальных угроз безопасности, разработка и осуществление комплекса оперативных и долговременных мер по их предупреждению и нейтрализации;
- анализ и прогнозирование негативных тенденций социально-экономического развития с точки зрения влияния на ее безопасность;
- информационное обеспечение руководства фирмы в области безопасности;
- координация деятельности подразделений службы безопасности и обеспечения взаимодействия со всеми структурными подразделения в решении проблемы безопасности.

Основными задачами обеспечения безопасности персонала является охрана личности от любых противоправных посягательств на его жизнь, материальные ценности и личную информацию.

Основными задачами сохранности и физической защиты продукции и объектов являются:

- установление режима охраны производственных объектов и объектов жизнедеятельности;
- осуществление допускного и пропускного режимов;
- обеспечение защищенного хранения ценностей и документов (носителей информации), оснащение объектов современными инженерно-техническими средствами охраны;
- организация физической защиты продукции в процессе ее внутриобъектовой транспортировки;
- осуществление контроля за сохранностью продукции на всех стадиях технологического процесса;
- организация личной безопасности определенной категории руководящего состава и ведущих специалистов;
- обеспечении физической защиты.

Основными задачами направления безопасности информационных ресурсов являются:

- организация и осуществление разрешительной системы допуска исполнителей к работе с документами и сведениями ограниченного доступа;
- организация хранения и обращения с конфиденциальными документами (носителями информации);
- осуществление закрытой переписки и шифрованной связи;

- организация и координация работ по защите информации, обрабатываемой и передаваемой средствами и системами вычислительной техники и связи;
- обеспечение безопасности в процессе проведения конфиденциальных совещаний, переговоров;
- осуществление контроля за сохранностью конфиденциальных документов (носителей информации), за обеспечение защиты информации, обрабатываемой и передаваемой средствами и системами вычислительной техники и связи.

Кроме того, общими задачами для всех указанных направлений могут являться:

- разработка нормативной и методической документации, мероприятий по соответствующим направлениям безопасности;
- участие в решении вопросов подбора, расстановки и профессиональной подготовки кадров.

В этих условиях целесообразно создать территориальную распределенную службу безопасности с централизованным организационно-методическим управлением и координацией деятельности по единым принципам и правилам.

Служба безопасности должна подчиняться непосредственно руководителю и возглавляться руководителем службы безопасности в ранге заместителя, который административно управляет службой информационно-аналитических исследований и прогнозных оценок безопасности и физической защиты ценностей и объектов и безопасности информационных ресурсов, создаваемых (реорганизуемых) для выполнения конкретных задач в соответствии с настоящей концепцией в структурных подразделениях фирмы и координирует их деятельность.

В своей деятельности служба безопасности руководствуется:

- инструкцией по организации режима и охране;
- инструкцией по защите коммерческих секретов;
- перечнем сведений, составляющих коммерческую тайну;
- инструкцией по работе с конфиденциальной информацией;
- инструкцией по инженерно-технической безопасности;
- положением об информационно-аналитической работе.

Организационно служба безопасности состоит из следующих структурных единиц:

- подразделения режима и охраны;

- подразделения специального делопроизводства и защиты коммерческой тайны;
- инспектората по работе с сотрудниками, допущенными к работе со сведениями, составляющими коммерческую тайну;
- подразделения инженерно-технической безопасности;
- информационно-аналитического подразделения.

Для обеспечения безопасности во всем многообразии структурных элементов коммерческого предприятия, угроз и каналов несанкционированного доступа должны применяться все виды и формы противодействия недобросовестной конкуренции, промышленному шпионажу и защиты информации. В этом случае безопасность может считаться комплексной. Комплексный характер противодействия проистекает из того, злоумышленники не брезгуют никакими способами, средствами и действиями, исходя из того, что «цель оправдывает средства».

3.5. Инженерно-техническое обеспечение безопасности

В настоящее время на вооружении недобросовестных конкурентов находятся самые разнообразные средства проникновения на объекты криминальных интересов и получения различными способами конфиденциальной информации, разработанные на основе новейших технологий. Противодействуя промышленному шпионажу и противоправными действиям службы безопасности оснащаются необходимой им аппаратурой, не уступающей по надежности и функциональным возможностям средствам злоумышленников.

Инженерно-техническая защита — это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах обеспечения безопасности коммерческого предприятия.

На практике все мероприятия по инженерно-техническому обеспечению безопасности подразделяются на три группы:

- организационные (в части использования технических средств);
- организационно-технические;
- технические.

Организационные меры — это мероприятия ограничительного характера, сводящиеся в основном к регламентации доступа и использованию технических средств охраны противодействия и защиты. Они, как правило, проводятся силами

самой организации путем использования простейших организационных мер и доступных для этого технических средств.

Организационные мероприятия предусматривают проведение следующих действий:

- определение границ охраняемой зоны, территории, рубежей внутри помещений и других пространственных узлов;
- определение технических средств, используемых для охраны, контроля и защиты информации в пределах охраняемых зон;
- определение «опасных», с точки зрения возможных каналов проникновения и способов неправомерного овладения конфиденциальной информации; путей и технических средств;
- организация строгого контроля прохода и проноса каких-либо предметов (устройств, средств, механизмов, веществ) в контролируемую зону, способных представлять собой технические средства несанкционированных действий;
- организация наблюдения за деятельностью персонала в контыролируемых помещениях;
- контроль за возможными неконтролируемыми излучениями за счет ПЭМИН или специально используемыми для доступа к коммерческим секретам.

Организационно-технические мероприятия обеспечивают блокирование несанкционированного проникновения, возможных каналов утечки информации через технические средства, а также пресечение разглашения конфиденциальной информации.

Технические мероприятия — это мероприятия, обеспечивающие приобретение,установку и использование в процессе производственной деятельности специальных, защищенных от побочных излучений средств обработки конфиденциальной информации и средств защиты имущества и людей.

Инженерно-техническое обеспечения безопасности коммерческого предприятия должно базироваться:

- на системе стандартизации и унификации;
- на системе лицензирования деятельности;
- на системах сертификации средств обеспечения безопасности и противодействия;
- на системе аттестации защищенных объектов.

Основными составляющими инженерно-технического обеспечения безопасности ресурсов являются:

- системы инженерно-физической защиты материальных объектов и финансовых средств;
- система безопасности информационных ресурсов.

Система инженерно-физической защиты должна предусматривать:

- организационные и инженерно-технические меры охраны;
- регулирование доступа.

Система охраны должна предусматривать:

- многорубежное построение охраны (территории, здания, помещения) по нарастающей к наиболее ценной оберегаемой конкретности;
- комплексное применение современных технических средств охраны, обнаружения, наблюдения, сбора и обработки информации, обеспечивающих достоверное отображение и объективное документирование событий;
- надежную инженерно-техническую защиту вероятных путей несанкционированного вторжения в охраняемые пределы;
- устойчивую, дублированную систему связи и управления всех взаимодействующих в охране структур;
- высокую подготовку и готовность основных и резервных сил охраны к оперативному противодействию нарушителю;
- самоохрану персонала.

Система регулирования доступа должна обеспечивать:

- объективное определение "надежности" лиц, допускаемые красоте на фирме;
- максимальное ограничение количества лиц, допускаемых в пределы контролируемых зон;
- установление для каждого работника(посетителя) дифференцированного по времени, месту и виду деятельности права доступа на объект;
- определение объемов контрольно-пропускных функций на каждом проходном и проездном пункте;
- оборудование контрольно-пропускных пунктов (постов) техническими средствами, обеспечивающими достоверный контроль проходящих, объективную регистрацию прохода и предотвращение несанкционированного (в т. ч. и силового) проникновения посторонних лиц;
- высокую подготовленность и защищенность персонала (нарядов) контрольно-пропускных пунктов;
- строго контролируемый доступ лиц в режимные зоны;
- максимальное сокращение количества лиц, обладающих досмотровым иммунитетом;

- организацию и осуществление присутственного (явочного) и дистанционного по техническим каналам (скрытного) контроля за соблюдением режима безопасности;
- организацию тщательного контроля любых предметов и веществ, перемещаемых за пределы региональных зон;
- обеспечение защищенного хранения документов, финансовых средств и ценных бумаг;
- оперативное выявление причин тревожных ситуаций в режимных зонах, пресечение их развития или ликвидацию во взаимодействии с силами охраны.

Система обеспечения безопасности информационных ресурсов должна предусматривать комплекс организационных, организационно-технических и технических (в том числе и программных и криптографических) средств и мер по защите информации в процессе традиционного документоборота при работе исполнителей с конфиденциальными документами и сведениями, при обработке информации в автоматизированных системах различного уровня и назначения, при передаче по каналам связи, при ведении конфиденциальных переговоров.

При этом основными направлениями реализации технической политики обеспечения информационной безопасности является: защита информационных ресурсов от несанкционированного доступа (хищения, уничтожения, искажения и подделки), утечки по техническим каналам и разглашения сотрудниками.

Для достижения этой цели необходимы:

- реализация разрешительной системы допуска исполнителей (пользователей) к работам, документам и информации конфиденциального характера;
- ограничение доступа исполнителей и посторонних лиц в здания, помещения, где проводятся работы конфиденциального характера, в том числе на объекты информатики, конфиденциального характера;
- разграничение доступа пользователей к базам данных автоматизированных систем различного уровня и назначения; учет документов информационных массивов, регистрация действий пользователей информационных систем, контроль за несанкционированным доступом и действиями пользователей;

- криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи;
- снижение уровня и информативности побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых различными элементами технических средств обеспечения производственной деятельности и автоматизированных информационных систем;
- снижение уровня акустических излучений;
- электрическая развязка цепей питания, заземление и других цепей технических средств (различных линий и проводов), выходящих за пределы контролируемой территории;
- активное защемление акустических и электромагнитных полей в различных диапазонах;
- противодействие оптическим и лазерным средствам наблюдения;
- проверка технических средств и объектов информатизации на предмет выявления включенных в них подслушивающих устройств;
- предотвращение внедрения в АИС программ вирусного характера.

В заключение раздела следует отметить, что практически безопасных технических средств нет. Любые используемые в производственной деятельности средства должны быть соответствующим образом проверены на наличие возможных каналов утечки информации им закладных устройств, установленных в них злоумышленниками. В целях противодействия в обязательном порядке проводится проверки опасных технических средств, осуществляемой специализированными организациями с помощью специальных установок и оборудование в стационарных условиях.

ГЛАВА IV

СЛУЖБА БЕЗОПАСНОСТИ ФИРМЫ

Существуют два принципиальных подхода к созданию службы безопасности.

Первый — обратиться в специализированную фирму, обладающую по Закону «О частной детективной и охранной деятельности» правом оказывать такие услуги. Но это небезопасно. Предприниматель доверяется посторонней фирме.

Второй — создать собственную службу безопасности. При этом следует учитывать, что для небольшой фирмы вовсе не обязательно иметь свои подразделения для реализации всех шести функций. Иногда достаточно трех-четырех квалифицированных специалистов, которые смогут взять на себя обязанность СБ с привлечением на абонентской основе необходимых специалистов.

Независимо от того, на каком из этих вариантов остановится предприниматель, у него обязательно должен быть специалист на правах заместителя, отвечающий исключительно за вопросы безопасности.

4.1. Основные задачи службы безопасности

Основными задачами службы безопасности фирмы являются:

- обеспечение безопасности производственно-торговой деятельности и защиты информации и сведений, являющихся коммерческой тайной;
- организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите коммерческой тайны;
- организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной;

- предотвращение необоснованного допуска и доступа к сведениям и работам, составляющим коммерческую тайну;
- выявление и локализация возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (аварийных, пожарных и др.) ситуациях;
- обеспечение режима безопасности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания, связанные с деловым сотрудничеством, как на национальном, так и на международном уровне;
- обеспечение охраны зданий, помещений, оборудования, продукции и технических средств обеспечения производственной деятельности;
- обеспечение личной безопасности руководства и ведущих сотрудников и специалистов;
- оценка маркетинговых ситуаций и неправомерных действий злоумышленников и конкурентов.

В своей деятельности служба безопасности руководствуется:

- инструкцией по организации режима и охраны;
- инструкцией по защите коммерческой тайны;
- перечнем сведений, составляющих коммерческую тайну;
- инструкцией по работе с конфиденциальной информацией для руководителей, специалистов и технического персонала;
- инструкцией по организации хранения дел, содержащих конфиденциальную информацию, в архиве;
- инструкцией по инженерно-технической защите информации;
- инструкцией о порядке работы с иностранными представителями и представительствами.

4.2. Общие функции службы безопасности

Служба безопасности фирмы выполняет следующие общие функции:

- организует и обеспечивает пропускной и внутриобъектовый режим в зданиях и помещениях, порядок несения службы охраны, контролирует соблюдение требований режима сотрудниками, смежниками, партнерами и посетителями;
- руководит работами по правовому и организационному регулированию отношений по защите коммерческой тайны;

- участвует в разработке основополагающих документов с целью закрепления в них требований обеспечения безопасности и защиты коммерческой тайны, в частности устава, правил внутреннего трудового распорядка, положений о подразделениях, а также трудовых договоров, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих;
- разрабатывает и осуществляет совместно с другими подразделениями мероприятия по обеспечению работы с документами, содержащими сведения, являющиеся коммерческой тайной, при всех видах работ организует и контролирует выполнение требований инструкции по защите коммерческой тайны;
- изучает все стороны производственной, коммерческой, финансовой и другой деятельности для выявления и закрытия возможных каналов утечки конфиденциальной информации, ведет учет и анализ нарушений режима безопасности, накапливает и анализирует данные о злоумышленных устремлениях конкурентов и других организаций в отношении деятельности фирмы и ее клиентов, партнеров, смежников;
- организует и проводит служебные расследования по фактам разглашения сведений, утрат документов и других нарушений безопасности предприятия;
- разрабатывает, ведет, обновляет и пополняет перечень сведений, составляющих коммерческую тайну и другие нормативные акты, регламентирующие порядок обеспечения безопасности и защиты информации;
- обеспечивает строгое выполнение требований нормативных документов по защите коммерческой тайны;
- осуществляет руководство службами и подразделениями безопасности подведомственных предприятий, организаций, учреждений в части оговоренных в договорах условий по защите коммерческой тайны;
- организует и регулярно проводит учебу сотрудников фирмы и службы безопасности по всем направлениям защиты коммерческой тайны, добиваясь, чтобы к охране коммерческих секретов был глубоко осознанный подход;
- ведет учет сейфов, металлических шкафов, специальных хранилищ и других помещений, в которых разрешено постоянное или временное хранение конфиденциальных документов;

- ведет учет выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации;
- поддерживает контакты с правоохранительными органами и службами безопасности соседних предприятий в интересах изучения криминогенной обстановки в районе (зоне).

4.3. Состав службы безопасности

Служба безопасности является самостоятельной организационной единицей, подчиняющейся непосредственно руководителю фирмы. Возглавляет службу безопасности начальник службы в должности заместителя руководителя фирмы по безопасности.

Организационно служба безопасности состоит из следующих структурных единиц:

- отдела режима и охраны в составе сектора режима и сектора охраны;
- специального отдела в составе сектора обработки секретных документов и сектора обработки документов с грифом «Коммерческая тайна»;
- инженерно-технической группы;
- группы контрразведки и информационно-аналитической деятельности.

Такой состав службы безопасности фирмы подтверждается отечественным и зарубежным опытом.

Так, служба государственной безопасности Израиля в своей деятельности руководствуется следующими принципами и составом:

«1. Сочетайте в своей системе безопасности меры трех видов: личную охрану (телохранители и служебные собаки), технические средства охраны (сигнализация, бронежилеты, замки, сейфы и пр.), правила поведения для всех членов семьи и наемного персонала.

2. Наличие одной лишь охраны является недостаточным для гарантирования 95% безопасности (100% дает только Господь Бог). Всегда требуется именно комплекс мер названных выше трех видов.

3. О ненадежности любой меры безопасности следует судить по самому слабому месту в ней (как о прочности цепи судят по ее слабому звену).

4. Все используемые меры безопасности должны находиться под постоянным контролем главы фирмы или ее специалиста в области безопасности.

5. Принятые меры безопасности должны совмещаться с условиями повседневной жизни предпринимателя, его семьи, не препятствовать работе фирмы.

6. *Эффективность мер безопасности будет выше, если они спланированы специалистами в этой области, с учетом специфики вашего бизнеса и местных условий.*

7. В тех случаях, когда вероятность совершения покушения на вас резко возрастает, необходимо не просто выполнять все меры предосторожности, а вводить качественно новый уровень безопасности (начиная с информационной защиты и кончая сменой места жительства)».

Многогранность сферы обеспечения безопасности фирмы, включая защиту ее коммерческих секретов, требует создания специальной службы для реализации всех защитных мероприятий.

Структура, численность и состав службы безопасности фирмы определяются реальными финансовыми возможностями, масштабом коммерческой деятельности, степенью конфиденциальности информации. В зависимости от этих факторов служба безопасности может варьировать от двух-трех человек, работающих по совместительству, до полномасштабной службы с развитой структурой.

С учетом накопленного зарубежного и отечественного опыта предлагается примерный вариант службы безопасности фирмы среднего масштаба. Она состоит из четырех секторов (или отделов). В свою очередь, каждый такой сектор имеет в своем составе от двух до десяти-пятнадцати человек. Это сектор охраны, сектор режима, сектор технической защиты и оперативный сектор. Их главные задачи следующие.

Сектор охраны:

- охрана помещений и зданий;
- охрана оборудования и имущества;
- охрана сотрудников и мероприятий;
- охрана перевозок.

Сектор режима:

- обеспечение секретности документов;
- обеспечение режима допуска;
- контроль посетителей и транспорта;
- расследование случаев нарушений режима.

Сектор технической защиты:

- выявлениетехническихканаловутечкиинформации;
- контроль за попытками несанкционированного доступа к информации с помощью техники;
- оборудование фирмы средствами сигнализации и связи;
- оборудование фирмы противопожарными средствами.

Сектор оперативной работы:

- выявление и изучение фирм и преступных сообществ, являющихся потенциальными конкурентами или врагами фирмы;
- учет и анализ попыток проникновения в секреты фирмы, осуществления каких-либо враждебных акций;
- выявление возможных «слабых» мест в деятельности фирмы;
- разработка и осуществление мер противодействия "наездам".

Требования к уровню подготовки руководителей служб безопасности и их ведущих сотрудников постоянно возрастают.

Сегодня специалисты по безопасности бизнеса должны обладать познаниями в следующих областях:

- информационно-аналитическая работа;
- методы разведки и контрразведки;
- оперативная работа;
- социальная психология и психология личности;
- основы банковского дела и бухгалтерский учет;
- основы менеджмента и маркетинга;
- гражданское и уголовное право.

Грамотный специалист обязан:

- разработать комплексные меры по обеспечению безопасности коммерческой фирмы и личной безопасности ее руководства;
- осуществить защиту конфиденциальной информации, в том числе хранящейся в компьютерной памяти;
- уметь применять технические средства скрытого наблюдения и прослушивания;
- противодействовать проведению аналогичных мероприятий конкурентами;
- разбираться в финансовой отчетности;
- заниматься профилактикой правонарушений в фирме;
- проводить внутреннее расследование случаев воровства, мошенничества, саботажа и финансовых преступлений;
- организовывать проверки (в том числе негласные) благонадежности сотрудников фирмы;
- предупреждать (выявлять) случаи сотрудничества работников фирмы с конкурентами или криминальными структурами;

- взаимодействовать со следственными органами и милицией при расследовании преступлений и иных происшествий;
- готовить документы, содержащие анализ финансово-экономического положения партнеров, оценку конкурентов и потенциальных клиентов;
- разрешать конфликты между сотрудниками фирмы;
- кратко и точно излагать свои мысли.

4.4. Права, обязанности и ответственность сотрудников службы безопасности

Сотрудники подразделений службы безопасности в целях обеспечения защиты сведений, составляющих коммерческую тайну, имеют право:

- требовать от всех сотрудников фирмы, партнеров, клиентов строгого и неукоснительного выполнения требований нормативных документов или договорных обязательств по защите коммерческой тайны;
- вносить предложения по совершенствованию правовых, организационных и инженерно-технических мероприятий по защите коммерческой тайны.

Сотрудники службы безопасности обязаны:

- осуществлять контроль за соблюдением инструкции по защите коммерческой тайны;
- докладывать руководству о фактах нарушения требований нормативных документов по защите коммерческой тайны и других действиях, могущих привести к утечке конфиденциальной информации или утрате документов или изделий;
- не допускать неправомерного ознакомления с документами и материалами, имеющими гриф «Коммерческая тайна», посторонних лиц.

Сотрудники службы безопасности несут ответственность за личное нарушение безопасности коммерческой тайны и за неиспользование своих прав при выполнении функциональных обязанностей по защите конфиденциальных сведений сотрудниками предприятия.

4.5. Нештатные структуры службы безопасности

С целью более широкого охвата и качественного исполнения требований защиты коммерческой тайны решением руководства фирмы и службы безопасности могут создаваться от-

дельные комиссии, выполняющие определенные контрольно-ревизионные функции на временной или постоянной основе, в том числе:

- квартальные или годовые комиссии по проверке наличия, состояния и учета документов (материалов, сведений, ценностей);
- комиссия по оценке возможностей публикации периодических документов, объявлений, проспектов, интервью и других выступлений в печати, на радио и телевидении, семинарах, симпозиумах, конференциях и т. п.;
- периодические проверочные комиссии для проверки знаний и умения выполнять требования нормативных документов по защите коммерческой тайны, а также для оценки эффективности и надежности защитных мероприятий по обеспечению безопасности фирмы;
- специальные группы по аудиту безопасности фирмы.

4.6. Автоматизация деятельности службы безопасности

Изложенные функции организационных структур и сложность решаемых задач по обеспечению безопасности коммерческой тайны объективно вызывают потребность использования средств вычислительной техники. В качестве конкретных решений может быть рекомендовано использование организационно-функциональных автоматизированных мест должностных лиц службы безопасности (АРМов СБ).

На первом этапе внедрения средств автоматизации возможна разработка АРМов для начальника службы безопасности; для группы обработки документов с грифом «Коммерческая тайна» специального отдела; для инженерно-технической группы, а в некоторых случаях для группы анализа внешней деятельности и группы режима и работы с персоналом.

На последующих этапах масштабы внедрения средств автоматизации могут быть расширены в направлении обеспечения оперативного управления текущей деятельностью СБ в зависимости от изменения условий.

На последующих этапах внедрения средств автоматизации целесообразно создание специальных групп администратора безопасности корпоративной автоматизированной системы фирмы.

4.7. Принципы и направления взаимодействия СБ с правоохранительными органами

Какой бы совершенной ни была самоорганизация безопасности коммерческого предприятия, она не обеспечит предотвращение преступных посягательств без взаимодействия с соответствующими правоохранительными органами, и прежде всего милицией.

Организационно-правовой основой такого взаимодействия являются:

- конституционные принципы равенства защиты всех форм собственности;
- законы Российской Федерации о милиции, об оперативно-розыскной деятельности, о прокуратуре и другие нормативно-правовые акты.

Целями сотрудничества являются: предупреждение и раскрытие преступных посягательств на персонал коммерческих предприятий, денежные средства и материальные ценности.

Приоритетными направлениями взаимодействия предприятия и территориального органа внутренних дел должны быть:

обмен информацией:

- о фактах (способах) совершения хищений денежных средств с использованием подложных банковских документов, кредитных карточек, подделки иных документов;
- о физических лицах, работающих в коммерческих предприятиях, подозреваемых в совершении правонарушений;

разработка совместных мер противодействия предполагаемым (реальным) фактам общеуголовных проявлений, угрозам убийства либо нанесения тяжких телесных повреждений, уничтожения имущества, руководителей, сотрудников и членов их семей по технической укрепленности и оборудованию средствами сигнализации объектов; по созданию так называемой «горячей линии» с территориальным органом внутренних дел (милицией); участия в формировании централизованного, регионального банка данных о предприятиях различных форм собственности, недобросовестных участниках деловых отношений;

работа по подбору, расстановке и профессиональной подготовке кадров служб безопасности: осуществление совместной проверки кандидатур на работу в службу безопасности с использованием информационных возможностей орга-

нов внутренних дел, сведений о судимости и т. д.; проведение совместной разработки и введение правил об ответственности персонала за противоправное использование либо разглашение коммерческой тайны; использование помощи милиции в обучении и повышении квалификации кадров службы безопасности.

Необходимость взаимодействия службы безопасности фирмы с правоохранительными органами обусловливается следующими причинами:

— недостатком сил и средств СБ;
— ограниченностью источников информации о криминальной обстановке и особенностях деятельности организованной преступности;
— сложностью охраны транспортных перевозок материальных ценностей и финансовых средств на значительные расстояния;
— необходимостью получения информации о новых сотрудниках фирмы и СБ;
— необходимостью привлечения органов правопорядка к отражению нападения и оказанию содействия в поимке и задержании преступников и злоумышленников.

4.8. Управление безопасностью

Под управлением безопасностью будем понимать организованные действия, обеспечивающие согласованность функционирования всех служб, подразделений и сотрудников в целях устранения различных угроз деятельности фирмы.

По своей сущности управление безопасностью является непрерывным процессом поддержания заданной степени защищенности.

По содержанию управление безопасностью есть своевременное, строгое и четкое выполнение плановых мероприятий, разработанных на случай возникновения тех или иных критических ситуаций.

Необходимость планирования деятельности по обеспечению безопасности не вызывает сомнения, так как служба безопасности должна быть всегда готова к возникновению критических (кризисных) ситуаций, проявляющихся в результате столкновения интересов бизнеса и преступного мира.

Кризисная ситуация — это проявление фактов угроз со стороны отдельных лиц или групп. Кризисная ситуация может

проявляться и развиваться по-разному: медленно или спонтанно, мгновенно.

При оценке и анализе кризисной ситуации очень важно как можно быстрее определиться с ответом на вопрос, способна ли СБ справиться с ситуацией своими силами, либо для ее разрешения необходимо привлечение правоохранительных органов. Однако в любом случае, учитывая возможность возникновения кризисных ситуаций, любая фирма стремится создать в составе СБ отдельное формирование, именуемое кризисная группа. Она создается из числа ключевых фигур фирмы: директор, руководители линейных подразделений, филиалов, служб, юрист, главный бухгалтер и др. Кризисная группа может быть создана на постоянной основе с непременным включением в число ее членов:

- руководителя фирмы;
- юриста;
- финансиста;
- руководителя службы безопасности.

Руководство кризисной группой может быть возложено на главу фирмы. Перечисленные лица, как правило, в силу своего служебного положения, обладания специальными знаниями, опытом располагают реальными возможностями достаточно эффективно воздействовать на обстоятельства, в условиях которых возникает и протекает кризисная ситуация, не выпуская при этом рычагов влияния на повседневную коммерческую и производственную деятельность.

В каждом конкретном случае в состав кризисной группы могут включаться и иные специалисты.

Кризисная группа решает следующие задачи:

- оценка обстановки;
- принятие неотложных мер по безопасности;
- управление деятельностью фирмы в экстренных условиях;
- обеспечение оперативного взаимодействия с органами правопорядка.

Главная цель создания кризисной группы — противодействие внешним угрозам безопасности фирмы. Рабочие заседания группы должны проходить в условиях предельной конфиденциальности.

Как правило, деятельность кризисной группы регламентируется типовым планом действий руководства и персонала фирмы. В зависимости от складывающейся ситуации планы могут быть следующего вида:

- план действий при угрозе взрыва;
- план действий при захвате заложников или похищении сотрудников фирмы;
- план действий при вымогательстве;
- план действий при нападении на помещения фирмы;
- план действий при нападении на инкассаторов.

Типовые кризисные планы должны быть документами конфиденциального характера, доступ к которым должен иметь узкий круг лиц. Составляться подобные планы должны не более чем в двух-трех экземплярах. Один хранится у руководителя, другой — у начальника службы безопасности, третий может находиться у лица, замещающего руководителя фирмы в его отсутствие.

Осуществляя планирование, надо исходить из того, что план — это не набор мероприятий, а последовательная линия поведения, стратегия деятельности фирмы в конкретной кризисной ситуации, направленная на обеспечение эффективной безопасности.

Рассмотрим возможные режимы функционирования системы безопасности.

Специалисты выделяют три режима: повседневной деятельности, повышенной готовности и чрезвычайного положения.

Повседневный режим — это нормальное функционирование системы безопасности, включающее в себя:

1) действия по прогнозированию, выявлению, оценке, предотвращению и нейтрализации всех видов угроз;

2) разработку, корректировку планов и программ обеспечения безопасности;

3) подбор, обучение, мониторинг и совершенствование кадров и ряд других действий.

Режим повышенной готовности — это функционирование системы безопасности при наличии угроз, требующих мер по их пресечению. Этому режиму свойственно проведение мер по нейтрализации угроз, уточнение и совершенствование планов отражения с учетом особенностей ситуации, повышение готовности сил поддержки. При этом режиме возможно начало работы группы оперативного управления безопасностью (кризисной группы). Группа оперативного управления принимает любые необходимые меры по защите фирмы по ходу обеспечения безопасности.

В соответствии с этим режимом осуществляются следующие действия, в дополнение к уже проведенным по повседневной готовности:

4) уточнение и совершенствование планов отражения угроз;

5) повышение готовности сил поддержки;

6) начало работы группы оперативного управления.

Режим чрезвычайного положения — это функционирование СБ при наличии реальных угроз, требующих отражения или пресечения активных действий злоумышленников.

В этом случае:

7) совет по безопасности начинает работать ежедневно;

8) обеспечивается полная готовность СБ, сотрудников фирмы и сил усиления к непосредственному отражению угроз;

9) привлекаются силы поддержки и усиления органов внутренних дел.

4.9. Начальник службы безопасности

Начальник службы безопасности является прямым начальником для всего личного состава службы.

Он непосредственно подчинен директору фирмы либо одному из его заместителей, определенному штатным расписанием или приказом по фирме. Начальник СБ осуществляет руководство всей текущей деятельностью СБ, решает все организационные вопросы деятельности СБ, кроме тех, которые отнесены к исключительной компетенции дирекции фирмы. При передаче дирекцией фирмы части принадлежащих ему прав в компетенцию начальника СБ начальник СБ осуществляет указанные в решении дирекции фирмы функции.

Начальник СБ назначается дирекцией фирмы из лиц, имеющих высшее образование. Директор фирмы по поручению дирекции заключает с ним трудовой договор, в котором подробно оговариваются его должностные обязанности и условия труда.

Начальник СБ подотчетен директору фирмы и несет перед ним ответственность за осуществление деятельности СБ и выполнение возложенных на нее задач и функций.

Начальник СБ без доверенности действует от имени СБ во всей его деятельности, имеет право подписи всех правовых и бухгалтерских документов СБ, определяет должностные оклады сотрудников СБ, решает вопросы о поощрениях и взысканиях, заключает трудовые договоры с сотрудниками СБ, привлекает для работы работников на основе гражданско-правовых договоров, самостоятельно определяя условия их оплаты, представляет на согласование дирекции фирмы кандидатуры на должность заместителя начальника СБ, руководителей отделов и групп СБ.

На время своего отсутствия начальник СБ передает свои права заместителю.

Начальник службы безопасности отвечает за:

- оказание охранных и сыскных услуг в интересах безопасности своей фирмы-учредителя при строгом и точном соблюдении действующего законодательства Российской Федерации;
- обеспечение сохранности специальных средств, оружия и боеприпасов, приобретенных фирмой;
- качество профессиональной подготовки лиц из состава службы безопасности.

Он обязан:

- руководствоваться в своей деятельности требованиями Закона Российской Федерации «О частной детективной и охранной деятельности в Российской Федерации», другими законами и правовыми актами Российской Федерации, нормативами устава фирмы и положения о службе безопасности;
- на себя лично и на вверенную ему службу безопасности получить лицензии на право заниматься охранной деятельностью;
- организовать несение службы подчиненными лицами и контролировать ее качество;
- принять незамедлительные меры по обеспечению сохранности вверенного имущества собственника, организовать отражение противоправных посягательств на него, на здоровье и жизнь граждан и личного состава службы безопасности; обо всех таких посягательствах и их последствиях немедленно докладывать своему непосредственному руководителю;
- обо всех случаях применения огнестрельного оружия личным составом службы немедленно уведомлять органы внутренних дел по месту применения оружия;
- немедленно уведомлять прокурора о всех случаях смерти или причинения телесных повреждений;
- представлять на подпись руководству фирмы договоры с предприятиями и организациями на услуги инкассации, заключаемые по распоряжению руководства фирмы;
- своевременно организовывать подготовку, переподготовку и повышение квалификации личного состава службы безопасности, используя для этих целей на договорной основе специализированные базы (центры, полигоны, тиры,

стрельбища и т. п.) государственных либо негосударственных лицензированных учебных (образовательных) учреждений;

- организовывать в порядке, определяемом Министерством внутренних дел Российской Федерации, прохождение периодической проверки частных охранников и детективов на их пригодность к действиям, связанным с применением специальных средств и огнестрельного оружия;
- осуществлять взаимодействие с кадровыми и финансовыми органами фирмы по вопросам исчисления трудового стажа для работников службы, стажа для начисления пособий по государственному социальному страхованию, обязательности страхования на случай гибели, получения увечья или иного повреждения здоровья в связи с осуществлением охранных действий;
- контролировать сроки действия лицензий на личный состав и службу безопасности, принимать своевременные меры для их продления;
- организовать учет и обеспечить надежную сохранность оружия, боеприпасов и специальных средств;
- осуществлять контроль за порядком учета, хранения, ношения и перевозки огнестрельного оружия, боеприпасов к нему и специальных средств;
- проводить служебное расследование по каждому случаю недостачи, порчи, излишков специальных средств, огнестрельного оружия и боеприпасов;
- своевременно выполнять налоговые и иные финансовые обязательства службы безопасности и контролировать соблюдение аналогичных обязательств личным составом службы;
- предоставлять уполномоченным лицам органов, осуществляющих контроль за деятельностью частных детективных и охранных предприятий и служб безопасности, требуемые документы, письменную и (или) устную информацию, необходимую для выполнения контрольных функций.

Начальнику службы безопасности не разрешается совмещать охранную деятельность с государственной службой либо выборной оплачиваемой должностью в общественных объединениях, а также оказывать услуги лично или через своих подчиненных, связанные с обеспечением безопасности сторонних предприятий.

По мнению американских специалистов в области безопасности, высказанному на международной конференции «Бизнес и безопасность», для успешной работы руководителю службы безопасности требуются следующие затраты времени:

Таблица 10

1.	6% - менеджмент
2.	5% - организационные вопросы
3.	*1%* - безопасность персонала
4.	16% - физическая безопасность фирмы
5.	*1%* - защита информации
6.	20% — средства безопасности
7.	4% - рассмотрение злоупотреблений со стороны персонала и сотрудников СБ
8.	14% - предотвращение угроз
9.	*8%* - связь с другими организациями и с органами внутренних дел
10.	18% - прочие вопросы

ГЛАВА V

ОТДЕЛ РЕЖИМА И ОХРАНЫ СЛУЖБЫ БЕЗОПАСНОСТИ

Основной задачей службы безопасности по обеспечению режима и охраны является организация и осуществление мер по обеспечению безопасности деятельности и защите информации всеми возможными в конкретных условиях способами и средствами.

В целях обеспечения надежной охраны материальных ценностей, конфиденциальных документов и информации, содержащей сведения коммерческого характера, а также своевременного предупреждения попыток несанкционированного доступа к ним устанавливается определенный режим деятельности, соблюдение которого обязательно для всех сотрудников, посетителей и клиентов.

Руководители и сотрудники фирмы, обеспечивающие и осуществляющие режим и охрану, руководствуются в своей деятельности соответствующим законодательством, нормативными документами и настоящими рекомендациями.

Основными задачами организации режима и охраны являются:

- предупреждение проникновения в служебные помещения, в охраняемые зоны и на территорию объекта посторонних лиц;
- обеспечение порядка вноса (выноса), ввоза (вывоза) материальных ценностей и входа (выхода) сотрудников и клиентов.

Все помещения фирмы в зависимости от назначения и характера совершаемых в них актов, действий или операций разделяются на несколько зон доступности (безопасности), которые учитывают степень важности различных частей объекта с точки зрения возможного ущерба от криминальных угроз.

Зоны безопасности располагаются последовательно, от забора на территории объекта до хранилища ценностей и информации, создавая цепь чередующихся препятствий, которые придется преодолевать злоумышленнику.

5.1. Требования внутриобъектового режима

1. Внутриобъектовый режим — это установленный в фирме порядок выполнения правил внутреннего трудового распорядка, направленных на обеспечение экономической безопасности, сохранения материальных средств и защиты конфиденциальной информации.

2. Внутриобъектовый режим предусматривает следующие основные требования:

- установление четкого распорядка рабочего времени;
- строгое соблюдение сотрудниками правил экономической и информационной безопасности, правил противопожарной и противоаварийной безопасности и техники безопасности;
- установление порядка приема и работы с посетителями сторонних организаций;
- оборудование фирмы техническими средствами обеспечения производственной деятельности (связь, автоматизация, охранная и пожарная сигнализация, замки, ограждения и др.);
- порядок сдачи и приема помещений под охрану;
- порядок ведения телефонных, факсовых и телекоммуникационных обменов информацией с соблюдением режима конфиденциальности и экономии.

3. Работа с представителями сторонних организаций осуществляется в следующем порядке:

- принимающий специалист накануне делает заявку канцелярии на следующий день с указанием Ф.И.О. прибывающих, их места работы и времени предполагаемого прибытия;
- в день прибытия приглашенных канцелярия фиксирует их прибытие в журнале учета посетителей и приглашает специалиста фирмы;
- специалист встречает прибывших, получает в канцелярии ключи от комнаты переговоров и сопровождает туда посетителей. Запрещается прием представителей сторонних

организаций в других помещениях офиса без специального на то разрешения директора или его заместителя;

- в ходе работы необходимо плотно закрывать окна и шторы;
- по окончании работы с посетителями принимающий их специалист провожает их до выхода из офиса и делит в журнале учета посетителей соответствующие заметки о времени их ухода. Во время пребывания посетителей принимающий специалист обязан контролировать их пребывание и действия. После завершения встречи специалист фирмы закрывает комнату переговоров и сдает ключи от нее канцелярии.

5.2. Пропускнойрежим

Пропускной режим — это установленный в фирме, организации, на предприятии порядок, при котором исключается возможность бесконтрольного прохода (проезда), вноса (выноса) материальных ценностей.

Проход (проезд) сотрудников, служащих и других лиц на территорию охраняемого объекта и обратно, внос и вынос материальных ценностей производится по пропускам через контрольно-проходные и проездные переходы.

Пропускной режим предусматривает:

- установление определенного порядка допуска на территорию объекта рабочих и служащих данного объекта и посетителей;
- установление определенного порядка вывоза (выноса), ввоза (вноса) продукции и материальных ценностей;
- устройство ограждения, освещения, оборудование контрольно-проходных и проездных пунктов (постов) и бюро пропусков средствами сигнализации, связи и др. необходимой техникой, обеспечивающей осуществление пропускного режима, а также обеспечение их документацией и инвентарем;
- определение круга должностных лиц, имеющих право выдачи и подписи всех видов пропусков;
- оборудование камер хранения личных вещей и площадок для личного автотранспорта.

5.2.1. Организация пропускного режима

Система регулирования доступа в фирму должна предусматривать:

- объективное определение надежности лиц, допускаемых к работе;
- максимальное ограничение количества лиц, допускаемых на объекты фирмы;

установление для каждого работника (или посетителей) дифференцированного по времени, месту и виду деятельности права доступа на объект;
четкое определение порядка выдачи разрешений и оформление документов для входа (въезда) на объект;
определение объемов контрольно-пропускных функций на каждом пропускном и проездном пункте;
оборудование контрольно-пропускных пунктов (постов) техническими средствами, обеспечивающими достоверный контроль проходящих, объективную регистрацию прохода и предотвращение несанкционированного (в том числе силового) проникновения посторонних лиц;
высокую подготовленность и защищенность персонала контрольно-пропускных пунктов.

Таблица 11

Классификация зон режимности фирмы

Категории режима доступа	Наименование	Функциональное назначение	Условия доступа сотрудников	Условия доступа посетителей	Наличие охраны	Наличие технических средств охраны
0	Свободная	Зона свободного посещения	Свободный	Свободный	Нет	Нет
1	Наблюдаемая	Зона приема посетителей	Свободный	Свободный	Ограниченная	Средства наблюдения и записи
2	Регистрационная	Зона служебных помещений и кабинетов сотрудников	Ограниченный служебной необходимостью	Регистрируемый по разовым пропускам	В отдельных зонах	Средства охраны и контроля
3	Режимная	Зона руководящего состава, специальных подразделений, финансовых служб	Строго ограниченный	Регистрируемый по разовым пропускам с сопровождением	Усиленная многозональная	Средства охраны, контроля и наблюдения

5.2.2. Пропускные документы

Обычно устанавливаются следующие виды пропускных документов, дающих право прохода сотрудников и посетителей на территорию фирмы, вноса (выноса), ввоза (вывоза) материальных ценностей:

- удостоверения;
- пропуска.

Пропуска могут быть постоянные, временные и разовые для сотрудников и посетителей, а также материальные для ввоза (вывоза) материальных ценностей.

На удостоверениях и пропусках проставляются печати, предусмотренные правилами режима, и цифровые знаки, определяющие зону доступности, период их действия, право проноса портфелей (кейсов, папок и др.). Период пребывания сотрудников на территории фирмы в рабочее и нерабочее время определяется руководством с проставлением цифрового знака на удостоверении или пропуске. Образцы удостоверений и пропусков разрабатываются службой безопасности и утверждаются руководством фирмы.

Утвержденные образцы удостоверений личности, пропусков, оттисков цифровых знаков, печатей (штампов), проставляемых на удостоверениях и пропусках, списки с образцами подписей руководителей или уполномоченных лиц, имеющих право подписывать удостоверения и пропуска, передаются начальнику отдела режима и охраны под расписку.

Полная замена удостоверений и постоянных пропусков производится, как правило, через 3-5 лет. Через 2-3 года производится перерегистрация с проставлением соответствующей отметки.

Для перерегистрации, замены или изменения пропускных документов ежегодно по состоянию на 1 января в службу безопасности направляются отделом кадров списки сотрудников с указанием должности, фамилии, имени, отчества и наименования документа с соответствующими пометками (круглосуточно, рабочее время с____по___, с портфелем, в какую зону и т. п.).

Удостоверения и постоянные пропуска могут выдаваться лицам, не работающим на данной фирме, по отдельному утвержденному руководством списку с указанием учреждения, должности, фамилии, имени, отчества и сопроводительных помет. Эти документы должны постоянно храниться в бюро пропусков (или у уполномоченного лица) и выдаваться посетителю в момент его прибытия. После завершения работы эти лица сдают документы в бюро пропусков.

Удостоверения и постоянные пропуска выдаются указанным лицам на основании письменных ходатайств руководителей учреждений, где они состоят в штате.

Временные пропуска с фотографиями на срок до трех месяцев выдаются лицам, работающим временно, или прикоманди-

рованным. Временные пропуска без фотографии на срок до одного месяца действуют при предъявлении паспорта (удостоверения личности).

Продление действия временных пропусков допускается на срок не более двух месяцев.

Удостоверения или постоянные пропуска выдаются сотрудникам при поступлении на работу на основании приказа о зачислении в штат. Разовые и материальные пропуска.

Разовый пропуск действителен в течение 30 минут с момента выдачи до входа в здание, а также в течение 15 минут после отметки на пропуске о времени ухода посетителя из фирмы. Руководитель подразделения, в котором находится посетитель, обязан на обороте разового пропуска сделать отметку о времени ухода посетителя и расписаться с указанием своей фамилии.

Материальные пропуска выдаются лицом, ответственным за сохранность материальных средств.

Учет бланков удостоверений и пропусков, их оформление и выдача осуществляются бюро пропусков в соответствующих учетно-контрольных документах.

По окончании рабочего дня сотрудники бюро пропусков получают от охраны выданные ими разовые пропуска с контрольными талонами к ним и материальные пропуска под расписку в журнале учета разовых и материальных пропусков.

Контроль, сличение и подклеивание пропусков к их корешкам производится ежедневно сотрудниками бюро пропусков, выдавшими их в этот же день.

Книжки использованных разовых и материальных пропусков с подклеенными отрывными талонами, а также заявки на них хранятся в течение трех месяцев, после чего они подлежат уничтожению в coofBeTCTByroiueM порядке.

Использованные постоянные и временные пропуска уничтожаются по мере необходимости, но не реже одного раза в год.

Для учета документов по пропускному режиму ведутся следующие дела, книги и журналы учета:

- дело с приказами и распоряжениями по пропускному режиму;
- дело с заявками структурных подразделений на удостоверения, постоянные и временные пропуска;
- дело с инструкциями по пропускному режиму и образцами подписей на материальные пропуска;

- дело с актами на уничтожение пропускных документов;
- дело переписки по пропускному режиму;
- книга учета ежедневного расхода бланков разовых пропусков;
- книга учета выдачи удостоверений, постоянных и временных пропусков.

Кроме того, бюро пропусков ведет книгу учета посетителей по разовым пропускам.

Для оформления всех видов пропускных документов бюро пропусков должно иметь следующие печати и штампы:

- круглая (диаметр 25 мм) или треугольная каучуковая печать для разовых и материальных пропусков;
- круглая рельефная металлическая или каучуковая печать для удостоверений и постоянных пропусков (диаметр 20 мм);
- штампы цифровых знаков;
- штампы «ПОГАШЕН», «ОБРАЗЕЦ», «ВРЕМЕННЫЙ».

В журнале учета печатей и штампов фирмы против оттиска каждого штампа или печати делается описание его содержания и назначения.

При замене печатей и штампов на новые старые уничтожаются (оформление актом), а в журнале делается соответствующая запись. На новые заводятся новые графы.

5.3. Обеспечение охраны стационарных объектов

Обеспечение безопасности стационарных объектов представляет собой многогранный процесс реализации охранных мероприятий, по большей части предупреждающего характера. Действительно, эффективной может считаться лишь такая система охраны, которая либо просто не позволяет злоумышленникам найти лазейку в режиме безопасности, либо создает возможность пресечения преступных посягательств на самой ранней стадии.

В основе разработки системы защиты объекта и организации ее функционирования лежит принцип создания последовательных рубежей безопасности, на которых угрозы должны быть своевременно обнаружены. Такие рубежи должны располагаться последовательно, от забора вокруг территории объекта до главного, особо важного помещения, такого, например, как хранилище ценностей и коммерческой информации.

В качестве примера рассмотрим защиту от несанкционированного проникновения. Злоумышленник проникает на территорию объекта, на котором располагаются здания и стоянки автомашин посетителей и сотрудников. Возможная угроза для территории — это кража автомобилей, их порча или установка взрывных либо подслушивающих устройств. Защита территории должна состоять из различного рода ограждений ее периметра и специально оборудованных въездов и проходов, охранной сигнализации, охранного освещения и охранного телевизионного наблюдения.

Но злоумышленник может не остановиться и попытаться проникнуть дальше в здание, а затем в хранилище ценностей и информации. Отсюда ясно, что средства защиты всех участков объекта должны взаимно дополнять друг друга, и эффективность всей системы защиты от несанкционированного проникновения будет оцениваться по минимальному времени (несколько десятков минут), которое злоумышленник затратит на преодоление всех рубежей безопасности. За это время должна сработать охранная сигнализация, сотрудники охраны должны установить причину тревоги, принять меры к задержанию злоумышленника.

Таким образом, эффективность системы защиты оценивается как время с момента возникновения угрозы до начала ее ликвидации. Чем более сложна и разветвлена система защиты, тем больше времени требуется на ее преодоление и тем больше вероятность того, что угроза будет обнаружена, определена, отражена и ликвидирована.

К числу факторов, влияющих на выбор приемов и средств охраны, относятся:

- возможные способы преступных посягательств на охраняемый объект;
- степень технической укрепленности охраняемого объекта;
- наличие и качество средств охранно-пожарной сигнализации;
- наличие уязвимых мест в технической укрепленности объекта, которые известны только охране и службе безопасности;
- условия местности, на которой расположен охраняемый объект, а также его конструктивные особенности;
- режим и характер работы охраняемого объекта, его технологические характеристики, имеющиеся на объекте материальные и финансовые ценности;

- режим охраны объекта;
- количественные и качественные характеристики сил охраны;
- вооруженность и техническая оснащенность охранников, наличие у них автотранспорта, средств связи, сигнализации и специальных средств.

Режим охраны объекта по времени может иметь круглосуточный, частичный (определенные часы суток) или выборочный характер. В зависимости от количества используемых сил и средств, плотности контроля территории и объекта режим охраны может быть простой или усиленный.

На значительной части охраняемых объектов охранники присутствуют круглосуточно. В дневное время они контролируют посетителей, прибывающих на объект, осуществляют контрольно-про-пускной режим, а в ночное время несут закрытую охрану объекта, принимая на себя полную ответственность за его сохранность. Некоторые объекты охраняются лишь эпизодически, т. е. выборочно по времени. К таким объектам относятся квартиры, охраняемые на период отсутствия хозяина, временные хранилища или территории в период завоза товарно-материальных ценностей и др.

Существует несколько видов охраны, в том числе:

- охрана с помощью технических средств — с подключением на пульт централизованного наблюдения и с установкой автоматической сигнализации;
- охрана путем выставления постов (силами отдела охраны или милиции);
- комбинированная охрана.

5.3.1. Охрана с помощью технических средств

Для охраны и контроля состояния помещений на объекте широко используются различные по назначению и техническому исполнению средства охраны. С их помощью можно обнаружить возникновение пожара, проникновение постороннего лица через периметр помещения, просто нарушение периметра (например, если ветром распахнет окно или будет разбито стекло), перемещение кого или чего-либо внутри помещения, прикосновение к контролируемому предмету, например, сейфу, находящемуся внутри помещения.

Как правило, для охраны помещений, проникновение в которые посторонних лиц нежелательно, используется комплекс технических средств, реализующих многорубежную защиту.

Применение многорубежной защиты существенно повышает надежность охраны, так как появляется страховка на случай,

если один из рубежей не сработает из-за неисправности или каких-то преднамеренных действий злоумышленника, возможно, знакомого с современными системами охранной сигнализации.

Первым рубежом защищаются строительные конструкции периметров помещений, оконные и дверные проемы, люки, вентиляционные каналы, тепловые вводы, тонкостенные перегородки и другие элементы помещений, доступные для проникновения с внешней стороны, в том числе и те из них, которые оборудованы стальными решетками.

Вторым рубежом с помощью специальных приборов охранной сигнализации защищаются помещения внутри здания. Третий рубеж перекрывает охраняемые хранилища внутри помещений, средства и материальные ценности и др.

5.3.2. Охрана путем выставления постов

Охрана с подключением помещений фирмы на пульт централизованной охраны не всегда представляется возможной. В таких случаях рекомендуется организовать постовую охрану.

Посты могут выставляться и для усиления уже имеющейся охраны. Наличие постов значительно снижает возможность преступных посягательств на собственность фирмы как в ночное, так и в дневное время. Особенно эффективен этот вид охраны в случаях попыток преступников остаться в помещениях фирмы после окончания рабочего дня.

5.3.3. Комбинированная охрана

И охрана путем выставления постов, и охрана с помощью технических средств имеют свои сильные и слабые стороны. Вторая обладает рядом несомненных преимуществ по сравнению с постовой охраной. Это и одновременный контроль за большим количеством помещений при минимальном участии человека, и непрерывная работа в течение длительного времени. В то же время она уступает постовой охране в том, что в полной мере может использоваться только в нерабочие часы. Разумное сочетание этих двух видов охраны позволяет с максимальной надежностью защитить помещения фирмы от нежелательных посещений как в рабочее, так и в нерабочее время. Особенно эффективна комбинированная охрана, если ее объектом является многоэтажное или любое другое здание со множеством помещений.

5.4. Режимы охраны

Эффективный режим охраны призван обеспечить сохранность зданий и помещений на объекте, сохранность и контроль за перемещением материальных ценностей и людей, предупредить утечку информации о деятельности объекта, поддерживать противопожарную безопасность. Решающее значение для режима охраны играют квалифицированный подбор, подготовка и расстановка сил и средств охраны, сбор и анализ информации о состоянии режима охраны, а также контроль функционирования службы безопасности на объекте. Основными принципами режима охраны являются:

- активность и предупредительный характер охраны, заключающиеся в опережающем выявлении признаков готовящейся атаки объекта и своевременном принятии мер по ее предупреждению или пресечению (отражению);
- целесообразность и обоснованность организации режима охраны объекта, своевременность его усиления, рациональное использование сил и средств охраны;
- разумное сочетание собственных возможностей и возможностей сил правоохранительных органов для обеспечения безопасности объекта;
- осуществление охраны по единому плану;
- скрытность или демонстративность охраны в зависимости от ситуации, складывающейся вокруг охраняемого объекта;
- максимальная информированность охраны обо всех событиях, происходящих на объекте, условиях коммерческих сделок фирмы и т.п. для правильного определения ключевого звена, воздействие на которое позволяет обеспечить безопасность объекта.

5.4.1. Задачи режима охраны

В практике деятельности подразделений охраны по обеспечению безопасности объекта выделяются две группы задач:

- аналитические и предупредительные задачи;
- процедурно-отражательные задачи.

Аналитические задачи решаются путем систематического сбора информации о субъектах преступной деятельности и состоянии собственного режима охраны. Главным здесь является соблюдение принципов непрерывности и постоянства сбора информации.

Решение предупредительных задач связано в первую очередь с созданием имиджа сильного и надежного режима охраны. Подобный имидж может быть создан серией имитацион-

ных мероприятий, демонстрирующих «неудачные» попытки посягательства на объект и мощное противодействие охраны преступникам. Все это может быть дополнено впечатляющей демонстрацией элементов режима охраны (внушительного вида охранники, современная охранная сигнализация, присутствие милиции на объекте и т. д.). Предупредить покушение на охраняемый объект можно также путем его маскировки, перекрытия информационных каналов о его деятельности и дезинформацией конкурентов и криминальных элементов о характере деятельности, форме собственности, состоянии режима охраны, объеме имеющихся на объекте товарно-материальных ценностей и т. д.

Вторая группа задач режима охраны объекта решается путем своевременного обнаружения признаков готовящегося посягательства с последующим его отражением предварительно подготовленными силами и средствами. Как правило, подобное мероприятие (операцию) следует проводить во взаимодействии с сотрудниками органов внутренних дел, которые будут иметь возможность своевременно зафиксировать следы преступной деятельности. В тех случаях, когда время начала посягательства трудно предугадать, имеет смысл в отдельных случаях «подтолкнуть» преступников к началу посягательства. Это может быть достигнуто путем дезинформирования криминальных элементов о времени и месте завоза ценных грузов, крупной суммы денег и т. п.

При организации охраны объекта служба безопасности должна предусмотреть в перечне служебных обязанностей охранников варианты их действий на случай возникновения на объекте или поблизости от него различного рода критических ситуаций. В таких случаях обязанностью охранника является:

— принятие мер к задержанию преступника и сопровождение задержанного в орган внутренних дел;
— обеспечение охраны места происшествия, находящихся на нем следов и вещественных доказательств до прибытия сотрудников милиции;
— оказание помощи пострадавшим от преступления или несчастного случая до прибытия медицинских работников;
— установление свидетелей и очевидцев происшествия, в том числе и для того, чтобы обеспечить самому себе оправдательную свидетельскую базу;
— сообщение в орган внутренних дел о фактах нарушения общественного порядка поблизости от объекта.

Особое внимание деятельности охранников следует уделять при организации на охраняемом объекте деловых встреч и приемов партнеров по бизнесу. В этом случае служба охраны должна обеспечить:

1) встречу гостей, прибывающих на деловой прием;

2) взаимодействие основной охраны и телохранителей приглашенных лиц;

3) охрану одежды, вещей гостей и их автомашин на прилегающей территории;

4) предупреждение инцидентов между гостями на деловом приеме или встрече;

5) контроль состояния напитков, закусок и других угощений, приготовленных для гостей;

6) выявление участников мероприятия, которые дольше обычного задерживаются возле стола, ведут себя необычно;

7) наблюдение за лицами:

- приходящими на деловую встречу или прием со свертками, портфелями, кейсами и т. п.;
- приносящими на мероприятие аудио- или видеоаппаратуру;
- быстро покинувшими место встречи;

8) выявление в зале приемов и смежных помещениях предметов, которые могут быть источником опасности для гостей;

9) проведение мероприятий против прослушивания разговоров организаторов и гостей в помещениях и по телефону.

Важным условием эффективности охраны стационарных объектов является их техническая укрепленность, наличие на них технических средств обеспечения безопасности.

Элементами технической укрепленности стационарных объектов являются:

— инженерно-технические средства защиты периметра объекта, включающие: запретную зону, средства и системы контроля проникновения в нее, контрольно-следовые полосы и другие системы;
— освещение объектов охраны;
— контрольно-пропускные пункты;
— средства видеонаблюдения;
— средства связи.

5.5. Охранники

Администрация редко рассматривает охранный персонал как составную часть службы безопасности. Охранники становятся составной частью системы безопасности, когда руковод-

ство хорошо понимает задачи, сложность и степень надежности ее функциональных элементов и четко представляет себе роль охраны персонала в работе всего комплекса безопасности.

Задачи и деятельность охраны подчинены прежде всего одной цели — выполнению охранных функций. Охранники при этом должны уметь абстрактно мыслить, импровизировать, быть инициативными, иметь вероятностный подход к событиям, т. е. охранник должен развивать в себе целый ряд качеств - интеллект, здравомыслие, гибкость мышления, физическую силу, чутье, сдержанность и др.

Эти качества должны проявиться при любых формах его деятельности:

- при внутреннем и наружном патрулировании;
- контроле за проходом и проездом персонала;
- в процессе наблюдения;
- при проведении расследования;
- при наблюдении за деятельностью персонала и посетителей;
- при подготовке докладов, справок и других документов;
- при преследовании и задержании преступников и нарушителей;
- сопровождении людей и грузов и др.

Охранникам запрещается:

- скрывать от правоохранительных органов ставшиеим известными факты готовящихся или совершенных преступлений;
- выдавать себя за сотрудников правоохранительных органов;
- собирать сведения, связанные с личной жизнью, с политическими и религиозными убеждениями отдельных лиц;
- осуществлять видео- и аудиозаписи, фото- и киносъемки в служебных помещениях без письменного согласия на то соответствующих должностных лиц;
- прибегать к действиям, посягающим на права и свободу граждан;
- совершать действия, ставящие под угрозу жизнь, здоровье, честь, достоинство и имущество граждан;
- передавать свою лицензию для пользования другими лицами.

5.6. Охрана финансовых средств

В целях безопасности финансовых средств необходимо обеспечить условия их сохранности на всех этапах обращения: полу-

чение (сдача) в банке, транспортирование, временное хранение в кассе — выдача (прием). Каждая из этих ситуаций требует специальных знаний и умений, профессионализма и предусмотрительности.

5.6.1. Обеспечение безопасности финансовых средств в фирме

В соответствии с законодательством РФ ответственность за безопасность кассовых операций возлагается на руководителя фирмы. В своих действиях он должен руководствоваться «Едиными требованиями по технической укрепленности и оборудованию сигнализацией помещений кассы и предприятия».

В них в частности указывается, что для обеспечения надежной сохранности наличных денежных средств и ценностей помещения кассы должны отвечать следующим требованиям:

- быть изолированными от других служебных помещений;
- иметь капитальные стены, прочные перекрытия пола и потолка;
- иметь сейф (металлический шкаф) для хранения денег и ценностей, в обязательном порядке прочно прикрепленный к строительным конструкциям;
- двери, окна, вентиляционные шахты должны быть оборудованы надежными средствами, исключающими проникновение в помещение.

В организационном плане помещения кассы оборудуются, как правило, несколькими рубежами охраны, как минимум — двумя, а также средствами охранно-пожарной сигнализации.

5.6.2. Транспортировка денег и ценностей

Особой опасности финансовые средства подвергаются при их перевозке.

Перевозка денежных средств и ценностей должна осуществляться только на специально оборудованных автомобилях. Автотранспорт для перевозки денег и ценностей должен отвечать следующим требованиям:

а) иметь закрытые или специальные кузова (броневая защита кузова, включая пол и потолок, внутренние металлические ставни на окнах или металлические жалюзи, специальные стекла и т. д.);

б) обладать улучшенными ходовыми характеристиками;

в) иметь средства сигнализации, радиосвязи и взаимосвязи между кабиной водителя и кузовом;

г) в кузове для перевозки денег должно быть смонтировано достаточное освещение, и он должен быть снабжен обогревательными устройствами;

д) двери кабины водителя и кузова должны иметь специальные внутренние запорные устройства.

Для перевозки денег и ценностей аренда стороннего транспорта запрещена. Во время инкассации запрещается нахождение и проезд посторонних лиц в специальном автомобиле. В случае необходимости оказания помощи пострадавшим инкассаторы обязаны связаться по радиостанции с дежурным и сообщить о происшествии по пути следования. При этом останавливаться инкассаторская машина не имеет права.

Прием сумок с денежной выручкой должен производиться инкассатором-сборщиком в изолированных помещениях. За процессом передачи сумки инкассатору не должны иметь возможность наблюдать не только посторонние лица, но и сотрудники фирмы, не связанные с денежными операциями.

По пути следования инкассаторской автомашины к объекту инкассации, а также по пути следования инкассатора-сборщика недопустимы:

- захламленные подъездные пути;
- близко прилегающие к маршруту криминогенные объекты;
- темные коридоры;
- неосвещенные дворы;
- проход инкассатора-сборщика через смежные организации, не имеющие отношения к инкассируемому объекту;
- отсутствие удобной стоянки для автомобиля инкассаторов.

Важным правилом безопасности инкассации является обязанность представителя фирмы встречать инкассатора с деньгами и ценностями при выходе его из автомобиля и провожать до машины, когда он собирает сумки с выручкой. При сопровождении инкассатора с деньгами и ценностями помощь должна заключаться только в присутствии представителя (охранника) на случай нападения, приставания и т. д. Сумки с деньгами и ценностями перед сдачей или после приема инкассатор должен нести сам.

Время инкассации, последовательность объезда инкассируемых объектов и маршрут инкассаторского автомобиля должны сохраняться в тайне. Для обеспечения безопасности груза и сопровождающих его лиц маршруты и время транспортировки должны периодически меняться. Оптимальна такая организация операций, при которой водитель автомашины узнает о предстоящем маршруте движения и получателе денег только при приеме груза или даже во время движения автомашины.

Инкассацию денежных средств осуществляет, как правило, отдел инкассации.

5.7. Отдел инкассации

Отдел инкассации является структурным подразделением службы безопасности. Отдел инкассации возглавляется начальником отдела, подчиняющимся начальнику СБ и его заместителю. В состав отдела входят несколько маршрутных групп и группа внутренней инкассации.

В состав каждой маршрутной группы входят: старший инкассатор, инкассатор и водитель. Группа внутренней инкассации состоит из старшего инкассатора и двух инкассаторов.

Личный состав отдела инкассации непосредственно подчинен начальнику отдела и его заместителю.

На отдел возлагаются следующие задачи:

- сбор денежной выручки непосредственно на предприятиях и в организациях, с которыми банк заключил договоры на инкассацию денежной выручки, доставка и сдача ее в кассу банка;
- выполнение по поручению руководства банка заданий по перевозке денег и других ценностей;
- доставка клиентам заранее подготовленных по их заявкам денежных сумм и их сдача установленным порядком в кассу клиента.

Личный состав отдела инкассации комплектуется из охранников, годных к выполнению обязанностей инкассатора или водителя специального транспортного средства, на котором перевозятся ценности.

Работники инкассации несут материальную ответственность за сохранность денег и других ценностей, принятых ими для доставки по назначению. В случае утери или хищения ценностей материальная ответственность по возмещению причиненного ущерба возлагается солидарно на всех членов бригады, ответственных за доставку ценностей. С членами бригады заключается договор о коллективной (бригадной) материальной ответственности.

5.7.1. Начальник отдела инкассации

Начальник отдела инкассации осуществляет руководство работой отдела инкассации и является прямым начальником для всего личного состава указанного отдела.

Он непосредственно подчинен начальнику службы безопасности и его заместителю.

Начальник отдела инкассации отвечает за:

- обеспечение бесперебойной инкассации и перевозку денег в соответствии с договорами и точное выполнение распоряжений руководства на перевозки денег и ценностей;
- разработку маршрутов и графиков заездов инкассаторов на предприятия и в организации, составление явочных карточек предприятий и организаций;
- формирование бригад инкассаторов для инкассации денежной выручки и перевозки денег и ценностей;
- проведение периодических проверок соблюдения инкассаторами правил работы с ценностями;
- обеспечение сохранности специальных средств, оружия и боеприпасов, находящихся в пользовании личного состава отдела;
- качество профессиональной подготовки инкассаторского состава.

Он обязан:

- руководствоваться в своей деятельности требованиями Закона Российской Федерации «О частной детективной и охранной деятельности в Российской Федерации», другими законами и правовыми актами Российской Федерации, знать законодательство, устав, нормативные документы по кассовой работе, кассовому обслуживанию и работе инкассации, порядок хранения и использования оружия и специальных средств, а также требования Положения о службе безопасности;
- систематически контролировать выполнение работниками инкассации правил сбора и перевозки денежных сумм и других ценностей;
- принять незамедлительные меры по обеспечению сохранности вверенного имущества собственника, организовать отражение противоправных посягательств на него, на здоровье и жизнь граждан и личного состава службы безопасности, обо всех таких посягательствах и их последствиях немедленно докладывать своему непосредственному начальнику;
- обо всех случаях применения огнестрельного оружия личным составом отдела немедленно уведомлять начальника службы безопасности;
- организовать в отделе необходимое материальное обеспечение и исправную работу технических средств для перевозки и защиты ценностей;

- руководить подготовкой, переподготовкой (повышением квалификации) личного состава отдела;
- организовывать в порядке, определяемом Министерством внутренних дел Российской Федерации, прохождение периодической проверки инкассаторского состава на их пригодность к действиям, связанным с применением специальных средств и огнестрельного оружия;
- осуществлять взаимодействие с кадровыми и финансовыми органами предприятия по вопросам исчисления трудового стажа для работников отдела, стажа для начисления пособий по государственному социальному страхованию, обязательности страхования на случай гибели, получения увечья или иного повреждения здоровья в связи с осуществлением охранных действий;
- контролировать сроки действия лицензий на сотрудников отдела и себя лично, принимать своевременные меры для их продления;
- организовать учет и обеспечить надежную сохранность оружия, боеприпасов и специальных средств;
- осуществлять контроль за порядком учета, хранения, ношения и перевозки огнестрельного оружия, боеприпасов к нему и специальных средств;
- по распоряжению начальника службы безопасности проводить служебное расследование по каждому случаю недостачи, порчи, излишков специальных средств, огнестрельного оружия и боеприпасов;
- разрабатывать и вносить руководству службы безопасности банка предложения по совершенствованию и повышению эффективности работы отдела;
- вести документацию отдела, предусмотренную нормативными документами, составлять установленную отчетность.

5.7.2. Инкассатор

Инкассатор — должностное лицо, производящее прием денег от организации для сдачи их в банк.

Он обеспечивает:

- доставку выручки торгующих организаций в банковское учреждение;
- доставку денежной выручки из торговых точек коммерческой структуры в ее офис для последующей сдачи в банк;
- доставку денег из банка в офис фирмы для последующей выдачи заработной платы сотрудникам;

- перевозку денег из банка в место приобретения товара, под покупку которого берется банковский кредит, и другие действия валютно-финансового оборота.

В процессе исполнения своих функциональных обязанностей инкассатору запрещается:

- совершать действия, не связанные с инкассацией и перевозкой ценностей;
- вести разговоры с посторонними лицами в момент остановки автомашины или отходить от автомобиля;
- передавать по радиостанции сведения, отличные от перечня сведений, разрешенных к открытой передаче;
- приобретать товары и продукты, а также пользоваться иными услугами в обслуживаемых организациях;
- оставлять вверенные ценности без личного присмотра;
- допускать нахождение или проезд посторонних лиц в специальном автомобиле;
- принимать к исполнению распоряжения, не соответствующие установленным правилам инкассации и перевозки ценностей.

При возникновении ситуаций, в которых охранники, перевозящие деньги и ценности, могут применять оружие, им следует пользоваться правилами и требованиями, изложенными в ст. 16 и 18 Закона о частной детективной и охранной деятельности. Вместе с тем представляется небезынтересным привести правила, регламентирующие применение огнестрельного оружия профессиональными инкассаторами.

Табельное оружие применяется инкассаторами:

- для защиты инкассируемых или перевозимых денежных средств и ценностей;
- для отражения нападения преступников, когда жизни инкассатора угрожает опасность;
- для задержания преступников, совершивших нападение на работников инкассации или охраняемые ими ценности и объекты.

После применения оружия:

- о данном факте сообщается дежурному по инкассации и дежурному территориального органа внутренних дел;
- до прибытия на место происшествия работников банка и милиции инкассаторы остаются на месте и обеспечивают сохранность ценностей.

Сотрудникам службы инкассации запрещается применять огнестрельное оружие в следующих случаях:

- на многолюдных улицах, площадях и в других общественных местах, где в результате выстрела могут пострадать посторонние лица;
- в отношении женщин и несовершеннолетних, за исключением случаев вооруженного нападения с их стороны;
- в отношении граждан, имеющих при себе детей.

5.8. Обеспечение безопасности персонала

Личная безопасность персонала, включая и главных должностных лиц фирмы, слагается из:

- охраны с использованием охранников-телохранителей;
- собственной безопасности лица, включающей физическую готовность к отражению преступных действий, психологическую готовность к восприятию и реагированию на критические условия;
- использования средств собственной безопасности, разрешенных к использованию в личных целях соответствующими законами.

Личную безопасность могут обеспечить личные охранники, обладающие наряду с высокими моральными качествами умением владеть собой в критических ситуациях, способностью быстро и решительно действовать в любой обстановке. Они должны быть хорошо развиты физически, психологически совместимы с охраняемым лицом и членами его семьи и профессионально подготовлены к этой работе.

А как защищается личность, выступающая свидетелем по тем или иным делам? Вот ответ на этот вопрос, опубликованный в одной из российских газет.

«СВИДЕТЕЛЬ БУДЕТ ЗАЩИЩЕН!

В западных фильмах о мафии часто показывают, как специальные агенты-полицейские денно и нощно охраняют до окончания суда важных свидетелей. А есть ли у нас такая практика защиты свидетелей?

О. МОРГУЛИС

ОТВЕТ: *Конечно же, есть. Не так давно было утверждено Положение <<О мерах социальной защиты и материального стимулирования граждан, способствовавших раскрытию преступлений, совершенных организованными преступными группами (М791-РП).*

Для защиты жизни и здоровья свидетелей, потерпевших, их родственников и близких, с учетом их желания и конкретных обстоятельств могут применяться следующие меры безопасности:

— личная охрана, охрана жилища и имущества;
— выдача в установленном законодательством порядке оружия, специальных средств индивидуальной защиты;
— временное (от месяца до года) помещение в безопасное место;
—обеспечение конфиденциальности сведений о защищаемых лицах в информационных системах;
— перевод на другую работу (службу), изменение места работы или учебы;
— предоставление другого места жительства;
—замена в установленном порядке документов, изменение внешности.

Обеспечение защиты и безопасности возлагается на специальное подразделение ГУВД г. Москвы».

Мерами социальной защиты являются материальная компенсация вреда, причиненного жизни, здоровью и имуществу граждан, а также в случае их потерь из-за применения мер защиты (потери в зарплате, в стаже работы и т. п.) и материальная помощь их наследникам в случае гибели.

Весьма распространенной формой реализации угроз личности является анонимный звонок с теми или иными требованиями.

Мотивы у террористов могут быть различные, от простых угроз и вымогательства до угроз убийством. Такие действия держат в страхе не только отдельную личность, но и семью, и фирму. Естественно, что каждый такой звонок в интересах противодействия террору должен учитываться: либо это запись на магнитофон, либо заполнение формализованной карты характерных особенностей угрожающего по телефону.

Наличие этих материалов позволит службе безопасности проводить оперативно-розыскные и защитные мероприятия.

Карта характерных особенностей лица, угрожающего по телефону

Пол	отм	Возраст	отм	Голос	отм	Речь	отм
Мужской		Взрослый		Звонкий		Быстрая	
Женский		Подросток		Грубый		Медленная	
Форма общения	отм	Ребенок		Мягкий		Отчетливая	
Простая		Особенности		Резкий		Неясная	
Грубая				Гнусавый		Заика	
Вежливая				Хриплый		Особенности	
Деликатная				Особенности			
Особенности							

Дикция	отм	Язык	отм	Манера разговора	отм	Фон	отм
Четкая		Простой		Спокойная		Отсутствует	
Хорошая		Интеллигентный		Истерическая		Разговор	
Шамкающая		Непристойный		Сбивчивая		Музыка	
Плохая		Хамоватый		Нервная		Шумы	
Особенности		Особенности		Особенности		Особенности	

Содержание разговора	Дополнительные сведения

Дата_____ Время Ф.И.О. составителя

Принятые меры:

ГЛАВА VI

ОТДЕЛ КАДРОВ

Давно известный афоризм «кадры решают все» и сегодня не потерял своего значения — не только потому, что без классных специалистов не выживешь, но и потому, что надежность сотрудников оставляет желать лучшего. Статистика показывает, что до 80% убытков фирма несет из-за прямого участия собственных сотрудников в тех или иных преступных деяниях.

Специалисты выделяют несколько критериев надежности персонала, и в идеале сотрудник коммерческого предприятия должен соответствовать каждому из них. К ним относятся:

- профессиональная надежность;
- психологическая надежность;
- моральная надежность.

Анализ конкретных случаев угроз безопасности фирмы со стороны собственного персонала показывает, что возникают они чаще всего «благодаря» следующим причинам:

- низкая квалификация;
- моральная неудовлетворенность работой;
- вредные привычки и др.

Вообще говоря, мотивация труда и лояльность фирме всегда обусловлены множеством переплетающихся мотивов. Одним важен высокий заработок, другим — карьера, третьим — социальная защищенность, четвертым — престиж или возможность заниматься творческой работой. Обиженный сотрудник — это мина замедленного действия, которая рано или поздно сработает.

Универсальных рецептов, позволяющих полностью обезопасить фирму от негативных действий собственных сотрудников, пока еще нет, как нет и средств обеспечения стопроцентной безопасности. Однако есть возможность максимально снизить эту опасность, держать ее под контролем и избежать

нежелательных последствий. Это — осознанная, организованная, последовательная и целенаправленная кадровая политика. Она составляет столь же необходимое условие нормальной работы фирмы, как и продуманные бизнес-планы. Эта политика базируется на трех основных принципах:

- разумный отбор персонала с помощью современных методов;
- продуманная и грамотно построенная система вознаграждения и служебного роста;
- организационная культура, поддерживающая в фирме климат взаимоотношений, благоприятный для совместной работы персонала.

Все это и составляет суть кадровой политики, одного из главных условий безопасности.

6.1. Особенности работы с сотрудниками, допущенными к конфиденциальной информации

Кадровая служба коммерческого предприятия организует проверку достоверности сведений, сообщенных о себе гражданином при его оформлении на соответствующую должность.

Основанием для проведения проверки могут служить:

- информация, полученная от правоохранительных органов, органов государственной налоговой службы, судебных органов, организации и предприятий по прежнему месту работы;
- недостоверность или неполнота сведений, полученных от правоохранительных органов.

Проверка сведений о кандидате осуществляется в месячный срок. Срок может быть продлен при условии установления испытательного срока кандидату.

С целью проверки можно направлять соответствующие запросы в правоохранительные органы и органы управления, на предприятия и учреждения с указанием срока удовлетворения запроса.

Документы проверки относятся к конфиденциальной информации и приобщаются к личному делу кандидата.

Лицо, в отношении которого проводится проверка, вправе знакомиться с документами проверки и давать письменные объяснения. Указанные объяснения приобщаются к документам проверки.

При установлении в ходе проверки обстоятельств, свидетельствующих, что лицо, в отношении которого она проводи-

лась, сообщило о себе неполные или недостоверные сведения либо представило заведомо ложные сведения, администрация вправе отказать лицу в трудоустройстве.

При наборе новых сотрудников большинство предприятий, организаций, фирм сталкивается с определенным риском. Несмотря на различные формы собеседования и проверки, сотрудники фирм не всегда лояльны по отношению к своей организации. Статистика показывает, что персонал любой фирмы состоит на 25% из честных людей, которые остаются таковыми при любых обстоятельствах. Еще 25% —это сотрудники, ожидающие удобного случая поживиться за счет интересов фирмы, а остальные 50% — лица, которые могут остаться честными или попытаются поживиться за счет интересов фирмы в зависимости от тех или иных обстоятельств.

Как показывает мировой опыт, задача обеспечения кадровой безопасности эффективно решается с помощью психофизиологического тестирования на полиграфе (детекторе лжи). Этот метод имеет целый ряд преимуществ по сравнению с традиционными собеседованиями и проверками.

По оценкам зарубежных специалистов, при отборе сотрудников на ответственные должности в частные фирмы с использованием полиграфа выявляется, что треть кандидатов скрывает какие-либо сведения из своего прошлого или личные негативные черты. Сведения, получаемые методом психофизиологического тестирования, далеко не всегда могут быть получены с помощью других методов даже при их комплексном применении.

Метод психофизиологического тестирования обеспечивает высокую надежность и достоверность получаемых результатов. Достаточно отметить, что достоверность сведений, получаемых опытным специалистом, превышает 90%.

6.2. Порядок ведения личных дел лиц, допущенных к конфиденциальной информации

Кадровая служба в лице инспектора по работе с сотрудниками, допущенными к работе с конфиденциальной информацией, ведет личные дела на них. Эти дела относятся к категории конфиденциальной информации с соблюдением режима безопасности.

К личному делу приобщаются заявление о согласии работать на должности с режимом конфиденциальной информации,

добровольное согласие (подписка) о неразглашении сведений, отнесенных предприятием к конфиденциальной информации, личный листок по учету кадров.

Кадровая служба вносит в досье сведения обо всех случаях и обстоятельствах нарушений требований и положений по сохранению режима конфиденциальности, объяснения сотрудника по данным фактам и принятые руководством меры административного характера.

ТРУДОВОЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ
(Извлечение)

ГЛАВА 14. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА

Статья 85. Понятие персональных данных работника. Обработка персональных данных работника

Персональные данные работника — информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

Обработка персональных данных работника — получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.

Статья 86. Общие требования при обработке персональных данных работника и гарантии их защиты

В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

1) обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

2) при определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, настоящим Кодексом и иными федеральными законами;

3) все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель

должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

4) работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

5) работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом;

6) при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

7) защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом;

8) работники и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;

9) работники не должны отказываться от своих прав на сохранение и защиту тайны;

10) работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

Статья 87. Хранение и использование персональных данных работников

Порядок хранения и использования персональных данных работников в организации устанавливается работодателем с соблюдением требований настоящего Кодекса.

Статья 88. Передача персональных данных работника

При передаче персональных данных работника работодатель должен соблюдать следующие требования:

не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;

- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

осуществлять передачу персональных данных работника в пределах одной организации в соответствии с локальным нормативным актом организации, с которым работник должен быть ознакомлен под расписку;

разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

передавать персональные данные работника представителям работников в порядке, установленном настоящим Кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

Статья 89. Права работников в целях обеспечения защиты персональных данных, хранящихся у работодателя

В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право на:

полную информацию об их персональных данных и обработке этих данных;

свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;

определение своих представителей для защиты своих персональных данных;

доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований настоящего Кодекса. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

Статья 90. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

ГЛАВА VII

СПЕЦИАЛЬНЫЙ ОТДЕЛ. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОММЕРЧЕСКОЙ ТАЙНЫ

Конфиденциальная информация — это документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации. По степени обеспечения защиты информация классифицируется по следующему параметру: открытая информация, или информация общего пользования, и информация ограниченного использования (охраняемая информация). В свою очередь охраняемая информация подразделяется на конфиденциальную информацию и информацию, отнесенную к государственной тайне (Закон РФ «О государственной тайне»). Сведения конфиденциального характера утверждены указом Президента РФ № 188 от 6 марта 1997 г. в виде перечня сведений конфиденциального характера. Содержание перечня структурно приведено в таблице12.

Источниками конфиденциальной информации на каждом предприятии, на каждой фирме являются:

1. Персонал, люди.
2. Документы.
3. Публикации.
4. Технические носители информации.
5. Технические средства обеспечения производственной и трудовой деятельности.
6. Продукция.
7. Промышленные и производственные отходы.

Служба безопасности должна четко знать, у кого (у какого источника) и где (в каком подразделении и в каком виде) присутствует конфиденциальная информация, а также кто способствует неправомерному овладению охраняемыми сведениями.

По общему мнению, неправомерному овладению конфиденциальной информацией способствуют:

- разглашение конфиденциальной информации ее обладателем (источником);
- утечка конфиденциальной информации по техническим каналам;
- несанкционированный доступ к конфиденциальной информации со стороны злоумышленников и других элементов.

Таблица 12

Конфиденциальная информация (документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации)

Личная	Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленном порядке
Судебно-следственная	Сведения, составляющие тайну следствия и судопроизводства
Служебная	Служебные сведения, доступ к которым ограничен органами государственной власти (служебная тайна)
Профессиональная	Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и т.д.)
Коммерческая	Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен законами (коммерческая тайна)
Производственная	Сведения о сущности изобретения полезной модели промышленного образца до официальной публикации информации о них

7.1.Коммерческаятайна

Информация составляет служебную или коммерческую тайну в случае, когда она имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности (ст. 139ГКРФ).

Одними из важных источников коммерческой информации являются люди, документы и публикации. От того, как организована работа с людьми и документами, зависит и безопасность фирмы. Целям предотвращения нанесения экономического, финансового и материального ущерба фирме, вызванного неправомерными или неосторожными действиями, а также неквалифицированным обращением или разглашением коммерческой тайны, служат следующие предложения.

Предложения по обеспечению коммерческой тайны носят общий рекомендательный характер, не являются нормативным документом, ориентированы в основном на работу с документами, содержащими сведения коммерческого характера, и предусматривают главным образом организационные меры защиты коммерческих секретов.

Под коммерческой тайной понимаются не являющиеся государственными секретами сведения, связанные с производственно-техни-ческой, научно-исследовательской, опытно-конструкторской и другой деятельностью фирмы, а также с ее технологической информацией, управлением, финансами и т. п., разглашение, утечка и несанкционированный доступ к которым может нанести ущерб ее интересам.

К сведениям, составляющим коммерческую тайну, относятся несекретные сведения, предусмотренные перечнем конкретных сведений, составляющих коммерческую тайну, утвержденным и введенным в действие приказом директора фирмы.

Коммерческая тайна является ее собственностью. Если коммерческая тайна является результатом совместной деятельности с другими предприятиями, основанной на договорных началах, то эта тайна может быть собственностью двух сторон. Это обстоятельство должно найти отражение в договоре.

Следует отметить, что единой установки на обозначение грифа ограничения доступа к документу, содержащему коммерческую тайну, нет. Таким грифом могут быть слова: «коммерческая тайна», «секрет предприятия», «тайна предприятия»

и др. Подобный ограничительный гриф не является грифом секретности, а лишь показывает, что право собственности на данную информацию охраняется законодательством.

Таблица 13

Коммерческая тайна

Определения	Содержание
Субъект	Предприятия, организации, коллективы, граждане
Объект	Понятие применимо к широкому спектру интеллектуальной и промышленной собственности
Характеристики	1. Активный ресурс 2. Конфиденциальная информация 3. Особая форма собственности 4. Товар рыночной новизны
Ценность	Реально (потенциально) создает преимущества в конкурентной борьбе
Требования	1. Потенциально полезная 2. Не общеизвестная
Срок действия	Определяется жизненным циклом товара
Защита	1. Правовая 2. Организационная 3. Инженерно-техническая

КОММЕРЧЕСКАЯ ТАЙНА - не являющиеся государственными секретами сведения, связанные с производством, технологией, управлением, финансами и другой деятельностью, разглашение, утечка и несанкционированный доступ к которым может нанести ущерб их владельцам.

К коммерческой тайне не относятся:

1. Охраняемые государством сведения.
2. Общественные на законных основаниях сведения.
3. Общедоступные сведения, патенты, товарные знаки.
4. Сведения о негативной стороне деятельности.
5. Учредительные документы и сведения хозяйственной деятельности.

7.2. Порядок определения информации, содержащей коммерческую тайну и сроков ее действия

Определение необходимости проставления грифа «Коммерческая тайна» («КТ») производится на основании перечня, упомянутого выше:

на документе — исполнителем и лицом, подписывающим документ, а на издании — автором (составителем) и руководителем, утверждающим издание к печати.

Сроки действия коммерческой тайны, содержащейся в документе, определяются в каждом конкретном случае исполнителем или лицом, подписавшим документ, в виде конкретной даты или «до заключения трудового договора», или «бессрочно».

На документах, делах и изданиях, содержащих сведения, составляющие коммерческую тайну, проставляется гриф «Коммерческая тайна» («КТ»), а в документах и изданиях, кроме того, — номера экземпляров.

Гриф «Коммерческая тайна» и номер экземпляра проставляются в правом верхнем углу первой страницы документа, на обложке и титульном листе издания и на первой странице сопроводительного письма к этим материалам.

На обратной стороне последнего листа каждого экземпляра документа, содержащего коммерческую тайну, печатается разметка, в которой указывается: количество отпечатанных экземпляров, номер, фамилия исполнителя и его телефон, дата, срок действия коммерческой тайны, содержащейся в документе (конкретная дата или «до заключения трудового договора», или «бессрочно»), фамилия машинистки.

Решение вопроса о снятии грифа «Коммерческая тайна» возлагается на создаваемую в установленном порядке специальную комиссию, в состав которой включаются представители службы безопасности и соответствующих структурных подразделений.

Решение комиссии оформляется составляемым в произвольной форме актом, который утверждается директором или его замести-телем по направлению. В акте перечисляются дела, с которых гриф «КТ» снимается. Один экземпляр акта вместе с делами передается в архив, а на дела постоянного хранения — в государственный архив.

На обложках дел гриф «КТ» погашается штампом или записью от руки с указанием даты и номера акта, послужившего основанием для его снятия.

Аналогичные отметки вносятся в описи и номенклатуры дел.

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ от 5 декабря 1991 г. №35

(с учетом изменений, внесенных Постановлением *Правительства РФ от 3 октября 2002 г. №731)*

О перечне сведений, которые не могут составлять коммерческую тайну

В целях обеспечения деятельности государственной налоговой службы, правоохранительных и контролирующих органов, а также предупреждения злоупотреблений в процессе приватизации Правительство РСФСР **постановляет:**

1. Установить, что коммерческую тайну предприятия и предпринимателя не могут составлять:

учредительные документы (решение о создании предприятия или договор учредителей) и Устав;

документы, дающие право заниматься предпринимательской деятельностью (документы, подтверждающие факт внесения записей о юридических лицах в Единый государственный реестр юридических лиц, свидетельства о государственной регистрации индивидуальных предпринимателей, лицензии, патенты);

сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему РСФСР;

документы о платежеспособности;

сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;

документы об уплате налогов и обязательных платежах;

сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, реализации продукции, причиняющей вред здоровью населения, а также других нарушениях законодательства РСФСР и размерах причиненного при этом ущерба;

сведения об участии должностных лиц предприятия в кооперативах, малых предприятиях, товариществах, акционерных обществах, объединениях и других организациях, занимающихся предпринимательской деятельностью.

2. Запретить государственным и муниципальным предприятиям до и в процессе их приватизации относить к коммерческой тайне данные:

о размерах имущества предприятия и его денежных средствах;

о вложении средств в доходные активы (ценные бумаги) других предприятий, в процентные облигации и займы, в уставные фонды совместных предприятий;

о кредитных, торговых и иных обязательствах предприятия, вытекающих из законодательства РСФСР и заключенных им договоров;

о договорах с кооперативами, иными негосударственными предприятиями, творческими и временными трудовыми коллективами, а также отдельными гражданами.

3. Предприятия и лица, занимающиеся предпринимательской деятельностью, руководители государственных и муниципальных предприятий обязаны представлять сведения, перечисленные в пунктах 1 и 2 настоящего постановления, по требованию органов власти, управления, контролирующих и правоохранительных органов, других юридических лиц, имеющих на это право в соответствии с законодательством РСФСР, а также трудового коллектива предприятия.

4. Действие настоящего постановления не распространяется на сведения, относимые в соответствии с международными договорами к коммерческой тайне, а также на сведения о деятельности предприятия, которые в соответствии с действующим законодательством составляют государственную тайну.

Б. ЕЛЬЦИН

7.3. Способы неправомерного овладения конфиденциальной информацией

Сведения, составляющие коммерческую тайну фирмы, могут быть получены злоумышленниками в результате таких действий, как разглашение, утечка либо несанкционированный доступ.

Каждое из этих действий обладает определенными свойствами и особенностями.

7.3.1.Разглашение

Под разглашением коммерческой таймы имеются в виду противоправные, умышленные или неосторожные действия должностных или иных лиц, приведшие к преждевременному, не вызванному служебной необходимостью, оглашению охраняемых сведений, подпадающих под эту категорию, а также передача таких сведений по открытым техническим каналам или обработка их на некатегорированных ЭВМ.

Под открытым опубликованием вышеуказанных сведений имеется в виду публикация материалов в открытой печати, передача по радио и телевидению, оглашение на международных и внутрироссийских съездах, конференциях, совещаниях, симпозиумах, при публичной защите диссертаций и других публичных выступлениях, свободная рассылка[1], вывоз материалов за границу или передача их в любой форме иностранным фирмам, организациям или отдельным лицам вне сферы прямых служебных обязанностей.

Необходимость и возможность открытого опубликования этих сведений, а также их объемы, формы и время опубликования определяются директором или его заместителями по направлениям по заключению постоянно действующей экспертной комиссии.

Меры по ограничению открытых публикаций коммерческой информации не могут быть использованы во вред принципу гласности и для сокрытия от общественности фактов бесхозяйственности, расточительства, недобросовестной конкуренции и других негативных явлений.

Использование для открытого опубликования сведений, полученных на договорной или доверительной основе или являющихся результатом совместной производственной деятельности, допускается лишь с общего согласия партнеров.

Передача информации сторонним организациям, не связанным прямыми служебными контактами, должна регулироваться, как правило, договорными отношениями, предусматривающими обязательства и ответственность пользователей, включая возмещение материальных затрат на предоставление информации и компенсацию за нарушение договорных обязательств.

Предоставление коммерческой информации представителям служебных, ревизионных, фискальных и следственных органов, депутатам Госдумы, органам печати, радио и пр. регулируется соответствующими положениями.

Тиражированные документы и издания с грифом «Коммерческая тайна» рассматриваются как материалы, содержащие сведения ограниченного распространения.

Ответственность за обеспечение режима при работе с материалами с грифом «КТ>>, своевременную разработку и осуществление необходимых мероприятий по сохранению коммерческой тайны возлагается на директора, его заместителей по направлениям и руководителей структурных подразделений. Ответственность за организацию и осуществление работы по защите коммерческой тайны и проведение постоянного контроля за ее соблюдением возлагается на службу безопасности.

Служба безопасности принимает меры по сохранению коммерческой тайны путем максимального ограничения круга лиц, физической сохранности документов, содержащих такие сведения, обработки информации с грифом «КТ» на защищенных ЭВМ, внесения требований по конфиденциальности конкретной информации в договоры с внутренними и внешнеторговыми партнерами и других мер по решению руководства.

Защита коммерческой тайны предусматривает:

— порядок определения информации, содержащей коммерческую тайну, и сроков ее действия;
—систему допуска сотрудников, командированных и частных лиц к сведениям, составляющим коммерческую тайну;
—порядок работы с документами с грифом «КТ»;
—обеспечение сохранности документов, дел и изданий с грифом «КТ»;
— обязанности лиц, допущенных к сведениям, составляющим коммерческую тайну;
— принципы организации и проведения контроля за обеспечением режима при работе со сведениями, составляющими коммерческую тайну;
— ответственность за разглашение сведений, утрату документов, содержащих коммерческую тайну.

Контроль за осуществлением учета, размножения, хранения и использования документов, дел и изданий с грифом «коммерческая тайна» возлагается на уполномоченных службы безопасности.

Контроль за неразглашением сведений, содержащихся в документах, делах и изданиях с грифом «коммерческая тайна», осуществляется отделами службы безопасности.

7.3.2. Утечка

Утечку конфиденциальной информации в общем плане можно рассматривать как неконтролируемый выход охраняемых сведений за пределы организации или круга лиц, которым эти сведения были доверены.

Утечка конфиденциальной информации осуществляется по техническим каналами при определенных условиях.

К факторам и обстоятельствам, способствующим утечке коммерческих секретов, относятся:

— недостаточное знание сотрудником правил защиты коммерческой тайны и непонимание (недопонимание)необходимости их тщательного соблюдения;
— использование неаттестованных технических средств обработки конфиденциальной информации;
— слабый контроль за соблюдением правил защиты информации правилами, организационными и инженерно-техническими мерами.

Возможные каналы утечки речевой информации

В зависимости от физической природы возникновения информационных сигналов, среды распространения акустических колебаний и способов их перехвата механические каналы утечки акустической (речевой) информации можно разделить на воздушные, вибрационные, оптико-электронные и параметрические.

/. Воздушные технические каналы утечки информации

В этих каналах средой распространения акустических сигналов является воздух, и для их перехвата используются миниатюрные высокочувствительные микрофоны и специальные направленные микрофоны. Миниатюрные микрофоны объединяются (или соединяются) с портативными звукозаписывающими устройствами или миниатюрными передатчиками. Автономные устройства, конструктивно объединяющие миниатюрные микрофоны и передатчики, называют акустическими закладками.

Перехваченная закладными устройствами речевая информация может передаваться по радиоканалу, оптическому каналу, по сети переменного тока, соединительным линиям вспомогательных технических средств и систем (ВТСС), посторонним проводникам (трубам водоснабжения и канализации, металлоконструкциям и т. п.). Причем для передачи информации по трубам и металлоконструкциям могут использоваться не только электромагнитные, но и механические ультразвуковые колебания.

Прием информации, передаваемой закладными устройствами, осуществляется, как правило, на специальные приемные устройства, работающие в соответствующем диапазоне волн. Однако встречаются закладные устройства, прием информации с которых можно осуществить с обычного телефонного

аппарата. Такие устройства устанавливаются или непосредственно в корпусе телефонного аппарата, находящегося в контролируемом помещении и называемом «телефоном-наблюдателем», или подключаются к телефонной линии, чаще всего в телефонной розетке. Побочное устройство конструктивно объединяет миниатюрный микрофон и специальный блок коммуникации и часто называется «телефонное ухо». Использование информационных акустических закладок требует проникновения на контролируемый объект (в помещение). В том случае, когда это не удается, для перехвата речевой информации используются направленные микрофоны.

2. Вибрационные технические каналы

В вибрационных технических каналах утечки информации средой распространения акустических сигналов являются конструкции зданий, сооружений, канализации и другие твердые тела. Для перехвата акустических колебаний в этом случае используются контактные микрофоны (стетоскопы).

По вибрационному каналу также возможен перехват информации с использованием закладных устройств. В основном для передачи информации используется радиоканал, поэтому такие устройства часто называют радиосистемами. Возможно использование закладных устройств с передачей информации по оптическому каналу, а также по ультразвуковому каналу (по металлоконструкциям здания).

3. Электроакустические каналы утечки информации

Электроакустические каналы утечки информации возникают за счет электроакустических преобразований акустических сигналов в электрические и включают перехват акустических колебаний через ВТСС, обладающих «микрофонным эффектом», а также путем высокочастотного навязывания.

Некоторые элементы ВТСС, в том числе трансформаторы, катушки индуктивности, электромагниты вторичных электрочасов, звонков телефонных аппаратов, дроссели ламп дневного света и т. д., обладают свойствами изменять свои параметры (емкость, индуктивность, сопротивление) под действием акустического поля, создаваемого источником акустических колебаний. Изменения параметров приводит либо к появлению на данных элементах ЭДС, изменяющейся по закону воздействующего информационного сигнала (акустического поля), либо к модуляции токов, протекающих по этим элементам информационным сигналом. ВТСС кроме указанных элементов могут содержать непосредственно электроакустические преобразователи: неко-

торые датчики пожарной сигнализации, громкоговорители ретрансляционной сети и т. д. Причем из ВТСС, обладающих «микрофонным эффектом», наибольшую чувствительность к акустическому полю имеют абонентские громкоговорители.

Перехват акустических колебаний в данном канале утечки осуществляется путем непосредственного подключения к соединительным линиям ВТСС специальных высокочувствительных усилителей НЧ.

Например, подключая такие средства к соединительным линиям телефонных аппаратов с электромеханическими вызывными звонками, можно прослушивать разговоры, ведущиеся в помещениях, где установлены эти аппараты.

Технический канал утечки информации путем высокочастотного (ВЧ) навязывания может быть осуществлен путем несанкционированного контактного введения токов высокой частоты в линии, имеющие функциональные связи с нелинейными или параметрическими элементами ВТСС, на которых происходит модуляция ВЧ-сигнала информационным. Информационный сигнал в данных элементах ВТСС появляется вследствие «микрофонного эффекта» последних. В силу того, что нелинейные или параметрические элементы для ВЧ-сигнала, как правило, представляют собой несогласованную нагрузку, промоделированный ВЧ-сигнал будет от нее отражаться и распространяться в противоположном направлении по линии или излучаться. Для приема отраженных или излученных ВЧ-сигналов используются спецприемники с высокой чувствительностью. Для исключения влияния зондирующего и переотраженного сигналов могут использоваться импульсные сигналы.

4. Оптико-электронный технический канал утечки

Этот канал образуется при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол, картин, зеркал). Отраженное лазерное излучение модулируется по амплитуде и фазе (по закону вибрации поверхности) и принимается приемником лазерного излучения, при демодуляции которого выделяется речевая информация. Причем лазер и приемник могут быть установлены в одном или разных местах.

Исходя из вышеперечисленных особенностей технические средства передачи информации (ТСПИ) и ВТСС, а также возможностей современных технических разведок, можно заключить, что существует потенциальная возможность несанкционированного доступа.

7.3.3. Несанкционированный доступ

Несанкционированный доступ (НСД) к конфиденциальной информации — это преднамеренные противоправные действия злоумышленников с целью получения охраняемых сведений. Несанкционированный доступ реализуется по каналам проникновения как легальным, так и нелегальным путем.

К числу наиболее распространенных способов несанкционированного доступа относятся следующие способы:

- инициативное сотрудничество, склонение к сотрудничеству, выпытывание, подслушивание, наблюдение, уничтожение, фотографирование (направлено на сотрудников);
- наблюдение, хищение, копирование, подделка, уничтожение, перехват, негласное ознакомление, фотографирование, сбор и обработка (направлено на документы);
- подделка, негласное ознакомление, сбор и аналитическая обработка(направлено на публикации);
- хищение, копирование, подделка, уничтожение, сбор и аналитическая обработка (направлено на технические носители);
- подслушивание, уничтожение, незаконное подключение, перехват (направлено на технические средства ОПД);
- подслушивание, наблюдение, хищение, копирование, подделка, уничтожение, незаконное подключение, перехват, негласное ознакомление (направлено на технические средства АСОД);
- наблюдение, хищение, копирование, подделка, уничтожение, негласное ознакомление, фотографирование (направлено на продукцию);
- хищение, сбор и аналитическая обработка (направлено на отходы).

7.4. Порядок допуска специалистов к конфиденциальной информации

1. Допуск специалистов к сведениям конфиденциального характера осуществляется в добровольном порядке назначенными для этого специалистами службы безопасности.

2. Допуск предусматривает:

— принятие специалистом обязательства о неразглашении доверенных ему сведений, составляющих коммерческую тайну предприятия;

— согласие специалиста на частичное ограничение его прав при работе с конфиденциальной информацией;
— согласие специалиста на проведение с ним проверочных и контрольных мероприятий (контроль знаний основных положений и требований по защите коммерческой тайны, наличия конфиденциальных документов и порядок их хранения);
— ознакомление специалиста с нормами законодательства России и предприятия о коммерческой тайне и ответственности за ее разглашение;
— инструктаж специалиста по защите коммерческой тайны;
— принятие решения о допуске к сведениям конфиденциального характера;
— контроль деятельности специалиста при работе со сведениями конфиденциального характер;

3. Допуск специалиста к коммерческим секретам обязывает:
— строго соблюдать требования инструкций по работе с коммерческими секретами;
— ответственность за нарушение режима информационной безопасности.

7.4.1. Система допуска сотрудников, командированных и частных лиц к сведениям, составляющим коммерческую тайну

Допуск сотрудников к сведениям, составляющим коммерческую тайну, осуществляется директором, его заместителями по направлениям и руководителями структурных подразделений.

Руководители подразделений и службы безопасности ответственны за подбор лиц, допускаемых к сведениям с грифом «КТ», обязаны обеспечить систематический контроль за тем, чтобы к этим сведениям получали доступ только те лица, которым такие сведения необходимы для выполнения своих служебных обязанностей.

К сведениям, составляющим коммерческую тайну, допускаются лица, обладающие необходимыми нравственными и деловыми качествами, способные хранить коммерческую тайну и только после оформления в службе безопасности индивидуального письменного обязательства по сохранению коммерческой тайны.

Допуск к работе с делами «КТ» сотрудников, имеющих к ним непосредственное отношение, производится в соответствии с оформленным на внутренней стороне обложки списком за подписью руководителя структурного подразделения, а к документам — согласно указаниям, содержащимся в резолюциях руководителей подразделений.

Командированные и частные лица допускаются к ознакомлению и работе с документами и изданиями с грифом «КТ» с письменного разрешения руководителей фирмы и подразделений, в ведении которых находятся эти документы, при наличии письменного запроса тех организаций, в которых они работают, с указанием темы и объема выполняемого задания, а также предписания на выполнение задания.

Выписки из документов и изданий, содержащих сведения с грифом «КТ», производятся в тетрадях, имеющих такой же гриф, и после окончания работы представителя высылаются в адрес организации.

Дела и издания с грифом «КТ» выдаются исполнителям и принимаются от них под расписку в карточке учета выдаваемых дел и изданий *(форма 4)*.

7.4.2. Порядок работы с документами с грифом «КТ»

Документы, содержащие сведения, составляющие коммерческую тайну, подлежат обязательной регистрации в канцелярии службы безопасности или в общем делопроизводстве подразделения уполномоченным службы безопасности. Они должны иметь реквизиты, предусмотренные положением, и гриф «КТ» (или полностью - «Коммерческая тайна»). На документах, передаваемых иностранцам, гриф «КТ» не проставляется. Полученные от иностранцев документы маркируются грифом «КТ» графитным карандашом.

В тексте документа и его реквизитах дополнительно могут оговариваться права на информацию, порядок пользования ею, сроки ограничения на публикацию и другие.

Отсутствие грифа «КТ» и предупредительных оговорок в тексте и реквизитах означает свободную рассылку и предполагает, что автор информации и должностное лицо, санкционирующее (подписавшее, утверждавшее документ) ее распространение, предусмотрели все возможные последствия свободной рассылки и несут за это всю полноту ответственности.

Вся поступающая корреспонденция с грифом «КТ» или другими грифами принимается и вскрывается сотрудниками канцелярии, которым поручена работа с этими материалами. При этом проверяется количество листов и экземпляров документов и изданий, а также наличие указанных в сопроводительном письме приложений.

В случае отсутствия в конвертах (пакетах) документов «КТ» или приложений к ним составляется акт в двух экземплярах, один из которых отправляется отправителю.

Регистрации подлежат все входящие, исходящие и внутренние документы, а также издания с грифом «КТ». Такие документы учитываются по количеству листов, а издания (книги, журналы, брошюры) — поэкземплярно.

Учет документов и изданий с грифом «КТ» ведется в журналах *{форма 1)* или на карточках *{форма 2)* отдельно от учета другой несекретной документации.

Листы журналов нумеруются, прошиваются и опечатываются. Издания, которые не подшиваются в дела, учитываются в журнале инвентарного учета *{форма 5)*.

Движение документов и изданий с грифом «КТ» должно своевременно отражаться в журналах или на карточках.

На каждом зарегистрированном документе, а также на сопроводительном листе к изданиям с грифом «КТ» проставляется штамп, в котором указываются наименование, регистрационный номер документа и дата его поступления.

Тираж издания с грифом «КТ», полученный для рассылки, регистрируется под одним входящим номером в журнале учета и распределения изданий *{форма 3)*.

Дополнительно размноженные экземпляры документа (издания) учитываются за номером этого документа (издания), о чем делается отметка на размножаемом документе (издании) и в учетных формах. Нумерация дополнительно размноженных экземпляров производится от последнего номера ранее учтенных экземпляров.

Печатание материалов с грифом «КТ» производится в бюро оформления технической документации или в структурных подразделениях под ответственность их руководителей.

Отпечатанные и подписанные документы с грифом «КТ» вместе с их черновиками и вариантами передаются для регистрации сотруднику канцелярии, осуществляющему их учет. Черновики и варианты уничтожаются этим сотрудником с подтверждением факта уничтожения записью на копии исходящего документа: «Черновик (и варианты) уничтожены» с указанием даты и подписью.

Размножение документов и изданий с грифом «КТ» в типографиях и на множительных аппаратах производится с разрешения службы безопасности и под контролем канцелярии по заказам, подписанным руководителем подразделения и утвержденным заместителем директора по направлению. Учет размноженных документов и изданий осуществляется поэкземплярно в специальном журнале.

Рассылка документов и изданий с грифом «КТ» осуществляется на основании подписанных руководителем структурного подразделения списков с указанием учетных номеров отправляемых экземпляров.

Документы с грифом «КТ» после исполнения группируются в отдельные дела. Порядок их группировки предусматривается номенклатурами дел несекретного делопроизводства. В номенклатуру дел в обязательном порядке включаются все справочные картотеки и журналы на документы и издания с грифом «КТ».

При пользовании открытой радиосвязью запрещается передавать сведения, имеющие гриф «КТ». Такие сведения могут передаваться только по закрытым техническим каналам связи или открытой телетайпной связью с проставлением на документах и телеграммах соответствующего штампа.

При пользовании проводной связью запрещается указывать должности адресатов и отправителей, разрешается указывать только телеграфные адреса и фамилии отправителей и получателей.

Снятие копий (рукописных, машинописных, микро- и фотокопий, электрографических и др.), а также производство выписок из документов и изданий с грифом «КТ» сотрудниками осуществляется по разрешению руководителей подразделений.

Снятие копий для сторонних организаций с документов и изданий с грифом «КТ» производится на основании письменных запросов по разрешению руководителей подразделений, подготовивших эти документы и издания.

Аналогичные отметки вносятся в описи и номенклатуры дел.

Порядок работы на ЭВМ при обработке информации с грифом «КТ» устанавливается в соответствии с требованиями инструкции о порядке работы на ПЭВМ при обработке несекретной информации.

7.4.3. Обеспечение сохранности документов, дел и изданий

Документы, дела и издания с грифом «КТ» должны храниться в служебных помещениях и библиотеках в надежно запираемых и опечатываемых шкафах (хранилищах). При этом должны быть созданы надлежащие условия, обеспечивающие их физическую сохранность.

Выданные для работы дела с грифом «КТ» подлежат возврату в канцелярию или уполномоченному службы безопасности в тот же день.

Отдельные дела с грифом «КТ» с разрешения начальника канцелярии или уполномоченного службы безопасности могут находиться у исполнителя в течение срока, необходимого для выполнения задания, при условии полного обеспечения их сохранности и соблюдения правил хранения.

Передача документов, дел и изданий с грифом «КТ» другим сотрудникам, допущенным к этим документам, производится только через канцелярию или уполномоченного службы безопасности.

Запрещается изъятие из дел или перемещение документов с грифом «КТ» из одного дела в другое без санкции канцелярии или уполномоченного службы безопасности, осуществляющего их учет. Обо всех проведенных изъятиях или перемещениях делаются отметки в учетных документах, включая внутренние описи.

Запрещается выносить документы, дела и издания с грифом «КТ» из служебных помещений для работы с ними на дому, в гостиницах и т. д.

В необходимых случаях директор, его заместители по направлениям или руководители структурных подразделений могут разрешать исполнителям или сотрудникам канцелярии вынос из здания документов с грифом «КТ» для их согласования, подписи и т. п. в организациях, находящихся в пределах данного города.

Лицам, командированным в другие города, запрещается иметь при себе в пути следования документы, дела или издания с грифом «КТ». Эти материалы должны быть направлены заранее в адрес организации по месту командировки сотрудника, как правило, заказными или ценными почтовыми отправлениями, а также с курьерами.

При смене сотрудников, ответственных за учет и хранение документов, дел и изданий с грифом «КТ», составляется по произвольной форме акт приема-передачи этих документов, утверждаемый заместителями директора по направлениям или руководителями структурных подразделений.

7.4.4. Контроль за выполнением требований внутриобъектного режима при работе со сведениями, содержащими коммерческую тайну

Под внутриобъектовым режимом при работе с коммерческой тайной подразумевается соблюдение условий работы, исключающих возможность утечки информации о сведениях, содержащих коммерческую тайну.

Контроль за соблюдением указанного режима осуществляется в целях изучения и оценки состояния сохранности коммерческой тайны, выявления и установления причин недостатков и выработки предложений по их устранению

Контроль за обеспечением режима при работе со сведениями, содержащими коммерческую тайну, осуществляют служба безопасности предприятия и руководитель структурного подразделения путем текущих и плановых проверок.

При проведении проверок создается комиссия, которая комплектуется из опытных и квалифицированных работников в составе не менее двух человек, допущенных к работе с материалами «КТ».

Плановые проверки проводятся не реже одного раза в год комиссиями на основании приказа или распоряжения руководителя предприятия (подразделения).

Проверяющие имеют право знакомиться со всеми документами, карточками и другими материалами, имеющими отношение к проверяемым вопросам, а также проводить беседы, консультироваться со специалистами и исполнителями, требовать представления письменных объяснений, справок и отчетов по всем вопросам, входящим в компетенцию комиссии.

При проверках присутствует руководитель структурного подразделения или его заместитель.

По результатам проверок составляется акт или справка о наличии документов, состоянии работы с материалами «КТ», выявленных недостатках и предложениях по их устранению. Акт утверждается руководителем предприятия (подразделения).

При выявлении случаев утраты документов или разглашения сведений, составляющих коммерческую тайну, ставятся в известность руководитель предприятия и его заместитель (помощник) по безопасности. Для расследования указанных случаев приказом руководителя предприятия создается комиссия, которая: определяет соответствие содержания утраченного документа проставленному грифу «КТ» и выявляет обстоятельства утраты (разглашения). По результатам работы комиссии составляется акт.

7.4.5. Обязанности сотрудников предприятия, работающих со сведениями, представляющими коммерческую тайну, и их ответственность за ее разглашение

Сотрудники предприятия, допущенные к сведениям, составляющим коммерческую тайну, несут ответственность за точ-

ное выполнение требований, предъявляемых к ним в целях обеспечения сохранности указанных сведений.

До получения доступа к работе, связанной с коммерческой тайной, им необходимо изучить требования настоящей инструкции и дать в службе безопасности письменное обязательство о сохранении коммерческой тайны.

Сотрудники предприятия, допущенные к коммерческой тайне, должны:

— строго хранить коммерческую тайну. О ставшей им известной утечке сведений, составляющих коммерческую тайну, а также об утрате документов с грифом «КТ» сообщать непосредственному руководителю и в службу безопасности;
— предъявлять для проверки по требованию представителей службы безопасности все числящиеся документы с грифом «КТ», а в случае нарушения установленных правил работы с ними представлять соответствующие объяснения;
— знакомиться только с теми документами и выполнять только те работы, к которым они допущены;
— строго соблюдать правила пользования документами, имеющими гриф «КТ», не допускать их необоснованной рассылки;
— все полученные в делопроизводстве службы безопасности или у ее уполномоченного документы с указанным грифом немедленно вносить во внутреннюю опись документов *(форма 55),* в которой отводится специальный раздел по учету «КТ»;
— исполненные входящие документы, а также документы, предназначенные для рассылки, подшивки в дело или уничтожения, сдавать в делопроизводство службы безопасности или уполномоченному службы безопасности;
— выполнять требования внутриобъектного режима, исключающие возможность ознакомления с документами «КТ» посторонних лиц, а также своих сотрудников, не имеющих к указанным документам прямого отношения;
— при ведении деловых переговоров с представителями сторонних организаций или частными лицами ограничиваться выдачей минимальной информации, действительно необходимой для их успешного завершения;
— исключить использование ставшей известной коммерческой тайны предприятия в свою личную пользу, а также деятельность, которая может быть использована конкурентами в ущерб предприятию - владельцу данной коммерческой тайны.

Ответственность за разглашение сведений, составляющих коммерческую тайну предприятия, и утрату документов или изделий, содержащих такие сведения, устанавливается в соответствии с действующим законодательством.

При этом подразумевается:

а) под разглашением сведений, составляющих коммерческую тайну, — предание огласке сведений лицом, которому эти сведения были доверены по службе, работе или стали известны иным путем, в результате чего они стали достоянием посторонних лиц;

б) под утратой документов или изделий (предметов), содержащих сведения, относящиеся к коммерческой тайне, — выход (в том числе и временный) документов или изделий из владения ответственного за их сохранность лица, которому они были доверены по службе или работе, являющийся результатом нарушения установленных правил обращения с ними, вследствие чего эти документы или изделия стали либо могли стать достоянием посторонних лиц.

Статья 183 УК РФ

Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну

1. Собирание сведений, составляющих коммерческую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом в целях разглашения либо незаконного использования этих сведений— наказывается штрафом в размере от 100 до 200 МРОТ или в размере заработной платы или иного дохода осужденного за период от одного до двух месяцев либо лишением свободы на срок до двух лет.

3. Незаконное разглашение или использование сведений, составляющих коммерческую или банковскую тайну, без согласия их владельца, совершенные из корыстной или иной личной заинтересованности и причинившие крупный ущерб — наказывается штрафом в размере от 200 до 500 МРОТ или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев либо лишением свободы на срок до трех лет со штрафом в размере 50 МРОТ или в размере заработной платы или иного дохода осужденного за период до одного месяца либо без такового.

7.4.6. Принципы организации и проведения контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну

Контроль за обеспечением режима при работе со сведениями, составляющими коммерческую тайну, осуществляется в целях изучения и оценки фактического состояния сохранноети коммерческой тайны, выявления недостатков и нарушений режима при работе с материалами с грифом «КТ», установления причин таких недостатков и нарушений и выработки предложений, направленных на их устранение и предотвращение.

Контроль за обеспечением режима при работе с материалами с грифом «КТ» осуществляют служба безопасности и руководители структурных подразделений.

Комиссия для проверки обеспечения режима при работе с материалами с грифом «КТ» комплектуется из опытных и квалифицированных работников в составе не менее двух человек, имеющих доступ к этой работе. Участие в проверке не должно приводить к необоснованному увеличению осведомленности проверяющих в этих сведениях.

Проверки обеспечения режима при работе с материалами с грифом «КТ» проводятся не реже одного раза в год комиссиями на основании предписания, подписанного директором или его заместителем по направлению.

Проверки проводятся в присутствии руководителя структурного подразделения или его заместителя.

Проверяющие имеют право знакомиться со всеми документами, журналами (карточками) учета и другими материалами, имеющими отношение к проверяемым вопросам, а также проводить беседы и консультации со специалистами и исполнителями, требовать предоставления письменных объяснений, справок, отчетов по всем вопросам, входящим в компетенцию комиссии.

По результатам проверок составляется акт (справка) с отражением в нем состояния режима при работе с материалами с грифом «КТ», выявленных недостатков и нарушений, предложений по их устранению.

С актом после утверждения его директором или заместителем под роспись знакомится руководитель структурного подразделения.

Об устранении выявленных в результате проверки недостатков и нарушений в режиме при работе с материалами «КТ» и реализации предложений руководитель подразделения в уста-

новленные комиссией сроки сообщает начальнику службы безопасности.

В случае установления факта утраты документов, дел и изданий с грифом «КТ» либо разглашения содержащихся в них сведений немедленно ставятся в известность директор, его заместители по направлениям и начальник отдела службы безопасности.

Для расследования факта утраты документов, дел и изданий с грифом «КТ» при установлении факта разглашения сведений, содержащихся в этих материалах, приказом директора (распоряжением руководителя структурного подразделения) назначается комиссия, заключение которой о результатах расследования утверждается руководителем, создавшим данную комиссию.

На утраченные документы, дела и издания с грифом «КТ» составляется акт. Соответствующие отметки вносятся в учетные документы.

Акты на утраченные дела постоянного хранения после их утверждения директором или его заместителями по направлениям передаются в архив.

7.5. Порядок проведения закрытых совещаний и переговоров

Разрешение на проведение совещаний и переговоров по вопросам, составляющим коммерческую тайну, имеют право давать руководители фирмы и лица, уполномоченные ими.

Руководитель, давший разрешение на проведение такого совещания (переговоров), назначает ответственного. Последний составляет список его участников с указанием фамилии, имени и отчества, должности и предприятия.

На совещание пропускаются только те лица, фамилии которых указаны в списке.

Проводящий совещание (переговоры) обязан напомнить участникам встречи о необходимости сохранения коммерческой тайны и уточнить конкретно, какие сведения являются охраняемыми. Это напоминание фиксируется в протоколе совещания (переговоров).

Совещания проводятся в специально отведенных для этого помещениях, исключающих возможность применения визуально-оптических, акустических и других технических средств,

которые могут быть использованы злоумышленниками как в самом помещении, так и за его пределами.

На каждом совещании, связанном с вопросами, составляющими коммерческую тайну, ведется протокол (письменный или магнитная запись), в котором фиксируются доклад, информация, выступления, вопросы, решения пофамильно.

Отдельные переговоры по вопросам коммерческих секретов оформляются в виде записи бесед.

Все материалы в копии передаются в группу обеспечения безопасности внешней деятельности СБ.

7.6. Организация архивного хранения конфиденциальных документов

Документы текущего делопроизводства по истечении года могут быть переданы на хранение в архив предприятия.

Оформление и передача дел с документами с грифом «КТ» осуществляются в соответствии с требованиями инструкции по организации хранения дел, содержащих конфиденциальную информацию, в архиве.

Инструкция по организации хранения дел отражает основные технические операции, в том числе:

— прием дел, содержащих конфиденциальную информацию, в архив;
— составление и оформление сводной описи дел, содержащих конфиденциальную информацию;
— составление и оформление сводной описи по личному составу;
— учет документов, содержащих конфиденциальную информацию.

ГЛАВА VIII

Отдел ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ

К основным средствам инженерно-технической защиты информации относятся:

- физические средства защиты;
- аппаратные средства защиты;
- программные средства защиты;
- математические (криптографические) методы защиты.

Указанные средства применяются для решения следующих задач:

- охраны территории и наблюдения за ней;
- охраны зданий, внутренних помещений и наблюдения за ними;
- охрана оборудования, хранилищ и перемещаемых носителей информации;
- осуществления контролируемого доступа в защищаемые зоны, охраняемые помещения и хранилища;
- создания препятствия визуальному наблюдению, подслушиванию и фотографированию;
- нейтрализации побочных электромагнитных излучений и наводок;
- исключения возможности перехвата электромагнитных излучений средств связи, обработки информации и электронно-вычислительной техники.

Для выполнения этих задач отдел инженерно-технической безопасности осуществляет организационные, организационно-технические и технические мероприятия.

8.1. Организационные мероприятия

К организационным мероприятиям относятся меры ограничительного характера, сводящиеся в основном к регламентации доступа и использования технических средств обеспече-

конфиденциальной информации в традиционных или автоматизированных режимах. Они, как правило, проводятся силами службы безопасности путем использования простейших организационных мер и доступных для этого технических средств.

Организационные мероприятия предусматривают:

- определение границ охраняемой зоны (территории);
- определение технических средств, используемых для обработки конфиденциальной информации в пределах охраняемой зоны (территории);
- определение опасных с точки зрения возможности образования каналов утечки информации или способов несанкционированного доступа к ней через технические средства;
- реализацию мер локализации или воспрещения возможных каналов утечки конфиденциальной информации или способов НСД к ней;
- организацию контроля (поиска и обнаружения) возможного неконтролируемого излучения опасных сигналов за счет побочных электромагнитных излучений и наводок (ПЭМИН) или специально используемых для этого сигналов; организацию строгого контроля прохода и проноса каких-либо предметов, устройств, средств, механизмов в контролируемую зону, способных представлять собой технические средства получения и передачи конфиденциальной информации.

8.2. Организационно-технические мероприятия

Организационно-технические мероприятия обеспечивают блокирование возможных каналов утечки информации через технические средства обеспечения производственной и трудовой деятельности с помощью специальных технических средств, устанавливаемых на элементы конструкции зданий, помещений и технических средств, потенциально образующих возможные каналы утечки информации.

Для этих целей возможно использование:

— технических средств пассивной защиты: фильтры, ограничители и т. п. средства развязки электрических и электромагнитных сигналов, системы защиты сетей электроснабжения, радио- и часофикации и др.;
— технических средств активной защиты: датчики акустических шумов и электромагнитных помех.

8.3. Технические мероприятия

Технические мероприятия обеспечивают приобретение, установку и использование в процессе производственной деятельности специальных, защищенных от побочных излучений и наводок, технических средств обработки конфиденциальной информации или средств, ПЭМИН которых не превышают норм на границе охраняемой территории.

Средства технической защиты:

- *Средства охраны*
  - — охранная и охранно-пожарная сигнализация
  - — охранное телевидение
  - — системы контроля доступа
  - — средства линейной безопасности
- *Средства защиты информации*
  - — средства обнаружения и выявления КУ в НСД
  - — средства защиты и противодействия
  - — средства системного исследования
- *Средства защиты программ*
  - — программные
  - — аппаратные
  - — комбинированные
- *Средства контроля*
  - — радиологические
  - — токсикологические
  - — пиротехнические
  - — металлообнаружители

8.4. Мероприятия по блокированию несанкционированного получения информации с помощью технических средств

Мероприятия по блокированию несанкционированного получения конфиденциальной информации с помощью технических средств сводятся к следующим основным направлениям:

- защита от наблюдения и фотографирования;
- защита от подслушивания;
- защита от перехвата.

Защита от наблюдения и фотографирования предполагает:

- выбор оптимального расположения средств документирования, размножения и отображения (экраны ПЭВМ) ин-

формации с целью исключения прямого или дистанционного наблюдения (фотографирования);

- использование светонепроницаемых стекол, занавесок, драпировок, пленок и других защитных материалов и конструкций (решетки, ставни, жалюзи и др.);
- выбор помещений, обращенных окнами в безопасные зоны, направления;
- использование программных средств гашения экранов ПЭВМ после определенного времени работы (работа по режиму времени).

Защита от подслушивания реализуется:

- применением звукопоглощающих облицовок, специальных тамбуров дверных проемов, двойных оконных переплетов;
- использованием средств акустического зашумления объемов и поверхностей (стены, окна, радиаторы отопления, вентиляционные каналы);
- закрытием вентиляционных каналов, систем ввода в помещения отопления, питания, телефонных и радиокоммуникаций, систем охранно-пожарной сигнализации;
- использованием специальных аттестованных помещений, исключающих появление каналов утечки конфиденциальной информации.

Защита от перехвата побочных электромагнитных излучений и наводок самого различного характера обеспечивается:

- размещением источников ПЭМИН на максимально возможном удалении от границы охраняемой (контролируемой) зоны;
- экранированием помещений, средств канальных коммуникаций;
- использованием пространственного и линейного электромагнитного зашумления;
- использованием автономных телефонных систем, локальных систем ЭВМ, не имеющих выхода за пределы охраняемой территории (в том числе систем вторичной часофикации, радиофикации, телефонных систем внутреннего пользования, диспетчерских систем, систем энергоснабжения и т. п.);
- развязкой по цепям питания и заземления, размещенным в границах охраняемой зоны;
- использованием подавляющих фильтров в информационных цепях, цепях питания и заземления.

8.5. Аттестация защищенных помещений

Аттестация защищаемых техническими мерами помещений имеет целью установить наличие в этих помещениях технических средств обеспечения производственной и трудовой деятельности и определить соответствие их характеристик требованиям безопасности.

На каждое такое помещение составляется технический паспорт, в котором указываются технические средства, их типы, номера, реальные технические характеристики и соединительные линии связи, питания, заземления и их состояние.

Технические паспорта помещений хранятся в группе инженерно-технической защиты. При установке или изъятии каких-либо технических средств обязательно внесение изменений в паспорт помещения.

Состав технических средств каждого помещения исследуется на наличие ПЭМИН группой инженерно-технической защиты самостоятельно или с привлечением специализированных организаций, имеющих на это лицензию, необходимую контрольно-измерительную аппаратуру и определенные методики проведения специальных исследований.

С учетом результатов анализа состава технических средств в защищаемых помещениях и результатов их специсследований устанавливается опасность тех или иных устройств как потенциальных источников образования каналов утечки охраняемых сведений, и вырабатываются целесообразные мероприятия по их локализации.

ЗАКЛЮЧЕНИЕ

Автор не претендовал на полное и всестороннее изложение всего множества вопросов, образующих проблему безопасности фирмы, и всех аспектов деятельности службы безопасности.

Важно своевременно уяснить факторы опасности, такие как нарастающая криминализация общества и необходимость противодействовать им. В настоящее время нет достаточного опыта защиты предпринимательских структур, в связи с чем многие рекомендации и правила еще предстоит выработать как на государственном, законодательном уровне, так и на уровне конкретной фирмы. Опыт приходит со временем. Необходимо также осознать, что не может быть готовых решений на все случаи жизни. Сегодня нужна готовность к систематической повседневной работе в данной области и постоянная, а не от случая к случаю озабоченность вопросами безопасности. Автор надеется, что данная книга поможет читателю определить свое отношение к данной проблеме и сделать практические выводы на основе приводимых рекомендаций. Желаем читателям безопасного бизнеса. Помните: безопасность лишней не бывает.

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ 1

Федеральный закон о государственной поддержке малого предпринимательства в Российской Федерации

Принят Государственной думой 12 мая 1995 года.

Настоящий федеральный закон направлен на реализацию установленного Конституцией Российской Федерации права граждан на свободное использование своих способностей и имущества для осуществления предпринимательской и иной не запрещенной законом экономической деятельности. Настоящий федеральный закон определяет общие положения в области государственной поддержки и развития малого предпринимательства в Российской Федерации, устанавливает формы и методы государственного стимулирования и регулирования деятельности субъектов малого предпринимательства. Настоящий федеральный закон действует на всей территории Российской Федерации в отношении всех субъектов малого предпринимательства независимо от предмета и целей их деятельности, организационно-правовых форм и форм собственности.

Статья 1. Законодательство Российской Федерации о государственной поддержке малого предпринимательства

1. Государственная поддержка малого предпринимательства в Российской Федерации осуществляется в соответствии с настоящим федеральным законом, издаваемыми в соответствии с ним иными федеральными законами, указами Президента Российской Федерации, постановлениями Правительства Российской Федерации, а также законами и иными нормативными правовыми актами субъектов Российской Федерации. Если

международным договором Российской Федерации установлены иные правила, чем предусмотренные настоящим федеральным законом, то применяются правила международного договора.

Статья 2. Разграничение полномочий между Российской Федерацией и субъектами Российской Федерации

1. Ведению Российской Федерации подлежат определение общих принципов, приоритетных направлений и методов государственной поддержки малого предпринимательства в Российской Федерации, установление порядка создания и деятельности федеральных органов государственной власти в области государственной поддержки малого предпринимательства, разработка и реализация федеральных программ развития и поддержки малого предпринимательства, финансируемых не менее чем на 50 процентов за счет средств федерального бюджета и специализированных внебюджетных фондов Российской Федерации, установление льгот для субъектов малого предпринимательства по федеральным налогам и иным платежам в федеральный бюджет и специализированные внебюджетные фонды Российской Федерации.

2. Субъекты Российской Федерации в соответствии со своими полномочиями решают все вопросы в области поддержки малого предпринимательства, в том числе могут применять дополнительные меры по поддержке малого предпринимательства за счет собственных средств и ресурсов.

Статья 3. Субъекты малого предпринимательства

1. Под субъектами малого предпринимательства понимаются коммерческие организации, в уставном капитале которых доля участия Российской Федерации, субъектов Российской Федерации, общественных и религиозных организаций (объединений), благотворительных и иных фондов не превышает 25 процентов, доля, принадлежащая одному или нескольким юридическим лицам, не являющимся субъектами малого предпринимательства, не превышает 25 процентов и в которых средняя численность работников за отчетный период не превышает следующих предельных уровней (малые предприятия):

в промышленности — 100 человек;
в строительстве — 100 человек;
на транспорте — 100 человек;
в сельском хозяйстве — 60 человек;

в научно-технической сфере — 60 человек;

в оптовой торговле — 50 человек;

в розничной торговле и бытовом обслуживании населения — 30 человек;

в остальных отраслях и при осуществлении других видов деятельности — 50 человек.

Под субъектами малого предпринимательства понимаются также физические лица, занимающиеся предпринимательской деятельностью без образования юридического лица. Малые предприятия, осуществляющие несколько видов деятельности (многопрофильные), относятся к таковым по критериям того вида деятельности, доля которого является наибольшей в годовом объеме оборота или годовом объеме прибыли.

2. Средняя за отчетный период численность работников малого предприятия определяется с учетом всех его работников, в том числе работающих по договорам гражданско-правового характера и по совместительству с учетом реально отработанного времени, а также работников представительств, филиалов и других обособленных подразделений указанного юридического лица.

3. В случае превышения малым предприятием установленной настоящей статьей численности указанное предприятие лишается льгот, предусмотренных действующим законодательством, на период, в течение которого допущено указанное превышение, и на последующие три месяца.

Статья 4. Государственная регистрация субъектов малогопредпринимательства

Субъект малого предпринимательства с момента подачи заявления установленного Правительством Российской Федерации образца регистрируется и получает соответствующий статус в органах исполнительной власти, уполномоченных действующим законодательством.

Субъекты Российской Федерации и органы местного самоуправления не вправе устанавливать дополнительные условия для регистрации субъектов малого предпринимательства по сравнению с условиями, установленными законами и иными нормативными правовыми актами Российской Федерации.

Уклонение от государственной регистрации субъектов малого предпринимательства или необоснованный отказ в государственной регистрации могут быть обжалованы в суде в установленном порядке с возмещением первоначально уплачен-

ной государственной пошлины истцу в случае решения в его пользу. Взыскание указанной пошлины производится с ответчика.

В случае признания судом незаконности действий органов регистрации последние возмещают расходы, перечисляемые на счет субъекта малого предпринимательства после его регистрации на основании решения суда.

Статья 5. Порядок представления отчетности малыми предприятиями

Государственная статистическая и бухгалтерская отчетность малых предприятий представляется в утверждаемом Правительством Российской Федерации порядке, предусматривающем упрощенные процедуры и формы отчетности, содержащие в основном информацию, необходимую для решения вопросов налогообложения.

Статья 6. Государственная поддержка малого предпринимательства

1. Государственная поддержка малого предпринимательства осуществляется по следующим направлениям:

формирование инфраструктуры поддержки и развития малого предпринимательства;

создание льготных условий использования субъектами малого предпринимательства государственных финансовых, материально-технических и информационных ресурсов, а также научно-технических разработок и технологий;

установление упрощенного порядка регистрации субъектов малого предпринимательства, лицензирования их деятельности, сертификации их продукции, представления государственной статистической и бухгалтерской отчетности;

поддержка внешнеэкономической деятельности субъектов малого предпринимательства, включая содействие развитию их торговых, научно-технических, производственных, информационных связей с зарубежными государствами;

организация подготовки, переподготовки и повышения квалификации кадров для малых предприятии.

2. Федеральные органы исполнительной власти в пределах своих полномочий при проведении политики, направленной на государственную поддержку малого предпринимательства:

разрабатывают предложения по совершенствованию законодательств Российской Федерации в области государственной поддержки малого предпринимательства;

проводят анализ состояния малого предпринимательства и эффективности применения мер по его государственной поддержке, подготавливают прогнозы развития малого предпринимательства и предложения по приоритетным направлениям и формам его государственной поддержки, представляют указанные предложения в Правительство Российской Федерации;

организуют разработку и реализацию Федеральной программы государственной поддержки малого предпринимательства, обеспечивают участие субъектов малого предпринимательства в реализации государственных программ и проектов, а также в поставках продукции и выполнении работ (услуг) для федеральных нужд;

подготавливают предложения об установлении для субъектов малого предпринимательства льгот по налогообложению и иных льгот, а также об использовании средств федерального бюджета и специализированных внебюджетных фондов Российской Федерации для поддержки малого предпринимательства;

оказывают содействие органам исполнительной власти субъектов Российской Федерации при разработке и реализации мер по поддержке малого предпринимательства;

координируют деятельность федеральных специализированных организаций с государственным участием, осуществляющих поддержку малого предпринимательства.

Статья 7. Государственные программы поддержки малого предпринимательства

1. Государственная поддержка малого предпринимательства осуществляется в соответствии с Федеральной программой государственной поддержки малого предпринимательства региональными (межрегиональными), отраслевыми (межотраслевыми) и муниципальными программами развития и поддержки малого предпринимательства, разрабатываемыми соответственно Правительством Российской Федерации, органами исполнительной власти субъектов Российской Федерации и органами местного самоуправления.

Правительство Российской Федерации ежегодно перед представлением федерального бюджета вносит на рассмотрение Федерального Собрания Российской Федерации проект федеральной программы государственной поддержки малого предпринимательства.

В федеральном бюджете ежегодно предусматривается выделение ассигнований на ее реализацию.

2. Государственные и муниципальные программы поддержки малого предпринимательства включают в себя следующие основные положения:

меры по формированию инфраструктуры развития и поддержки малого предпринимательства на федеральном, региональном и местном уровнях:

перспективные направления развития малого предпринимательства и приоритетные виды деятельности субъектов малого предпринимательства:

меры, принимаемые для реализации основных направлений и развития форм поддержки малого предпринимательства:

меры по вовлечению в предпринимательскую деятельность социально не защищенных слоев населения, в том числе инвалидов, женщин, молодежи, уволенных в запас (отставку) военнослужащих, безработных, беженцев и вынужденных переселенцев, лиц, вернувшихся из мест заключения;

предложения по установлению налоговых льгот и ежегодному выделению средств из соответствующих бюджетов на поддержку малого предпринимательства;

меры по обеспечению передачи субъектам малого предпринимательства результатов научно-исследовательских, опытно-конструкторских и технологических работ, а также инновационных программ;

меры по обеспечению передачи субъектам малого предпринимательства не завершенных строительством и пустующих объектов, а равно нерентабельных и убыточных предприятий на льготных условиях:

меры по обеспечению субъектам малого предпринимательства возможности для первоочередного выкупа арендуемых ими объектов недвижимости с учетом вложенных в указанные объекты средств.

Государственные программы поддержки малого предпринимательства разрабатываются в порядке, установленном действующим законодательством, и должны быть соотнесены с государственными программами содействия занятости населения, реализации миграционной политики, решения экологических проблем и ликвидации последствий чрезвычайных ситуаций.

3. Финансовое обеспечение государственных и муниципальных программ поддержки малого предпринимательства осуществляется ежегодно за счет средств федерального бюджета,

средств бюджетов субъектов Российской Федерации и средств местных бюджетов, а также за счет других источников, предусмотренных частью первой статьи 8 настоящего федерального закона.

Объем обязательных ежегодно выделяемых средств указывается в расходной части федерального бюджета отдельной строкой по представлению Правительства Российской Федерации.

Объем финансирования указанных программ за счет средств бюджетов субъектов Российской Федерации и средств местных бюджетов указывается в расходной части соответствующих бюджетов отдельной строкой по представлению органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления.

4. Предприятия, учреждения, организации независимо от организационно-правовой формы и формы собственности, общественные объединения вправе самостоятельно разрабатывать и реализовывать программы поддержки малого предпринимательства, создавать фонды поддержки малого предпринимательства, а также вносить предложения в органы исполнительной власти и органы местного самоуправления о включении отдельных проектов и мероприятий в государственные и муниципальные программы поддержки малого предпринимательства.

5. Правительство Российской Федерации ежегодно представляет в Государственную думу доклад о состоянии и развитии малого предпринимательства в Российской Федерации и мерах по его государственной поддержке, включая отчет об использовании средств федерального бюджета на цели государственной поддержки малого предпринимательства.

Статья 8. Фонды поддержки малого предпринимательства

1. Фондом поддержки малого предпринимательства является некоммерческая организация, создаваемая в целях финансирования программ, проектов и мероприятий, направленных на поддержку и развитие малого предпринимательства, путем аккумулирования бюджетных средств, средств, поступающих от приватизации государственного и муниципального имущества, доходов от собственной деятельности, добровольных взносов физических и юридических лиц, в том числе иностранных, доходов от выпуска и размещения ценных бумаг, а также доходов, получаемых по процентам от льготных кредитов, выде-

ленных на конкурсной основе субъектам малого предпринимательства.

Фонд поддержки малого предпринимательства является юридическим лицом.

Основными направлениями деятельности фонда поддержки малого предпринимательства являются:

содействие в формировании рыночных отношении на основе государственной поддержки малого предпринимательства и развития конкуренции путем привлечения и эффективного использования финансовых ресурсов для реализации целевых программ, проектов и мероприятий в области малого предпринимательства;

участие в разработке, проведении экспертизы и конкурсном отборе, а также в реализации федеральных, региональных (межрегиональных), отраслевых (межотраслевых) и муниципальных программ развития и поддержки малого предпринимательства, проектов в области малого предпринимательства, демонополизации экономики, развития конкуренции, насыщения товарного рынка, создания новых рабочих мест:

участие в формировании инфраструктуры рынка, обеспечивающей равные условия и возможности для осуществления деятельности в области малого предпринимательства:

поддержка инновационной деятельности предпринимательских структур, стимулирование разработки и производства принципиально новых видов продукции, содействие в освоении новых технологии и изобретении;

содействие в привлечении отечественных и иностранных инвестиций для реализации приоритетных направлений деятельности по созданию конкурентной среды и развитию малого предпринимательства;

организация консультаций по вопросам налогообложения и применения норм законодательства.

2. Финансовое обеспечение федеральной политики в области государственной поддержки малого предпринимательства осуществляет Федеральный фонд поддержки малого предпринимательства, создаваемый Правительством Российской Федерации.

Средства Федерального фонда поддержки малого предпринимательства формируются за счет средств федерального бюджета, а также за счет других источников, предусмотренных настоящей статьей.

Федеральный фонд поддержки малого предпринимательства является заказчиком Федеральной программы государственной поддержки малого предпринимательства.

Федеральный фонд поддержки малого предпринимательства может выступать гарантом по целевым иностранным кредитам, предоставляемым Российской Федерации на поддержку малого предпринимательства, а также по инвестиционным кредитам, предоставляемым кредитными организациями Российской Федерации субъектам малого предпринимательства на коммерческой основе для реализации конкретных программ и проектов в области малого предпринимательства.

Взаимодействие Федерального фонда поддержки малого предпринимательства, государственных и муниципальных фондов поддержки малого предпринимательства осуществляется на основе принципов равенства участников, взаимной экономической заинтересованности и ответственности.

Положение о Федеральном фонде поддержки малого предпринимательства (Устав) утверждается Правительством Российской Федерации.

3. Государственными и муниципальными, в том числе специализированными, фондами поддержки малого предпринимательства являются учрежденные уполномоченными на то федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации (органами местного самоуправления) фонды, в уставном капитале которых участие Российской Федерации, субъектов Российской Федерации, муниципальных образований составляет не менее 50 процентов. Доходы от деятельности Федерального фонда поддержки малого предпринимательства, государственных и муниципальных фондов поддержки малого предпринимательства остаются в их распоряжении, не подлежат налогообложению и направляются на реализацию целей и задач, предусмотренных в настоящем Федеральном законе.

Порядок выделения средств из государственных и муниципальных фондов поддержки малого предпринимательства и предоставления за счет этих средств гарантии субъектам малого предпринимательства устанавливается указанными фондами при наличии технико-экономических обоснований программ, проектов и мероприятий в области малого предпринимательства.

Государственные и муниципальные фонды поддержки малого предпринимательства имеют право на предоставление

субъектам малого предпринимательства льготных кредитов, беспроцентных ссуд, краткосрочных займов без приобретения лицензии на банковскую деятельность.

Задачи и функции государственных и муниципальных фондов поддержки малого предпринимательства определяются в их уставах, утверждаемых федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления, уполномоченными создавать такие фонды.

К основным задачам указанных фондов относятся:

предоставление финансовой помощи на возмездной и безвозмездной основе при осуществлении программ демонополизации, перепрофилирования производства в целях развития конкуренции и насыщения товарного рынка в соответствии с действующим законодательством;

выполнение функций залогодателя, поручителя, гаранта по обязательствам малых предприятий;

долевое участие в создании и деятельности хозяйствующих субъектов, обеспечивающих развитие инфраструктуры рынка, специализированных консультационных организаций и информационных систем поддержки малого предпринимательства и развития конкуренции, систем потребительской экспертизы и сертификации товаров и услуг;

финансирование мероприятий по подготовке, переподготовке и повышению квалификации кадров для малых предприятий, поддержке новых экономических структур, защите прав потребителей;

• финансирование научных исследований, научно-практических конференций, симпозиумов, совещаний, в том числе международных, связанных с деятельностью указанных фондов;

проведение мероприятий, направленных на привлечение и эффективное использование средств отечественных и иностранных инвесторов, в том числе проведение конкурсов, аукционов, выставок, лотерей, а также совершение операций с ценными бумагами в порядке, установленном действующим законодательством;

организация сбора, обработки правовой, патентно-лицензионной и иной информации, представляющей интерес для субъектов малого предпринимательства, изучение конъюнктуры внутреннего рынка, предоставление консультационной и организационно-методической помощи при разработке программ и проектов в области малого предпринимательства;

осуществление в установленном порядке внешнеэкономической деятельности, участие в международных программах и проектах в области малого предпринимательства.

4. Порядок направления в государственные (муниципальные) фонды поддержки малого предпринимательства средств из соответствующих бюджетов и порядок контроля за использованием указанных средств устанавливаются соответствующими органами представительной власти (органами местного самоуправления).

Статья 9. Налогообложение субъектов малого предпринимательства

1. Порядок налогообложения, освобождения субъектов малого предпринимательства от уплаты налогов, отсрочки и рассрочки их уплаты устанавливается в соответствии с налоговым законодательством.

В случае если изменения налогового законодательства создают менее благоприятные условия для субъектов малого предпринимательства по сравнению с ранее действовавшими условиями, то в течение первых четырех лет своей деятельности указанные субъекты подлежат налогообложению в том же порядке, который действовал на момент их государственной регистрации.

2. Законами Российской Федерации и законами субъектов Российской Федерации устанавливаются льготы по налогообложению субъектов малого предпринимательства, фондов поддержки малого предпринимательства, инвестиционных и лизинговых компании, кредитных и страховых организаций, а также предприятий, учреждений и организаций, создаваемых в целях выполнения работ для субъектов малого предпринимательства и оказания им услуг.

Статья 10. Ускоренная амортизация

Субъекты малого предпринимательства вправе применять ускоренную амортизацию основных производственных фондов с отнесением затрат на издержки производства в размере, в два раза превышающем нормы, установленные для соответствующих видов основных фондов.

Наряду с применением механизма ускоренной амортизации субъекты малого предпринимательства могут списывать дополнительно как амортизационные отчисления до 50 процентов первоначальной стоимости основных фондов со сроком службы до трех лет.

В случае прекращения деятельности малого предприятия до истечения одного года с момента ввода его в действие суммы дополнительно начисленной амортизации подлежат восстановлению за счет увеличения балансовой прибыли указанного малого предприятия.

Статья 11. Льготное кредитование субъектов малого предпринимательства

1. Кредитование субъектов малого предпринимательства осуществляется на льготных условиях с компенсацией соответствующей разницы кредитным организациям за счет средств фондов поддержки малого предпринимательства. При этом кредитные организации, осуществляющие кредитование субъектов малого предпринимательства на льготных условиях, пользуются льготами в порядке, установленном законодательством Российской Федерации и законодательством субъектов Российской Федерации.

2. Фонды поддержки малого предпринимательства вправе компенсировать кредитным организациям полностью или частично недополученные ими доходы при кредитовании субъектов малого предпринимательства на льготных условиях.

Размер, порядок и условия компенсации устанавливаются договором между кредитной организацией и соответствующим фондом поддержки малого предпринимательства.

Статья 12. Общества взаимного кредитования субъектов малого предпринимательства

1. Общества взаимного кредитования субъектов малого предпринимательства создаются для аккумулирования временно свободных денежных средств участников указанных обществ в целях оказания им финансовой помощи.

2. Общества взаимного кредитования субъектов малого предпринимательства:

вправе не размещать обязательные резервы в Центральном банке Российской Федерации;

могут поручать управление собственными ресурсами банку-депозитарию или иной кредитной организации;

определяю тразмер, периодичность и порядок внесения вкладов (взносов) участниками указанных обществ, а также предельные размеры, сроки и условия оказания им финансовой помощи;

не вправе предоставлять денежные средства физическим и юридическим лицам, которые не являются участниками указанных обществ.

Статья 13. Страхование субъектов малого предпринимательства

Страхование субъектов малого предпринимательства осуществляется на льготных условиях. При этом страховые организации, осуществляющие страхование субъектов малого предпринимательства, пользуются льготами в порядке, установленном действующим законодательством.

Фонды поддержки малого предпринимательства вправе компенсировать страховым организациям полностью или частично недополученные ими доходы при страховании на льготных условиях субъектов малого предпринимательства.

Размер, порядок и условия компенсации устанавливаются договором между страховой организацией и соответствующим фондом поддержки малого предпринимательства.

Статья 14. Участие субъектов малого предпринимательства в производстве продукции и товаров (услуг) для государственныхнужд

Правительство Российской Федерации, органы исполнительной власти субъектов Российской Федерации предусматривают резервирование для субъектов малого предпринимательства определенной доли заказов на производство и поставку отдельных видов продукции и товаров (услуг) для государственных нужд.

Государственные заказчики при формировании и размещении заказов и заключении государственных контрактов на закупку и поставки продукции и товаров (услуг) для государственных нужд по видам продукции, отнесенным Правительством Российской Федерации, органам исполнительной власти субъектов Российской Федерации к приоритетным, обязаны размещать у субъектов малого предпринимательства не менее 15 процентов от общего объема поставок для государственных нужд данного вида продукции на основе конкурсов на указанные поставки, проводимые между субъектами малого предпринимательства.

Статья 15. Поддержка внешнеэкономической деятельности субъектов малого предпринимательства

1. Федеральные органы исполнительной власти и органы исполнительной власти субъектов Российской Федерации осуществляют меры по расширению участия субъектов малого пред-

принимательства в экспортно-импортных операциях, а также осуществляют меры по участию этих субъектов в реализации программ и проектов в области внешнеэкономической деятельности, содействию их участию в международных выставках и ярмарках.

2. Размер, порядок и условия компенсации расходов, связанных с поддержкой внешнеэкономической деятельности, устанавливаются договором между субъектом малого предпринимательства и соответствующим государственным (муниципальным) фондом поддержки малого предпринимательства.

Статья 16. Поддержка субъектов малого предпринимательства в информационной сфере

1. Федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации и органы местного самоуправления разрабатывают и осуществляют меры по созданию соответствующей информационной инфраструктуры в целях получения субъектами малого предпринимательства экономической, правовой, статистической, производственно-технологической и иной информации, необходимой для их эффективного развития, и в целях обмена между ними указанной информацией.

2. Информационное обслуживание субъектов малого предпринимательства осуществляется на льготных условиях, предусмотренных действующим законодательством. При этом предприятия, учреждения и организации, предоставляющие информационные услуги субъектам малого предпринимательства, пользуются льготами в порядке, установленном действующим законодательством. "

3. Фонды поддержки малого предпринимательства вправе компенсировать субъектам малого предпринимательства полностью или частично расходы, связанные с информационным обслуживанием их деятельности.

4. Размер, порядок и условия компенсации устанавливаются договором между субъектом малого предпринимательства и соответствующим фондом поддержки малого предпринимательства.

Статья 17. Производственно-технологическая поддержка субъектов малого предпринимательства

1. Федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации и органы местного самоуправления разрабатывают и осуществляют комплекс мероприятий по содействию в обеспечении субъек-

тов малого предпринимательства современным оборудованием и технологиями, в создании сети технопарков, лизинговых фирм, бизнес-инкубаторов, производственно-технологических центров и других объектов инфраструктуры, создаваемых в целях поддержки субъектов малого предпринимательства.

2. Федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации и органы местного самоуправления осуществляют меры по размещению заказов на производство и поставки специализированного оборудования и иных видов продукции для субъектов малого предпринимательства, содействуют в создании и организации деятельности субъектов малого предпринимательства, специализированных оптовых рынков, ярмарок продукции субъектов малого предпринимательства, в том числе путем предоставления зданий, сооружений, оборудования, производственных и служебных помещений, иного имущества, находящихся в государственной или муниципальной собственности.

3. Производственно-технологическая поддержка субъектов малого предпринимательства может осуществляться на льготных условиях. При этом предприятия, учреждения и организации, осуществляющие производственно-технологическую поддержку субъектов малого предпринимательства, пользуются льготами в порядке, установленном действующим законодательством.

Статья 18. Поддержка субъектов малого предпринимательства в области подготовки, переподготовки и повышения квалификации кадров

Федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации и органы местного самоуправления обеспечивают развитие системы подготовки, переподготовки и повышения квалификации кадров для малого предпринимательства. Учреждения и организации, осуществляющие подготовку, переподготовку и повышение квалификации кадров для малого предпринимательства, пользуются льготами в порядке, установленном действующим законодательством.

Статья 19. Союзы (ассоциации) субъектов малого предпринимательства

1. Федеральные органы исполнительной власти субъектов Российской Федерации и органы местного самоуправления оказывают поддержку в организации и обеспечении деятель-

ности союзов (ассоциаций) субъектов малого предпринимательства, создаваемых в установленном порядке как общественные объединения в целях обеспечения наиболее благоприятных условий для развития малого предпринимательства, добросовестной конкуренции, повышения ответственности и компетентности субъектов малого предпринимательства, коллективной защиты их интересов в органах государственной власти.

2. Государственная поддержка союзов (ассоциаций) субъектов малого предпринимательства осуществляется путем содействия в обеспечении их на льготных условиях помещениями и средствами связи, необходимыми для деятельности указанных союзов (ассоциаций) и создаваемых ими предприятий, учреждений и организаций, а также для проведения организационных или публичных мероприятий, привлечения представителей союзов (ассоциаций) субъектов малого предпринимательства к подготовке проектов законов и иных нормативных правовых актов, программ социально-экономического развития субъектов Российской Федерации, предоставления возможностей для использования средств массовой информации в целях популяризации идей малого предпринимательства.

3. В целях совершенствования системы государственной поддержки малого предпринимательства, координации деятельности союзов (ассоциаций) субъектов малого предпринимательства из числа представителей органов государственной власти, союзов (ассоциаций) субъектов малого предпринимательства, общественных объединений предпринимателей при органах исполнительной власти Российской Федерации, органах исполнительной власти субъектов Российской Федерации и органах местного самоуправления могут создаваться советы по развитию малого предпринимательства, функции и полномочия которых определяются соответствующими органами исполнительной власти и органами местного самоуправления.

Статья 20. Некоммерческие объединения субъектов малого предпринимательства

В целях решения совместных задач, связанных с развитием и деятельностью субъектов малого предпринимательства, последние могут создавать некоммерческие объединения, которые вправе осуществлять производственную и иную предпринимательскую деятельность только для реализации своих уставных задач.

Статья 21. Приведение нормативных правовых актов в соответствие с настоящим федеральным законом

Нормативные акты Президента Российской Федерации, Правительства Российской Федерации, ведомственные нормативные правовые акты органов государственной власти субъектов Российской Федерации и органов местного самоуправления подлежат приведению в соответствие с настоящим федеральным законом в течение двух месяцев со дня его вступления в силу.

Статья 22. Переходные положения

Субъекты малого предпринимательства, зарегистрированные в любой организационно-правовой форме и относившиеся к категории малых предприятий до введения в действие настоящего Федерального закона, пользуются льготами, установленными для субъектов малого предпринимательства в полном объеме и в течение сроков, определенных действующим законодательством до введения в действие настоящего федерального закона.

Статья 23. Вступление в силу настоящего федерального закона

Настоящий федеральный закон вступает в силу со дня его официального опубликования.

ПРИЛОЖЕНИЕ 2.

Федеральный закон об упрощенной системе налогообложения, учета и отчетности для субъектов малого предпринимательства

Принят Государственной думой 8 декабря 1995 года.

Одобрен Советом Федерации 20 декабря 1995 года.

Настоящий федеральный закон определяет правовые основы введения и применения упрощенной системы налогообложения, учета и отчетности для субъектов малого предпринимательства — юридических лиц (далее — организаций) и физических лиц, осуществляющих предпринимательскую деятельность без образования юридического лица (далее — индивидуальные предприниматели).

Статья 1. Общие положения

1. Упрощенная система налогообложения, учета и отчетности для субъектов малого предпринимательства — органи-

заций и индивидуальных предпринимателей применяется наряду с принятой ранее системой налогообложения, учета и отчетности, предусмотренной законодательством Российской Федерации.

Право выбора системы налогообложения, учета и отчетности, включая переход к упрощенной системе или возврат к принятой ранее системе, предоставляется субъектам малого предпринимательства на добровольной основе в порядке, предусмотренном настоящим федеральным законом.

2. Применение упрощенной системы налогообложения, учета и отчетности организациями, подпадающими под действие настоящего федерального закона, предусматривает замену уплаты совокупности установленных законодательством Российской Федерации федеральных, региональных и местных налогов и сборов уплатой единого налога, исчисляемого по результатам хозяйственной деятельности организаций за отчетный период.

Для организаций, применяющих упрощенную систему налогообложения, учета и отчетности, сохраняется действующий порядок уплаты таможенных платежей, государственных пошлин, налога на приобретение автотранспортных средств, лицензионных сборов, отчислений в государственные социальные внебюджетные фонды.

3. Применение упрощенной системы налогообложения, учета и отчетности индивидуальными предпринимателями предусматривает замену уплаты установленного законодательством Российской Федерации подоходного налога на доход, полученный от осуществляемой предпринимательской деятельности, уплатой стоимости патента на занятие данной деятельностью (далее — патент).

4. Организациям, применяющим упрощенную систему налогообложения, учета и отчетности, предоставляется право оформления первичных документов бухгалтерской отчетности и ведения книги учета доходов и расходов по упрощенной форме, в том числе без применения способа двойной записи, плана счетов и соблюдения иных требований, предусмотренных действующим положением о ведении бухгалтерского учета и отчетности.

Упрощенная форма первичных документов бухгалтерской отчетности и ведения книги учета доходов и расходов устанавливается Министерством финансов Российской Федерации и является единой на всей территории Российской Федерации.

5. Для организации и индивидуальных предпринимателей, применяющих упрощенную систему налогообложения, учета и отчетности, сохраняется действующий порядок ведения кассовых операций и представления необходимой статистической отчетности.

Статья 2. Субъекты упрощенной системы налогообложения,учета и отчетности

1. Действие упрощенной системы налогообложения, учета и отчетности распространяется на индивидуальных предпринимателей и организации с предельной численностью работающих (включая работающих по договорам подряда и иным договорам гражданско-правового характера) до 15 человек независимо от вида осуществляемой ими деятельности.

Предельная численность работающих для организации включает численность работающих в их филиалах и подразделениях.

2. Под действие упрощенной системы налогообложения, учета и отчетности не подпадают организации, занятые производством подакцизной продукции, организации, созданные на базе ликвидированных структурных подразделений действующих предприятий, а также кредитные организации, страховщики, инвестиционные фонды, профессиональные участники рынка ценных бумаг, предприятия игорного и развлекательного бизнеса и хозяйствующие субъекты других категорий, для которых Министерством финансов Российской Федерации установлен особый порядок ведения бухгалтерского учета и отчетности.

3. Субъекты малого предпринимательства имеют право в предусмотренном настоящим федеральным законом порядке перейти на упрощенную систему налогообложения, учета и отчетности, если в течение года предшествующего кварталу, в котором произошла подача заявления на право применения упрощенной системы налогообложения, учета и отчетности, совокупный размер валовой выручки данного налогоплательщика не превысил суммы стотысячекратного минимального размера оплаты труда, установленного законодательством Российской Федерации на первый день квартала, в котором произошла подача заявления.

Вновь созданная организация или вновь зарегистрированный индивидуальный предприниматель, подавшие заявление на право применения упрощенной системы налогообложения, учета и отчетности, считаются субъектами упрощенной систе-

мы налогообложения, учета и отчетности с того квартала, и котором произошла их официальная регистрация.

Статья 3. Объекты налогообложения организаций и упрощенной системы налогообложения, учета и отчетности

1. Объектом обложения единым налогом организации в упрощенной системе налогообложения, учета и отчетности устанавливается совокупный доход, полученный за отчетный период (квартал), или валовая выручка, полученная за отчетный период. Выбор объекта налогообложения осуществляется органом государственной власти субъекта Российской Федерации.

2. Совокупный доход исчисляется как разница между валовой выручкой и стоимостью использованных в процессе производства товаров (работ, услуг) сырья, материалов, комплектующих изделий, приобретенных товаров, топлива, эксплуатационных расходов, текущего ремонта, затрат на аренду помещений, используемых для производственной и коммерческой деятельности, затрат на аренду транспортных средств, расходов на уплату процентов за пользование кредитными ресурсами банков (в пределах действующей ставки рефинансирования Центрального банка Российской Федерации плюс 3 процента), оказанных услуг, а также сумм налога на добавленную стоимость, уплаченных поставщикам, налога на приобретение автотранспортных средств, отчислений в государственные социальные внебюджетные фонды, уплаченных таможенных платежей, государственных пошлин и лицензионных сборов.

3. Валовая выручка исчисляется как сумма выручки, полученной от реализации товаров (работ, услуг), продажной цены имущества, реализованного за отчетный период, и внереализационных доходов.

Статья 4. Ставки единого налога

1. Для субъектов малого предпринимательства, применяющих упрощенную систему налогообложения, учета и отчетности, устанавливаются следующие ставки единого налога на совокупный доход, подлежащего зачислению:

в федеральный бюджет — в размере 10 процентов от совокупного дохода:

в бюджет субъекта Российской Федерации и местный бюджет — в суммарном размере не более 20 процентов от совокупного дохода.

В случае, когда объектом налогообложения для субъектов малого предпринимательства определенных категорий является валовая выручка, устанавливаются следующие ставки единого налога, подлежащего зачислению:

в федеральный бюджет — в размере 3,33 процента от суммы валовой выручки:

в бюджет субъекта Российской Федерации и местный бюджет — в размере не более 6,67 процента от суммы валовой выручки.

Годовая стоимость патента, уплаченная индивидуальными предпринимателями, направляется полностью в бюджет субъекта Российской Федерации.

2. Конкретные ставки единого налога в зависимости от вида осуществляемой деятельности субъектов малого предпринимательства, а также пропорции распределения зачисляемых налоговых платежей между бюджетом субъекта Российской Федерации и местным бюджетом устанавливаются решением органа государственной власти субъекта Российской Федерации.

3. Органы государственной власти субъектов Российской Федерации вместо объектов и ставок налогообложения, предусмотренных статьями 3 и 4 настоящего федерального законв, вправе устанавливать для организаций в зависимости от вида осуществляемой ими деятельности:

расчетный порядок определения единого налога на основе показателей по типичным организациям-представителям. При этом суммы единого налога, подлежащие уплате организациями за отчетный период, не могут быть ниже определенных расчетным путем, а порядок их распределения между бюджетами всех уровней должен соответствовать нормам, установленным настоящим федеральным законом:

льготы и (или) льготный порядок по уплате единого налога для отдельных категорий плательщиков в пределах объема налоговых поступлений, подлежащих зачислению в бюджет субъекта Российской Федерации и местный бюджет.

Статья 5. Порядок применения упрощенной системы налогообложения, учета и отчетности

1. Официальным документом, удостоверяющим право применения субъектами малого предпринимательства упрощенной системы налогообложения, учета и отчетности, является патент, выдаваемый сроком на один календарный год налоговы-

ми органами по месту постановки организаций и индивидуальных предпринимателей на налоговый учет.

Форма патента устанавливается Государственной налоговой службой Российской Федерации и является единой на всей территории Российской Федерации.

2. Годовая стоимость патента для субъектов малого предпринимательства, подпадающих под действие нас настоящего Федерального закона, устанавливается с учетом ставок единого налога решением органа государственной власти субъекта Российской Федерации в зависимости от вида деятельности.

Выплата годовой стоимости патента осуществляется организациями и индивидуальными предпринимателями ежеквартально с распределением платежей, устанавливаемым органом государственной власти субъекта Российской Федерации. Оплата стоимости патента засчитывается в счет обязательства по уплате единого налога организации.

3. Для организаций, применяющих упрощенную систему налогообложения, учета и отчетности, уплачиваемая годовая стоимость патента зачисляется в федеральный бюджет, а также в бюджеты субъектов Российской Федерации и местные бюджеты в соотношении один к двум.

Для индивидуальных предпринимателей уплачиваемая годовая стоимость патента является фиксированным платежом, заменяющим уплату единого налога на доход за отчетный период.

4. Организациям и индивидуальным предпринимателям патент выдастся налоговыми органами по месту их постановки на налоговый учет на основе письменного заявления, подаваемого на позднее чем за один месяц до начала очередного квартала, при соблюдении следующих условий:

если общее число работников, занятых в организации, не превышает предельной численности, установленной в соответствии с настоящим федеральным законом;

если организация не имеет просроченной задолженности по уплате налогов и иных обязательных платежей за предыдущий отчетный период;

если организацией своевременно сданы необходимые расчеты по налогам и бухгалтерская отчетность за предыдущий отчетный период.

Филиалы и подразделения, являющиеся налогоплательщиками, представляют в налоговый орган по месту постановки на налоговый учет нотариально заверенные копии патентов, выданных организации, не позднее чем за 15 дней до начала очередного квартала.

5. Решение о переходе организации или индивидуального предпринимателя на упрощенную систему налогообложения, учета и отчетности или мотивированный отказ от этого выносится налоговым органом в пятнадцатидневный срок со дня подачи заявления организацией или индивидуальным предпринимателем.

6. При получении патента в налоговом органе организация или индивидуальный предприниматель предъявляет для регистрации книгу учета доходов и расходов, в которой указываются наименование организации (фамилия, имя, отчество индивидуального предпринимателя), вид осуществляемой деятельности (только для индивидуальных предпринимателей), местонахождение, номера расчетных и иных счетов, открытых в учреждениях банков. Налоговый орган на первой странице книги учета доходов и расходов фиксирует регистрационный номер патента и дату его выдачи. При выдаче патента заполняется также и его дубликат, который хранится в налоговом органе.

По истечении срока действия патента по заявлению организации или индивидуального предпринимателя налоговый орган выдает патент на очередной (годичный) срок действия с регистрацией новой книги учета доходов и расходов.

На патент и книгу учета доходов и расходов распространяются правила обращения с отчетностью, установленные действующими нормативными актами Российской Федерации.

При утрате патента он подлежит возобновлению налоговым органом с соблюдением указанных в настоящей статье условий и наложением на организацию или индивидуального предпринимателя штрафа, размер которого устанавливается органом государственной власти субъекта Российской Федерации.

Форма книги учета доходов и расходов и порядок отражения хозяйственных операций субъектами малого предпринимательства, применяющими упрощенную систему налогообложения, учета и отчетности, устанавливаются Министерством финансов Российской Федерации.

7. По итогам хозяйственной деятельности за отчетный период (квартал) организация представляет в налоговый орган в срок до 20-го числа месяца, следующего за отчетным периодом, расчет подлежащего уплате единого налога с зачетом оплаченной стоимости патента, а также выписку из книги доходов и расходов (по состоянию на последний рабочий день отчетного периода) с указанием: совокупного дохода (валовой выручки), полученного за отчетный период.

При представлении в налоговый орган указанных документов организация предъявляет для проверки патент, книгу учета доходов и расходов, кассовую книгу, а также платежные поручения об уплате единого налога за отчетный период (с отметкой банка об исполнении платежа).

При превышении определенной настоящим федеральным законом предельной численности работающих налогоплательщики переходят на принятую ранее систему налогообложения, учета и отчетности начиная с квартала, следующего за кварталом, в котором должен быть представлен отчет согласно пункту 7 настоящей статьи.

8. Отказ от применения упрощенной системы налогообложения, учета и отчетности и обратный переход (возврат) к принятой ранее системе налогообложения, учета и отчетности могут осуществляться субъектами малого предпринимательства с начала очередного календарного года при условии подачи соответствующего заявления в налоговый орган в срок не позднее чем за 15 дней до завершения календарного года.

Статья 6. Ответственность субъектов малого предпринимательства, применяющих упрощенную систему налогов

Ответственность субъектов малого предпринимательства, применяющих упрощенную систему налогообложения, учета и отчетности, наступает в соответствии с Законом Российской Федерации «Об основах налоговой системы в Российской Федерации» и другими законодательными актами Российской Федерации.

ПРИЛОЖЕНИЕ 3

Примерный перечень сведений, составляющих коммерческую тайну

1. Производство

Сведения о структуре и масштабах производства, производственных мощностях, типе и размещении оборудования, запасах сырья, материалов, комплектующих и готовой продукции.

2. Управление

Сведения о применяемых оригинальных методах управления предприятием.

Сведения о подготовке, принятии и исполнении отдельных решений руководства предприятия по коммерческим, организационным, производственным, научно-техническим и иным вопросам.

3. Планы

Сведения о планах расширения или свертывания производства различных видов продукции и их технико-экономических обоснованиях.

Те же сведения о планах инвестиций, закупок и продаж.

4. Совещания

Сведения о фактах проведения, целях, предмете и результатах совещаний и заседаний органов управления предприятия.

5. Финансы

Сведения о кругообороте средств предприятия.

Сведения о финансовых операциях предприятия.

Сведения о состоянии банковских счетов предприятия и проводимых операциях.

Сведения об уровне доходов предприятия.

Сведения о долговых обязательствах предприятия.

Сведения о состоянии кредита предприятий (пассивы и активы).

Главная книга предприятия.

6. Рынок

Сведения о применяемых предприятием оригинальных методах изучения рынка.

Сведения о результатах изучения рынка, содержащие оценки состояния и перспектив развития рыночной конъюнктуры.

Сведения о рыночной «стратегии предприятия.

Сведения о применяемых предприятием оригинальных методах осуществления продаж.

Сведения об эффективности коммерческой деятельности предприятия.

7. Партнеры

Систематизированные сведения о внутренних и зарубежных заказчиках, подрядчиках, поставщиках, потребителях, покупателях, компаньонах, спонсорах, посредниках, клиентах и других партнерах деловых отношений предприятия.

8. Конкуренты

Систематизированные сведения о внутренних и зарубежных предприятиях как потенциальных конкурентах в деятельности предприятия, оценки качества деловых отношений с конкурирующими предприятиями в различных сферах деловой активности.

9. Переговоры

Сведения о подготовке, проведении и результатах переговоров с деловыми партнерами предприятия.

10. Контракты

Сведения, условие конфиденциальности которых установлено в договорах, контрактах, соглашениях и других обязательствах предприятия.

11. Цены

Сведения о методах расчета, структуре, уровне реальных цен на продукцию и размеры скидок.

12. Торги, аукционы

Сведения о подготовке к участию в торгах и аукционах, участии и результатах приобретения или продажи товаров.

13. Наука и техника

Сведения о целях, задачах, программах перспективных научных исследований.

Ключевые идеи научных разработок.

Точные значения конструкционных характеристик создаваемых изделий и оптимальных параметров разрабатываемых технологических процессов (размеры, объемы, конфигурация, процентное содержание компонентов, температура, давление, время и т. д.).

Аналитические и графические зависимости, отражающие найденные закономерности и взаимосвязи.

Данные об условиях экспериментов и оборудовании, на котором они проводились.

Сведения о материалах, из которых изготовлены отдельные детали.

Сведения об особенностях конструкторско-технологического, художественно-технического решения изделия, дающие положительный экономический эффект.

Сведения о методах защиты от подделки товарных и фирменных знаков.

Сведения о состоянии парка ЭВМ и программного обеспечения.

14. Технология

Сведения об особенностях используемых и разрабатываемых технологий и специфике их применения.

Сведения об условиях производства и транспортировки продукции.

15. Безопасность

Сведения о порядке и состоянии организации защиты коммерческой тайны.

Сведения о порядке и состоянии организации охраны, пропускном режиме, системе сигнализации.

Сведения, составляющие коммерческую тайну предприятия, предприятий-партнеров и переданные на доверительной основе.

ПРИЛОЖЕНИЕ 4

Обеспечение сохранения коммерческой тайны предприятия

Введение

Важными источниками конфиденциальной информации являются люди, документы и публикации. От того, как организована работа с людьми и документами, зависит и безопасность предприятия. Целям предотвращения нанесения экономического, финансового и материального ущерба предприятию (организации), вызванного неправомерными или неосторожными действиями, а также неквалифицированным обращением или разглашением коммерческой тайны, служат настоящие предложения.

Предложения по обеспечению коммерческой тайны носят общий рекомендательный характер, не являются нормативным документом, ориентированы в основном на работу с документами, содержащими сведения коммерческого характера, и предусматривают главным образом организационные меры защиты коммерческих секретов.

При подготовке данного пособия были использованы материалы и опыт государственных и коммерческих структур по защите информации.

/. Общие положения

1.1. Под коммерческой тайной понимаются не являющиеся государственными секретами сведения, связанные с производственно-технической, научно-исследовательской, опытно-конструкторской и другой деятельностью предприятия, а также с их технологической информацией, управлением, финансами и др., разглашение, утечка или неправомерное овладение которыми может нанести ущерб его интересам.

1.2. К сведениям, составляющим коммерческую тайну, относятся несекретные сведения, предусмотренные «Перечнем конкретных сведений, составляющих коммерческую тайну», утвержденным и введенным в действие приказом директора предприятия.

Коммерческая тайна является собственностью предприятия. Если коммерческая тайна является результатом совместной деятельности с. другими предприятиями, основанной на договорных началах, то коммерческая тайна может быть соб-

ственностью двух сторон. Это обстоятельство должно найти отражение в договоре.

Примечание. Единой установки на обозначение грифа ограничения доступа к документу, содержащему коммерческую тайну, нет, таким грифом может быть «коммерческая тайна». На других предприятиях могут быть: «коммерческая тайна», «секрет предприятия», «тайна предприятия» и др. Такой ограничительный гриф не является грифом секретности, а лишь показывает, что право собственности на данную информацию охраняется законодательством.

1.3. Под разглашением коммерческой тайны имеются в виду противоправные, умышленные или неосторожные действия должностных или иных лиц, приведшие к преждевременному, не вызванному служебной необходимостью оглашению охраняемых сведений, подпадающих под эту категорию, а также передача таких сведений по открытым техническим каналам или обработка их на некатегорированных ЭВМ.

1.4. Под открытым опубликованием вышеуказанных сведений имеется в виду публикация материалов в открытой печати, передача по радио и телевидению, оглашение на международных, зарубежных и открытых внутренних съездах, конференциях, совещаниях, симпозиумах, при публичной защите диссертаций и других публичных выступлениях, свободная рассылка, вывоз материалов за границу или передача их в любой форме иностранным фирмам, организациям или отдельным лицам вне сферы прямых служебных обязанностей.

1.5. Необходимость и возможность открытого опубликования этих сведений, а также их объемы, формы и время опубликования определяются директором или его заместителями по направлениям по заключению постоянно действующей экспертной комиссии.

1.6. Меры по ограничению открытых публикаций коммерческой информации не могут быть использованы во вред принципу гласности и для сокрытия от общественности фактов бесхозяйственности, расточительства, недобросовестной конкуренции и других негативных явлений.

Использование для открытого опубликования сведений, полученных на договорной или доверительной основе или являющихся результатом совместной производственной деятельности, допускается лишь с общего согласия партнеров.

1.7. Передача информации сторонним организациям, не связанным прямыми служебными контактами, должна регулироваться, как правило, договорными отношениями, предусматривающими обязательства и ответственность пользователей, включая возмещение материальных затрат на предоставление информации и компенсацию за нарушение договорных обязательств.

1.8. Предоставление коммерческой информации представителям служебных, ревизионных, фискальных и следственных органов, народным депутатам, органам печати, радио регулируется соответствующими положениями.

1.9. Тиражированные документы и издания с грифом «коммерческая тайна» рассматриваются как материалы, содержащие сведения ограниченного распространения.

1.10. Ответственность за обеспечение режима при работе с материалами с грифом «КТ», своевременную разработку и осуществление необходимых мероприятий по сохранению коммерческой тайны возлагается на директора, его заместителей по направлениям и руководителей структурных подразделений. Ответственность за организацию и осуществление работы по защите коммерческой тайны и проведение постоянного контроля за ее соблюдением возлагается на службу безопасности.

Служба безопасности принимает меры по сохранению коммерческой тайны путем максимального ограничения круга лиц, физической сохранности документов, содержащих такие сведения, обработки информации с грифом «КТ» на защищенных ЭВМ, внесения требований по конфиденциальности конкретной информации в договоры с внутренними и внешнеторговыми партнерами и других мер по решению руководства.

1.11. Защита коммерческой тайны предусматривает:

порядок определения информации, содержащей коммерческую тайну, и сроков ее действия;

систему допуска сотрудников, командированных и частных лиц к сведениям, составляющим коммерческую тайну;

порядок работы с документами с грифом «КТ»;

обеспечение сохранности документов, дел и изданий с грифом «КТ»;

обязанности лиц, допущенных к сведениям, составляющим коммерческую тайну;

принципы организации и проведения контроля за обеспечением режима при работе со сведениями, составляющими коммерческую тайну;

ответственность за разглашение сведений, утрату документов, содержащих коммерческую тайну.

1.12. Контроль за осуществлением учета, размножением, хранением и использованием документов, дел и изданий с грифом «КТ» возлагается на уполномоченных службы безопасности.

1.13. Контроль за неразглашением сведений, содержащихся в документах, делах и изданиях с грифом «КТ», осуществляется отделами службы безопасности.

2. Порядок определения информации, содержащей коммерческую тайну, и сроков ее действия

2.1. Определение необходимости проставления грифа «коммерческая тайна» производится на основании перечня, указанного в п. 1.2: на документе — исполнителем и лицом, подписывающим документ, а на издании — автором (составителем) и руководителем, утверждающим издание к печати.

2.2. Срок действия коммерческой тайны, содержащейся в документе, определяется в каждом конкретном случае исполнителем или лицом, подписавшим документ, в виде конкретной даты, или «до заключения контракта», или «бессрочно».

2.3. На документах, делах и изданиях, содержащих сведения, составляющие коммерческую тайну, проставляется гриф «коммерческая тайна», а на документах и изданиях, кроме того, — номера экземпляров.

Гриф «коммерческая тайна» и номер экземпляра проставляются в правом верхнем углу первой страницы документа, на обложке, титульном листе издания и на первой странице сопроводительного письма к этим материалам.

На обратной стороне последнего листа каждого экземпляра документа, содержащего коммерческую тайну, печатается разметка, в которой указывается: количество отпечатанных экземпляров, номер, фамилия исполнителя и его телефон, дата, срок действия коммерческой тайны, содержащейся в документе (конкретная дата, «до заключения контракта», или «бессрочно»), фамилия машинистки.

2.4. Решение вопроса о снятии грифа «коммерческая тайна» возлагается на создаваемую в установленном порядке специальную комиссию, в состав которой включаются представители службы безопасности и соответствующих структурных подразделений.

Решение комиссии оформляется составляемым в произвольной форме актом, который утверждается директором или

его заместителем по направлению. В акте перечисляются дела, с которых гриф «КТ» снимается. Один экземпляр акта вместе с делами передается в архив, а на дела постоянного хранения — в государственный архив.

2.5. На обложках дел гриф «КТ» погашается штампом или записью от руки с указанием даты и номера акта, послужившего основанием для его снятия.

Аналогичные отметки вносятся в описи и номенклатуры дела.

3. Система допуска сотрудников, командированных и частных лиц к сведениям, составляющим коммерческую тайну

3.1 .Допуск сотрудников к сведениям, составляющим коммерческую тайну, осуществляется директором, его заместителями по направлениям и руководителями структурных подразделений.

Руководители подразделений и службы безопасности ответственны за подбор лиц, допускаемых к сведениям с грифом «КТ», обязаны обеспечить систематический контроль за тем, чтобы к этим сведениям получали доступ только те лица, которым такие сведения необходимы для выполнения своих служебных обязанностей.

3.2. К сведениям, составляющим коммерческую тайну, допускаются лица, обладающие необходимыми высоконравственными и деловыми качествами, способные хранить коммерческую тайну, и только после оформления в службе безопасности индивидуального письменного обязательства по сохранению коммерческой тайны.

3.3. Допуск сотрудников к работе с делами с грифом «КТ», имеющих к ним непосредственное отношение, производится в соответствии с оформленным на внутренней стороне обложки списком за подписью руководителя структурного подразделения, а к документам — согласно указаниям, содержащимся в резолюциях руководителей подразделений.

3.4. Командированные и частные лица допускаются к ознакомлению и работе с документами и изданиями с грифом «КТ» с письменного разрешения руководителей предприятия и подразделений, в ведении которых находятся эти материалы, при наличии письменного запроса тех организаций, в которых они работают, с указанием темы и объема выполняемого задания, а также предписания на выполнение задания.

Выписки из документов и изданий, содержащих сведения с грифом «КТ», производятся в тетрадях, имеющих такой же гриф, и после окончания работы представителя высылаются в адрес организации.

3.5. Дела и издания с грифом «КТ» выдаются исполнителям и принимаются от них под расписку в «Карточке учета выдаваемых дел и изданий» (форма 4).

4. Порядок работы с документами с грифом «КТ»

4.1. Документы, содержащие сведения, составляющие коммерческую тайну, подлежат обязательной регистрации в канцелярии службы безопасности или в общем делопроизводстве подразделения уполномоченным службы безопасности. Они должны иметь реквизиты, предусмотренные п. 2.3, и гриф «КТ» (или полностью «коммерческая тайна»). На документах, передаваемых иностранцам, гриф «КТ» не проставляется. Полученные от иностранцев документы маркируются грифом «КТ» графитным карандашом.

В тексте документа и его реквизитах дополнительно могут оговариваться права на информацию, порядок пользования ею, сроки ограничения на публикацию и др.

Отсутствие грифа «КТ» и предупредительных оговорок в тексте и реквизитах означает свободную рассылку и предполагает, что автор информации и должностное лицо, санкционирующее (подписавшее, утверждавшее документ) ее распространение, предусмотрели все возможные последствия от свободной рассылки и несут за это всю полноту ответственности.

4.2. Вся поступающая корреспонденция с грифом «КТ» или другими грифами, указанными в п. 1.2, принимается и вскрывается сотрудниками канцелярии, которым поручена работа с этими материалами. При этом проверяется количество листов и экземпляров документов и изданий, а также наличие указанных в сопроводительном письме приложений.

В случае отсутствия в конвертах (пакетах) документов «КТ» или приложений к ним составляется акт в двух экземплярах, один из которых отправляется адресанту.

4.3. Регистрации подлежат все входящие, исходящие и внутренние документы, а также издания с грифом «КТ». Такие документы учитываются по количеству листов, а издания (книги, журналы, брошюры) — поэкземплярно.

4.4. Учет документов и изданий с грифом «КТ» ведется в журналах (форма 1) или на карточках (форма 2) отдельно от учета другой несекретной документации.

Листы журналов нумеруются, прошиваются и опечатываются. Издания, которые не подшиваются в дела, учитываются в журнале инвентарного учета (форма 5).

Движение документов и изданий с грифом «КТ» должно своевременно отражаться в журналах или на карточках.

4.5. На каждом зарегистрированном документе, а также на сопроводительном листе к изданиям с грифом «КТ» проставляется штамп, в котором указываются наименование, регистрационный номер документа и дата его поступления.

4.6. Тираж издания с грифом «КТ», полученный для рассылки, регистрируется под одним входящим номером в журнале учета и распределения изданий (форма 3).

Дополнительно размноженные экземпляры документа (издания) учитываются за номером этого документа (издания), о чем делается отметка на размножаемом документе (издании) и в учетных формах. Нумерация дополнительно размноженных экземпляров производится от последнего номера ранее учтенных экземпляров.

4.7. Печатание материалов с грифом «КТ» производится в бюро оформления технической документации или в структурных подразделениях под ответственность их руководителей.

4.8. Отпечатанные и подписанные документы с грифом «КТ» вместе с их черновиками и вариантами передаются для регистрации сотруднику канцелярии, осуществляющему их учет. Черновики и варианты уничтожаются этим сотрудником с подтверждением факта уничтожения записью на копии исходящего документа: «Черновик (и варианты) уничтожены». Дата. Подпись.

4.9. Размножение документов и изданий с грифом «КТ» в типографиях и на множительных аппаратах производится с разрешения службы безопасности и под контролем канцелярии по заказам, подписанным руководителем подразделения и утвержденным заместителем директора по направлению. Учет размноженных документов и изданий осуществляется поэкземплярно в специальном журнале.

4.10. Рассылка документов и изданий с грифом «КТ» осуществляется на основании подписанных руководителем структурного подразделения разнарядок с указанием учетных номеров отправляемых экземпляров.

4.11. Документы с грифом «КТ» после исполнения группируются в отдельные дела. Порядок их группировки предусматривается номенклатурами дел несекретного делопроизводства.

В номенклатуру дел в обязательном порядке включаются все справочные картотеки и журналы и издания с грифом «КТ».

4.12. При пользовании открытой радиосвязью запрещается передавать сведения, имеющие гриф «КТ». Такие сведения могут передаваться только по закрытым техническим средствам связи или по открытой телетайпной связи с проставлением на документах и телеграммах соответствующего штампа.

При пользовании проводной связью запрещается указывать должности адресатов, отправителей, разрешается указывать только телеграфные адреса и фамилии отправителей и получателей.

4.13. Снятие копий (рукописных, машинописных, микро- и фотокопий, электрографических и др.), а также производство выписок из документов и изданий с грифом «КТ» сотрудниками производится по разрешению руководителей подразделений.

Снятие копий для сторонних организаций с документов и изданий с грифом «КТ» производится на основании письменных запросов по разрешению руководителей подразделений, подготовивших эти документы и издания.

Аналогично отметки вносятся в описи и номенклатуры дел.

4.14. Порядок работы на ЭВМ при обработке информации с грифом «КТ» осуществляется в соответствии с требованиями «Инструкции о порядке работы на ПЭВМ при обработке несекретной информации».

5. Обеспечение сохранности документов, дел и изданий

5.1. Документы, дела и издания с грифом «КТ» должны храниться в служебных помещениях и библиотеках в надежно запираемых и опечатываемых шкафах (хранилищах). При этом должны быть созданы надлежащие условия, обеспечивающие их физическую сохранность.

5.2. Выданные для работы дела с грифом «КТ» подлежат возврату в канцелярию или уполномоченному службы безопасности в тот же день.

Отдельные дела с грифом «КТ» с разрешения начальника канцелярии или уполномоченного службы безопасности могут находиться у исполнителя в течение срока, необходимого для выполнения задания, при условии полного обеспечения их сохранности и соблюдения правил хранения.

5.3. Передача документов, дел и изданий с грифом «КТ» другим сотрудникам, допущенным к этим документам, произво-

дится только через канцелярию или уполномоченного службы безопасности.

5.4. Запрещается изъятие из дел или перемещение документов с грифом «КТ» из одного дела в другое без санкции канцелярии или уполномоченного службы безопасности, осуществляющего их учет. Обо всех проведенных изъятиях или перемещениях делаются отметки в учетных документах, включая внутренние описи.

5.5. Запрещается выносить документы, дела и издания с грифом «КТ» из служебных помещений для работы с ними дома, в гостиницах и др.

В необходимых случаях директор, его заместители по направлениям или руководители структурных подразделений могут разрешить исполнителям или сотрудникам канцелярии вынос из здания документов с грифом «КТ» для их согласования, подписи и др. в организации, находящиеся в пределах данного города.

5.6. Лицам, командированным в другие города, запрещается иметь при себе в пути следования документы, дела или издания с грифом «КТ». Эти материалы должны быть направлены заранее в адрес организации по месту командировки сотрудника, как правило, заказными или ценными почтовыми отправлениями, а также с курьерами.

5.7. При смене сотрудников, ответственных за учет и хранение документов, дел и изданий с грифом «КТ», составляется по произвольной форме акт приема-передачи этих материалов, утверждаемый заместителями директора по направлениям или руководителями структурных подразделений.

6. Обязанности лиц, допущенных к сведениям, составляющим коммерческую тайну

6.1 Лица, допущенные к работам, документам и сведениям, составляющим коммерческую тайну, несут личную ответственность за соблюдение ими установленного режима. Прежде чем получить доступ к коммерческой информации, они должны изучить требования настоящей инструкции и других нормативных документов по защите коммерческой тайны в части, их касающейся, сдать зачет на знание указанных требований и дать индивидуальное письменное обязательство по сохранению коммерческой тайны.

6.2. Лица, допущенные к работам, документам и сведениям, составляющим коммерческую тайну, обязаны:

а) строго хранить коммерческую тайну, ставшую им известной по службе или работе или иным путем, пресекать дей-

ствия других лиц, которые могут привести к разглашению коммерческой тайны. О таких фактах, а также о других причинах или условиях возможной утечки коммерческой тайны немедленно информировать непосредственного начальника и службу безопасности;

б) в течение договорного периода не использовать известную коммерческую тайну в своих личных целях, а также без соответствующего разрешения руководства не заниматься любой деятельностью, которая в качестве конкурентного действия может нанести ущерб предприятию, являющемуся владельцем этой коммерческой тайны;

в) выполнять только те работы и знакомиться только с теми документами, к которым получили доступ в силу своих служебных обязанностей; знать степень важности выполняемых работ, правильно определять ограничительный гриф документов, строго соблюдать правила пользования ими, порядок их учета и хранения;

г) при составлении документов со сведениями, составляющими коммерческую тайну, ограничиваться минимальными, действительно необходимыми в документе этими сведениями; определять количество экземпляров документов в строгом соответствии с действительной служебной необходимостью и не допускать рассылки их адресатам, к которым они не имеют отношения;

д) на черновиках документов проставлять соответствующий ограничительный гриф и другие необходимые реквизиты. Передавать их для печатания только с письменного разрешения руководителя подразделения;

е) после получения из машинописного бюро отпечатанных документов проверять их наличие, сличать эти данные с записями в журнале и расписываться (с указанием даты) за получение отпечатанных документов и черновиков, после чего учесть в канцелярии или у уполномоченного службы безопасности;

ж) получать документы с грифом «КТ» лично в канцелярии или у уполномоченного службы безопасности. Своевременно знакомиться с полученными документами и разборчиво расписываться на них с указанием даты ознакомления;

з) поступившие документы с грифом «КТ» своевременно направлять для приобщения к делу с соответствующими отметками об исполнении (номер дела, что сделано по документу, дата, подпись) и с резолюцией начальника подразделения;

и) сдавать в канцелярию или уполномоченному по службе безопасности исполненные входящие документы, а также пред-

назначенные для рассылки, подшивки в дело, уничтожения и взятия на инвентарный учет под расписку в журналах учета;

к) иметь внутреннюю опись документов с грифом «КТ», в которой отводится отдельный раздел, и немедленно вносить с нее все полученные для исполнения документы, хранить их только в рабочей папке, а при выходе в рабочее время из помещения рабочую папку с документами запирать в сейф;

л) по окончании работы с документами с грифом «КТ» своевременно возвращать их в канцелярию или уполномоченному службы безопасности;

м) об утрате или недостаче документов с грифом «КТ», ключей от сейфов, личных печатей немедленно сообщать в службу безопасности;

н) при увольнении, перед уходом в отпуск, отъездом в командировку своевременно сдать или отчитаться перед канцелярией или уполномоченным за все числящиеся за ним документы;

о) знакомить представителей других учреждений с документами с грифом «КТ» с ведома и с письменного разрешения руководителя подразделения; лично знакомиться с разрешениями указанных руководителей на предписании, в котором должны быть определены вопросы и объем сведений, подлежащих рассмотрению; требовать от командированных лиц расписки на документах, с которыми они ознакомились, или в учетных карточках этих документов;

п) документы с грифом «КТ» во время работы располагать так, чтобы исключить возможность ознакомления с ними других лиц, в том числе допущенных к подобным работам и документам, но не имеющих к ним прямого отношения;

р) по первому требованию канцелярии и отдела службы безопасности предъявлять для проверки все числящиеся и имеющиеся документы с грифом «КТ»; представлять по требованию начальника отдела устные или письменные объяснения о нарушениях установленных правил выполнения работ с грифом «КТ», учета и хранения документов с грифом «КТ», а также о фактах разглашения сведений с грифом «КТ», утраты документов, содержащих такие сведения.

7. Принципы организации и проведения контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну

7.1. Контроль за обеспечением режима при работе со сведениями, составляющими коммерческую тайну, осуществляется

в целях изучения и оценки фактического состояния сохранности коммерческой тайны, выявления недостатков и нарушений режима при работе с материалами с грифом «КТ», установления причин таких недостатков и нарушений и выработки предложений, направленных на их устранение и предотвращение.

7.2. Контроль за обеспечением режима при работе с материалами с грифом «КТ» осуществляет служба безопасности и руководители структурных подразделений

7.3. Комиссия для проверки обеспечения режима при работе с материалами с грифом «КТ» комплектуется из опытных и квалифицированных работников в составе не менее 2 человек, имеющих допуск к этой работе. Участие в проверке не должно приводить к необоснованному увеличению осведомленности проверяющих об этих сведениях.

7.4. Проверки обеспечения режима при работе с материалами с грифом «КТ» проводятся не реже одного раза в год комиссиями на основании предписания, подписанного директором или его заместителем по направлению.

7.5. Проверки проводятся в присутствии руководителя структурного подразделения или его заместителя.

7.6. Проверяющие имеют право знакомиться со всеми документами, журналами (карточками) учета и другими материалами, имеющими отношение к проверяемым вопросам, а также проводить беседы и консультации со специалистами и исполнителями, требовать представления письменных объяснений, справок, отчетов по всем вопросам, входящим в компетенцию комиссии.

7.7. По результатам проверок составляется акт (справка) с отражением в нем состояния режима при работе с материалами с грифом «КТ», выявленных недостатков и нарушений, предложений по их устранению.

С актом после утверждения его директором или заместителем под роспись знакомится руководитель структурного подразделения.

7.8. Об устранении выявленных в результате проверки недостатков и нарушений в режиме при работе с материалами с грифом «КТ» и реализации предложений руководитель подразделения в установленные комиссией сроки сообщает начальнику службы безопасности.

7.9. В случае установления фактаутраты документов, дел и изданий с грифом «КТ» либо разглашения содержащихся в них сведений немедленно ставятся в известность директор и его заместители по направлениям и начальник службы безопасности.

Для расследования факта утраты документов, дел и изданий с грифом «КТ» при установлении факта разглашения сведений, содержащихся в этих материалах, приказом директора (распоряжением руководителя структурного подразделения) назначается комиссия, заключение которой о результатах расследования утверждается руководителем, создавшим данную комиссию.

На утраченные документы, дела и издания с грифом «КТ» составляется акт. Соответствующие отметки вносятся в учетные документы.

Акты на утраченные дела постоянного хранения после их утверждения директором или его заместителями по направлениям передаются в архив для включения в дело фонда.

8. Ответственность за разглашение, утрату документов, содержащих коммерческую тайну

8.1. Разглашение сведений, составляющих коммерческую тайну, — это предание огласке сведений лицом, которому эти сведения были доверены по службе, работе или стали известны иным путем, в результате чего они стали достоянием посторонних лиц.

8.2. Утрата документов, содержащих сведения коммерческой тайны, — это выход (в том числе и временный) документов из владения ответственного за их сохранность лица, которому они были доверены по службе или работе, являющийся результатом нарушения установленных правил обращения с ними, вследствие чего эти документы стали или могли стать достоянием посторонних лиц.

8.3. Иные нарушения режима при работе с материалами коммерческой тайны — это нарушение требований, могущее привести к разглашению этих сведений, утрате документов, содержащих такие сведения.

8.4. За утрату и незаконное уничтожение документов, дел и изданий с грифом «КТ», за разглашение сведений, содержащихся в этих материалах, а также за нарушение требований виновные лица привлекаются к ответственности в установленном порядке.

ПРИЛОЖЕНИЕ 5

ИНСТРУКЦИЯ
по защите конфиденциальной информации
при работе с зарубежными партнерами

1. Общие положения

1.1. Настоящая инструкция определяет порядок работы с зарубежными партнерами. Положениями настоящей инструкции необходимо руководствоваться также и при контактах с представителями совместных предприятий и с представителями конкурирующих фирм и организаций.

1.2. При работе с зарубежными партнерами также следует руководствоваться положениями «Инструкции по защите коммерческой тайны».

1.3. Инструкция устанавливает режим работы с иностранцами с целью защиты конфиденциальной информации.

1.4. Под работой с иностранцами следует понимать совокупность всех видов деятельности при контактах с иностранными компаниями, фирмами (переписка, телефонные разговоры, передача телексных и факсимильных сообщений) либо личных встреч с их представителями по служебным делам.

1.5. Ответственность за организацию работы с зарубежными партнерами и соблюдение требований настоящей инструкции несут руководство, служба безопасности и руководители соответствующих структурных подразделений фирмы.

1.6. Для работы с зарубежными партнерами ежегодно составляются списки сотрудников, выделенных для этой работы.

2. Основания для работы с зарубежными партнерами

2.1. Основанием для работы с зарубежными партнерами по служебной необходимости являются: планы международных научно-технических связей, заключенные контракты и протоколы, соглашения об установлении прямых производственных, научно-технических связей, решения о совместной деятельности, а также инициатива самих зарубежных представителей и представителей российской стороны.

2.2. Решение о приеме иностранцев принимается генеральным директором или его заместителями по представлениям руководителей структурных подразделений, согласованных с отделом по международным связям, службой безопасности, техническим отделом и отделом документационного обеспечения.

2.3. Основанием для командирования сотрудников за рубеж служит решение генерального директора или его заместителей, выносимое на основании представляемых руководителями соответствующих отделов материалов, оформленных в установленном порядке. Принятое решение излагается письменно непосредственно на докладной записке, представляемой в установленные сроки.

2.4. В докладной записке отражаются следующие сведения: цель выезда; страна командирования и принимающая организация (фирма); срок командирования; условия финансирования поездки; фамилия, имя, отчество и занимаемая должность командируемого.

3. Формы работы с зарубежными партнерами

3.1. Прием зарубежных делегаций.

3.1.1. Прием приглашенных зарубежных делегаций осуществляется на основе утвержденных программ, составляемых по установленной форме, а также сметы расходов по приему.

Программы пребывания приглашенных зарубежных делегаций и сметы расходов составляются соответствующими подразделениями, отвечающими за прием, согласовываются с отделом международных связей, службой безопасности и утверждаются генеральным директором.

Ответственным за выполнение программы пребывания иностранной делегации является руководитель соответствующего отдела.

3.2. Организация деловых встреч (переговоров).

3.2.1. Деловые встречи с зарубежными партнерами организуются на основе заявок, оформленных соответствующими отделами, отвечающими за прием по установленной форме.

3.2.2. Заявки согласовываются с руководителем отдела международных связей, службой безопасности, отделом технического обеспечения и утверждаются генеральным директором или его заместителями.

3.2.3. Переводчиков на деловые встречи приглашает отдел, принимающий зарубежных представителей.

3.2.4. Для участия в деловых встречах с зарубежными партнерами, как правило, привлекаются специалисты из числа сотрудников, выделенных для работы с зарубежными представителями, в количестве не менее двух человек.

3.2.5. Деловые встречи могут проводиться в кабинете генерального директора, кабинете его первого заместителя и специально выделенном для этого помещении.

3.2.6. Встречу, сопровождение и проводы зарубежных партнеров осуществляют сотрудники соответствующих отделов и отдела по международным связям.

3.2.7. Лица, участвующие в переговорах, обязаны:

— хранить конфиденциальную информацию фирмы;

— не входить в обсуждение вопросов, не относящихся к их компетенции.

3.3. Посещение приемов, симпозиумов, семинаров, выставок и других мероприятий, организуемых зарубежными партнерами или с их участием.

3.3.1. Сотрудники фирмы посещают приемы, симпозиумы и семинары, организуемые зарубежными партнерами или с участием зарубежных партнеров, по служебным вопросам по согласованию с отделом международных связей, отделом технического обеспечения и с разрешения генерального директора.

3.3.2. При поступлении письменных или устных приглашений на подобные мероприятия непосредственно в адрес сотрудников следует руководствоваться п. 3.3.1. настоящей инструкции.

3.4. Передача материалов зарубежным представителям.

Передача зарубежным партнерам научно-технических и других материалов допускается после их предварительного рассмотрения руководством и службой безопасности с целью определения возможности их передачи.

3.5. Ведение служебной переписки. Прием и передача телексных и факсимильных сообщений, ведение телефонных разговоров с зарубежными партнерами.

3.5.1. Общие положения.

3.5.1.1. Руководство фирмы, отделы и подразделения фирмы ведут служебную переписку, прием и передачу телексных и факсимильных сообщений через отдел документационного обеспечения.

3.5.1.2. Вся входящая международная корреспонденция (вне зависимости от ее вида) регистрируется и первично рассматривается в отделе документационного обеспечения. Корреспонденция докладывается генеральному директору или его заместителям или направляется на рассмотрение и исполнение непосредственно в отделы.

3.5.1.3. После рассмотрения руководством корреспонденция в соответствии с резолюцией направляется исполнителям, и контроль за сроками исполнения поручения осуществляется в соответствии с установленным порядком.

3.5.1.4. Право подписи корреспонденции в адрес зарубежных представительств имеют генеральный директор, его заместители и начальники отделов.

3.5.1.5. Любая корреспонденция в адрес зарубежных представительств подлежит визированию у руководства и в службе безопасности фирмы. Один экземпляр документов остается в отделе документационного обеспечения.

3.5.2. Работа с письмами.

3.5.2.1. Служебные письма, адресуемые зарубежным партнерам, пишутся на фирменных бланках с указанием наименования фирмы на английском языке, а также с разрешенными номерами телефонов, факсов и телексов, выделенных для работы с зарубежными представителями. Ставить какие-либо штампы и печати на таких письмах не разрешается.

3.5.2.2. Проекты писем в адрес зарубежных партнеров готовятся в отделах фирмы при строгом соблюдении конфиденциальности. Наименование отдела, фамилия и номер телефона исполнителя письма на подлиннике не указываются, а приводятся на копиях.

3.5.3. Работа с телексными сообщениями.

3.5.3.1. Телексные сообщения от иностранцев принимаются на специально выделенный аппарат сети Телекс.

3.5.3.2. Подготовка проектов телексных сообщений осуществляется отделами по установленной форме на иностранном языке.

3.5.3.3. Отправка телексных сообщений зарубежным партнерам осуществляется в порядке, установленном настоящей Инструкцией.

3.5.4. Работа с факсимильными сообщениями.

3.5.4.1. Все факсимильные сообщения от иностранцев подлежат регистрации в отделе документационного обеспечения.

3.5.4.2. Подготовка проектов факсимильных сообщений осуществляется отделами на бланках, используемых для письменной корреспонденции и со специальным титульным листом. Тексты сообщений могут быть как на русском, так и на иностранных языках. Требования к реквизитам исполнителя аналогичны требованиям п. 3.5.2.2. настоящей инструкции.

3.5.4.3. Передача факсимильных сообщений иностранцам осуществляется отделами со специально выделенного аппарата факсимильной связи с предварительной регистрацией в отделе документационного обеспечения.

3.5.5. Ведение телефонных разговоров.

Сотрудники фирмы могут вести телефонные разговоры с зарубежными партнерами с телефонов, выделяемых для этих целей в каждом отделе: список телефонов подлежит согласованию с отделом международных связей и службой безопасности.

3.6. Командирование за рубеж.

3.6.1. Состав делегаций, командируемых за рубеж за счет собственных средств, формируется соответствующими отделами и согласовывается с отделом международных связей, службой безопасности и руководством фирмы.

3.6.2. При командировании за рубеж по служебной линии делегациям и отдельным специалистам выдается техническое задание, в котором отражается перечень конкретных вопросов, для решения которых организуется поездка.

Технические задания составляются отделом международных связей и представляются на утверждение руководству не позднее чем за две недели до выезда.

3.6.3. Оформление выездных документов производится в отделе международных связей в установленном порядке.

4. Оформление результатов работы с иностранцами, учет и отчетность

4.1. Соответствующие отделы, принимающие иностранцев, по итогам работы с зарубежными партнерами и командирования за рубеж составляют отчеты произвольной формы. По итогам деловых встреч составляются записи бесед по установленной форме. Записи бесед представляются в отдел по международным связям в двухдневный срок после окончания работы с иностранцами, а отчеты, как правило, — в двухнедельный срок (два печатных экземпляра).

4.2. В записях бесед и отчетах указывается: когда, где, с кем состоялась встреча; ее основание и цель; кем дано разрешение на встречу, какое учреждение, организацию или фирму представляли иностранцы, их фамилии и должностное положение; кто присутствовал со стороны фирмы; содержание беседы (существо вопросов и ответы на них); какая документация и какие образцы изделий и материалов переданы зарубежным представителям или получены от них, обязательства сторон по существу обсуждавшихся вопросов, а также другая заслуживающая внимания информация.

4.3. Отдел международных связей ведет учет принимаемых иностранных делегаций и деловых встреч, а также учет сообщений от фирмы о контактах с иностранцами.

5. Организационные мероприятия по результатам работы с иностранцами

5.1. Отчеты по результатам работы с зарубежными представительствами и записи бесед, содержание обязательства и предложения сторон докладываются соответствующими отделами, организовавшими встречу, руководству фирмы и службе безопасности.

5.2. Координация работ по выполнению поручений руководства по данным документам возлагается на отдел международных связей и службу безопасности.

5.3. Контроль за выполнением положений настоящей инструкции возлагается на руководство фирмы, отдел международных связей и службу безопасности.

ПРИЛОЖЕНИЕ 6

ПАМЯТКА
работнику (служащему) о сохранении коммерческой тайны

В условиях рынка и конкуренции коммерческая тайна выступает как элемент маркетинга и предприимчивости, как способ максимизации прибыли и конкурентоспособности предприятия. Утечка коммерческих секретов может привести к снижению доходов предприятия или к его банкротству.

Работник (служащий) обязан строго хранить в тайне сведения, отнесенные к коммерческой тайне предприятия, ставшие ему известными по службе или иным путем. Разглашение коммерческой тайны предприятия, утрата ее носителей, передача третьим лицам, публикация без согласия предприятия, а также использование для занятия любой деятельностью, которая в качестве конкретного действия может нанести ущерб предприятию, влечет уголовную, административную, гражданско-правовую или иную ответственность в соответствии с действующим законодательством.

Коммерческая тайна определяется руководителем предприятия и отражается в «Перечне сведений, составляющих ком-

мерческую тайну предприятия» (объявлен приказом по предприятию №_____от_____г.).

Коммерческая тайна других предприятий, с которыми имеются деловые отношения предприятия, доводится до работника, в части его касающейся, руководителем структурного подразделения.

Порядок обращения со сведениями, отнесенными к коммерческой тайне предприятия, регулируются «Положением по обеспечению сохранности коммерческой тайны предприятия» (объявлено приказом по предприятию №_____от_____г.).

Работник обязан работать только с теми сведениями и документами, содержащими коммерческую тайну предприятия, к которым он получил доступ в силу служебных обязанностей, знать, какие конкретные сведения подлежат защите, а также строго соблюдать правила пользования ими.

Работник должен знать также, кому на сотрудников предприятия разрешено работать со сведениями, составляющими коммерческую тайну предприятия, к которой он сам допущен, и в каком объеме эти сведения могут быть доведены до этих сотрудников.

При участии в работах сторонних организаций работник может знакомить их представителей со сведениями, составляющими коммерческую тайну предприятия, только с письменного разрешения руководителя структурного подразделения. При этом руководитель должен определить конкретные вопросы, подлежащие рассмотрению, и указать, кому и в каком объеме может быть доведена информация, подлежащая защите.

Запрещается помещать без необходимости сведения, составляющие коммерческую тайну предприятия, в документы, содержащие государственные секреты, и имеющие в связи с этим соответствующий гриф секретности. Такое нарушение порядка обращения со сведениями, составляющими коммерческую тайну предприятия, рассматривается как их разглашение и влечет ответственность в соответствии с установленным законом порядком.

Об утрате или недостаче документов, изделий, содержащих коммерческую тайну предприятия, удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов, металлических шкафов, личных печатей, а также о причинах и условиях возможной утечки таких сведений работник обязан немедленно сообщить руководителю структурного подразделения и в службу безопасности предприятия.

При увольнении, перед уходом в отпуск, отъездом в длительную командировку (более 1 месяца) необходимо сдать лицу, указанному руководителем структурного подразделения, все носители коммерческой тайны предприятия, которые находились в распоряжении работника в связи с выполнением им служебных обязанностей.

Работник обязан по первому требованию представителей службы безопасности предприятия предъявить для проверки все числящиеся за ним материалы, содержащие коммерческую тайну предприятия, представлять устные или письменные объяснения о нарушениях установленных правил выполнения закрытых работ, учета и хранения документов и изделий, содержащих коммерческую тайну, а также о фактах ее разглашения, утраты документов и изделий, содержащих такие сведения.

В случае попытки посторонних лиц или организаций, в том числе зарубежных, получить информацию, составляющую коммерческую тайну предприятия, работник обязан сообщить об этом руководителю структурного подразделения и в службу безопасности.

Обязательства, связанные с защитой коммерческой тайны предприятия, не ограничивают прав работника на интеллектуальную собственность, в частности, в подаче заявки на изобретение, в возможном патентовании и т. д. Реализация прав работника на интеллектуальную собственность осуществляется в соответствии с установленным законом порядком.

Срок действия ограничений, связанных с необходимостью защиты коммерческой тайны предприятия, определяется администрацией при заключении трудового договора с работником. Об окончании ограничений работник уведомляется администрацией в письменной форме.

ПРИЛОЖЕНИЕ 7

Памятка
сотрудникам на случай вооруженного нападения

1. В случае внезапного нападения, когда преступники вооружены либо объявили о наличии при них взрывного устройства, сотрудники банка обязаны в целях сохранения жизни и

здоровья как своего, так и окружающих не допускать резких движений, выполнять требования нападающих.

2. По команде «лечь на пол» не спеша опуститься, лечь на живот, руки положить у головы, лицо обращено в противоположную от нападающих сторону, или, не оборачиваясь к преступнику лицом, подойти к противоположной от него стене, руки положить или за голову, или прислонить к стене выше головы, лицо обращено к стене.

3. На вопросы преступников отвечать, не поворачивая головы.

4. Если при нападении выдвигаются только требования отдать деньги, без команды «лечь на пол», необходимо остаться на местах, не перемещаться, не пытаться спрятаться под стол или за каким-либо предметом мебели.

5. Не рекомендуется смотреть преступникам в глаза, ухмыляться, вслух комментировать их требования, перешептываться.

6. Если в начальный момент нападения упущена возможность экстренного сообщения в органы милиции — «тревожная кнопка», то в процессе длящегося нападения воспользоваться этой сигнализацией можно лишь в случае, полностью исключающем обнаружение этого со стороны преступников.

7. Если в процессе нападения было применено оружие и есть пострадавшие, нельзя самостоятельно пытаться оказывать им медицинскую помощь.

8. Все сотрудники банка должны сосредоточить свою память и попытаться запомнить, можно мысленно несколько раз про себя повторить, приметы одежды, лиц, особенности походки и речи преступников.

9. После ухода преступников из помещения банка до приезда сотрудников милиции необходимо обозначить и не наступать на те места пола, где стояли и перемещались преступники. Обозначить и не прикасаться к предметам, к которым прикасались руками преступники.

(Памятка разработана Службой безопасности МОСТ-банка)

ПРИЛОЖЕНИЕ 8

Классификация информационных ресурсов

Предлагается следующая классификация информационных ресурсов.

По виду информации:

правовая;
научно-техническая;
политическая;
финансово-экономическая;
статистическая;
о стандартах и регламентах; метрологическая;
социальная;
о здравоохранении;
о чрезвычайных ситуациях;
персональная (персональные данные);
кадастры (земельный, градостроительный, имущественный, лесной и др.);

По режиму доступа:

- Открытая (без ограничения);
- ограниченного доступа:
  - государственная тайна,
  - конфиденциальная информация,
  - коммерческая тайна,
  - профессиональная тайна,
  - служебная тайна,
  - личная (персональная)тайна.

По виду носителя:

на бумаге;
на машиночитаемых носителях;
в виде изображения на экране ЭВМ;
в памяти ЭВМ;
в канале связи;
на других видах носителей.

По способу формирования и распространения:

- стационарные ресурсы;
- передвижные (мобильные) ресурсы.

По способу организации хранения и использования:

- Традиционные:
  - массив документов;
  - фонд документов;
  - архив;
- автоматизированные формы:

БД (сеть);
- автоматизированная информационная система (сеть);
- база знаний.

По форме собственности:'
- общероссийское национальное достояние;
- государственная собственность:
  - федеральная;
  субъектов Федерации;
  - совместная (федеральная и субъектов Федерации);
- муниципальная собственность;
- частная собственность;
- коллективная собственность.

Адресная информация

Наиболее активные участники данного сектора информационного рынка — Агентство деловой информации (АДИ) и АО АСУ-ИМПУЛЬС.

АДИ издает бизнес-карты по областям, краям, республикам РФ, странам СНГ, по 17 секторам экономики, 20 отраслям и подотраслям. О каждом предприятии даются следующие сведения: наименование, год основания, форма собственности, данные для контакта, ФИО руководителя, численность, продукция и услуги, объем продукции в натуральных и стоимостных показателях, остаточная стоимость и износ основных фондов, используемое сырье и материалы, экспорт, импорт, дата предоставления информации для бизнес-карты. Издание сопровождается алфавитно-предметными указателями. Информация поставляется также в виде БД на дискетах. Обновление информации происходит с помощью дискет с периодичностью 1 раз в месяц, квартал, полугодие, год. С 1998 г. АДИ начал издавать журнал «Информация и бизнес».

АСУ-ИМПУЛЬС издает отраслевые справочники в бумажном и в электронном вариантах. О каждом предприятии приводятся следующие сведения: полное наименование и адрес, ФИО руководителя, подробнейшая номенклатура продукции предприятия, экспорт, импорт. Издание сопровождается алфавитно-предметным указателем. АСУ-ИМПУЛЬС также подготавливает ответы на разовые запросы по телефону, в письменном виде и по факсу России. Доступ к БД АСУ-ИМПУЛЬС возможен также в режиме он-лайн.

АСУ-ИМПУЛЬС имеет представительства в следующих городах: Белгород, Вильнюс, Волгоград, Волжский, Дзержинск, Днепропетровск, Екатеринбург, Казань, Калининград, Киев, Киров, Кишинев, Кострома, Луганск, Минск, Нижний Новгород, Новокузнецк, Новосибирск, Новороссийск, Пенза, Пермь, Псков, Рига, Ростов-на-Дону, Самара, Санкт-Петербург, Тольятти, Томск, Ульяновск, Уфа, Харьков, Челябинск, Ярославль.

Информация об общероссийском классификаторе технико-экономической информации

Главный межрегиональный центр обработки и распространения статистической информации Государственного комитета РФ по статистике (ГМЦ Госкомстата) ведет БД общероссийских классификаторов технико-экономической информации (ТЭИ) и социальной информации. Общее количество классификаторов — 20. Периодичность обновления — по мере возникновения изменений в законодательных и нормативных актах РФ. Классификаторы содержат кодовые обозначения следующих объектов: продукция, экономические районы, органы государственной власти и управления, страны мира, административно-территориальное деление, отрасли народного хозяйства, валюты и др.

Информация о внешнеэкономической деятельности

Фирма «Инфосеть» предоставляет следующую информацию по внешнеэкономической деятельности: действующие законодательные документы, документы Таможенного комитета, Таможенный кодекс, методические материалы (4000 документов).

По заказу предприятия компания ИНФОРМБЮРО может сделать анализ внешнеэкономической деятельности.

Информация о выставках

Информация об отечественных и зарубежных выставках, планируемых и проводящихся в городах России, публикуется в газете «УДАЧА-БИЗНЕС». Газета распространяется по подписке, а также во всех городах России, где проходят выставки.

Информация о специализированных выставках по безопасности в России и за рубежом публикуется в журналах БДИ, «Конфидент», «Мир безопасности» и «Системы безопасности».

Информация о деловой документации

Информацию о деловой документации (типовые договора, учредительные документы и др., всего 600 наименований) может предоставить фирма «Инфосеть».

Информация о деятельности фирм, предприятий РФ

Такую информацию предоставляет ГМЦ Госкомстата. Он ведет БД «Единый государственный регистр предприятий и организаций» (ЕГ-РПО), которая включает сведения о 2,5 млн. объектов, прошедших государственную регистрацию в соответствии с законодательством РФ.

Можно получить следующие данные: наименование предприятия, местонахождение, вид деятельности, форма собственности, учредители.

Количественные данные предоставляются по отраслям, территориям, организационно-правовым формам, формам собственности.

Подробную информацию о предприятии могут предоставить также компания ИНФОРМБЮРО и Специальная информационная служба (СИНС).

Информация о законодательных и нормативных документах

Одним из наиболее активных участников в этом секторе информационного рынка является общероссийская сеть распространения правовой информации «Консультант Плюс». Она предоставляет в виде БД следующую юридическую информацию: нормативные документы РФ, многосторонние документы СНГ, документы органов власти и управления субъектов РФ, документы Высшего арбитражного суда и Верховного суда, судебные акты.

О правовых документах можно узнать также через информационную коммерческую систему «Международные интеллектуальные рынки» (ИКС МИР), фирмы «Интегрум-Техно» и «Инфосеть», юридическое информационное агентство INTRALEX.

Тексты нормативных документов из законодательной базы по проблемам информационной безопасности можно найти по адресу: http:/ /www.emoney.ru/laws/Flaws.htm и http:// www.spymarket.com/bibl/pl/index.html

Информация о маркетинговых исследованиях

Маркетинговая информация — результат маркетинговых исследований. Одна из немногих фирм, осуществляющих по заказу коммерческих предприятий маркетинговые исследования, — это фирма ИНФО, входящая в АО «Мосвнешинформ». Структура отчета по результатам маркетингового исследования выглядит следующим образом:

- анализ предложения по данному продукту или услуге (производители, их контактные сведения, объемы производства в натуральных и стоимостных показателях, экспорт, экспортеры и их контактные данные, объемы экспорта в натуральных и стоимостных показателях, анализ и прогноз соотношения объемов экспорта и внутреннего потребления, экспортные тарифы и правила);
- анализ спроса (потребность в продукте или услуге в натуральных и стоимостных показателях, потенциальные потребители, платежеспособность, фактическая реализация, импорт: объемы, тарифы и правила, прогноз спроса на ближайшие 5 лет);
- стратегия и методы реализации продукта и услуги;
- нормативно-законодательные документы, имеющие отношение к теме маркетингового исследования.

Это типичная, но не стандартная структура маркетингового исследования. АО ИНФО готово скорректировать ее по требованию заказчика.

Подробная структура маркетингового исследования приведена не только затем, чтобы продемонстрировать информационный продукт, но и потому, что она выполняет методологическую функцию для тех, кто самостоятельно хочет проводить маркетинговые исследования.

Информация о надежности иностранного партнера

Если необходимо установить надежность иностранного партнера, то рекомендуется обращаться к американским информационным системам LEXIS-NEXIS (L-N) и «Dun and Bradstreet» (D&B). Представительство первой находится в Санкт-Петербурге, второй — в Москве. Эти фирмы имеют информацию также о российских предприятиях, но, по мнению специалистов, пользовавшимися их услугами, информация о наших предприятиях у американских фирм менее качественная, чем у российских источников.

мационным организациям LIONS, СИНС, АРСИН, НПК «Кронос», ГМЦГоскомстата.

Охранно-сыскная ассоциация LIONS осуществляет весь комплекс детективных и детективно-информационных услуг в рамках действующего законодательства:

- бизнес-справки по банкам, страховым компаниям и фирмам России, СНГ и стран Балтии;
- сбор экономической информации о фирмах и компаниях стран Европы, Америки, Африки, Азии, Австралии и Новой Зеландии;
- многоуровневая проверка потенциальных партнеров и клиентов, информационная «подсветка» и сопровождение контрактов в любой точке мира;
- проверка желающих получить кредит;
- деловые и кредитные истории, финансовая надежность, выявление связи с организованной преступностью;
- выявление неправомерного использования товарных знаков;
- корпоративные расследования;
- работа по уголовным и гражданским делам;
- розыск скрывшихся должников и лиц, без вести пропавших;
- проведение комплексных расследований с применением полиграфа (детектора лжи);
- преднаймовые психофизиологические тестирования.

Структура стандартной бизнес-справки LIONS включает следующие данные:

- полное и краткое наименование предприятия, в том числе прежние наименования и наименования на английском языке;
- организационно-правовая форма;
- год основания;
- сведения о регистрации;
- коды;
- юридический и фактический адреса;
- номера телефонов, факсов, телексов, адрес электронной почты, код SWIFT и «Reuter Dealing»;
- лицензии;
- основные корреспонденты;
- основные учредители, владельцы, акционеры;

- руководители, краткая информация по персоналу;
- наличие филиалов и представительств;
- уставный фонд;
- финансовое состояние;
- деловая история;
- информация негативного характера.

Данная справка, как правило, — продукт первого уровня проверки партнера. Чаще всего она бывает достаточной.

Если требуется более глубокое изучение фирмы, то составляется подробный контракт. Примером более высокого уровня проверки может быть проверка фирмы за рубежом. Решение последней задачи облегчается тем, что руководитель LIONS является членом ряда зарубежных детективных организаций.

Постоянный мониторинг за ситуацией на рынке позволяет LIONS прогнозировать, какой вид преступлений или какая его схема «входит в моду».

Фирма СИНС создана в 1995 г. на базе информационного подразделения муниципального предприятия ИКАР и объединяет около 150 выходцев из КГБ и ГРУ. СИНС осуществляет не только информационное обеспечение безопасности клиентов, но информационно-аналитическое обеспечение предпринимательских рисков. СИНС имеет доступ в более чем 6000 БД по всему миру. Фирма постоянно отслеживает проблематику нефтяного комплекса нашей страны, банковского, фондового, страхового рынков, черной и цветной металлургии, лесной и деревообрабатывающей промышленности и ряда других.

СИНС имеет более 10 дочерних предприятий. Среди них есть и такие, которые известны в узком кругу профессионалов, например, информационно-аналитический журнал «Факт» (http://www.fact.ru).

Есть и несравненно более заметные на рынке, такие как НПК «Союзспецавтоматика», специализирующаяся в области производства, разработки и монтажа интегрированных систем пожарно-охранной сигнализации функциями управления доступом.

СИНС создал и поддерживает клуб безопасности в Интернете (http://www.securityclub.ru), где крупнейшие субъек-

ты рынка безопасности имеют возможность обмениваться мнениями и представить свою продукцию, услуги.

СИНС производит исследования по поручению заказчика, ставшего жертвой пиратства торговой марки. У СИНС есть возможность назвать пострадавшим фирмам имена производителя и нелегального поставщика такой продукции и установить мафиозные образования, которые контролируют поставщиков.

Корпорация АРСИН по заказу предприятий может подготовить полную справку о фирме, в частности провести специальное финансовое расследование.

НПК «Кронос» имеет такие БД, как «Должники Сбербанка РФ», «Черный список РТСБ», «Детективные агентства».

Особенность информационного продукта НПК «Кронос» состоит в том, что это готовая система управления БД, с помощью которой предприятие может решать следующие задачи:

- оценка делового партнера (по показателям кредитоспособности, добропорядочности, стабильности, характеру связей и др.);
- оценка событий, текущих и будущих (экономических, политических, региональных, криминальных и др.), с целью принятия оптимального коммерческого решения для фирмы;
- оценка сферы влияния конфликтных и кризисных ситуаций;
- поиск активов заемщика и др.

При использовании системы «Кронос» штат программистов не требуется. Специалисты владеют нестандартным подходом к каждому клиенту. Информация, предоставляемая ими, строго учитывает индивидуальные особенности клиента.

Особого внимания заслуживает информация ГМЦ Госкомстата. Во-первых, это официальный орган государственной статистики; во-вторых, он ведет БД «Годовая бухгалтерская отчетность», которая должна быть объектом особого внимания при решении проблем экономической безопасности предприятия. В последнем легко убедиться, если изучить содержа-

ние аналитической справки, которая может быть составлена на отдельное российское предприятие на основе вышеуказанной БД. Аналитическая справка включает:

- важнейшие учетно-регистрационные данные (полное и сокращенное наименование предприятия, код ОКПО, основной вид деятельности по бухгалтерскому балансу и др.);
- доли учредителей — юридических лиц в уставном капитале;
- дата регистрации;
- наименование регистрирующего органа;
- номенклатура и объем выпуска продукции;
- основные показатели бухгалтерского баланса (основные средства, оборотные активы, дебиторская задолженность, убытки, капитал и резервы, долгосрочные и краткосрочные пассивы, кредиторская задолженность, валюта баланса, выручка, прибыль, среднесписочная численность работников);
- доля продукции (в %) от общего объема производства по России и региону;
- поставка продукции на экспорт (наименование, количество, стоимость);
- сведения об инвестициях в Россию из-за рубежа и из России за рубеж.

Информация о репутации партнера

Фирмы L-N и D&B активно пополняют свои БД из СМИ. Фирма L-N, например, имеет около 14 тыс. постоянно обновляемых полнотекстовых источников деловой информации и новостей, включая крупнейшие газеты, журналы, информационные агентства, такие как «Agence France Press», BCC, ASAHI, ИТАР-ТАСС, «Associated Press», BLOOMBERG, UPI, CNN, «Callup», «ABC News», «Washington Post», «CBC News», «The New-York Times», «Business Wire», «Central News Agency» и др.

L-N поможет также найти законы, дела из судов и другую юридическую информацию США, ЕС, Великобритании, Франции, Канады, Австралии, Новой Зеландии, Китая, России и других стран.

Специалисты D&B также отслеживают, как они выражаются, публичную информацию, чтобы накопить относительно конкретной фирмы информацию о решениях и приговорах суда,

закладных, штрафах и других фактах, образующих репутацию фирмы.

Российская информационная фирма «Агентство обзора средств массовой информации» (Агентство WPS) подготавливает еженедельный дайджест «Бизнес-репутация», в котором на основе анализа прессы, радио- и телепередач даются обзоры всевозможных санкций в отношении предприятий, а также предприятий с испорченной репутацией, деловых споров и криминальных разборок. Предоставляется также информация о методах государственного контроля за коммерческой деятельностью. Дайджест подготавливается на основе обработки почти 70 центральных и более 500 региональных газет РФ.

Информация о ситуации в России в целом, в регионе, отрасли

Основной источник информации по данному направлению — ГМЦ Госкомстата. БД ГМЦ Госкомстата предоставляет следующую информацию:

- «Статистика России» (ежемесячный доклад Госкомстата «Социально-экономическое положение России», издания региональных органов государственной статистики, официальные статистические данные и др.);
- Основные итоги функционирования экономики (данные с 1992 г.; развитие отраслей и секторов экономики, инфраструктуры, социальной сферы);
- промышленность России (данные с 1985 г. по настоящее время; число промышленных предприятий, объемы выпуска, численность занятых, стоимость основных производственных фондов, балансовая прибыль; информация представлена в разрезе отраслей промышленности и по регионам);
- сельское хозяйство (данные с 1997 г. по настоящее время; информация по отраслям и регионам: динамика обобщенных стоимостных показателей, размер и структура посевных площадей, производство сельхозпродукции в натуральном выражении, численность поголовья скота и птицы);
- статистика внешнеэкономической деятельности (данные с 1995 г. по настоящее время, информация по секторам экономики и по регионам: сводные показатели хозяйственной деятельности совместных предприятий, движение иностранной валюты, иностранные инвестиции в экономику России);

- паспорт территорий РФ (данные с 1965 г.; численность и состав населения, развитие секторов экономики, развитие инфраструктуры и социальной сферы, структура занятости и уровень безработицы);
- регистр городов РФ (данные с 1970 г. по 1068 городам: численность, прирост, состав и занятость населения, уровень безработицы, развитие секторов экономики, инфраструктуры и социальной сферы, площадь городских земель).

Ситуацию по региону можно также изучить на основе данных территориальных органов статистики.

Информацию о положении экономики РФ, макроэкономических показателях, уровне производства, внешнеторговом обороте и состоянии финансовой системы предоставляет информационное агентство ФИНМАРКЕТ.

Предприниматель не успевает отслеживать текущие события. В связи с этим появилась новая информационная услуга — обзоры СМИ.

Фирма «Аргус-информ» подготавливает еженедельные обзоры центральных и московских СМИ по теме «Преступность». Фирма анализирует более 30 газет и журналов, многие из которых являются специализированными и остаются без внимания большого числа предпринимателей.

Основное содержание обзоров — схемы злоупотреблений против личности, в сфере экономики, против общественного порядка. Такие обзоры помогут качественно обеспечить безопасность бизнеса.

Агентство WPS ведет мониторинг новостных, общественно-политических и экономических передач российского телевидения и радио, предоставляя потребителю транскрипты программ и видеосюжеты. Эфир отслеживается по следующим каналам радио и телевидения: ОРТ, РТР, НТВ, «ТВ-Центр», ТВ-6, «Маяк», «Радио России», «Эхо Москвы», «Открытое радио».

Все остальные передачи отслеживаются, записываются и транскрипируются по индивидуальным заказам. Архив транскриптов радио- и телепередач на компактном диске содержит записи с июня 1992 г. по настоящее время. Тематическая обработка информации осуществляется не только на основе мониторинга телерадиоэфира, но и центральной, московской и региональной прессы.

Основная тематика: экономика (самый подробный отчет об экономическом эфире дня), банки и биржи сегодня (оперативный дайджест центральной и московской печати, 70 изданий), бизнес-экспресс (оперативный обзор аналитических публикаций центральной и московской печати, посвященных состоянию фондового или денежного рынков), драгоценные металлы, ВПК и бизнес, бизнес-нефть, авиадайджест, страхование в России, реклама и рекламная деятельность, Интернет, коммуникации и компьютеризация в России, рынок телекоммуникационных услуг, компании-регистраторы и регистрационная деятельность и др.

Потребитель получает информацию в форме клиппинговых бюллетеней, на компакт-дисках или полнотекстовые БД.

Полнотекстовые БД разработаны совместно с «Интегрум-Техно».

Еженедельная международная общественно-политическая газета «Московские новости» (МН, «Moscow News») в 1998 г. впервые на информационном рынке объявила о выходе полнотекстового архива на компакт-дисках популярнейших и авторитетных общественно-политических изданий за 1992-1998 гг.

Актуализации архива основана на технологии информационно-поисковой системы «Артефакт»; данная поисковая система разработана информационных агентством «Интегрум-Техно».

Вот некоторые из рубрик данного архива, дающие представление о том, какую пользу он может принести при изучении предпринимателем ситуации в мире, стране или регионе:

- подоплека политических событий в России и за рубежом;
- экономические прогнозы, конфликты и победы;
- терроризм, преступность, безопасность (корреспонденты «Московских новостей» в более чем 20 странах мира и в России рассказывают о самых громких судебных процессах, терактах, практике борьбы с преступностью и пр.).

Предлагается также версия БД на английском языке.

Мониторинг СМИ по указанным заказчиком темам выполняет компания ИНФОРМБЮРО.

Информация о ценах

БД ГМЦ Госкомстата «Цены на продовольственные товары» и «Цены на непродовольственные товары» содержат информацию об уровне цен на товары по 198 городам России, начиная с марта 1997 г.

Фирма «Международная ценовая информация» ИНФОРМВЭС отвечает на разовые запросы по странам и товарам. Ответы в течение 1-4 дней.даются по телефону, факсу или по почте.

Фирма ИКС МИР дает сведения о ценах на мировых товарных и сырьевых биржах (черные, цветные и драгоценные металлы, агропродукция, нефть и нефтепродукты).

Финансовая информация

По типу выпускаемых продуктов всех производителей информационной продукции на финансовом рынке можно разделить на три группы:

- поставщики «сырой» финансовой информации (Центральный банк (ЦБ) РФ, Министерство финансов РФ, банки, биржи);
- издательские дома и газетные объединения («Финансовая газета», издательский дом «Коммерсантъ», «Экономика и жизнь» и др.);
- информационные, консультационные агентства и центры.

Организации первых двух групп достаточно известны.

На рынке финансовой информации активно функционируют около 20 информационных и консультационных агентств и центров. Ограничимся описанием информационных услуг лишь некоторых информационных агентств — представителей третьей группы.

Информационное агентство «Прайм» с 1993 г. работает в области обработки и анализа финансовой информации и является официальным распространителем информации ЦБ РФ. В изданиях «Прайм» содержится следующая информация: валютные, фондовые, кредитные рынки, деятельность коммерческих банков РФ и СНГ, курсы валют, котировки акций промышленных предприятий, инвестиционных, торговых и венчурных компаний, пластиковые карточки и др.

Информационное агентство ФИНМАРКЕТ предоставляет ежедневную оперативную информацию с финансовых рын-

ков — денежного, валютного, ценных бумаг. Агентство информирует о ходе торгов в ММВБ, РТС, МЦФБ, МФБ и РБ в реальном времени.

В ИКС МИР имеются БД о фондовых и валютных рынках мира и СНГ, рынках ценных бумаг, вексельных рынках и др.

Доступ к мировым источникам финансовой информации может быть организован с помощью ЛЕКСИС-НЕКСИС.

Содержание

Глава VIII

Учебное издание

Ярочкин Владимир Иванович
Бузанова Яна Валерьевна

ОСНОВЫ БЕЗОПАСНОСТИ БИЗНЕСА И ПРЕДПРИНИМАТЕЛЬСТВА

Редактор *Н. Кондратович*
Компьютерная верстка *О. Буцен*
Корректор *Е. Маркелова*

Фонд «Мир»
111399, Москва, ул. Мартеновская, 3

ООО «Академический Проект»
Изд. лиц. № 04050 от 20.02.01.
111399, Москва, ул. Мартеновская, 3
Санитарно-эпидемиологическое заключение
Департамента государственного
эпидемиологического надзора
№ 77.99.02.953.Д.0086.63.11.03 от 28.11.2003 г.

По вопросам приобретения книги просим обращаться в ООО «Трикста»:
111399, Москва, ул. Мартеновская, 3, стр. 4
Тел.: (095) 305 3702; 305 6092; факс: 305 6088
E-mail: aproject@ropnet.ru
www.ropnet.ru/aprogect

Налоговая льгота — общероссийский классификатор продукции ОК-005-093, том 2; 953000 — книги, брошюры.

Подписано в печать с готовых диапозитивов 22.11.04
Формат 84x108/32. Гарнитура Балтика. Бумага офсетная
Печать офсетная. Усл.-печ. л. 10,92. Тираж 3000 экз.
Заказ № 5891.

Отпечатано в полном соответствии с качеством предоставленных диапозитивов в ОАО «Дом печати — ВЯТКА»
610033, г. Киров, ул. Московская, 122

Издательство
«АКАДЕМИЧЕСКИЙ ПРОЕКТ»
предлагает:

Ярочкин В. И.
Бузанова Я. В.

ТЕОРИЯ БЕЗОПАСНОСТИ

2005.-84x108/32,176 с, пер.

В книге с позиций системного подхода рассмотрена проблема безопасности существования и развития человека и человечества. На основе анализа опасностей, рисков и угроз человеку, обществу, земной цивилизации показана необходимость комплексного рассмотрения проблемы обеспечения безопасности.

Книга содержит значительное количество таблиц, графиков, структурных схем, рисунков. Предназначена для специалистов органов управления различных уровней, занимающихся вопросами обеспечения безопасности, для преподавателей, аспирантов и студентов вузов.