Министерство Образования и науки РФ

Федеральное агентство по образованию

Ангарская государственная техническая академия

Кафедра экономики, маркетинга и психологии управления

**ПРАВОВОЙ СТАТУС СЛУЖБЫ БЕЗОПАСНОСТИ И ЕЕ ФУНКЦИИ ПО ОБЕСПЕЧЕНИЮ ЭКОНОМИЧЕСКОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БИЗНЕСА**

**Курсовая работа по дисциплине "Экономическая и информационная безопасность бизнеса"**

Выполнил: студент группа

Проверил:

Ангарск

2006

Содержание

Введение

1. Правовой статус службы безопасности на предприятии

2. Устав службы безопасности

3. Функции службы безопасности фирмы и их развитие

Заключение

Список литературы

## Введение

Правовой статус в научной литературе определяется как юридически закрепленное положение организации или гражданина. В частности элементами правового статуса службы безопасности (СБ) являются:

правовые нормы, устанавливающие данный статус;

правосубьектность;

основные права и обязанности;

законные интересы;

гражданство;

юридическая ответственность;

правовые принципы;

вид правоотношения, в котором участвует СБ.

Актуальность данной темы курсовой работы в том, что служба безопасности имеется на каждом крупном и среднем предприятии и выполняет многообразные функции по обеспечению экономической и информационной безопасности бизнеса.

Цель деятельности СБ - своевременное пресечение (нейтрализация) противоправных посягательств на экономические интересы и персонал предприятия.

Информационной базой исследования являются периодические издания отечественных и зарубежных авторов, а также нормативные акты, касающиеся вопросов безопасности бизнеса.

## 1. Правовой статус службы безопасности на предприятии

"Служба безопасности - это правоохранительная некоммерческая организация, оказывающая охранно-сыскные услуги своему (своим) учредителю (учредителям) и другим организациям на основе действующего законодательства, собственного Устава и заключенного с ними договора"[[1]](#footnote-1)

При анализе правового статуса СБ нельзя обойти вопрос о том, является ли она субъектом права или таковой не может быть по определению?

Известно, что до настоящего времени большинство исследователей к субъектом права относит физические и юридические лиц, государство в целом, национально - государственные, административно - территориальные, муниципальные образования, социальные общности (народ, нации, население региона, трудовой коллектив).

Если следовать этому постулату, то СБ, имеющие статус структурного подразделения предприятия, не могут считаться субъектами права и, в соответствии с правилами логики, субъектами частной правоохранительной деятельности.

Субъективные и юридические права СБ зафиксированы не только в законе, но и в Уставе.

Таким образом, исходя из того, что СБ наделена определенными юридическими обязанностями и субъективными правами, ее следует признать самостоятельным субъектом права. Косвенным подтверждением этого факта является отнесение СБ к субъекту правоохранительной деятельности.

Правоспособность СБ является ограниченной (целевой), ибо она имеет только такие права, которые соответствуют определенным законам "О частной детективной и охранной деятельности в Российской Федерации", и Уставом, целям его деятельности, и, соответственно, может нести лишь связанные с этой деятельностью обязанности.

Законом установлено, что штаты СБ могут быть укомплектовано только гражданами России[[2]](#footnote-2).

За неправомерные действия СБ административную ответственность несет, как правило, предприятие-учредитель (юридическое лицо).

В частности, в соответствие с Кодексом административных правонарушений РФ оно несет ответственность за следующие правонарушения:

невыполнение в установленный срок законного предписания (постановления, представления) органа (должностного лица), осуществляющий государственный надзор (контроль) об устранении нарушений законодательства (ст. 19.5);

осуществление деятельности, не связанной с извлечением прибыли, без специального разрешения (лицензии), а также нарушений требований или условий специального разрешения (лицензии) (ст. 19.20);

нарушение правил учета хранения оружия и патронов к нему (ст. 20.8);

создание в организации СБ без специального разрешения (лицензии) (ст. 20.16).

Предприятие - учредитель СБ, который в соответствии со ст.20 ТК РФ является работодателем, несет материальную ответственность перед ее сотрудниками за ущерб:

А) причиненный в результате незаконного лишения его возможности трудиться;

Б) причиненный его имуществу;

В) за задержку выплаты заработной платы;

Г) за причиненный ему моральный вред (ст. ст.234-237 ТК РФ).

Гражданско-правовую ответственность за вред, причиненный сотрудниками СБ, также несет ее предприятие-учредитель.

Учредителями СБ не могут быть физические лица (даже имеющие лицензии на осуществление частной детективной и охранной деятельности) или несколько юридических лиц.

В соответствии с Законом учредителем СБ может быть только одно предприятие. При создание СБ предприятие-учредитель может предоставить ей право открывать текущий и расчетный счет в банке (это должно быть отражено в Уставе).

Текущий счет предназначен только для операций, связанных с выдачей наличных денег, а по расчетному счету производятся операции, связанные с безналичными перечислениями.

Однако это не позволяет относить СБ к юридическому лицу, т. к его важнейший признак - наличие у него обособленного имущества - отсутствует. Кроме того, применение в Законе термина "охранно-сыскное подразделение на предприятии" (ст.13 Закона) означает, что такое оргструктурное формирование как СБ, может функционировать только в рамках другого юридического лица, т.е. предприятия - учредителя.

Ликвидация СБ может произойти при добровольном отказе его персонала от выполнения своих обязанностей, по инициативе предприятия - учредителя, при ликвидации предприятия - учредителя и в случае аннулирования органом внутренних дел лицензий всем охранникам и детективам.

## 2. Устав службы безопасности

Типовой Устав СБ (на основе их конкретизации создаются индивидуальные Уставы) пока не разработан.

В Устав СБ должны быть включены следующие разделы:

I. Общие положения

II. Основные задачи

III. Функции

IV. Права и обязанности

V. Руководство

VI. Взаимоотношения и связи

VII. Охранная и детективная деятельность

VIII. Имущество и средства

IX. Контроль, проверка и ревизия деятельности

X. Реорганизация и ликвидация

Рассмотрим поподробнее содержание некоторых разделов Устава.

Раздел "Общие положения" содержит:

перечень нормативных актов, которыми должны руководствоваться в своей деятельности сотрудники СБ;

полное наименование и адрес местонахождения предприятия-учредителя;

название документа, на основании которого создается СБ (протокол, приказ, решение коллегии и т.д.) и дату его учреждения;

место СБ и его подчиненность в структуре предприятия: деятельность СБ, принципы деятельности;

наличие текущего, расчетного счета: порядок финансирования

Раздел "Основные задачи". В разделе "Основные задачи" перечисляются только те задачи, выполнение которых возможно в рамках предоставленной СБ компетенции и реализация которых приведет к достижению обозначенных целей. Применительно к приведенной выше цели основные задачи, вытекающие из анализа Закона, можно сформулировать следующим образом:

охрана собственности;

защита персонала предприятия от противоправных посягательств;

координация действий сотрудников и подразделений предприятия по вопросам обеспечения безопасности;

содействие правоохранительным органам по вопросам, затрагивающим интересы предприятия;

защита от несанкционированного доступа к закрытой информации о персонале и деятельности предприятия;

сбор, обработка и анализ конфиденциальной информации среди персонала предприятия и в сфере предпринимательства.

Раздел "Функции". Сами функции можно разделить на внутренние и внешние. К внешним функциям относятся те из них, которые названы в Законе видами предоставляемых услуг:

обеспечение порядка в местах проведения предприятием представительских, конфиденциальных и массовых мероприятий:

консультирование и предоставление рекомендаций руководству и персоналу предприятия по вопросам обеспечения безопасности;

охрана имущества предприятий;

защита жизни и здоровья персонала от противоправных посягательств;

сбор информации о проведении деловых переговоров;

изучение криминальных аспектов рынка;

выявление ненадежных деловых партнеров;

сбор сведений по гражданским делам;

розыск без вести пропавших сотрудников предприятия;

выявление некредитоспособных партнеров;

поиск утраченного имущества предприятия;

расследование фактов неправомерного использования товарных знаков предприятия;

сбор информации о лицах, заключивших с предприятием контракты;

расследование фактов разглашения коммерческой тайны предприятия;

сбор сведений по уголовным делам;

установление обстоятельств недобросовестной конкуренции со стороны других предприятий;

проектирование, монтаж и эксплуатационное обслуживание средств охранно-пожарной сигнализации.

Перечень внешних (основных) функций является исчерпывающим. Этот вывод вытекает из анализа ст.14 Закона, о соотношении между контрразведовательными и разведовательными функциями СБ среди разных предприятий различна, что связано со спецификой их деятельности, финансовыми возможностями и т.д. и. т.п.

## 3. Функции службы безопасности фирмы и их развитие

На современном этапе для СБ фирм приоритетными являются следующие направления развития[[3]](#footnote-3):

правильное наполнение комплекта организационно-распорядительных документов как правовой основы управления СБ фирмы;

информационная безопасность фирмы;

технологии против терроризма;

бизнес-разведка;

защита от "недружественных поглощений";

углубленные кадровые проверки.

Комплект организационно-распорядительных документов фирмы. Прежде всего СБ должна иметь Устав (Положение) СБ, а также трудовые договора с начальником СБ, руководителями структурных подразделений и сотрудниками СБ.

Отдел режима и охраны должен иметь:

положения (об отделе режима и охраны, о секторе охраны, бюро пропусков);

должностные инструкции (начальника смены, караула или наряда, сотрудника сектора охраны, инженера сектора охраны, коменданта здания, мастера по обеспечению вневедомственной охраны, начальника, инспектора и дежурного бюро пропусков, инкассатора);

бланки (заявок на разовые пропуска, постоянного, разового и материального пропусков);

книги (учета удостоверений и пропусков, посетителей по разовым пропускам, учета ежедневного расхода бланков пропусков и количества действующих пропусков);

журналы (учета разовых и материальных пропусков, приема металлических пеналов с ключами от спецпомещений, проверок состояния средств сигнализации и регистрации ее срабатывания).

Спецотдел должен иметь:

положения о спецотделе и о секторе обработки документов с грифом "коммерческая тайна" (КТ);

должностные инструкции (делопроизводителя, машинистки, оператора ЭВМ сектора обработки документов с грифом "КТ");

памятку работнику (служащему) фирмы о сохранении КТ;

договорное обязательство работника (служащего) фирмы о сохранении КТ;

журналы учета документов и изданий с грифом "КТ".

Отдел инженерно-технической безопасности должен иметь:

положение об отделе инженерно-технической безопасности;

должностную инструкцию инженера отдела инженерно-технической безопасности;

акт категорирования выделенного помещения;

технический паспорт на защищаемое помещение;

памятку по обеспечению режима безопасности и эксплуатации оборудования, установленного в защищаемом помещении.

Группа информационно-аналитической деятельности работает на основе соответствующего положения о группе.

Информационная безопасность фирмы должна строиться на принципах непрерывности и комплексности, а это означает, что обеспечение защиты информации не может быть одноразовым актом или затрагивать только отдельную сторону деятельности фирмы. Злоумышленники постоянно ищут слабые звенья в системе защиты информации.

Правильное построение системы защиты информации зависит от знания угроз конфиденциальной информации (КИ). Основными угрозами КИ являются ее разглашение, утечка и несанкционированный доступ к ее источникам. Причем, разглашение коммерческих секретов составляет примерно 42% от всех угроз, поэтому особое внимание следует обращать на пресечение разглашения КИ собственным персоналом фирмы[[4]](#footnote-4).

Комплекс мероприятий по созданию системы информационной безопасности фирмы включает три направления: правовое, организационное и инженерно-техническое.

Правовую базу информационной безопасности на государственном уровне составляют законы РФ ("О государственной тайне", "Об участии в международном информационном обмене", "Об информации, информатизации и защите информации","Об авторском праве и смежных правах", "О патентах и др.), "Доктрина информационной безопасности", "Указ Президента РФ "Об утверждении перечня сведений конфиденциального характера", "Положение о лицензировании деятельности по технической защите конфиденциальной информации", Гражданский и Уголовный кодексы, а также соответствующие нормативно-правовые акты (ГОСТы, положения, инструкции и др.)

Особое внимание следует обратить на правильное применение ст.139 "Служебная и коммерческая тайна" Гражданского кодекса РФ.

К основным организационным мероприятиям можно отнести:

организацию режима и охраны. Их цель - исключение возможности проникновения посторонних лиц на территорию и в помещения, создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа и др.;

организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая знакомство с сотрудниками, обучение правилам работы с КИ, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;

организацию мониторинга телефонных переговоров, ведущихся из офиса;

организацию работы по систематическому и строгому контролю пребывания в контролируемой зоне сотрудников и посетителей, контролю за работой персонала с КИ, за порядком учета, хранения и уничтожения документов и технических носителей;

разработку соответствующих организационно-распорядительных документов, обеспечивающих выполнение всех вышеперечисленных действий.

Задачи инженерно-технического направления заключаются в том, чтобы предотвратить утечку КИ по различным каналам: визуально-оптическим, акустическим, электромагнитным и материально-вещественным (отходы производства, бракованные изделия и др.)

В целях защиты от наблюдения и фотографирования обьект защиты необходимо располагать так, чтобы исключить отражение света в сторону возможного расположения злоумышленника, использовать средства преграждения или значительного ослабления отраженного света: ширмы, экраны, шторы, ставни, темные стекла и другие преграждающие среды и преграды, применять средства маскирования и имитации с целью введения в заблуждение злоумышленника.

Для защиты от подслушивания используют звукоизоляционные и звукопоглощающие материалы: вату, ворсистые ковры, пенобетон, пористую сухую штукатурку, герметические акустические панели, изготавливаемы из стекловаты.

Для защиты информации от утечки через стены, потолки, полы, окна, двери, трубы, вентиляционные коммуникации используют генераторы шума.

Наибольшее распространение получает установка телефонных радиозакладок. Простейшими и в тоже время крайне важными мерами борьбы с подслушиванием телефонных переговоров являются мероприятия по обеспечению строгой дисциплины ведения телефонных переговоров. Внешней телефонной связью должен пользоваться ограниченный круг лиц. Никакие частные переговоры из выделенных помещений не допускаются. Наименования организаций, учреждений, должностных лиц, фамилия и другие сведения не должны употребляться в ходе переговоров. Запрещается передача по телефону распоряжений, отчетов, сведений о составе, состоянии и деятельности фирмы.

Прокладка телефонных линий должна быть выполнена таким образом, чтобы можно было удобно их контролировать и трудно использовать для подслушивания.

В целях своевременного определения постороннего включения необходимо обеспечить постоянное наблюдение за состоянием телефонных линий выделенных помещений. О всяком изменении слышимости разговоров или появлении шумов, тресков могущих свидетельствовать о включении в линию прослушивающей аппаратуры, необходимо сообщать в СБ фирмы.

Рекомендуется отключать телефонный аппарат от телефонной линии посредством разъемной розетки на период проведения конфиденциальных переговоров. Таким образом, очень просто ликвидируется источник (телефон подслушивания).

Весьма эффективной мерой противодействия подслушиванию переговоров является использование для конфиденциального общения маскираторов речи или скремблеров, шифрующий речевой сигнал до его передачи в телефонную линию.

Для обнаружения радиомикрофонов и телефонных радиозакладок применяются индикаторы поля.

Нелинейные локаторы обеспечивают обнаружение в предметах интерьера и строительных конструкциях помещения технических средств несанкционированного подключения и подслушивания.

Особый случай - посещение злоумышленниками различных мероприятий, исключающие изъятие принесенных радиозакладок. В этом случае прибегают к постановке активных радиоэлектронных помех, нарушающих работу системы радиоподслушивания.

Для обнаружения незаконных подключений к линиям связи применяется аппаратура проверки проводных линий (анализаторы телефонных линий, тесты-комплекты для выявления подключений к любой проводной линии).

Для защиты от радиоперехвата рекомендуется [[5]](#footnote-5):

выбирать направление радиосигнала в сторону наименьшей возможности его приема;

сокращать до минимума время радиоразговора;

использовать направленные антенны;

уменьшать ширину диаграммы направленности антенн;

использовать скрытые режимы передачи информации;

снижать интенсивность излучения;

использовать радиомолчание;

создавать активные и пассивнее помехи;

организовать ложную работу;

изменять режимы работы.

В целях выявления брешей в системе защиты информации и объективной оценки уровня информационной безопасности фирмы необходимо своевременно осуществлять аудит информационной безопасности фирмы.

Технологии против терроризма. Как известно, терроризм постоянно "обогащается" новейшей информационной технологией, "интеллектуализируется" и "подбирается" к совремнному оружию массового поражения (ядерному, радиоционному, биологическому, химическому).

Терроризм не имеет определенного объекта нападения. В любой момент им может стать крупный политический или финансовый лидер, большое скопление народа или офис фирмы. Причем, теракт, как правило, кропотливо и тщательно готовится. Большое преимущество у террористов - фактор внезапности.

Поэтому необходимо каждодневно предпринимать превентивные (упреждающие) меры против теракта. Чтобы предотвратить пронос средств терроризма на территорию, необходимо организовать посты наблюдения, проверки посетителей, ручной клади ввозимых (вывозимых) грузов. Такие посты должны быть оснащены биноклями (зрительными трубами), приборами ночного видения (возможно тепловизорами), детекторами взрывчатых веществ, металлоискателями, рентгенотелевизионной аппаратурой (при необходимости и др.).

Помочь в получении сведений о планах и намерениях террористов могут средства радиоконтроля разговоров, средства радиоперехвата каналов и линии связи террористов.

Следует подчеркнуть, что основным методом в работе сотрудников поста проверки должен стать аналитический подход, когда выявляются не только объекты, подозрительные своей схожестью с предметами терроризма, но и подозрительные моменты в поведении людей.

Для обеспечения личной безопасности на фирме рекомендуется[[6]](#footnote-6):

не заводить знакомства с криминальными элементами;

не совершать противоправных и аморальных поступков, которые могут стать причиной шантажа;

периодически отслеживать не установлено ли за сотрудником фирмы наблюдение;

быть бдительным при подходе к офису. Обращать внимание на возможность наличия рядом необычных проводов и предметов, подозрительных людей;

не оставлять никому ключи от своего кабинета;

закрывать свой кабинет, даже если нужно выйти всего на несколько минут;

не принимать посетителей при открытых сейфах, расположенных на столе документах;

до приема посетителей убирать со стола предметы, которые могут использоваться для внезапного нападения;

отказываться от угощений со стороны посетителей во избежание отравления; с посетителями вести себя спокойно, если их действия становятся агрессивными, пригласить сотрудника СБ или вызвать сотрудника милиции;

о замеченных вблизи офиса подозрительных моментах и проишествиях на рабочем месте незамедлительно сообщить в СБ фирмы.

Чтобы избежать почтового терроризма, необходимо знать признаки подозрительных почтовых отправлений, а также рекомендуется организовать пост проверки почтовой корреспонденции. Последний должен находиться в отдельном помещении и должен быть оснащен металлоискателем, индикатором ионизирующего излучения, рентгенотелевизионной установкой[[7]](#footnote-7).

Особую бдительность должна проявлять секретарь руководителя. Чисто психологически собственный секретарь, передающий пакет, сувенир или лекарство своему руководителю, не вызывает естественной настороженности, испытываемой к незнакомому посыльному.

## Заключение

Служба безопасности (СБ) имеется на каждом крупном и среднем предприятии (фирме) и выполняет многообразные функции по обеспечению экономической и информационной безопасности бизнеса.

Служба безопасности - это правоохранительная некоммерческая организация, оказывающая охранно-сыскные услуги своему (своим) учредителю (учредителям) и другим организациям на основе действующего законодательства, собственного Устава и заключенного с ними договора.

Цель деятельности СБ - своевременное пресечение (нейтрализация) противоправных посягательств на экономические интересы и персонал предприятия.

Служба безопасности выполняет многообразные функции и обеспечивает экономическую и информационную безопасность бизнеса.

Исходя из всего вышеизложенного, можно сделать следующие выводы - без службы безопасности не сможет стабильно работать ни одно крупное и среднее предприятие (фирма), поскольку СБ - это гарант бесперебойной и безопасной работы предприятия.

## Список литературы

1. Гражданский кодека РФ. М: Юрайт, 2005-521с.

2. Кодекс административных правонарушений РФ. М: Высшая школа, 2005-429с.

3. Трудовой кодекс РФ. М: Феникс, 2004-512с.

4. Л.Г. Кедровская, В.И. Ивакин "Мир безопасности", N11 (120), 2003, 56с.

5. И.Н. Морозова "Технологии против терроризма"-М: ОЛМА-ПРЕСС, 2004,87с.

6. Общая теория государства и права. Том 3 М: ИКД "Зерцало-М", 2004,.219 с.

7. А.П. Полежаев, М.Ф. Савелий "Борьба с почтовым терроризмом", "Мир безопасности", N 12 (121), 2003,.62с.

8. Развитие правовой основы деятельности служб безопасности. В.П. Мак-8. Мак, "Мир безопасности", N 10 (119), 2003г, 58с.

9. В.И. Ярочкина "Система безопасности фирмы"-М: Ось-89, 2004. - 345с.

10. В.И. Ярочкина "Информационная безопасность"-М: Академический проспект; "Фонд мир", 2004-321с.

1. Развитие правовой основы деятельности служб безопасности. В.П. Мак-Мак, «Мир безопасности», N 10(119),2003г, с.47 [↑](#footnote-ref-1)
2. Общая теория государства и права. Том 3 М: ИКД «Зерцало-М», 2004,с.219 [↑](#footnote-ref-2)
3. Л.Г.Кедровская, В.И.Ивакин «Мир безопасности», N11(120), 2003,с.43 [↑](#footnote-ref-3)
4. В.И. Ярочкина «Система безопасности фирмы»-М:Ось-89,2004.-112с. [↑](#footnote-ref-4)
5. В.И. Ярочкина «Информационная безопасность»-М: Академический проспект; «Фонд мир»,2004-321с. [↑](#footnote-ref-5)
6. И.Н.Морозова «Технологии против терроризма» - М: ОЛМА-ПРЕСС, 2004, 87с. [↑](#footnote-ref-6)
7. А.П.Полежаев, М.Ф.Савелий «Борьба с почтовым терроризмом», «Мир безопасности», N 12(121), 2003, с.32 [↑](#footnote-ref-7)