

МЕКРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

Київський інститут
менеджменту
С.В.Н.І.
МАУП

В.Е.Карпов
П.Ф.Закревский

Служба безопасности - залог успеха предпринимательства



СЛУЖБА БЕЗОПАСНОСТИ -
ЗАЛОГ УСПЕХА ПРЕДПРИНИМАТЕЛЬСТВА

1 ТОМ

МЕЖРЕГИОНАЛЬНАЯ АКАДЕМИЯ УПРАВЛЕНИЯ ПЕРСОНАЛОМ

Кировоградский институт имени Святого Николая

СЛУЖБА БЕЗОПАСНОСТИ

Учебно-практическое пособие в 2 томах

1 том:

**“Служба безопасности —
залог успеха предпринимательства”**

Авторы не претендуют на абсолютность данного учебно-практического пособия. Мы высказываем свою точку зрения на многие, жизненно-важные вопросы профессиональной подготовки, пытаемся раскрыть механизмы действия по организационным вопросам негосударственной Службы безопасности. Прежде, чем высказывать свои мысли, авторы ознакомились с материалами видных специалистов, выражают им искреннюю благодарность за использованные материалы, подсказки в подготовке и составлении данного издания. Мы заранее благодарим читателей за будущие критические замечания и выражаем уверенность в том, что все их пожелания будут учтены в следующем выпуске книги.

Авторы

Кировоград
2008

ББК 88.59
УДК 351.749; 159.98
К 26

Межрегиональная академия управления персоналом
Кировоградский институт имени Святого Николая

Карпов В.Е. Закревский П.Ф.
Служба безопасности. 1 том. “Служба безопасности – залог успеха предпринимательства”, – Кировоград, МАУП, – 2008, 312с.

Рецензент: **СВИРЕНЬ Н.А.**, академик, канд. техн. наук, профессор.

Учебно-практическое издание, (на рус. яз.)
Рекомендовано к изданию Кировоградский институтом имени
Св. Николая, МАУП. м.Кировоград.

Под общей редакцией: В.Е. Карпова, академика, доктора философии
по психологии, член-корреспондента, старшего преподавателя Киро-
воградского института им. Святого Николая, МАУП.

Книга охватывает проблемы организационного менеджмента по созданию негосударственной Службы безопасности, трудовой адаптации, социально-психологическим проблемам службы безопасности хозяйствующего субъекта и психологии межличностных отношений на современном этапе с учетом конкретной специфики профессионально – служебной деятельности. Рассчитано на специалистов и работников предприятий различных форм собственности, банков, фирм и личной предпринимательской деятельности. Рекомендовано студентам, курсантам Вузов, средних учебных заведений, слушателям курсов подготовки и переподготовки, повышения квалификации кадров, руководителям подразделений и служб кадровой работы, массового читателя.

ББК 88.59
© Карпов В.Е. Закревский П.Ф.

Кировоград. 2008.

Оглавление

Введение	6
Служба безопасности – залог успеха предпринимательства	12
Система безопасности предприятия	13
Политика, положение и стратегия безопасности предприятия ..	17
Научная теория обоснования безопасности предприятия	18
Субъекты безопасности предприятия	20
Средства и методы обеспечения безопасности	21
Концепция деятельности службы безопасности предприятия. (Типовой проект)	22
Методика разработки комплексной концепции безопасности коммерческой структуры	23
Концепция деятельность службы безопасности (Строго конфиденциально)	25
1. Общее положение, (применительно к Украине).	25
2. Организация службы безопасности	30
3. Деятельность службы	41
4. Обеспечение деятельности службы	45
Правовые основы деятельности службы безопасности	46
Правовые основы деятельности службы безопасности предприятия в Украине	48
Особенности национальных рынков безопасности	52
Изменения и реформы.	54
Перед Законом – все должны быть равны	56
Государственная и негосударственная СБ	59
Организация, (создание) службы безопасности	61
Задачи, положение и типовая структура СБ.	70
Типовая структура службы безопасности	71
Штатная структура и профессиональные требования к сотрудникам СБ.	71
Функции подразделений службы безопасности	72
Практическая документация по созданию СБ.	74
Охрана стационарных объектов	85
Характеристика и виды стационарных объектов	86
Система обеспечения безопасности объекта.	87
Классификация охраняемых стационарных объектов	88
Приёмы осмотра и контроля охраняемого объекта	95
Порядок приема стационарных объектов под охрану	96
Защита персонала предприятия от насильственных преступлений.	98
Охрана имущества предприятия	98
Организация инженерно-технической защиты охраняемого объекта	99
Обеспечение порядка в местах проведения руководством предприятия массовых мероприятий	99
Устранение причин способствующих совершению преступлений против собственности предприятия	99
Способы охранной деятельности	101
Движение по объекту с временными остановками и осмотром уязвимых мест	102

Система “Диспетчер”	103
Основные требования к режиму охраны объекта	105
Образцы служебной документации	
по охране стационарных объектов	108
1. Журнал дежурства	109
ЖУРНАЛ дежурства охранников по охране	
офиса Предприятия	109
2. График дежурства охранников на месяц	109
3. Табель поста	110
4. Журнал приема под охрану ключей от кабинетов	113
5. Журнал приема помещений на КМЕ	
(концентратор малой емкости)	113
6. Журнал распоряжений и указаний охране	113
7. Паспорт на офис предприятия	114
Инструкция работнику охраны	
по охране труда и технике безопасности	116
Система охраны периметра	118
Нормативные требования к построению системы	
охранной сигнализации	119
Понятия “Концепция охраны периметра предприятия”	119
Модель периметра	120
Варианты типовых моделей нарушителей	124
Раннее обнаружение нарушителя – задача ПСО	128
Как подойти к выбору?	128
Что надо знать о компонентах ПСО?	129
Блоки и системы питания, включая дистанционное управление	132
Заграждения – как элемент комплекса технических	
средств охраны периметра	138
Автономные и быстро разворачиваемые системы	140
Ложные тревоги охранной системы периметра	141
Три подхода борьбы с ложными тревогами	145
Новинки систем видеонаблюдения	146
Оборона Вашего дома	151
Предложение рынка Украины	152
Приложение	154
Основные марки взломостойких замков, представленных	
на украинском рынке (2008 г.)	154
Технические средства охраны	155
Контрольно-пропускной режим на предприятии	157
Организация контрольно – пропускного	
режима предприятия (КПР)	158
Подготовка исходных данных для разработки	
контрольно-пропускного режима	159
Классификация категорий режимности	160
Разработка инструкций пропускного режима	161
Виды пропусков	162
Контрольно-пропускной пункт. (КПП)	163
КПП для прохода людей	163
Автотранспортные КПП	164
Допуск сотрудников и посетителей на объект	166

Допуск на территорию предприятия транспортных средств, вывоз материальных ценностей	167
Основные признаки возможного нападения на объект охраны .	168
Критерии эффективности работы охранного подразделения .	170
Типовой перечень документов, находящихся на КПП. (Для России)	170
Типовой перечень документов, находящихся на КПП. (Для Украины)	173
Защита коммерческой тайны предприятия	177
Роль руководства банка в обеспечении безопасности	178
Промышленный шпионаж против банков и фирм	180
Подготовки и совершения преступных акций против предпринимательских структур	180
Структура, функции, цели и задачи службы безопасности банка	183
Объекты защиты, силы и средства службы безопасности банка	186
Комплекс мер по обеспечению безопасности банка, (предприятия, фирмы)	186
Особенности работы службы безопасности банка	191
Особенности сохранения банковской тайны	193
Открытие банковской тайны	197
Инкассация денежных средств.	201
Правила и приемы безопасности при инкассации денежных средств.	205
Документы, закрепляющие право предприятия на коммерческую тайну	207
«Перечень сведений, составляющих коммерческую тайну предприятия»	207
Приложение к 1 книге	213
Типовое положение о конфиденциальной информации и защите коммерческой тайны.	213
Инструкция по защите конфиденциальной информации . . .	225
Типовая инструкция по охране труда и технике безопасности .	258
Типовой перечень содержимого аптечки первой доврачебной помощи	272
Общая инструкция по пожарной безопасности охраняемого объекта	273
Инструкции, регламенты, договоры, справочные материалы	286
1.) Служба безопасности и охраны (21)	286
2.) Режим и защита информации (25).	287
3.) Пожарная безопасность (10)	288
4.) Договоры (9)	288
5.) Дополнение (По необходимости).	288
Словарь специальных терминов.	289
Список использованной литературы	301

ВВЕДЕНИЕ

С учетом сложившейся правовой и экономической ситуации: в России, Украине и странах СНГ, уже сформировался интерес к негосударственной службе безопасности, проблеме защиты предприятия и предпринимательских интересов, личности предпринимателя в целом, его физической защиты в частности. Пренебрежение вопросами защиты предпринимательства уже оказывает существенное негативное воздействие на экономическую инфраструктуру государства, на все важные стороны общественной жизни, в том числе экономику, управление, социальную и правовую сферы, международные отношения. Вместе с тем, пока еще не сформировалась единая точка зрения на обеспечение безопасности в комплексе, где охрана и защита – являлась бы органичным элементом этого комплекса. Необходимость высокой профессиональной подготовки специалистов предпринимательской, (негосударственной) службы безопасности, частных детективов и охранников очевидна и ни у кого не вызывает сомнения. Особенно это важно, когда речь идет о больших предприятиях, влияющих на экономику государства, охране личности, жизни и здоровья человека, который доверил эти высшие ценности – профессионалу.

Долгое время собирался и накапливался материал по общей теме: «Безопасность Бизнеса и Бизнесмена». В ранее изданных учебных пособиях, мы рассматривали, в основном, практические и психологические вопросы системы службы безопасности предприятий с различными формами собственности и охраны физических лиц в сфере предпринимательства. Сейчас авторы предлагают рассмотреть эти вопросы с практических позиций руководителя негосударственной, (коммерческой) службы безопасности, (НСБ) и задач сегодняшнего дня:

- 👁 Физическая охрана объектов
- 👁 Пультовая охрана
- 👁 Охрана грузов при транспортировке.
- 👁 Охрана инкассаторов и материальных ценностей.
- 👁 Обеспечение порядка при проведении массовых мероприятий.
- 👁 Личная охрана
- 👁 Экстренная помощь
- 👁 Информационно-аналитические услуги
- 👁 Безопасность бизнеса, и т.д.

В новом учебном пособии подробно изложены, практические рекомендации, применительно к менеджменту безопасности предпринимательства по проведению профилактической, аналитической, консультационной, кадровой работы и применения нормативно-правовой базы деятельности негосударственных служб безопасности хозяйствующего субъекта.

Авторы книги обладают поразительной способностью всецело погружаться в любые области жизни, в которых воплощаются на практике самые ценные знания, переводя их в эффективную и общедоступную форму

понимания. Целенаправленностью и скрупулезностью в исполнении любой задачи они напоминают опытного “мастерового”, а глубиной познаний и широтой взглядов – корифеев новой науки. Иметь такую личность в кругу своих коллег – огромная честь для любого коллектива.

Заинтересованным лицам, массовому читателю, наши авторы предлагают ознакомиться с ранее изданными учебными пособиями: “Менеджмент безопасности” в 2 томах, (теория и практика). 2007. “Наука совершенствования” 2008., электронные книги с практическими рекомендациями по теме: «Безопасность Бизнеса и Бизнесмена», и другими наработками, (см. подробнее) на сайте >>> http://alpha-shop.com.ua/book_Sec.htm). Много интересных изданий по данной теме, есть и у других авторов, но каждая в отдельности книга, просто технически не может ответить Вам на повседневно возникающие практические вопросы по осуществлению безопасности Вашего предприятия.

Мы утверждаем, универсальной системы безопасности не существует. Каждая система безопасности – это уникальный продукт. Торговое предприятие, например, и страховая компания очень отличаются друг от друга. Тем не менее, существует общий алгоритм выявления, предупреждения, и пресечения угроз, которые могут носить скрытый или открытый характер, и который, применим для любой системы.

Особенно актуальной эта проблема становится в “эпоху перемен”, при смене одного общественного строя, экономического уклада другим, поскольку криминальные элементы используют обстановку законодательного вакуума, правового нигилизма, экономико-правовой незащищенности, активизируют свои преступные посягательства на экономику в целом, на формирующийся класс частных предпринимателей, их собственность, права, а, зачастую, и жизнь. Негосударственные службы безопасности предприятий, частные детективные и охранные организации, как в России, так и в Украине за последние годы получили широкое распространение, о чем пишут авторы настоящей книги, и тенденция их увеличения продолжают иметь место. Следует заметить, что в отличие от других стран, охранные предприятия в Украине развиваются, но они не входят в единую государственную систему охраны. Эти подразделения сегодня имеют право осуществлять охрану объектов, имущества и персонала только коллективной или частной форм собственности.

Свойство любой информации – «может к вечеру устареть», но к вопросам безопасности это относится в меньшей степени.

Мы с полной ответственностью заявляем, что меняются политические линии наших государств, подходы к принципам работы СБ в странах СНГ, России и Украины, их нормативно-правовое обеспечение, но основы организации коммерческих служб безопасности и их востребованность – остаются неизменными.

К вопросу о личной безопасности, охраны предприятия, многие руководители относятся – скептически, “пока не грянет гром”. Именно этим наши авторы и воспользовались в вопросах создания новой книги в 2 томах: «**Служба безопасности**», (учебно-практическое пособие).

Книга предназначена, для руководителей подразделений частных служб безопасности и охранных предприятий, (подготовки и переподготовки кадров службы безопасности хозяйствующего субъекта), частной охраны предпринимателей в системе негосударственных служб безопасности, а также, как практическое пособие для частных охранников и телохранителей, при организации и непосредственном осуществлении ими мероприятий по охране предпринимателей, членов их семей, персонала коммерческих структур и т.п.

Основными задачами обучения по разработанным в книге практическим программам – являются основы формирования у будущих работников службы безопасности хозяйствующего субъекта, охраны и телохранителей, профессионально-психологической готовности к осуществлению своих профессиональных действий, овладение специальными методами и навыками, развитие и совершенствование профессионально-значимых личностных качеств и, на основании этого, формирование профессионального мышления у выше назначенных специалистов.

Одной из наиболее интенсивных форм участия хозяйствующих субъектов в обеспечении безопасности лица и предпринимательства является их деятельность, например, в рамках обществ с ограниченной ответственностью, связанных с охраной коллективной, частной собственности, офисов, граждан, обеспечения технической защиты информации и т. д.; информационного, детективного, консультационного характера по вопросам права безопасности. Эффективность решения задач по защите предпринимательства в условиях реализации курса радикальных реформ в Украине и странах СНГ, требует комплексного подхода и единства действий государственных органов и негосударственной системы безопасности предпринимательства, в частности милиции, органов госбезопасности, охранных, охранно-технических и детективных предприятий частной формы собственности. Однако эта деятельность не стала приоритетной даже для правоохранительных органов. Назрела необходимость практических решений по следующим задачам:

- **во-первых**, выяснения научно-познавательной основы защиты предпринимательства в условиях рыночной экономики и проведения анализа эффективности функционирования в государстве механизма правовой системы защиты хозяйствующего субъекта;

- **во-вторых**, обоснованного установления и определения функций правоохранительных органов и хозяйствующих субъектов в организации и осуществлении защиты предпринимательской деятельности;

- **в-третьих**, рассмотрения характеристик форм деятельности, субъектов негосударственной системы безопасности предпринимательства по организации защиты хозяйствующих субъектов от противоправных посягательств и методов их работы в сфере правопорядка.

Названные вопросы относятся к ряду тех проблем теории и практики безопасности предпринимательства, которые можно назвать ключевыми, требующими тщательного исследования.

Научная новизна двухтомной книги: “Служба безопасности”, определяется целенаправленным функциональным анализом деятельности субъектов, (негосударственной) системы безопасности предпринимательства по защите предприятия от внешних и внутренних угроз, выражается концептуальным подходом к анализу исследуемого объекта, постановкой проблемы и избранной методикой ее разрешения, а также теоретическими и практическими выводами, положениями и обоснованными предложениями.

Осуществление действий негосударственной службой безопасности по защите предприятия от внешних и внутренних угроз, в научной литературе преимущественно освещается в плане общетеоретической характеристики отдельных ее аспектов. В написании книги, авторы руководствовались: научными методами системно-структурного и функционального анализа, направленного на выявление закономерностей деятельности негосударственной службы безопасности, а также методами нормативно-юридического анализа, отдельными общенаучными исследованиями как логическими (аналогия, сравнение, анализ и др.), так и эмпирическими, (непосредственное наблюдение практики работы структурных подразделений негосударственной службы безопасности). При этом выделили приоритетные направления:

1 – Объектом – является **деятельность** службы безопасности хозяйствующего субъекта (предприятия) по нейтрализации дестабилизирующих факторов, которые причиняют или могут причинить ущерб функционированию предприятия или сделать его невозможным;

2 – Предметом – организационно-правовые **вопросы управления** системой обеспечения безопасности предприятия, формы и методы осуществления подразделением безопасности конкретных функций по защите хозяйствующего субъекта от внешних и внутренних угроз.

3 – Цель состоит в том, чтобы на основе уяснения сущности “безопасности” в контексте социальных реалий авторы предлагают соответствующее комплексное решение проблемы защиты хозяйствующего субъекта (предприятия) от внешних и внутренних угроз.

4 – Основами написания книги – служат представленные в современной литературе наработки, идеи и концепции по развитию негосударственной системы безопасности предприятия и отдельной личности, в Украине, России и странах СНГ. Например, при анализе законодательства по защите предпринимательства, использовались формально-юридические и сравнительные подходы этих государств.

Субъективное отношение авторов к этой комплексной проблеме в большой степени зависит от самой специфики подхода к решению данного вопроса. По нашему мнению, для дальнейшей разработки научно-познавательных основ охранной, детективной деятельности и всей службы безопасности хозяйствующего субъекта, будет способствовать учет ряда отправных положений, на которые хотелось бы обратить внимание.

👁 Безопасность хозяйствующих субъектов – способ защиты и отстаивания своих прав, свободы и других ценностей, помогая

государству в решении этих проблем, контролируя и поправляя его.

- ☞ Цель безопасности хозяйствующих субъектов – защита своих прав, свобод, имущества, интересов.
- ☞ Критерий безопасности хозяйствующих субъектов – наличие организации, стратегии, тактики отстаивания своих интересов, умение противостоять произволу и агрессивности других субъектов безопасности.
- ☞ Безопасность личности – это способность и готовность государства, общества и индивидов ограждать и освобождать себя от опасностей и угроз для жизни и здоровья, имущества, а также фундаментальных гражданских ценностей – законных прав и свобод.
- ☞ Эффективное решение задач по защите, безопасности и правовому обеспечению субъектов детективно-консультационного обеспечения.
- ☞ Цель безопасности лиц – защита жизни, здоровья, имущества, прав и свобод каждого человека.
- ☞ Критерий безопасности лица – сохранение и увеличение средней продолжительности жизни.
- ☞ Объекты безопасности личности: человек и его жизненные интересы.

Нашими авторами, при написании данного учебного пособия, использовались известные отечественные и зарубежные литературные источники по службе безопасности хозяйствующих субъектов, проблемам осуществления охранной деятельности и подготовки телохранителей, а также собственные исследовательские и методические материалы о социально-психологических проблемах службы безопасности субъекта предпринимательства. Назрела необходимость в том, чтобы поднять вопрос о совместной деятельности милиции, СБУ, коммерческих служб безопасности предприятий разных форм собственности в сфере защиты предпринимательства, и эта проблема, носила плановый характер, предусматривала согласование действий по защите от противоправных посягательств со стороны различных злоумышленников.

Авторы выражают искреннюю признательность тем, кто оказывал на них влияние и помогал в написании книги. Авторы подчеркивают, что не претендуют на абсолютность мыслей в данном издании, возможно аналогичные мысли высказывали и другие издатели, но авторам это не известно. Если будут пожелания и предложения по дальнейшем усовершенствованию книги – авторы будут благодарны читателям.

Невозможно упомянуть всех поименно, кто помогал в написании книги: С.К.Деликатный и Ж.Ю.Половникова, В.П.МакМак и А.В.Тимченко, А.И.Белоусов и В.Е.Христенко, Э.И.Низенко и А.Н.Бандурко, А.А.Чернявский и А.Г.Шаваев. Особенно следует выделить работы других авторов: Ю.Кюгута и А.Крысина, И.Давыдова и А.Тодурова,

В.Гаченкова и А.Барановского, Ю.Антоняна и А.Алексеева, С.Тарарухина и В.Кабачного и многих других авторов.

Наши авторы особенно признательны:

Макарову Р.Н. доктору психологических наук, доктору педагогических наук, профессору, академику, президенту Международной академии проблем Человека в авиации и космонавтике, автору более 650 научных трудов;

Петкову В.П. доктору юридических наук, профессору, академику, отличнику народного образования Украины, автору более 50 научных трудов;

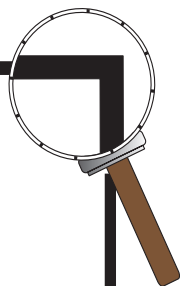
Михайлову В.М. академику МАК, специалисту с национально-патриотического воспитания молодежи, главному редактору по техническому оформлению нашей 2 томной книги.

Цуркану Л. П., полковнику в отставке МВС Украины, ведущему специалисту ГСО в Кировоградской области, почётному академику МАПЧАК, автору уникальных пособий по подготовке молодых специалистов в системе охранной деятельности.

Лебедеву С.В., полковнику запаса ВСУ, военному специалисту, директору АБ “Тайфун”, начальнику специального подразделения охраны общественного порядка в г. Львове, который имеет уникальные организаторские способности, а также специалистам УМВС Украины во Львовской и Кировоградской областях и многим другим заинтересованным и порядочным людям.

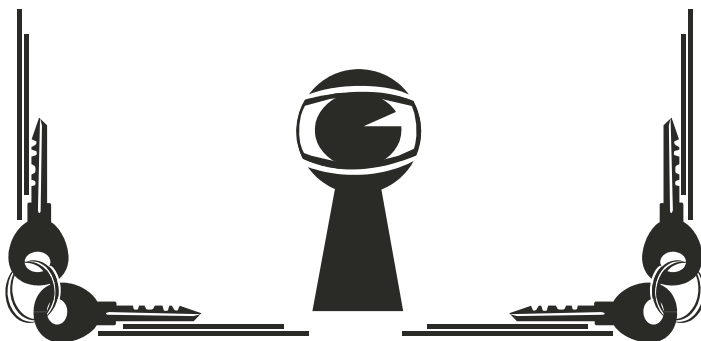
Особая признательность ведущим специалистам по техническому обеспечению: Плаксиенко Л.Л., Дудниковой Л.В. и Власенко В.П. (г.Кировоград) — их ответственность позволила наработать необходимый банк данных и провести колоссальную работу по исполнению данной книги.

***Н.А.Свирень**, академик, канд..тех.наук, профессор.
Директор Кировоградского института
имени Святого Николая, МАУП.*



РАЗДЕЛ 1

Служба безопасности — залог успеха предпринимательства





Система безопасности предприятия

В период реализации рыночных реформ в странах СНГ, России и Украины было предложено и одобрено множество программ экономического и социального развития. Их выполнение позволило создать необходимые условия для рыночных социально-экономических преобразований в стране, привело к кардинальным изменениям общественных отношений. Центральной фигурой в негосударственном секторе экономики становится предприниматель: (частный предприниматель, юридическое лицо).

Весьма важным фактором в оценке развития и демократии социального государства является правовая защита граждан с учетом правового статуса личности, включающего права, свободу и обязанности граждан. Поэтому в современных условиях защита прав и интересов от противоправных посягательств приобретает в странах СНГ, России и Украине особое значение. Авторы книги отмечают, что исследуя другие авторские работы на данную тему, везде акцентируется совокупность элементов и отношений между ними, образующих систему обеспечения безопасности: личности, предпринимательства, государства, основанного на комплексно-системном подходе с конкретной подготовкой целенаправленных программ.

Как ранее отмечалось, авторы книги, (имея соответствующий практический опыт работы, преподавания в ВУЗе, издавши более 20 учебно-методических пособий по тематике книги, в 2007 г. написали 2 томный учебник, (теория и практика): “Менеджмент безопасности”) для студентов, курсантов и слушателей специализированных курсов. Дополнительно издали: “Наука совершенствования” 2008., и уникальные по практическому применению – электронные книги: «Безопасность Бизнеса и Бизнесмена», (см. на сайте > http://alpha-shop.com.ua/book_Sec.htm). А также другие практические рекомендации по нашей теме.

Много интересных изданий по данной теме, есть и у других авторов, но каждая в отдельности книга, просто технически не может ответить Вам на повседневно возникающие практические вопросы по осуществлению безопасности Вашего предприятия. При написании данной главы: “Системы безопасности предприятия”, мы обратились за помощью к изданиям ведущих специалистов, в которых проблемы защиты предприятия от внешних и внутренних угроз стали предметом специального анализа. Изучались мнения начальников отделов, руководителей подразделений, непосредственных исполнителей, при обосновании важнейших теоретических позиций и специалистов службы безопасности различных направлений.

Мы с полной уверенностью должны сказать, что понять любое поведение, в том числе и преступное, невозможно без подлинного знания психологии личности, психологических механизмов и мотивов, социально-психологических явлений и процессов, а нередко и психиатрии

ческих факторов. А такие знание ни в коем случае не могут быть получены только путем изучения чужих работ, что еще раз подтверждает неразрывную связь между личностью и поведением.

Созданию службы безопасности предприятия обычно предшествуют два события: либо это острое желание руководителей предприятия отреагировать на внезапно возникшие реальные угрозы имуществу, физической расправы с персоналом и т.д., либо это основанный на результатах исследования вывод о неудовлетворительном состоянии безопасности предприятия. В первом случае созданная поспешно служба безопасности способна в некоторой степени отразить угрозы и в дальнейшем реагировать на их появление по принципу «угроза – отражение». Дело меняется существенным образом при реализации второго варианта. После детального изучения состояния безопасности предприятия (с привлечением специалистов, если их нет на предприятии) у его руководителей появится реальное представление о системе безопасности предприятия.

Такое системное представление (зафиксированное в письменной форме) позволяет осознанно и целенаправленно проводить работу по обеспечению безопасности предпринимательской деятельности и самого предприятия всеми его подразделениями и сотрудниками. При этом ведущая роль службы безопасности не исчезает, наоборот, понимание своей роли и места в системе безопасности предприятия приведет только к положительным результатам.

Следует однако подчеркнуть, что до настоящего времени нет единого подхода к определению понятия «система безопасности предприятия». Чтобы дать такое определение, необходимо предварительно выявить элементы этой системы. Изучение научной литературы и практики позволили автору прийти к выводу, что структурными элементами системы безопасности предприятия являются научная теория его безопасности, политика и стратегия безопасности, средства и методы обеспечения безопасности и, наконец, концепция безопасности предприятия.

Совокупность вышеперечисленных элементов составляет систему безопасности предприятия. Под объектом безопасности предприятия следует понимать степень устойчивости и развития предприятия, его способность противостоять угрозам.

В объекте безопасности предприятия можно выделить:

- различные структурные подразделения или группы сотрудников либо владельцы акций предприятия;
- ресурсы предприятия (информационные, кадровые, материально-технические, информационные, интеллектуальные и финансовые);
- различные виды деятельности (управленческая, производственная, снабженческая и т.д.).

Целью обеспечения безопасности предприятия является комплексное воздействие на потенциальные и реальные угрозы, позволяющее ему успешно функционировать в нестабильных условиях внешней и внутренней среды.

Достижение этой цели требует реализации следующих задач:

- выявление угроз для стабильности и развития предприятия и выработка мер по их противодействию;
- обеспечение защиты технологических процессов;

- реализация мер противодействия всех видов шпионажа (промышленного, научно-технического, экономического и т.д.);
- своевременное информирование руководства предприятия о фактах нарушения законодательства со стороны государственных и муниципальных органов, коммерческих и некоммерческих организаций, затрагивающих интересы предприятия;
- предупреждение переманивания сотрудников предприятия, обладающих конфиденциальной информацией;
- всестороннее изучение деловых партнеров;
- своевременное выявление и адекватное реагирование на дезинформационные мероприятия;
- разработка и совершенствование локальных правовых актов, направленных на обеспечение безопасности предприятия;
- реализация мер по защите коммерческой и иной информации;
- организация мероприятий по противодействию недобросовестной конкуренции;
- обеспечение защиты всех видов ресурсов предприятия;
- реализация мер по защите интеллектуальной собственности;
- организация и проведение мер по предотвращению чрезвычайных ситуаций;
- выявление негативных тенденций среди персонала предприятия, информирование о них руководства предприятия и разработка соответствующих рекомендаций;
- организация взаимодействия с правоохранительными и контрольными органами в целях предупреждения и пресечения правонарушений, направленных против интересов предприятия;
- разработка и реализация мер по предупреждению угроз физической безопасности имущества предприятия и его персоналу;
- возмещение материального и морального ущерба, нанесенного предприятию в результате неправомерных действий организаций и отдельных физических лиц.

Система безопасности предприятия может быть построена на основе следующих принципов:

1.) Приоритет мер предупреждения. Содержание этого принципа предполагает своевременное выявление тенденций и предпосылок, способствующих развитию угроз, на основе анализа которых вырабатываются соответствующие профилактические меры по недопущению возникновения реальных угроз.

2.) Законность. Меры безопасности предприятия разрабатываются на основе и в рамках действующих правовых актов. Локальные правовые акты предприятия не должны противоречить законам и подзаконным актам.

3.) Комплексное использование сил и средств. Для обеспечения безопасности используются все имеющиеся в распоряжении предприятия силы и средства. Каждый сотрудник должен в рамках своей компетенции участвовать в обеспечении безопасности предприятия. Организационной формой комплексного использования сил и средств является программа обеспечения безопасности предприятия.

4.) Координация и взаимодействие внутри и вне предприятия. Меры противодействия угрозам осуществляются на основе взаимодействия и скоординированности усилий всех подразделений, служб предприятия, а

также установления необходимых контактов с внешними организациями, способными оказать необходимое содействие в обеспечении безопасности предприятия. Организовать координацию и взаимодействие внутри и вне предприятия может комитет (группа совет и т.д.) безопасности предприятия.

5.) Сочетание гласности с конспирацией. Доведение до сведения персонала предприятия и общественности в допустимых пределах мер безопасности выполняет важнейшую роль – предотвращение потенциальных и реальных угроз. Такая гласность, однако, должна непременно дополняться в оправданных случаях мерами конспиративного характера.

6.) Компетентность. Сотрудники и группы сотрудников должны решать вопросы обеспечения безопасности на профессиональном уровне, а в необходимых случаях специализироваться по основным его направлениям.

7.) Экономическая целесообразность. Стоимость финансовых затрат на обеспечение безопасности не должна превышать тот оптимальный уровень, при котором теряется экономический смысл их применения.

8.) Плановая основа деятельности. Деятельность по обеспечению безопасности должна строиться на основе комплексной программы обеспечения безопасности предприятия, подпрограмм обеспечения безопасности по основным его видам (экономическая, научно-техническая, экологическая, технологическая и т.д.) и разрабатываемых для их исполнения планов работы подразделений предприятия и отдельных сотрудников.

9.) Системность. Этот принцип предполагает учет всех факторов, оказывающих влияние на безопасность предприятия, включение в деятельность по его обеспечению всех сотрудников подразделений, использование в этой деятельности всех сил и средств.

Система безопасности предприятия включает в себя ряд следующих подсистем:

Экономическая безопасность – состояние наиболее эффективного использования всех видов ресурсов в целях предотвращения (нейтрализации, ликвидации) угроз и обеспечения стабильного функционирования предприятия в условиях рыночной экономики.

Техногенная безопасность – совокупность действий по обеспечению проектирования, строительства и эксплуатации сложных технических устройств с соблюдением необходимых требований безаварийной их работы.

Экологическая безопасность – состояние защищенности жизненно важных интересов персонала предприятия и его имущества от потенциальных или реальных угроз, создаваемых последствиями антропогенного воздействия на окружающую среду, а также от стихийных бедствий и катастроф.

Информационная безопасность – это способность персонала предприятия обеспечить защиту информационных ресурсов и потоков от угроз несанкционированного доступа к ним).

Психологическая безопасность – состояние защищенности от негативных психологических воздействий персонала предприятия и других лиц, вовлеченных в ее деятельность.

Физическая безопасность – состояние защищенности жизни и здоровья отдельных лиц (групп, всех лиц) предприятия от насильственных преступлений.

Научно-техническая безопасность – способность персонала предприятия обеспечить защиту собственной ценной научно-технической продукции от недобросовестных конкурентов.

Пожарная безопасность – состояние объектов предприятия, при котором меры предупреждения пожаров и противопожарной защиты соответствуют нормативным требованиям.

Следует отметить, что вышеуказанные подсистемы второго уровня могут включать в себя подсистемы третьего уровня. Например, подсистемами экономической безопасности могут быть финансовая, коммерческая, имущественная и др. подсистемы безопасности.

Кроме этого, сами подсистемы не разделены между собой непроходимой границей, поскольку они настолько взаимосвязаны друг с другом, что в органическом единстве образуют единую систему безопасности предприятия. Разделение же единой системы безопасности предприятия на подсистемы второго и третьего уровня производится из методических соображений, поскольку это позволяет более детально изучить все его элементы.

Надежность и эффективность системы безопасности предприятия оценивается на основе одного критерия – степени отсутствия или наличия нанесенного ему материального ущерба и морального вреда. Содержание этого критерия раскрывается через ряд показателей:

- 1) – недопущение фактов утечки (разглашения) конфиденциальных сведений;
- 2) – предупреждение или пресечение противоправных действий со стороны персонала предприятия, его посетителей, клиентов;
- 3) – сохранность имущества и интеллектуальной собственности предприятия;
- 4) – предупреждение чрезвычайных ситуаций;
- 5) – пресечение насильственных преступлений в отношении отдельных (специально выделенных) сотрудников и групп сотрудников предприятия;
- 6) – своевременное выявление и пресечение попыток несанкционированного проникновения на охраняемые объекты предприятия.

Политика, положение и стратегия безопасности предприятия

Политика безопасности предприятия – это общие ориентиры для действий и принятия решений, которые облегчают достижение целей. Таким образом для установления этих общих ориентиров необходимо первоначально сформулировать цели обеспечения безопасности предприятия (общая цель нами уже определена ранее). Такими целями могут быть:

- укрепление дисциплины труда и повышение его производительности;
- защита законных прав и интересов предприятия;
- укрепление интеллектуального потенциала предприятия;
- сохранение и приумножение собственности;
- повышение конкурентоспособности производимой продукции;
- максимально полное информационное обеспечение деятельности предприятия и повышение его эффективности;
- ориентация на мировые стандарты и лидерство в разработке и освоении новой технологии и выпускаемой продукции;
- выполнение производственных программ;

- оказание содействия управленческим структурам в достижении целей предприятия;
- недопущение зависимости от случайных и недобросовестных деловых партнеров.

С учетом вышеизложенного можно определить следующие общие ориентиры для действий и принятия решений, которые облегчают достижение этих целей:

- сохранение и наращивание ресурсного потенциала;
- проведение комплекса превентивных мероприятий по повышению уровня защищенности собственности и персонала предприятия;
- включение в деятельность по обеспечению безопасности предприятия всех его сотрудников;
- профессионализм и специализация персонала предприятия;
- приоритетность несиловых методов предотвращения и нейтрализации угроз.

Для успешного выполнения этой политики необходимо реализовать стратегию безопасности предприятия, под которой понимается совокупность наиболее значимых решений, направленных на обеспечение приемлемого уровня безопасности функционирования предприятия.

Выделяются следующие типы стратегий безопасности:

- 1) – ориентированные на устранение существующих или предотвращение возникновения возможных угроз;
- 2) – нацеленные на предотвращение воздействия существующих или возможных угроз на предмет безопасности;
- 3) – направленные на восстановление (компенсацию) нанесенного ущерба.

Первые два типа стратегий предусматривают такую деятельность по обеспечению безопасности, в результате которой не происходит угрозы либо создается заслон ее влиянию. В третьем случае ущерб допускается (возникает), однако он компенсируется действиями, которые предусматривает соответствующая стратегия. Совершенно очевидно, что стратегии третьего типа могут разрабатываться и реализовываться применительно к ситуациям, где ущербы восполнимы, либо тогда, когда нет возможности осуществить какую-либо программу реализации стратегий первого или второго типа.

Научная теория обоснования безопасности предприятия

Строго говоря, такая теория находится в стадии формирования. Относится это прежде всего к понятийному аппарату. Разберем некоторые из этих понятий.

Понятие безопасности наши авторы характеризуют так: «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз». Раскрытие этого понятия через термин «защищенность», на наш взгляд, значительно суживает ее смысл, подчеркивает пассивность при реагировании на угрозы. Сущность безопасности, как представляется, связана с понятиями «развитие» и «устойчивость». В связи с этим под безопасностью следует понимать состояние объекта (в нашем случае – предприятия) в системе его связей с точки зрения способности к устойчивости (самовыживанию) и развитию в условиях внутренних и внешних угроз, действий непредсказуемых и трудно прогнозируемых факторов. Отталкиваясь от этого понятия, определим сле-

дующие **9 основных функций** безопасности: выявление, предупреждение, снижение, ослабление, нейтрализация, пресечение, локализация, отражение и устранение.



Под угрозой безопасности предприятия следует понимать потенциально или реально возможное событие, действие, процесс или явление, которое способно нарушить его устойчивость и развитие или привести к остановке его деятельности. Угрозу можно классифицировать по различным основаниям и измерить их в количественных параметрах. Например, возможный ущерб оценивается числом погибших людей, потерявших (ухудшивших) здоровье, денежной сумме экономических потерь и т.д. По степени вероятности угроза оценивается как невероятная, маловероятная, вероятная, весьма вероятная и вполне вероятная.

По степени развития угроза **проходит четыре этапа**: возникновение (зарождение), экспансия, стабилизация и ликвидация. **Отдаленность** угрозы во времени определяется как непосредственная, близкая (до 1 года) и далекая (свыше 1 года), а отдаленность в пространстве – территория предприятия, прилегающая к предприятию территория, территория региона, территория страны, зарубежная территория. Темпы нарастания угрозы измеряются по месяцам, кварталам, годам. **Напряженность угрозы** отражается в двух измерениях:

- а)** – нормальная, повышенная, близкая к пределу (порог), избыточная;
- б)** – рост, стабильность или снижение.

Кроме этого, **угрозы делятся** по природе их возникновения на два класса:

1) – естественные, (объективные), т.е. вызванные стихийными природными явлениями, не зависящими от человека, (наводнения, землетрясения, ураганы и т.п.);

2) – искусственные (субъективные), т.е. вызванные деятельностью человека непреднамеренные (неумышленные) и преднамеренные (умышленные) угрозы.

Различают также экономические, социальные, правовые, организационные, информационные, экологические, технические и криминальные угрозы.

Под объектом безопасности предприятия следует понимать степень устойчивости и развития предприятия, его способность противостоять угрозам.

Субъекты безопасности предприятия

Обеспечением безопасности предприятия занимаются две группы субъектов.

Первая группа занимается этой деятельностью непосредственно на предприятии и подчинены его руководству. Среди этой группы можно выделить специализированные субъекты: (совет или комитет безопасности предприятия, служба безопасности, пожарная часть, спасательная служба и т.д.), основным предназначением которых является постоянная профессиональная деятельность по обеспечению безопасности предприятия (в рамках своей компетенции). Другую часть субъектов этой группы условно можно назвать полуспециализированной, т.к. часть функций этих субъектов предназначена для обеспечения безопасности предприятия (медицинская часть, юридический отдел и т.д.). Наконец, к третьей части этой группы субъектов относится весь остальной персонал и подразделения предприятия, которые в рамках своих должностных инструкций и положений о подразделениях обязаны принимать меры к обеспечению безопасности. Следует иметь в виду, что эффективно обеспечивать безопасность предприятия эти субъекты могут только в том случае, если цели, задачи, функции, права и обязанности будут распределены между ними таким образом, чтобы они не пересекались друг с другом.

Ко **второй группе** субъектов относятся внешние органы и организации, которые функционируют самостоятельно и не подчиняются Руководству предприятия, но при этом их деятельность оказывает существенное (положительное или отрицательное) влияние на безопасность предприятия. Субъектами этой группы являются:

1). Законодательные органы. Принятые на уровне Российской Федерации, (а равно – иных государств СНГ) законы составляют правовую основу деятельности по обеспечению безопасности предприятия.

2). Органы исполнительной власти. Принятые на уровне этих органов подзаконные акты во многом дополняют, уточняют, детализируют требования законов.

3). Суды. Судебные органы обеспечивают соблюдение законных прав и интересов предприятия, в т.ч. в сфере безопасности.

4). Правоохранительные органы. Такие органы осуществляют борьбу с правонарушениями, которые отрицательным образом влияют на состояние безопасности предприятия.

5). Научно-образовательные учреждения. Последние (особенно негосударственные образовательные учреждения для подготовки частных охранников и детективов) призваны обеспечить научно-методическую проработку проблем безопасности предприятия и подготовку соответствующих специалистов в сфере безопасности предприятий.

Совершенно очевидно, что субъекты второй группы по своей инициативе подключаются эпизодически, (или никогда) к деятельности предприятия по обеспечению своей безопасности. Организационной формой такого подключения может стать комплексная программа безопасности предприятия, в которой необходимо предусмотреть формы и методы этой работы. Кроме того, можно рекомендовать разработку планов структур-

ных подразделений и всего предприятия в целом по организации взаимодействия с вышеуказанными органами и организациями.

Средства и методы обеспечения безопасности

Среди существующих средств обеспечения безопасности можно выделить следующие:

1). Технические средства. К ним относятся охранно-пожарные системы, видео-радиоаппаратура, средства обнаружения взрывных устройств, бронежилеты, заграждения и т.д.

2). Организационные средства. Создание специализированных организационных формирований, обеспечивающих безопасность предприятия.

3). Информационные средства. Прежде всего это печатная и видеопродукция по вопросам сохранения конфиденциальной информации. Кроме этого, важнейшая информация для принятия решений по вопросам безопасности сохраняется в компьютерах.

4). Финансовые средства. Совершенно очевидно, что без достаточных финансовых средств невозможно функционирование системы безопасности, вопрос лишь в том, чтобы использовать их целенаправленно и с высокой отдачей.

5). Правовые средства. Здесь имеется ввиду использование не только изданных вышестоящими органами власти законов и подзаконных актов, но также разработка собственных, так называемых локальных правовых актов по вопросам обеспечения безопасности.

6). Кадровые средства. Имеется ввиду прежде всего достаточность кадров, занимающихся вопросами обеспечения безопасности. Одновременно с этим решают задачи повышения их профессионального мастерства в этой сфере деятельности.

7). Интеллектуальные средства. Привлечение к работе высококлассных специалистов, научных работников (иногда целесообразно привлекать их со стороны) позволяет внедрять новые системы безопасности.

Следует заметить, что применение каждого из вышеуказанных средств в отдельности не дает необходимого эффекта, он возможен только на комплексной основе. В то же время необходимо отметить, что одновременное внедрение всех вышеуказанных средств в принципе невозможно. Оно проходит обычно ряд этапов:

I этап. Выделение финансовых средств.

II этап. Формирование кадровых и организационных средств.

III этап. Разработка системы правовых средств.

IV этап. Привлечение технических, информационных и интеллектуальных средств.

Переведенные из статичного в динамичное состояние вышеуказанные средства становятся методами, т.е. приемами, способами действия. Соответственно, можно говорить о технических, организационных, информационных, финансовых, правовых, кадровых и интеллектуальных методах. Приведем краткий конкретный перечень этих методов:

Технические – наблюдение, контроль, идентификация и т.д.;

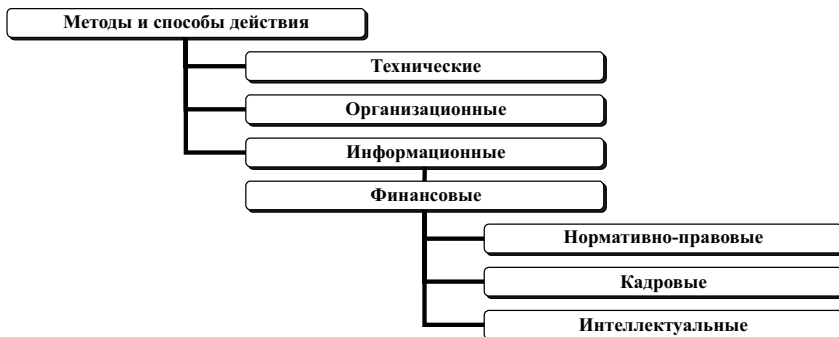
Организационные – создание зон безопасности, режим, расследование, посты, патрули и т.д.;

Информационные – составление детективами характеристик на сотрудников, аналитические материалы и учеты конфиденциального характера и т.д.;

Финансовые – материальное стимулирование сотрудников, имеющих достижения в обеспечении безопасности, денежное поощрение информаторов и т.д.;

Правовые – судебная защита законных прав и интересов, содействие правоохранительным органам и т.д.; **Кадровые** – подбор, расстановка и обучение кадров, обеспечивающих безопасность предприятия, их воспитание и т.д.;

Интеллектуальные – патентование, ноу-хау и т.д.



Концепция деятельности службы безопасности предприятия.

(Типовой проект)

Изучив и рассмотрев элементы системы безопасности предприятия необходимо составить концепцию деятельности службы безопасности.

Под концепцией безопасности предприятия понимается научно обоснованная система взглядов на определение основных направлений, условий и порядка практического решения задачи защиты деятельности предприятия от противоправных действий и недобросовестной конкуренции. Ниже приведем типовый проект(с комментариями) разработанной концепции деятельности службы безопасности предприятия (банка, фирмы) в соответствии с действующим законодательством Украины. Приведенный проект пригоден для разработки концепции безопасности предприятий в любых государствах бывшего Союза, при этом учитываются их действующая нормативная база, регулирующая эту деятельность.

Концепция выражает систему взглядов на проблему безопасности фирмы на различных этапах и уровнях производственной деятельности, а также основные принципы, направления и этапы реализации мер безопасности. Зарубежный и отечественный опыт обеспечения безопасности свидетельствует, что для борьбы со всей совокупностью преступных и противоправных действий необходима стройная и целенаправленная организация процесса противодействия. Причем в организации этого процесса должны участвовать профессиональные специалисты, администрация фирмы, сотрудники и пользователи, что и определяет повышенную значимость организационной стороны вопроса.

Не для профессионалов эта глава покажется “лишней писаниной”, но специалисты-профессионалы именно в Концепции, как “под нормативном” документе, видят процесс, заключающийся в обосновании и реализа-

ции наиболее рациональных форм, методов, способов и путей создания, совершенствования и развития системы безопасности, непрерывном управлении ею, контроле, выявлении ее узких мест и потенциальных угроз фирме.

В практике работы по организации службы безопасности коммерческих структур выработана определенная “Методика разработки комплексной концепции безопасности коммерческой структуры”. Ниже мы приводим пример такой наработки.

Методика разработки комплексной концепции безопасности коммерческой структуры

I. Анализ структуры и принципов построения предприятия

1.1. Форма собственности

1.2. Вид деятельности:

- 👁 некоммерческая общественная или государственная;
- 👁 производственная;
- 👁 торгово-посредническая;
- 👁 финансовая;
- 👁 страховая;
- 👁 инвестиционная;
- 👁 банковская;
- 👁 другое

1.3. Масштабы деятельности:

- 👁 размер уставного фонда;
- 👁 годовой оборот, доход, прибыль;
- 👁 штат сотрудников;
- 👁 количество и штат региональных подразделений;
- 👁 количество и виды развиваемых направлений

1.4. Состав и образовательный уровень:

- 👁 высшего и среднего руководящего звена;
- 👁 сотрудников службы безопасности;
- 👁 руководства и сотрудников региональных подразделений

1.5. Отношение руководства к проблеме безопасности:

- 👁 система безопасности отсутствует;
- 👁 ограничиваются только физической охраной и телохранительством;
- 👁 выделяют средства на технические средства безопасности и инженерной защиты офиса, производственных и складских помещений;
- 👁 выделяют средства на информационно-аналитическую работу;
- 👁 выделяют средства на регулярное повышение квалификации персонала службы безопасности

II. Анализ состояния безопасности предприятия

2.1. Наличие, штат службы безопасности (СБ), квалификация сотрудников

- 2.2. Степень участия руководства СБ в деятельности предприятия
- 2.3. Относительная величина расходов на безопасность и наличие бюджета СБ (характер распределения расходов)

III. Разработка и совершенствование концепции (программы) безопасности предприятия

3.1. Разработка долгосрочной программы, (примерный бизнес-план СБ)

- 3.1.1. Построение матрицы угроз
- 3.1.2. Экспертные оценки факторов угроз и распределение угроз по приоритетам

3.1.3. Разработка адекватных мер противодействия угрозам и определение расходов на реализацию этих мер

3.1.4. Оценка прогнозируемой прибыли от применения мер безопасности

3.2. Выбор и обоснование средств безопасности и защиты

3.2.1. Технические средства и инженерная защита

3.2.2. Физическая охрана (организация, обучение, экипировка, тактика)

3.2.3. Информационная защита

3.2.4. Экономическая безопасность

3.2.5. Безопасность руководства

3.2.6. Безопасность персонала

3.2.7. Организационные мероприятия

3.3. Разработка программы взаимодействия с кадровым и финансовым менеджментом предприятия

3.4. Разработка программ действий в кризисных ситуациях

3.5. Разработка программ взаимодействия с правоохранительными органами, властными структурами, средствами массовой информации.

3.6. Разработка программ реагирования на изменение политической ситуации

IV. Краткосрочный и долгосрочный прогноз безопасности предприятия

4.1. Экономический анализ и прогноз деятельности предприятия

4.2. Прогноз влияния факторов угроз на выживание предприятия

4.3. Разработка программы управления рисками в деятельности предприятия с точки зрения безопасности

V. Практические рекомендации по совершенствованию системы безопасности предприятия

5.1. Рекомендации по кадровой политике

5.1.1. Выбор форм и методов стимулирования работы персонала предприятия

5.1.2. Подбор и отбор персонала предприятия

5.1.3. Подбор кадров СБ

5.1.4. Подбор руководящих кадров

5.1.5. Обеспечение безопасности и сохранения конфиденциальной информации при увольнении сотрудников

5.1.6. Сохранение психологического контакта с уволенными сотрудниками

5.2. Рекомендации по обучению и повышению квалификации сотрудников СБ

5.2.1. Периодичность повышения квалификации

5.2.2. Периодичность проверок и тестовых процедур

5.2.3. Изучение и анализ информации, публикуемой в изданиях по СБ предпринимательской деятельности

5.2.4. Выбор форм и методов стимулирования работы персонала СБ

5.3. Охрана здоровья руководства и персонала предприятия

5.4. Сохранение конфиденциальной информации при работе с иностранными партнерами

Применив вышеуказанные наработки-рекомендации, ниже рассмотрим типовой пример “Концепции деятельности службы безопасности предприятия”. Концепция безопасности предприятия представляет собой официально утвержденный документ, в котором отражена система взглядов, требований и условий организации мер безопасности персонала и собственности предприятия. Примерная структура концепции может выглядеть следующим образом:

Концепция деятельность службы безопасности (Строго конфиденциально)

1. Общее положение, (применительно к Украине)

Концепция деятельности Службы безопасности предприятия /фирмы/ (в дальнейшем – Служба) разработана в соответствии с Законом Украины – “ХОЗЯЙСТВЕННЫЙ КОДЕКС УКРАИНЫ” от 16.01.2003. № 436-IV в соответствии Конституции Украины (254 к \ 96-ВР), другими законодательными и нормативными актами Украины, регулируемыми вопросы предпринимательства и деятельности коммерческих структур безопасности. Служба создана для решения комплекса задач по обеспечению безопасности фирмы или предприятия (далее Фирмы) помощи руководству в реализации её основных интересов.

Служба подчиняется Руководителю фирмы.

Основой организации и функционирования Службы является решение руководства фирмы о ее создании, Концепция ее деятельности и Положение о Службе.

Настоящая Концепция является строго конфиденциальным документом и предназначена только для руководства фирмы и сотрудников Службы при выполнении ими своих служебных обязанностей.

1.1. Основные понятия и определения

Безопасность фирмы – состояние устойчивой жизнедеятельности юридического лица, при котором обеспечивается реализация его основных интересов и приоритетных целей, приумножение прибылей и защита от различных внешних и внутренних дестабилизирующих факторов.

Обеспечение безопасности фирмы осуществляется по следующим направлениям:

- 1) – физическая безопасность;**
- 2) – экономическая безопасность;**
- 3) – социальная безопасность.**

В эти направления включается:

- 👁️ финансовая безопасность;
- 👁️ информационная безопасность;
- 👁️ техническая безопасность;
- 👁️ безопасность интеллектуальной собственности;

👁️ безопасность транспортировки грузов и др.

Угроза безопасности фирмы (дестабилизирующие факторы) – реальные и/или потенциальные воздействия, которые могут причинить ущерб интересам фирмы или сделать невозможной их практическую реализацию.

Конкуренты – фирмы, организации, учреждения, либо отдельные граждане, действия которых сознательно направлены на противодействие реализации основных интересов предприятия либо нанесение прямого ущерба фирме, ее служащим и учредителям.

Криминальные элементы (криминогенные структуры) – преступники-одиночки или преступники, объединенные в преступные группировки, действия которых направлены на нанесение фирме и/или его служащим имущественного или физического вреда.

Коммерческая тайна – конфиденциальная информация, циркулирующая в фирме, отражающая ее состояние (как настоящее, так и перспективное) и обеспечивающая устойчивую жизнедеятельность как отдельных подразделений, так и всей фирмы в целом.

Конфиденциальная информация подразделяется на два вида:

1) – **технологическая** – незащищенная патентом информация технологического (технического) характера, дающая фирме и/или ее услугам приоритет над аналогичными услугами других фирм (предприятий) в соответствующем сегменте рынка;

2) – **деловая** – информация внутреннего характера, которая позволяет фирме успешно проводить свою деятельность на основных направлениях и получать устойчивую прибыль.

1.2. Реальные и потенциальные конкуренты, их действия в отношении фирмы и ее служащих.

Реальными и потенциальными конкурентами фирмы являются другие фирмы, расположенные, прежде всего, в регионах по месту нахождения объектов или филиалов фирмы. Наибольшую опасность для фирмы представляют конкуренты, активно ведущие политику экспансии как в указанных регионах, так и в Украине в целом. Опасны также фирмы либо организации, которым требуются специалисты, аналогичные работающим в нашей фирме.

1.3. Реальные и потенциальные угрозы безопасности фирмы.

А) – Криминальные элементы.

Возможными объектами заинтересованности (нападения) с целью завладения имуществом фирмы со стороны криминальных элементов могут быть:

- 👁️ финансовые ресурсы фирмы;
- 👁️ оборудование офисов;
- 👁️ транспорт и прочее.

Б) – Кроме того, криминальные элементы могут быть использованы конкурентами для нанесения фирме следующего ущерба:

- 👁️ организация нападения на:
 - а) офисы;
 - б) служащих;

- в) клиентов;
 - г) транспорт и т.д.;
 - 👁️ организация поджогов непосредственно в помещениях фирмы, на объектах и в филиалах;
 - 👁️ организация уничтожения информационной системы фирмы либо заражение ее компьютерными вирусами;
 - 👁️ возможность использования коммуникаций для создания в фирме и его подразделениях аварийной обстановки.
- В) – Фирмы, непосредственно занимающиеся промышленной разведкой**

При выполнении возложенных на нее функций, Служба вероятнее всего будет сталкиваться с фирмами, занимающимися сбором конфиденциальной информации в пользу конкурентов, и службами безопасности конкурентов.

1.4. Реальные и потенциальные дестабилизирующие факторы для безопасности фирмы.

В данном подпункте рассматриваются враждебные действия, которые могут быть осуществлены в отношении фирмы, ее служащих, учредителей и клиентов со стороны банков, учреждений, предприятий и фирм, не являющихся конкурентами. Морально-психологическое давление – к ним относятся действия, направленные на создание нетерпимой моральной и психологической атмосферы вокруг фирмы (в том числе – с использованием средств массовой информации), ее деятельности, а также служащих.

Угроза:

а) натравливание на фирму (руководство, служащих, учредителей) соседей, населения, общественности района, города, республики, государственных властей, средств массовой информации (СМИ);

б) компрометирование фирмы либо отдельных сторон ее деятельности, служащих, учредителей в глазах населения, общественных движений, СМИ, властей;

в) заключение с фирмой заведомо нереальных договоров;

г) оказание давления на учредителей, клиентов и контрагентов по договорам с целью их отказа от партнерских отношений с фирмой.

Получение информации о фирме

Направления несанкционированного получения конфиденциальной информации о фирме:

а) похищение документов либо иных носителей, содержащих необходимые похитителем сведения;

б) выведывание конфиденциальных сведений у служащих фирмы;

в) скрытое наблюдение за помещениями и/или служащими фирмы;

г) внедрение “своих людей” в фирму;

д) подкуп сотрудников фирмы;

е) техническое проникновение к охраняемым фирмой секретам;

ж) добывание информации о фирме через своих информаторов, направленных для работы в органы государственной власти и управления.

1.5. Цели обеспечения безопасности фирмы

Они вытекают:

а) из главных направлений деятельности фирмы (как стратегических, так и тактических);

б) реальной и потенциальной угрозы внешнего и внутреннего порядка экономическому и финансовому благосостоянию фирмы и реализации его основных жизненных интересов – получению стабильной прибыли.

Основными целями обеспечения безопасности фирмы являются:

- 👁️ обеспечение реализации законных интересов фирмы в целом, входящих в него подразделений, а также его служащих, учредителей и клиентов. Поддержание устойчивого управления;
- 👁️ гарантирование сохранности материальной и интеллектуальной собственности фирмы, эффективного его использования в рамках реализации основных жизненных интересов фирмы;
- 👁️ выявление фактов готовящихся и реализуемых действий нарушения законов Украины о предпринимательской деятельности среди служащих государственных органов по отношению к деятельности фирмы, а также в отношении ее служащих и акционеров, актов недобросовестной конкуренции;
- 👁️ предупреждение и локализация вредных для фирмы последствий от указанных действий;
- 👁️ содействие руководству в достижении внутренней и внешней организационной стабильности в работе фирмы;
- 👁️ оказание помощи в повышении конкурентноспособности предлагаемых фирмой услуг, создании благоприятной рыночной конъюнктуры для их реализации на внутреннем и внешнем рынке;
- 👁️ способствование в формировании и повышении положительного имиджа фирмы среди внутренних и внешних партнеров и клиентов, а также среди населения и общественности;
- 👁️ сбор и своевременное предоставление полученной информации руководству фирмы и его подразделениям для реализации основных интересов на направлениях деятельности фирмы.

1.6. Основные задачи обеспечения безопасности фирмы

Задачи обеспечения безопасности фирмы определяются необходимостью достижения вышеназванных целей и являются основой требований для выработки и реализации системы взаимосвязанных мер по обеспечению безопасности фирмы и сохранения ее коммерческой тайны. Служба постоянно осуществляет изучение и контроль за обстановкой как внутри фирмы, так и вне ее с целью оперативного решения следующих задач:

- 👁️ защиты законных прав фирмы и ее сотрудников во взаимоотношениях с государственными органами, партнерами, посредниками, общественностью, средствами массовой информации;
- 👁️ своевременного выявления реальной и потенциальной угроз для коммерческой деятельности предприятия, ее служащих и учредителей;
- 👁️ вскрытия внутренних и внешних причин и условий, способствующих нанесению фирме, ее служащим материального, морального и иного ущерба, препятствующих ее нормальному функционированию и развитию;

- 👁️ разработки и реализации механизма оперативного реагирования на возникающую угрозу и негативные тенденции в развитии внешней и внутренней обстановки в отношении фирмы;
- 👁️ эффективного пресечения посягательств на законные интересы фирмы, ее служащих, учредителей и клиентов; использование юридических, технических, организационных и других средств в выявлении и предупреждении угрозы ее безопасности, а также их источников;
- 👁️ локализации и максимально полного возмещения нанесенного фирме неправомерными действиями со стороны физических и юридических лиц ущерба;
- 👁️ ослабления вредных последствий от акций конкурентов и/или криминальных элементов по непосредственному подрыву безопасности фирмы и создании неблагоприятных условий в деятельности по достижению стоящих перед ней целей.
- 👁️ поддержания стабильных и выгодных для фирмы отношений внутри коллектива и внешних отношений коллектива;
- 👁️ юридического, организационного и физического обеспечения усилий руководства фирмы по укреплению дисциплины труда, формированию стимулов для обеспечения экономической безопасности действиями всех сотрудников фирмы;
- 👁️ информационного обеспечения внутрипроизводственной деятельности предприятия, исключаящее как необоснованное ограничение коммерческой информации, так и разглашение коммерческой тайны;
- 👁️ юридически грамотное и экономически безопасное информационное обслуживание деятельности предприятия на рынке товаров, услуг, ценных бумаг, рабочей силы, взаимодействия с общественностью и средствами массовой информации;
- 👁️ физическое обеспечение сохранности транспортируемых грузов, личной имущественной безопасности как клиентов фирмы, представляющих особую важность для фирмы, так и особо ценных специалистов фирмы.

1.7. Принципы обеспечения безопасности фирмы.

Принципы обеспечения безопасности фирмы отражают основополагающие требования к стратегии и тактике, организации и осуществлению мероприятий Службы по защите его жизненно важных интересов.

Основные из них следующие:

1) – законность. Меры по обеспечению безопасности фирмы разрабатываются Службой на основе действующих в Украине законов в пределах определенной Положением о Службе компетенции с применением всех дозволенных методов обнаружения и пресечения угрозы безопасности предпринимательского дела;

2) – самостоятельность и ответственность. Служба располагает всеми необходимыми для эффективного выполнения своей деятельности видами ресурсов; обеспечивает строгое соответствие производимых затрат и достигаемых результатов по обеспечению безопасности;

3) – экономическая целесообразность. Мероприятия, проводимые Службой по обеспечению безопасности фирмы, не должны приводить к ухудшению экономических показателей ее деятельности и мешать реализации основных интересов фирмы. Главным критерием оценки качества работы Службы, определения размеров материального вознаграждения ее сотрудников является стабильность работы фирмы и получение ей гарантированных прибылей;

4) – профессионализм. Сотрудники Службы приобретают и постоянно поддерживают высокий профессиональный уровень;

5) – программно-целевое планирование. Деятельность Службы и ее служащих строится на основе разработанной и утвержденной руководством фирмы комплексной Программы обеспечения безопасности;

6) – координация и взаимодействие. Служба координирует усилия всех подразделений фирмы по выполнению мероприятий обеспечения безопасности фирмы, ее служащих, учредителей и клиентов.

С этой целью Служба устанавливает необходимые связи и взаимодействует с внешними организациями (органами государственного управления, правоохранительными органами, другими заинтересованными учреждениями и предприятиями);

7) – использование передового опыта. В своей деятельности Служба широко использует отечественный и зарубежный опыт по организации деятельности в сфере обеспечения безопасности фирм, учреждений, предприятий и их служащих, а также современные технические средства;

8) – конфиденциальность в сочетании с необходимой гласностью. Основой для работы Службы и ее сотрудников является принцип конфиденциальности, который предполагает сохранение в тайне некоторых методов ее деятельности.

Служба регулярно информирует Руководителя фирмы, а с его санкции – и руководителей других подразделений, о результатах своей деятельности по обеспечению безопасности.

По согласованию с руководством в целях профилактики Служба информирует коллективы подразделений фирмы о некоторых аспектах своей деятельности.

2. Организация службы безопасности

2.1. Организация обеспечения безопасности фирмы.

Организация обеспечения безопасности фирмы осуществляется на основе принципа централизованного управления стратегическими направлениями этой деятельности на уровне руководства фирмы в целях:

- 👁 координации действий основных подразделений фирмы и ее филиалов в этом направлении;
- 👁 упорядочении взаимоотношений фирмы и ее филиалов по вопросам обеспечения безопасности с правоохранительными органами, органами местного управления и другими внешними учреждениями и организациями;
- 👁 использования кадровых и иных сил и средств для устранения реальной и потенциальной угрозы нормальному функционированию фирмы и ее служащим.

Внешним органом управления обеспечением безопасности банка является ее Руководство.

Руководство рассматривает и рекомендует для утверждения ее Руководителем следующие вопросы:

- 👁 стратегические направления обеспечения безопасности фирмы;
- 👁 программу обеспечения безопасности фирмы, содержащую следующие целевые разделы:
 - 1) система обеспечения и поддержания безопасности фирмы;
 - 2) организация и осуществление режимно-конфиденциальной деятельности;
 - 3) формирование системы обеспечения физической безопасности фирмы, ее служащих, учредителей и клиентов;
 - 4) создания системы информационного обеспечения по вопросам безопасности фирмы;
 - 5) налаживание системы противодействия техническому проникновению конкурентов в подразделения фирмы;
 - 6) планы практической реализации целевых разделов Программы;
 - 7) введение и поддержание в фирме в целом, ее подразделениях и филиалах различных режимов безопасности;
 - 8) предложения о содержании и характере взаимодействия с правоохранительными органами, органами местного управления, а также с клиентами и партнерами фирмы в целях сохранения ее коммерческой тайны;
 - 9) решения об образовании, стратегии деятельности и реорганизации Службы;
 - 10) отчет руководителя Службы о деятельности Службы за определенный период;
 - 11) отчеты руководителей подразделений фирмы и филиалов по реализации Программы обеспечения безопасности (в части, их касающейся);
 - 12) другие проблемы, относящиеся к деятельности в сфере обеспечения безопасности фирмы и требующие принятия решения о привлечении дополнительных финансовых, материальных, кадровых и иных ресурсов подразделений фирмы.

2.2. Управление Службой.

Управление Службой осуществляется лично Руководителем фирмы, а в его отсутствие – исполняющим обязанности руководителя фирмы.

Служба является исполнительно-распорядительным подразделением, работающим по утвержденному плану, а также реализующим решения Руководителя фирмы по вопросам безопасности фирмы в целом.

Служба осуществляет функциональное управление деятельностью своих, а также других структурных звеньев фирмы и ее филиалов, обеспечивающих решение задач в сфере безопасности.

2.3. Структура Службы

Служба является подразделением фирмы, приравненным к управлению (отделу).

Для решения поставленных перед нею задач Служба образуется из следующих подразделений:

- 1) подразделение охраны фирмы и физической охраны руководства фирмы, включающее в себя группу “быстрого реагирования” (группа охраны объектов, группа сопровождения грузов, группа физической охраны и дежурная группа);

2) подразделение контроля за соблюдением служащими фирмы и ее филиалов всех видов режима, обеспечения работы с персоналом фирмы по защите тайны фирмы (отдел внутренней безопасности);

3) подразделение сбора информации, ее накопления и аналитической обработки (информационно-аналитический отдел);

4) подразделение технической защиты и обеспечения связи руководства с фирмой (отдел технических средств защиты);

2.4. Функции Службы

Для решения поставленных задач Служба осуществляет:

1) – административно-распорядительную функцию.

Она реализуется путем:

- ☉ разработки, внедрения и поддержания в фирме в целом, ее подразделениях и филиалах различных режимов безопасности;
- ☉ определения полномочий, прав, обязанностей и ответственности служащих фирмы по вопросам обеспечения безопасности; представительских функций в различных областях и направлениях деятельности;
- ☉ подготовки и проведения мероприятий по обеспечению физической безопасности и сохранности коммерческой тайны;

2) – учетно-контрольную функцию.

Она обеспечивается путем:

- ☉ организации своевременного обнаружения реальной и потенциальной угрозы финансовой стабильности и устойчивости деятельности фирмы по реализации своих основных интересов, оценки и контроля за источниками этой угрозы;
- ☉ налаживания контроля за неблагоприятными для фирмы ситуациями и факторами, ведение их учета;
- ☉ выявления критически важных направлений финансово – коммерческой деятельности фирмы;
- ☉ накоплением информации по проблемам обеспечения безопасности фирмы;

3) – социально-кадровую функцию.

Она реализуется путем:

- ☉ участия Службы в подборе, проверке и расстановке кадров;
- ☉ выявления негативных тенденций в коллективах подразделений фирмы и ее филиалов, возможных причин и условий возникающей социальной напряженности;
- ☉ в предупреждении и локализации возможных конфликтов;
- ☉ инструктажа и использования как гласно, так и конфиденциально служащих по вопросам своей компетенции;
- ☉ формирования у служащих чувства ответственности за обеспечение безопасности фирмы.

4) – организационно-управленческую функцию.

Эта функция реализуется путем:

- ☉ организационного, материально-технического и технологического обеспечения режимов безопасности в фирме и ее филиалах, освоения специальной техники и достижения уровня,

соответствующего потребностям обеспечения безопасности фирмы, ее служащих, учредителей и клиентов;

5) – методическую функцию. Она реализуется путем:

- 👁 выявления, накопления и внедрения в фирме позитивного опыта по проблемам обеспечения безопасности;
- 👁 организации обучения служащих фирмы, занимающихся обеспечением безопасности;
- 👁 методической разработки и сопровождения решения возникающих перед фирмой проблем обеспечения ее безопасности;

6) – информационно-аналитическую функцию. Она обеспечивается путем:

- 👁 целенаправленного сбора, накопления, обработки и выдачи информации, относящейся к сфере обеспечения безопасности, руководству фирмы, заинтересованным подразделениям и отдельным лицам;
- 👁 организации аналитической обработки информации по этим проблемам с использованием всей накопленной в фирме информации;
- 👁 создания и использования необходимых для этого технических, программных и методических средств. Служба самостоятельно определяет основные функции системы информационного обеспечения безопасности фирмы и структуру накапливаемой информации.

2.5. Функции подразделений Службы

5.1. Подразделение охраны фирмы и физической охраны руководства фирмы, включающее в себя группу “быстрого реагирования”.

- 🔊 осуществляет разработку и реализацию в подразделениях фирмы следующих видов режимов:
- 🔊 физической охраны территории, помещений, оборудования, служащих и клиентов фирмы (как в рабочее, так и в нерабочее время),
- 🔊 физической охраны руководства фирмы и некоторых главных специалистов (по указанию председателя),
- 🔊 физической охраны перевозок финансовых средств товаров (продукции) и других грузов фирмы;
- 🔊 обеспечивает физическое противодействие возможным акциям конкурентов и/или криминальных элементов в отношении объектов фирмы, финансовых средств, служащих, учредителей и клиентов;
- 🔊 обеспечивает взаимодействие с правоохранительными органами по вопросам обеспечения физической безопасности фирмы, ее служащих, учредителей и клиентов;
- 🔊 обеспечивает сбор и предоставление в информационную систему информации о фактах, имеющих значение для обеспечения физической безопасности фирмы и ее руководства;

- ☞ немедленно, по сигналу тревоги прибывает на место происшествия, в случае возникновения реальной угрозы служащим или имуществу фирмы;
- ☞ принимает меры к локализации угрозы, задержанию преступника или преступников и передаче их сотрудникам правоохранительных органов.

5.2. Подразделение контроля за соблюдением служащими фирмы и ее филиалов всех видов режима, обеспечения работы с персоналом фирмы по защите коммерческой тайны. Осуществляет:

1) контроль за выполнением служащими установленных на фирме режимов осуществляется путем проведения плановых и/или внезапных проверок; обеспечивается координация этого процесса с другими подразделениями;

2) учет персонала фирмы и ее филиалов; сбор информации о деловых и личных качествах каждого служащего;

- ☞ отслеживание опасных для фирмы отклонений в поведении служащего и информирование об этом руководства Службы;

- ☞ работа по проверке вновь поступающих на работу на фирму; отслеживание наличия опасных для фирмы тенденций в поведении уволившихся служащих;

3) проведение по поручению Руководства или начальника Службы служебных расследований по всем вопросам, когда возникает угроза безопасности фирмы;

4) контроль за исполнением служащими действующих на фирме режимов, направленных на соблюдение коммерческой тайны;

5) выявление фактов подготовки различных акций в отношении фирмы, ее служащих, учредителей и клиентов со стороны конкурентов и/или криминогенных структур, противодействие этим акциям;

6) выработка и проведение мероприятий по защите каналов связи и противодействию технической разведке конкурентов;

7) контроль за обстановкой в коллективах подразделений фирмы, в местах расположения помещений и других объектов фирмы и филиалов с целью выявления возможных каналов утечки сведений, составляющих коммерческую тайну;

8) сбор и предоставление в информационную систему данных о фактах, имеющих значение для обеспечения безопасности фирмы.

Руководством фирмы в зависимости от потребностей и обстановки подразделению может делегироваться выполнение других функций в рамках его компетенции.

5.3. Подразделение сбора информации, ее накопления и аналитической обработки.

Принцип функционирования подразделения сбора информации – конфиденциальность действий.

Основные функции:

- 1) сбор информации о конкурирующих фирмах;
- 2) сбор информации о потенциальных клиентах фирмы;
- 3) сбор информации по вопросам обеспечения безопасности фирмы от подразделений Службы, других подразделений фирмы и филиалов;
- 4) сбор информации об обстановке в тех регионах и странах, где фирма планирует выйти на рынок;

5) проведение мероприятий по созданию благоприятных условий для выхода фирмы на конкретный рынок;

6) представление собранной информации в информационную систему фирмы;

7) сбор информации об экономических, социальных и политических процессах, представляющих угрозу фирме; составление дайджестов отечественной и зарубежной прессы по направлениям, интересующим руководство;

8) аналитическая обработка добытой информации и систематический доклад ее руководству фирмы;

9) организация надежного хранения полученной информации;

10) выдача информации из системы в соответствии с запросами руководства фирмы и Службы;

11) защита информационного банка от умышленного (либо неумышленного) разрушения и утечки к конкурентам накопленной в нем информации;

12) организация координации и взаимодействия с другими базами данных (БД) фирмы и филиалов, а также, с разрешения руководства фирмы, с базами данных внешних фирм и организаций.

Руководство фирмы в зависимости от обстановки может делегировать подразделению выполнение и других функций в пределах его компетенции.

5.4. Подразделение технической защиты и обеспечения связи руководства с фирмой

Основные функции:

1) обеспечение и техническое обслуживание системы радиосвязи руководства фирмы и других служб с фирмой;

2) обеспечение режима защиты радиопереговоров в системе радиосвязи фирмы;

3) контроль эфира с целью выявления факторов, угрожающих безопасности фирмы;

4) проведение мероприятий по защите помещений фирмы, жилищ ее руководителей, телефонных и компьютерных сетей от несанкционированного съема информации с помощью технических средств.

5.5. Аппарат Руководителя фирмы

Основная функция: обеспечение безопасности деятельности Директора фирмы.

В аппарат Руководителя фирмы входят следующие сотрудники Службы:

- 👁️ помощник Руководителя ,
- 👁️ референт-переводчик,
- 👁️ секретарь приемной,
- 👁️ водители автомобилей, обслуживающих Руководство.

Примечание:

а) – по такой схеме построены аппараты обеспечения деятельности первых лиц многих западных государств;

б) – подобная практика более семидесяти лет эффективно использовалась руководством СССР. Введение указанных служащих в структуру Службы должно исключить возможности утечки конфиден-

циальной информации и повысить их ответственность за порученный участок работы;

в) – должности помощника Руководителя и референта-переводчика могут быть объединены в одну должность помощника. Руководителя, если служащий, который будет ее замещать, владеет необходимым иностранным языком и отвечает требованиям, предъявляемым к помощнику.

В составе Службы, в зависимости от обстановки, по решению руководства фирмы могут образовываться другие подразделения и создаваться временные структуры для выполнения дополнительных функций и решения конкретных задач в пределах компетенции Службы.

Руководителю Службы предоставлено право привлечения специалистов фирмы во временные структуры для устранения угрозы безопасности фирмы, его служащим, учредителям и клиентам, решения других задач в пределах компетенции Службы.

В случае, когда руководитель подразделения, в котором работает привлекаемый к мероприятиям Службы специалист, не согласен с таким решением, согласование вопроса проводится на уровне руководства фирмы.

Конкретные задачи, решаемые перечисленными подразделениями, их права, обязанности сотрудников этих подразделений определяются положениями о подразделениях и должностными инструкциями.

Данные положения и инструкции разрабатываются на основе законодательства Украины, Положения о Службе и других нормативных документов фирмы и утверждаются Руководителем фирмы.

2.6. Основные задачи Службы

6.1. Оценка фирмы и ее подразделений с позиции обеспечения безопасности:

6.1.1. помещения офиса, (планы помещений; размещение оборудования; документация, ее содержание и хранение; обрабатываемая информация; плотность посещения офисов; каналы связи; комнаты для проведения конфиденциальных переговоров и т.д.); служебные помещения (план размещения служащих и оборудования; какие операции реализуются в каждом помещении и т.д.); сейфы (помещения) для хранения денежных и других ценностей (планы размещения оборудования и ценностей; какие ценности хранятся, их характеристики и количество; способы хранения; способы транспортировки для хранения и выдачи и т.д.);

6.1.2. оборудование: офисов (конкретное оборудование, его значение для нормального функционирования офиса; цена; привлекательность для криминальных элементов и населения и т.д.);

6.1.3. транспорт (конкретный транспорт; его характеристики и значение для нормального функционирования фирмы; цена; привлекательность и т.д.); определение на фирме конкретного технологического оборудования, коммуникаций и др., вывод из строя которых может вывести фирму из рабочего режима либо нанести ему значительный экономический ущерб;

6.1.4. документы (которые содержат данные, наиболее притягательные для конкурентов и/или криминальных элементов):

– определение участков сосредоточения сведений, составляющих тайну фирмы и информационных потоков этих сведений; определение круга сторонних организаций, связанных с фирмой связями, через которые возможно получение сведений, составляющих коммерческую тайну, прямым либо косвенным путем;

– выявление на фирме круга лиц, проявляющих интерес к конфиденциальной информации фирмы, не допущенных к такой информации; разработка системы защиты документов, содержащих сведения о коммерческой тайне фирмы;

6.1.5. служащие, работающие непосредственно на фирме: обеспечение безопасности руководства фирмы, а также учредителей и главных специалистов и служащих (по указанию Руководителя фирмы); оценка степени осведомленности сотрудников в секретах фирмы; контроль обстановки в коллективах различных подразделений фирмы и филиалов; определение круга лиц, которые в силу служебного положения имеют доступ к сведениям, составляющим коммерческую тайну; определение помещений и участков на фирме, уязвимых во взрывопожарном отношении, повреждение которых может нанести фирме большой материальный ущерб и вред здоровью ее служащих;

6.2. изучение элементов среды, в которой функционирует фирма.

6.2.1. географические факторы среды: изучение планов размещения на местности офисов и других помещений фирмы;

- 👁️ оценка подходов к ним;
- 👁️ мест, удобных для нападения на помещения фирмы, служащих, транспорт и т.д.;
- 👁️ изучение планов соседних квартир; оценка удобства проникновения в офисы и другие помещения фирмы, слежения за служащими; контроля разговоров служащих фирмы, переговоров и т.д.;
- 👁️ изучение планов размещения коммуникаций; уязвимые точки и т.п.

6.2.2. этнические факторы среды:

- 👁️ изучение населения в районе работы офисов и других помещений фирмы;
- 👁️ изучение взаимоотношений различных социальных и этнических групп населения в районе расположения объектов фирмы и филиалов;
- 👁️ изучение взаимоотношений населения в районе расположения фирмы;
- 👁️ выявление отношения населения к фирме и предлагаемым услугам; проведение мероприятий по локализации негативных тенденций;
- 👁️ изучение обстановки в городе, районе расположения объектов фирмы и филиалов, а также в регионах ее деятельности;
- 👁️ прогноз дальнейшего развития этой обстановки;

6.2.3. политические факторы среды:

- 👁️ изучение отношения местных и других властей к фирме;
- 👁️ изучение отношения средств массовой информации к фирме, ее служащим, учредителям и клиентам;
- 👁️ проведение мероприятий по созданию благоприятного имиджа фирмы и ее деятельности;

6.2.4. экономические факторы среды:

- 👁️ выявление и оценка влияния экономических факторов на обеспечение безопасности фирмы.

6.3. Определение круга реальных и потенциальных конкурентов, организация их изучения:

- 👁 выявление круга организаций и фирм, как отечественных так и иностранных, заинтересованных в овладении информацией, составляющей коммерческую тайну фирмы, определение конечных целей этих организаций;
- 👁 анализ возможностей разведывательных служб реальных и потенциальных конкурентов и криминальных элементов в добывании информации о деятельности фирмы либо нанесению ей другого ущерба.

6.4. Анализ всех выявленных элементов обстановки и выработка на этой основе мер по эффективному обеспечению безопасности фирмы:

- 👁 изучение, анализ и оценка состояния обеспечения безопасности фирмы;
- 👁 разработка предложений и рекомендаций для совершенствования системы ее безопасности;
- 👁 разработка технико-экономических обоснований, направленных на приобретение технических средств, получение консультаций у специалистов, разработку необходимой документации в целях совершенствования системы мер по обеспечению безопасности фирмы;
- 👁 определение и обоснование мер технической защиты фирмы;
- 👁 обеспечение руководства фирмы, подразделений, филиалов и служащих информацией по вопросам безопасности;
- 👁 организация взаимодействия с правоохранительными органами по вопросам обеспечения безопасности фирмы, ее филиалов, служащих, учредителей и клиентов;
- 👁 внедрение в деятельность Службы технических достижений, эффективных методов в области обеспечения безопасности деятельности фирмы;
- 👁 организация обучения сотрудников Службы в соответствии с их должностными обязанностями.

2.7. Система мер, осуществляемых Службой

В процессе своей деятельности Служба разрабатывает и осуществляет две взаимосвязанные подсистемы мер по обеспечению безопасности фирмы, ее филиалов служащих, акционеров и клиентов.

Назначение первой подсистемы мер – предупреждать, затруднять и ограничивать возможности проведения акций в отношении фирмы, ее филиалов, служащих, учредителей и клиентов со стороны любого конкурента (криминальной структуры). Данная подсистема мер является превентивной и рассчитана на воспрепятствовать действиям любого лица, покушающегося на безопасность фирмы.

Назначение второй подсистемы мер – выявлять, локализовывать и не допускать конкретные акции конкурентов (криминальных элементов) в отношении фирмы, какую бы форму они не принимали.

Первая подсистема мер осуществляется подразделением охраны фирмы. В зависимости от обстановки и для более эффективной реализации

этих мер решением руководства Службы могут быть подключены другие подразделения Службы.

Первая подсистема включает следующие меры:

1) оказание организационно-правового влияния на деятельность руководителей подразделений в обеспечения безопасности. Подразделение охраны разрабатывает инструкции режимного характера, организует и поддерживает на территории и в помещениях (подразделениях) фирмы различные виды режимов;

2) осуществление гласного контроля за исполнением установленных на территории, в помещениях банка режимов;

3) осуществление непосредственного обеспечения безопасности фирмы, отдельных ее подразделений и служащих; обеспечение сохранности коммерческой тайны фирмы; противодействие легальной разведке конкурентов (криминогенных структур); противодействие их технической разведке;

4) защита применяемых на фирме средств связи, оргтехники и других технических средств;

5) осуществление предупредительно-профилактического воздействия на служащих фирмы с целью выполнения ими установленных режимов безопасности.

Вторая подсистема включают в себя следующие меры:

1) осуществление контроля за состоянием мер по обеспечению безопасности объектов фирмы,

за поддержанием служащими установленных на объектах фирмы режимов. Совершенствование этих режимов;

2) осуществление контроля за обстановкой в коллективах подразделений фирмы;

3) выявление возможных каналов утечки конфиденциальной информации фирмы;

4) проведение мероприятий по выявлению и проверке служащих фирмы, подозреваемых в работе на конкурентов;

5) осуществление профилактического воздействия на служащих фирмы, клиентов и контрагентов по договорам;

6) расследование по фактам утраты документов служащими фирмы;

7) расследование чрезвычайных происшествий, похожих на акции вредительства со стороны конкурентов;

8) оказание активного содействия правоохранительным органам в розыске пропавших без вести служащих фирмы;

9) конфиденциальный контроль:

а) переговоров по открытым каналам связи;

б) почты;

в) выход в информационные сети внешних организаций и общего пользования через модемы;

10) разработка и осуществление подготовки мер к кризисному периоду.

2.8. Взаимодействие Службы с другими подразделениями фирмы

На основании и в порядке, установленном Положением о Службе, руководству Службы предоставляются возможности использования технического и кадрового потенциала фирмы, его подразделений для решения задач по выявлению, предупреждению и локализации реальной и потенциальной угроз фирме, а также реализации других проблем по обеспечению ее безопасности.

Подразделения и служащие фирмы оказывают Службе как гласную, так и конфиденциальную помощь на добровольной основе в поддержании установленных на фирме режимов безопасности, подготовке и проведении специальных мероприятий, связанных с обеспечением безопасности. При возникновении реальной угрозы фирме, ее служащим и учредителям Служба обязана имеющимися у нее возможностями и средствами предупредить либо локализовать эту угрозу. В этих случаях Служба привлекает для выполнения своих задач материально-технические ресурсы фирмы, возможности ее подразделений, а также служащих.

Руководители подразделений и служащие могут обжаловать действия и требования Службы в адрес Руководителя. Решения руководителя фирмы являются обязательными для Службы.

2.9. Отношения Службы с правоохранительными органами

Отношения Службы с правоохранительными органами системы МВД, Службы безопасности и Генеральной прокуратуры Украины осуществляются на основе действующего законодательства. Служба обеспечивает соблюдение фирмой и ее служащими действующего законодательства, на основе которого в пределах своей компетенции оказывает не противоречащее интересам фирмы содействие правоохранительным органам.

Служба представляет правоохранительным органам информацию о выявленных ею фактах преступной деятельности; оказывает возможную помощь в расследовании возбужденных уголовных дел, проведении оперативно-розыскных мероприятий в отношении служащих, юридических и физических лиц, причинивших или пытавшихся причинить ущерб безопасности фирмы, а также в осуществлении этих мероприятий на территории и в помещениях фирмы.

Служба взаимодействует с органами МВД по вопросам охраны и физической защиты собственности фирмы, ее служащих, поддержания общественного порядка. Служба взаимодействует с органами прокуратуры, суда и арбитражного суда по вопросам поддержания законности и практической реализации норм права в сфере осуществления деятельности фирмы.

Служба с санкции руководства фирмы может устанавливать с правоохранительными органами взаимовыгодные отношения для более эффективного выполнения своих функций по обеспечению безопасности фирмы.

2.10. Взаимодействие Службы с органами государственной власти и управления.

Служба при разработке и реализации системы мероприятий по обеспечению безопасности фирмы учитывает местные условия, специфику действующего на данной территории законодательства и практику его применения.

Служба через своего руководителя с санкции Руководителя фирмы осуществляет взаимодействие с органами государственной власти и управления по вопросам обеспечения безопасности фирмы, решение которых входит в компетенцию этих органов и Службы.

Служба может направлять своих сотрудников для участия в различных комиссиях при реализации указанными органами своих полномочий.

2.11. Отношения Службы с подразделениями безопасности других фирм и организаций.

В случаях возникновения необходимости Служба организует взаимодействие с аналогичными подразделениями других фирм и организаций. Содержание и формы взаимодействия в рамках выполнения своих функций определяются в каждом конкретном случае на основе двусторонних договоров или устной договоренности с санкции Руководителя фирмы.

В случаях возникновения чрезвычайных обстоятельств, для предотвращения угрозы фирме, Служба и ее сотрудники могут инициативно вступать во взаимодействие с подразделениями безопасности других фирм и организаций. О таких контактах сотрудники обязаны информировать руководителя Службы.

3. Деятельность службы

3.1. Гарантии соблюдения Службой ее обязанностей; гарантии прав Службы.

При разработке и принятии нормативных документов по организации и осуществлению своей деятельности руководители подразделений фирмы руководствуются принятой Руководством фирмы Программой обеспечения безопасности и Положением о Службе.

Нормативные гарантии заключаются в:

- 👁️ разработке нормативных документов Службы на основе действующих норм права;
- 👁️ определении пределов их действия;
- 👁️ определении и обеспечении правомерного поведения сотрудников Службы и служащих фирмы по вопросам обеспечения ее безопасности;
- 👁️ грамотном применении правовых норм к физическим и юридическим лицам, посягающим на законные интересы фирмы;
- 👁️ постоянном совершенствовании правового аспекта деятельности Службы.

Организационные гарантии заключаются в:

- 👁️ разработке и построении эффективной структуры управления деятельностью по обеспечению безопасности фирмы;
- 👁️ участию в разработке и реализации программы по обеспечению безопасности всех подразделений фирмы;
- 👁️ выработке организационного механизма по балансу интересов и консолидации усилий всех подразделений фирмы и ее филиалов, участвующих в реализации Программы обеспечения безопасности.

Материальные гарантии заключаются в:

- 👁️ выделении достаточных финансовых, технических, кадровых, интеллектуальных и иных ресурсов фирмы для достижения Службой своей основной цели.

Все структурные и функциональные изменения в деятельности Службы осуществляются решением Руководства. Руководство обеспечивает силами фирмы защиту законных прав и интересов Службы, ее сотрудников при взаимодействии с юридическими и физическими лицами.

3.2. Кадры Службы

Служба комплектуется специалистами, имеющими высшее или среднее специальное образование, прошедшими специальную подготовку, либо имеющими опыт работы в правоохранительных органах, которые по

своим деловым, моральным и физическим качествам могут выполнять возложенные на них обязанности.

Сотрудник Службы должен обладать следующими качествами:

- 👁️ знать и грамотно применять в служебной деятельности в пределах своих полномочий нормы законодательства Украины;
- 👁️ знать соответствующие нормативные документы, регламентирующие деятельность Службы и свои должностные обязанности, руководствоваться ими в своей деятельности;
- 👁️ быть уравновешенным, ориентироваться и принимать взвешенные решения в экстремальных ситуациях.

Дополнительные специфические, профессиональные и квалификационные требования к уровню образования и специальной подготовки сотрудников определяются в положениях о подразделениях Службы и должностных инструкциях.

3.3. Организация труда сотрудников Службы

Руководители Службы и ее подразделений обязаны выявлять и эффективно использовать возможности своих подчиненных для решения задач, поставленных перед Службой.

Зарботная плата руководителей и сотрудников Службы определяется штатным расписанием фирмы.

Оценка трудового вклада сотрудников Службы осуществляется на основе конечных результатов деятельности Службы и подразделений.

Руководители подразделений фирмы вправе вносить руководству Службы и фирмы предложения о поощрении сотрудников Службы за конкретные результаты в работе по обеспечению безопасности.

Руководитель Службы вправе вносить Руководителю фирмы предложения о дополнительном поощрении коллективов подразделений и отдельных служащих фирмы за успехи в работе и участие в решении конкретных задач по обеспечению ее безопасности.

3.4. Планирование деятельности Службы

Служба планирует и осуществляет свою деятельность на основании Положения, настоящей Концепции и Программы обеспечения безопасности фирмы и ее служащих по разделам:

- 👁️ организация системы обеспечения и поддержания безопасности фирмы и филиалов;
- 👁️ организация и осуществление режимно-конфиденциальной деятельности;
- 👁️ организации обеспечения физической безопасности фирмы и ее служащих;
- 👁️ организации системы информационного обеспечения по вопросам безопасности фирмы;
- 👁️ организация системы противодействия техническим разведкам конкурентов и криминогенных структур.

На основании указанных разделов подразделения Службы и фирмы разрабатывают и реализуют планы своей деятельности.

Планы представляют собой лишь концептуальное видение направлений деятельности Службы и ее подразделений.

Планы утверждаются руководителем Службы. В случае несогласия с руководителем Службы руководители подразделений и сотрудники Службы имеют право обращения к Руководителю фирмы.

Служба самостоятельно разрабатывает перспективные программы своего развития и представляет их для утверждения председателю Правления банка.

3.5. Ответность и контроль деятельности Службы

Руководитель Службы периодически отчитывается перед Руководством фирмы по вопросам, входящим в компетенцию Службы, а также несет ответственность перед Руководителем за полноту и достоверность отчетной информации. Периодичность и форма отчетности определяется Руководителем фирмы.

Отчетность Службы осуществляется с целью организации эффективного управления обеспечением безопасности фирмы, своевременного выявления и устранения недостатков в проведении этой работы.

3.6. Деятельность Службы по предупреждению и локализации конфликтных ситуаций и процессов среди служащих фирмы и ее филиалов.

Возникновение конфликтов и других нежелательных процессов среди служащих создают серьезную угрозу эффективной деятельности фирмы, ее внутренней и внешней безопасности.

В этой связи Служба организует и осуществляет работу по своевременному выявлению:

- 👁️ реальных и потенциальных конфликтных ситуаций между отдельными служащими и группами служащих фирмы;
- 👁️ фактов осложнения взаимоотношений служащих и их групп с руководителями фирмы и ее подразделений;
- 👁️ социальной напряженности в отдельных группах служащих и между ними;
- 👁️ тенденций к деструктивному решению возникающих проблем (путем забастовок, создания угрозы жизни и здоровью отдельных служащих, групповых нарушений установленных в подразделениях фирмы режимов, выдвижения к администрации заведомо нереальных требований и т.д.);
- 👁️ причин и условий, способствующих возникновению указанных нежелательных процессов.

В рамках реализации системы мер обеспечения безопасности Служба осуществляет профилактическую деятельность по предупреждению нежелательных процессов среди служащих фирмы.

Указанная профилактическая деятельность направляется на:

- 👁️ превентивное обнаружение причин и условий возникновения и развития конфликтных ситуаций между служащими фирмы;
- 👁️ локализацию и устранение выявленных причин и условий с наименьшим для интересов фирмы ущербом;
- 👁️ консолидацию служащих вокруг основных целей и задач деятельности фирмы.

Служба анализирует морально-психологический климат, информирует руководство фирмы о причинах и условиях возникновения нежелатель-

ных процессов в подразделениях фирмы и принимает меры к их нейтрализации.

3.7. Обеспечение физической безопасности фирмы и ее служащих

Помимо выполнения указанных выше обязанностей, подразделения Службы выявляют факты:

- ☞ нарушения установленных технологических операций, которые могут привести к нанесению
- ☞ умышленного либо неумышленного материального ущерба фирме и ее служащим;
- ☞ реальной и потенциальной угрозы, создающей опасность для здоровья и жизни служащих фирмы, а также нанесению иного материального ущерба фирме.

О выявленных фактах Служба незамедлительно информирует руководителей заинтересованных подразделений и руководство фирмы.

3.8. Обеспечение технической безопасности фирмы

В рамках выполнения своих функций Служба обеспечивает безопасность и конфиденциальность технологических работ, имеющих для фирмы стратегическое значение.

Основными задачами Службы по технической безопасности фирмы являются:

- ☞ содействие обеспечению конкурентноспособности фирмой основных и перспективных услуг;
- ☞ обеспечение приоритетности ее технических разработок;
- ☞ осуществление надежной защиты информационной и интеллектуальной собственности фирмы.

3.9. Выявление, предупреждение и локализация Службой любых форм незаконных посягательств со стороны конкурентов, государственных органов и криминальных структур на информационную и интеллектуальную собственность фирмы.

Служба выявляет:

- ☞ реальную и потенциальную угрозу для обеспечения конкурентноспособности предлагаемых и реализуемых фирмой основных и перспективных услуг на внутреннем и внешнем рынках;
- ☞ нежелательные для фирмы тенденции финансового и технического характера;
- ☞ факты недобросовестного сотрудничества со стороны контрагентов и клиентов;
- ☞ обеспечивает их изучение.

Служба организует, осуществляет и координирует деятельность подразделений фирмы по:

- ☞ противодействию легальным способам сбора конфиденциальной информации о фирме, ее служащих и клиентах, а также о проводимых в ней перспективных работах.
- ☞ осуществлению контактов с представителями средств массовой информации;

Служба создает условия для накопления информационного потенциала, организует защиту фирмы, применяемых в ней технических средств и оргтехники от технических средств разведки конкурентов и криминогенных структур.

4. Обеспечение деятельности службы

4.1. Финансовое и материально-техническое обеспечение Службы

Финансовое и материально-техническое обеспечение (МТО) в сфере безопасности фирмы осуществляется для эффективной реализации основной функции Службы и решения предусмотренных Положением и настоящей Концепцией задач.

Обеспечение осуществляется в соответствии с утвержденной Руководителем Программой обеспечения безопасности фирмы.

Руководитель Службы имеет в своем распоряжении определенные Программой финансовые и материально-технические средства. С помощью этих средств реализуется выполнение Службой обусловленных обстановкой разовых мероприятий.

В случаях возникновения потребности в дополнительном финансировании и МТО отдельных мероприятий Службы, выходящих за рамки выделенных Программой средств, руководитель Службы для решения этого вопроса обращается к Руководству фирмы.

4.2. Информационное обеспечение деятельности Службы

Информационное обеспечение Службы осуществляется в соответствии с определяемой Положением и настоящей Концепцией ее компетенцией. Информационное обеспечение организуется и реализуется путем сбора подразделениями Службы информации, а также обязательного и инициативного направления информации в соответствующее подразделение Службы всеми подразделениями по вопросам, связанным с обеспечением безопасности фирмы. Служба разрабатывает перечень информации, которая должна поступать из подразделений фирмы, организует и контролирует ее поступление в Базу данных.

Служба по согласованию с заинтересованными подразделениями фирмы и отдельными служащими осуществляет мероприятия по сбору информации. Для этих целей Служба может привлекать служащих фирмы, разрабатывать им задания по сбору соответствующей информации и контролировать их выполнение.

Работники Службы вправе получать из Базы данных информацию по вопросам безопасности фирмы в рамках своей компетенции. Получаемая Службой информация обрабатывается и накапливается в подразделении накопления и аналитической обработки информации.

Как ранее отмечал в своей книге автор В.П.Мак-Мак “Служба безопасности предприятия” к любой концепции существуют следующие требования:

1) Конструктивность. Такое требование будет признано реализованным, если в концепции найдет отражение:

а) исходное состояние объекта, на преобразование которого направлена концепция;

б) состояние объекта, достигнутое в результате реализации концепции;

в) меры, необходимые для достижения сформулированных в концепции целей;

г) средства, необходимые и достаточные для достижения поставленных целей;

д) источники ресурсного обеспечения, используемые в ходе реализации концепции;

е) механизм реализации концепции, т.е. способы (методы) использования выделенных средств и ресурсов.

2) Вписываемость. Имеется в виду встроенность концепции преобразования какого-либо объекта в систему концепции преобразования взаимосвязанных в единую систему объектов, одним из компонентов которой этот объект является.

3) Открытость. Разработанная концепция должна давать возможность в ее рамках реагировать на изменение условий реализации концепции и вносить коррективы в реализацию в случае их необходимости.



Правовые основы деятельности службы безопасности

Прежде чем перейти к правовым основам деятельности предпринимательской службы безопасности, необходимо научиться выделять антагонистическую направленность:

1.) Столкновение интересов и конфликтные ситуации;

2.) Насилие над личностью и мошеннические действия;

3.) Кражи, грабежи, разбои и бандитизм потребительского направления;

4.) Корыстно-насильнические преступления производственного назначения и др.

Например, конфликты между организациями и отдельными людьми, нередко оказывают определяющее влияние на качество их деятельности, преступное поведение и методы борьбы с ней. Наши авторы постоянно говорят о решающей роли конфликтов в жизни отдельного человека, семьи, организации, государства, общества и человечества в целом.

Столкновение интересов – чаще всего описываемая и встречающаяся форма конфликтов, как между людьми, так и в других направлениях. Проявления таких форм – весьма многообразны. Часто их основной целью является установление господства над другими людьми, с тем, чтобы подчинить их своим интересам или использовать их ради собственной выгоды. Следующие – это денежные, имущественные, сексуальные или другие интересы.

Среди различных форм столкновения можно найти и такие, которые содержат конструктивные и ценные начала как для участников столкновений, так и для других людей и даже целых сообществ. Столкновение бывает следствием несовпадения установок, чувств, стремлений, целей,

моделей поведения, способов мышления и различные корыстные посягательства. Следует учесть, что корыстные посягательства против частной собственности делятся на такие виды, (для Украины):

1) – не связанные с насилием над личностью, (“тихие” преступления):

- кража – тайное похищение имущества (ст. 185 УК Украины);
- грабеж без насилия – открытое похищение имущества (ч. 1 ст. 186 УК Украины);
- требование без насилия (ч. 1 ст. 189 УК Украины);
- мошенничество – овладение имуществом или получение права на имущество посредством обмана или злоупотребление доверием (ст. 190 УК Украины);

2) связанные с насилием над лицом (“громкие” преступления):

- 🔊 умышленное убийство из корыстных мотивов (п. 6 ч. 2 ст. 115 УК Украины);



Заключение: Наши авторы отмечают, что наиболее полное представление о системе безопасности Вашего предприятия можно получить после изучения официально принятых документов по концепции безопасности, комплексной программы обеспечения безопасности и планов подразделений предприятия по реализации этой программы. Сформированная на научной основе система безопасности предприятия является организационной основой создания ее структурного подразделения – службы безопасности.

- 🔊 грабеж, объединенный с насилием (ч. 2 ст. 186 УК Украины);
- 🔊 разбой (ст. 187 УК Украины);
- 🔊 требование, объединенное с насилием (ч. 2-4 ст. 189 УК Украины);
- 🔊 бандитизм (ст. 257 УК Украины).

Кроме корыстных преступлений против частной собственности потребительского и производственного назначения такие самые преступления совершаются и против других форм собственности. Наши авторы подчеркивают, что преступления связанные с посягательством на частную собственность, совершаются значительно чаще, и криминологическая чувствительность населения к ним намного высшая.

Предметом корыстных и корыстно-насильных преступлений против частной собственности большей частью являются деньги, потребительские товары повышенного спроса и легкой реализации: ценности, предметы антиквариата, меха и кожаные носильные вещи, видео– и аудиопаратура, автотранспорт, компьютерная техника, музыкальные инструменты и т.п..

Естественно, что в жизни нельзя избежать разногласий, противоречий и конфликтов. Однако в действительности чаще всего не сами конфликты разрушительно действуют на людей и затрудняют их совместную жизнь, а следствия некоторых форм поведения в конфликтной ситуации: страх, враждебность, угрозы.

Оборонительная реакция в ответ на чувство страха и угрозы может проявляться в постоянной готовности к нападению, к уничтожению или обезвреживанию источника опасности. Часто для того, чтобы избежать потенциальной угрозы со стороны других людей, прибегают к попыткам подчинить их своей власти или постоянно контролировать их.

Иногда столкновение преобразуется в другую форму контактов, которую можно назвать отчуждением. Отчуждение может рассматриваться как конкретная форма самообороны в виде перемирия, часто связанная с ощущением собственного бессилия или усталости, наступающая в результате предшествующей борьбы. Несколько более смягченной формой отчужденности является так называемая конвенциональная корректность. Она основана на соблюдении некоторых жестко заданных границ, в рамках которых следует удерживать собственное поведение и поведение другого человека. Эти границы устанавливаются под влиянием действующих Законов Вашей страны, конвенционных норм, присущих данной среде или в результате действия неписаных законов при выполнении социальных ролей или функциональных обязательств работников предпринимательской службы безопасности.

Таким образом, можно сделать вывод, что каждый человек обладает личностными качествами, своими привычками и предубеждениями, которые с неизбежностью влияют на характер контактов с другими людьми и предприятием в целом. Поэтому общение в форме столкновений является результатом индивидуальных различий между людьми и возникают тогда, когда поступки участников одной ситуации имеют антагонистическую направленность. Вот сейчас уместно перейти к правовым основам деятельности предпринимательской Службы безопасности (НСБ) с учетом специфических особенностей Вашей страны.

Правовые основы деятельности службы безопасности предприятия в Украине

Авторы сразу ставят читателя в известность, что на сегодня в Украине не существует Законов (подзаконных нормативных актов), которые бы четко могли дать ответ на вопрос – чем руководствоваться при решении задач организации безопасности на предприятии предпринимателю любой формы собственности ?.

Основной правовой базой для создания службы безопасности предприятия в Украине (это мнение авторов) является Хозяйственный кодекс Украины (Закон Украины N 436-IV от 16.01.2003 г.). Официальная публикация: “Офіційний вісник України” от 28.03.2003 г. N 11. Дата вступления в силу: 01.01.2004 г.

Этот Кодекс определяет правовые основы хозяйствования в Украине и регулирует хозяйственные отношения, возникающие в процессе организации и осуществления хозяйственной деятельности между субъектами хозяйствования, а также между этими субъектами и другими участниками отношений в сфере хозяйствования.

С 1 января 2004 года признаны утратившими силу: – Закон Украины “О предпринимательстве” (N 698-XII от 07.02.91 г.), кроме статьи 4; – Закон Украины “О предприятиях в Украине” (N 887-XII от 27.03.91 г.).

Внимательно рассмотрим статью 64 Хозяйственного кодекса Украины (перевод на рус.авторов).

Статья 64. Организационная структура предприятия

1. Предприятие может состоять из производственных структурных подразделов (производств, цехов, отделений, участков, бригад, бюро, лабораторий и т.п.), а также функциональных структурных подразделов аппарата управления (управлений, отделов, бюро, служб и т.п.).

2. Функции, права и обязанности структурных подразделов предприятия определяются положениями о них, которые утверждаются в порядке, определенном уставом предприятия или другими учредительными документами.

3. Предприятие самостоятельно определяет свою организационную структуру, устанавливает численность работников и штатная роспись.

4. Предприятие имеет право создавать филиалы, представительства, отделения и прочие отдаленные подразделы, согласовывая вопрос о размещении таких подразделов предприятия с соответствующими органами местного самоуправления в установленном законодательством порядке. Такие отдаленные подразделы не имеют статуса юридического лица и действуют на основе положения о них, утвержденного предприятием. Предприятия могут открывать счета в учреждениях банков через своих отдаленные подразделы в соответствии с законом.

5. Деятельность расположенных на территории Украины отделенных подразделов предприятий, которые находятся за ее пределами, регулируется этим Кодексом и другими законами.

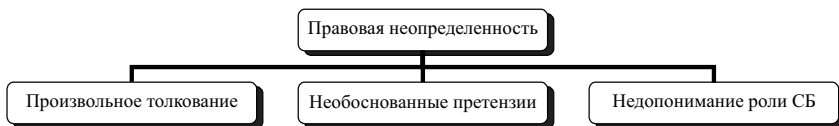
Обратим внимание, что "...подразделы не имеют статуса юридического лица и действуют на основе положения о них, утвержденного предприятием...". Вот почему в книге Вы встречаете один из главных внутренних нормативных документов "Положение (подчеркиваем) о службе безопасности предприятия", особенно, когда речь идет о предприятии в Украине.

Этой же нормой Кодекса определено и различие между охранный деятельностью служб безопасности предприятий и охранными фирмами (службами безопасности, агентствами безопасности, и иными ЧОПами) в Украине, которые занимаются хозяйственной деятельностью по предоставлению услуг, повязанных с охраной государственной и другой собственности, предоставлению услуг по охране граждан.

Деятельность последних регулируется ПРИКАЗОМ ГОСУДАРСТВЕННОГО КОМИТЕТА УКРАИНЫ ПО ВОПРОСАМ РЕГУЛЯТОРНОЙ ПОЛИТИКИ И ПРЕДПРИНИМАТЕЛЬСТВА И МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ УКРАИНЫ N 145/1501 от 14.12.2004 года "Об утверждении Лицензионных условий осуществления хозяйственной деятельности по предоставлению услуг, повязанных с охраной государственной и другой собственности, предоставлению услуг по охране граждан" { С изменениями, внесенными согласно с Приказами Государственного комитета Украины по вопросам регуляторной политики и предпринимательства N 22/230 (z0310-06) от 09.03.2006 N 17/24(z0187-07) от 19.02.2007г. }.

Учитывая эти моменты при решении задач безопасности любой предприниматель должен тщательно проанализировать состояние действующего законодательства и обосновать применение тех или иных мер безопасности, охраны, защиты коммерческой тайны, сбора информации и т.д.

При этом следует всегда помнить об основополагающем принципе – верховенстве закона над подзаконными актами (ведомственными инструкциями, положениями и т.д.)



Правовая неопределенность практически во многих аспектах деятельности СБ предприятия в Украине может приводить к таким последствиям:

- 🔊 произвольному толкованию со стороны правоохранительных органов в отношении статуса, прав и обязанностей СБ предприятия;
- 🔊 необоснованным претензиям к СБ со стороны правоохранительных органов, властных и силовых структур;
- 🔊 недопониманию роли СБ и важности решаемых ею задач со стороны руководства и персонала предприятия;

Для исключения или хотя бы нейтрализации подобных моментов настоятельно рекомендуем налаживать плодотворные контакты с упомянутыми выше органами и структурами.

В качестве первого шага необходимо подготовить Устав СБ предприятия или Положения о службе безопасности (или и то, и другое), утвердить их у руководителя предприятия и согласовать эти документы с местным милицейским руководством (хотя бы по вопросам координации и взаимодействия!).

Настоятельно так же рекомендуем руководителям СБ в своей деятельности по вопросам кадровой политики, организации учебного процесса, подготовки и проведения охранных мероприятий службой безопасности – придерживаться требований ПРИКАЗА ГОСУДАРСТВЕННОГО КОМИТЕТА УКРАИНЫ ПО ВОПРОСАМ РЕГУЛЯТОРНОЙ ПОЛИТИКИ И ПРЕДПРИНИМАТЕЛЬСТВА и МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ УКРАИНЫ N 145/1501 от 14.12.2004 года “Об утверждении Лицензионных условий осуществления хозяйственной деятельности по предоставлению услуг, повязанных с охраной государственной и другой собственности, предоставлению услуг по охране граждан”

Нужно всегда помнить, контроль за предоставлением охранных услуг субъектами предпринимательской деятельности в соответствии с требованиями действующего законодательства, в пределах своей компетенции осуществляют: Главное управление Государственной службы охраны при МВД Украины и их подразделения на местах.

Правовые основы деятельности службы безопасности предприятия в России (СНГ)

Происходящие в российской экономике преобразования, направленные на создание и развитие новых форм собственности, ставят вопрос о мерах правовой и специальной защиты предпринимательства от преступных посягательств с привлечением не только государственных, но и негосударственных правоохранительных структур.

Законодательную основу деятельности частных охранных предприятий составляют две группы нормативно-правовых актов (законов и подзаконных актов).

Первая группа – это нормативно-правовые документы общего характера, применяемые ко всем юридическим лицам, осуществляющим хозяйственную деятельность, а именно Конституция РФ; Гражданский и Налоговый кодексы РФ; федеральные законы о порядке создания и деятельности юридических лиц и т.д.

Вторая группа – это специальные нормативно-правовые акты, действие которых распространяется только на частные охранные предприятия.

К этой группе относятся:

Закон РФ от 11.03.1992 г. “О частной детективной и охранной деятельности в Российской Федерации”;

Закон РФ от 13.12.1996 г. “Об оружии”;

Постановление Правительства РФ от 14.08.1992 г. № 587 “Вопросы частной детективной и охранной деятельности”;

Положение о лицензировании негосударственной, частной охранной деятельности (введено в действие Постановлением Правительства РФ от 14.08.2002 № 600);

Инструкция по организации работы органов внутренних дел по контролю за оборотом гражданского и служебного оружия и патронов к нему на территории РФ (Приказ МВД России от 12.04.1999 г. № 288);

Инструкция о порядке лицензирования и осуществления органами внутренних дел контроля за частной детективной и охранной деятельностью (Приказ МВД России от 22.08.1992 г. № 292);

Тщательное изучение законодательства, позволит Вам не допустить ошибок и просчетов в работе.

Контроль за исполнением законодательства на местах возложен на отделы и службы лицензионно разрешительной системы МВД (ОЛРР)

Законодатель определяет особый порядок создания и ликвидации службы безопасности.

Под предприятием, которое вправе учреждать собственную службу безопасности, понимается исключительно коммерческая организация (полное товарищество, товарищество на вере, общество с ограниченной ответственностью, общество с дополнительной ответственностью, акционерное общество, производственный кооператив, государственное унитарное предприятие и муниципальное унитарное предприятие).

Для получения лицензии на создание частного охранного предприятия (СБ предприятия) учредители предприятия представляют в соответствующий орган внутренних дел:

а) заявление с просьбой выдать лицензию;

б) заявление о согласовании Устава службы безопасности;

в) Устав службы безопасности;

г) документы для получения лицензий руководителем предприятия и охранниками.

д) записку (сведения), в которой перечисляются виды охранных услуг и указываются предполагаемая территория деятельности создаваемого предприятия охраны, данные о планируемой численности его персонала, потребности в технических и иных средствах, а также специальных средствах и оружии;

СБ на предприятиях действуют на основе собственных уставов, согласованных по месту своего учреждения с органами внутренних дел. Их руководители и персонал обязаны получить лицензии в соответствии с пунктами 2.2.1., 2.2.2., 2.2.3. “Инструкции о порядке лицензирования и осуществления органами внутренних дел контроля за частной детективной и охранной деятельностью” (Утверждена приказом МВД РФ от “22” августа 1992 г., № 292).

Следует отметить, что по смыслу Закона РФ «О частной детективной и охранной деятельности в Российской Федерации» лицензии должны быть получены до образования службы безопасности, однако на практике это правило не соблюдается. Как правило, процесс учреждения службы безопасности и получения лицензий на частную сыскную и охранную деятельность происходит параллельно.

Учредителями службы безопасности не могут быть физические лица (даже имеющие лицензии на осуществление частной детективной и охранной деятельности) или несколько юридических лиц. В соответствии с Законом учредителем службы безопасности может быть только одно предприятие. Целесообразность такого порядка учреждения службы безопасности вызывает со стороны исследователей и практиков обоснованную критику, считающих его (т.е. этот порядок) бюрократизмом и ненужной преградой. Действительно, какие аргументы «против» могут быть в случае, например, желания руководителей нескольких мелких предприятий (выпускающих однородную продукцию и расположенных компактно на территории) создать единую для всех службу безопасности? Кроме того, существующий порядок учреждения службы безопасности можно легко обойти и физическому лицу, пожелай он создать собственную службу безопасности. Он может, например, вначале создать и зарегистрировать акционерное общество, единоличным собственником которого и станет, после чего учредит при нем службу безопасности. Следовательно, существующий порядок учреждения службы безопасности следует признать несовершенным, требующим внесения соответствующих корректив в действующий Закон.

При создании службы безопасности предприятие-учредитель может предоставить ей право открывать текущий и расчетный счета в банке (это должно найти отражение в Уставе). Текущий счет предназначен только для операций, связанных с выдачей наличных денег, а по расчетному счету проводятся операции, связанные с безналичными перечислениями. Однако это не позволяет относить службу безопасности 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. 14 Закона) означает: такое оргструктурное формирование, как служба безопасности, может функционировать только в рамках юридического лица, т.е. предприятия-учредителя.

Особенности национальных рынков безопасности

Авторы предлагают ознакомиться с материалами из журнала “BOS” – [19.03.2007]. В чем же состоит особенность национальных рынков безопасности в рамках СНГ? Если говорить в целом, то у стран СНГ есть одно неоспоримое преимущество – человеческий потенциал. В странах бывшего Советского Союза осталось огромное количество профессионалов, об-

ладающих уникальными знаниями и опытом. Многие сотрудники правоохранительных органов, армии и спецслужб пришли в негосударственную безопасность, где нашли себе успешное применение.

Кроме того, в наших странах великолепные технические специалисты, работающие ранее на военно-промышленный комплекс. В плане технических разработок самые сильные страны – Россия и Украина. Их продукция не только не уступает зарубежным образцам, но зачастую намного их превосходит, выгодно отличаясь при этом по цене.

Экономика в большинстве стран СНГ развивается достаточно поступательно и стабильно. Благосостояние народа пусть не везде, но увеличивается. Это дает основания утверждать, что сфера охранных услуг имеет самодостаточные перспективы для роста, зависящие только от экономических показателей. Ведь сами охранные предприятия ничего не производят. Пока экономика обеспечивает их заказами – они развиваются.

❖ Двигатель прогресса – это экономика. Есть развитие ВВП – есть работа для ЧОПов (частных охранных предприятий), если ее нет – что, собственно, охранять? – объясняет ситуацию президент НАСТ России Дмитрий Фонарев.

❖ Как Российский так и Украинский рынки огромны. И это главное отличие рынков. Еще одна наша особенность – крупные ЧОПы могут развивать собственные направления на стыке охранных технологий. Например, охранные сигнализации различного назначения. Индустрия охранных средств в Украине и России развивается как количественно, так и качественно. Достаточно рентабельным является бизнес по консалтингу. У коллег в странах СНГ, собственно нет таких условий, вот и все преимущества россиян.

Думаю, украинские коллеги могут согласиться не со всем. Да, наш рынок имеет меньшую емкость, на нем меньше игроков, но по отдельным направлениям безопасности мы идем впереди. В частности, обратимся к рынку централизованной охраны.

В качественном, функциональном и ценовом аспектах наши разработчики готовы заявить о своем лидерстве. Не будем голословны. На российском рынке уже не первый год успешно работают украинские системы линейки «Орлан» (Харьков) и «Дунай» (Киев). И это несмотря на жесткие законодательные ограничения по использованию зарубежного оборудования.

Планы по проникновению на Восток вынашивают и другие разработчики; и пока останавливает их только политика протекционизма, проводимая российскими органами сертификации.

Где мы пока действительно отстаем, так это в сфере формирования информационного поля. Консалтинг, информационно-аналитические услуги, маркетинг на рынке безопасности в Украине только начинают массовое внедрение в прейскуранты охранных предприятий и сознание потребителей.

И, конечно, нельзя не затронуть две другие основные проблемы украинского правового поля: отсутствие закона «Об охранный деятельности» и запрет на применение охранными предприятиями огнестрельного оружия и длинного перечня спецсредств. Первое говорит о некоторой неупорядоченности статуса негосударственных структур, второе – серьезно ограни-

чивает их возможности в оказании услуг личной и банковской охраны. С этим утверждением соглашаются специалисты Молдовы.

Серьезным преимуществом рынка безопасности нашей страны является тот факт, что граждане вправе приобретать, хранить и носить нарезное короткоствольное огнестрельное оружие (пистолеты и револьверы), – утверждает молдавский эксперт Анатолий Брединский. – Благодаря этой возможности у структур, занимающихся частной охранной деятельностью, нет проблем с вооружением своих сотрудников, в то время как в ряде стран СНГ эта проблема стоит перед коллегами очень остро. При этом другим преимуществом Молдовы, по мнению г-на Брединского, является не емкость, как в России, а компактность рынка.

Объединение интересов и контроль над деятельностью структур безопасности в таких условиях осуществлять намного проще.

Рынок более «прозрачен», проще бороться с недобросовестной конкуренцией. И хотя у маленького рынка есть серьезный недостаток – относительно небольшой объем, но это приводит к более жесткой конкуренции и как следствие к повышению качества товаров и услуг.

Еще одним преимуществом, пожалуй, является относительно невысокий уровень организованной преступности. Это создает хорошие предпосылки для развития бизнеса в стране и рождает стабильно растущий спрос на товары и услуги в области безопасности.

Немного о нормативной базе. В Украине давно обсуждают несовершенство нормативной базы. В частности, речь идет об исключительных полномочиях Департамента Госохраны, позволяющих ему в любой момент прекратить деятельность «непонравившейся» охранной фирмы.

– Это не так, – возражает заместитель начальника Департамента ГСО при МВД Украины Александр Крылач. – В той же России требования гораздо жестче. Например, частная фирма, выезжая в другой регион, обязана уведомить местные правоохранительные органы о том, на каком именно объекте она будет выполнять охранные функции. И если действия этой компании привели (или имели косвенное отношение) к захвату какого-либо предприятия или были применены запрещенные спецсредства – компания сразу лишается лицензии, без всяких контрольных сроков.

А в нормативной базе Казахстана четко прописано, что одно лицо может являться учредителем (соучредителем) только одной охранной компании. Подобные положения существуют и в законодательствах Армении и Грузии. Будь у нас введена такая норма, количество охранных фирм в Украине уменьшилось бы как минимум вдвое.

Изменения и реформы

Какие изменения необходимы на охранном рынке в отдельных странах и в масштабах всего СНГ? Реформы в первую очередь должны исходить изнутри рынка. Пора кончать с разобщенностью. Необходима единая эффективная структура, которая бы защищала и продвигала интересы субъектов рынка на всех уровнях. Надо всерьез заняться вопросами подготовки кадров для сферы негосударственной безопасности. Наладить обмен опытом и знаниями как внутри стран, так и с коллегами на международном уровне. Рынку жизненно необходимы профессиональные мероприятия: форумы, конференции, круглые столы и семинары по актуальным темам практического назначения.

Недостает специальных отраслевых изданий и литературы, что сказывается на уровне подготовки. Нужно также более тесно взаимодействовать с правоохранительными структурами, чтобы избавиться от «синдрома конкурента».

Необходимо совершенствовать нормативно-правовую базу. Об этом говорят даже в России, где профильный закон работает уже 14 лет. Но в сфере законодательства любой страны еще много недостатков.

Например, одной из главных проблем в Казахстане стали взаимоотношения с законом. Отдельные аспекты работы охранников, как и их права и обязанности, вообще не прописаны в казахстанских законах. Между тем, на руках у сотрудников охранных организаций 12 тысяч единиц огнестрельного оружия, половина которого нарезное. А порядок применения оружия неясен.

Неприятные инциденты происходят постоянно, – говорит заместитель директора ТОО «Специальное агентство «Барс» Сергей Захаров. – Своей деятельностью мы заслужили похвалу от высших руководителей МВД и правительственных чиновников.

При этом на рядовых охранников постоянно заводятся уголовные дела за нарушение правопорядка. Ни в одном законе не сказано, что наш сотрудник может остановить нарушителя закона на улице и силой привести его в полицию. Нередко, приводя нарушителя в участок, охранник остается там надолго – уже в качестве обвиняемого.

В Украине и Азербайджане до сих пор нет законодательства по охране. Кроме того, в этих странах, как и в Беларуси, только государственные структуры имеют право использовать в своей деятельности специальные средства при осуществлении охранной деятельности: оружие, парализующие средства, индивидуальные средства защиты и т.д. И, по мнению специалистов, такая ситуация требует переосмысления.

В государстве объективно не может быть двух систем обеспечения безопасности, отдельно частной, отдельно государственной, – утверждает вице-президент Украинской федерации негосударственных служб безопасности (УФРНСБ) Юрий Ермаков.

Есть единое правовое поле в рамках действующего законодательства, и если охранные предприятия де-факто выполняют часть функций по обеспечению имущественной и личной безопасности, то они по определению должны являться частью правоохранительной системы.

Также и охранная деятельность не может быть негосударственной, слишком это специфический вид деятельности. А вот осуществлять охранную деятельность могут предприятия с разной формой собственности.

Содержание одного полицейского отдела охраны обходится государству недешево. К тому же его зависимость от закона «О полиции» не дает ему возможность выполнять услуги в полном объеме для частной компании, – говорит президент Национальной ассоциации телохранителей Азербайджана Вагиф Кадыров.

И законодательное регулирование необходимо. Нужно, чтобы закон четко определял, кто имеет право на получение статуса частного охранника. Ведь мы не допускаем к работе водителя, не имеющего прав, потому что это приводит к угрозе безопасности граждан. А как же лицо может осуществлять охранную деятельность, не имея соответствующей квалификации?

Принятие закона о негосударственной охранной деятельности в этих странах позволит охранным структурам выйти на более высокий профессиональный уровень.

Необходима и реформа сознания лидеров рынка. Фаза зарабатывания денег сменяется фазой политической активности.

Рынок должен выделить из тысяч охранных предприятий – профессиональные, создать консолидирующую структуру и договориться с государством о новейших правилах игры.

Перед Законом – все должны быть равны

Авторы предлагают немного поговорить об проекте Закона Украины “Об охранной деятельности”, по обеспечению безопасности, усиление их правоохранительной направленности, организация реального взаимодействия с территориальными органами внутренних дел и ряд других вопросов. В Украине появились первые частные образовательные учреждения по подготовке специалистов охраны – разной направленности.

Продолжается создание профильных общественных организаций, объединяющих производителей технических средств охраны, противопожарных средств, профессиональных специалистов охраны. и телохранителей, планируется создание Ассоциации профессиональных служб безопасности юридических лиц. Некоторые из них уже «почили в обозе» другие – только в процессе развития. Все это безусловно, на пользу охранному сообществу. Но мы ставим вопрос о создании системы безопасности личности и предпринимательства как составной части национальной безопасности таким образом, что бы были:

- ❖ созданы условия для подготовки обсуждаемого проекта Закона;
- ❖ создание крупных и средних предприятий безопасности (ПБ), способных обеспечить комплексную безопасность, их количественный рост, увеличение числа людей, занимающихся различными вопросами обеспечения безопасности;
- ❖ создания равных условий всем субъектам охранной отрасли;
- ❖ создание, внедрение и развитие новых технологий в обеспечении безопасности, интеллектуализация частной охраны;
- ❖ антиконкурентное действий органов власти и ряд других актуальных вопросов.

Начало формирования рынка безопасности, борьба за выживание и, как следствие, происходит дальнейшее развитие предприятий, оказывающих услуги Закона. Мы подчеркивает, что это равенство относится только к вольнонаемным сотрудникам охраны подразделений Государственной службы охраны (ГСО) при (!) МВД Украины. А как быть с остальным личным составом ГСО, в т. ч. аттестованными ? Дело в том, что в ГСО работников с другим статусом (милиционера) просто быть не может! Как быть в плане равенства – частной охранной структуры, (предпринимательской Службы Безопасности).

Для начала давайте массовому читателю попытаемся объяснить в чем суть проблемы? ГСО как субъект хозяйствования – крупнейший оператор на рынке охранных услуг – занимается активной финансово-хозяйственной деятельностью, оказывая платные услуги по договорам. А так как ГСО не входит в организационно-штатную структуру МВД, (см. Закон «Об общей структуре и численности МВД Украины») и, соответственно,

не является подразделением центрального органа исполнительной власти, то для этой структуры нет никаких препятствий зарабатывать деньги, т. е. заниматься тем, для чего она создана. Тем более что часть из этих средств идет на содержание МВД, хронически недополучающего денежные средства из бюджета. В правительстве Украины четко высказываются за увеличение объема платных услуг по охране, оказываемых ГСО.

Методика определения цен на услуги по охране объектов, утвержденная приказом МВД Украины и Министерством экономики Украины от 02.03.2001 г. №171/51, (п.2.4.), предусматривает: «норму прибыли», ежегодно определяемую МВД Украины (!?). Базой для определения цены услуги охраны является расчет валовых затрат плательщика налога, непосредственно связанных с выполнением услуг охраны по договорам охраны (п.2.2). При определении валовых затрат необходимо руководствоваться ст. 5 Закона Украины «О налогообложении прибыли предприятия». В валовые затраты входит и оплата стоимости лицензии (п.2.3.5. абзац 7). Положением о примерном бизнес-плане ГСО, подготовленном на основе предписания Фонда госимущества от 26.05.1994 г. №301, предусмотрены разделы «Характеристика конкурентной среды», «План маркетинговой деятельности», а также создание общих предприятий с иностранными инвестициями.

Еще в 2004 году на совещании в Департаменте ГСО, инициированном министерством внутренних дел и посвященном проблемам конкуренции и перспективам развития, были названы четыре приоритета ГСО.

Первый – повышение конкурентной способности. Победить конкуренцию в борьбе за клиентов, (перечисляются способы) и «что особенно важно, использовать возможности ОВД и, прежде всего, участковых, ориентировать их на поиск объектов под охрану на своих участках». Крайне неотложная проблема – устранение неуместной конкуренции между бюджетной и внебюджетной (!?) милицией. Запретить реагирование подразделений первой на «сработку» частных ПЦН, т. к. это может стать началом конца ГСО.

Второй – развитие контактов с разными властными органами, которые могут привлекать ГСО к охране своих объектов.

Третий – привлечение общественности и общих организаций к решению проблем охраны в интересах МВД (!?). Например, УФРНСБ и Ассоциация украинских банков этого не делают, а требуют вооружить свою, частную охрану.

Четвертый – создание на базе ГСО общественной организации, которая бы действовала в интересах МВД. Сказано – сделано, создана Ассоциация профессиональных работников охранных структур – АПРОС. Но как и всякая искусственно созданная организация, она умерла сразу после рождения. Читайте Закон Украины «О защите экономической конкуренции» раздел III, ст.15, ч.2, абзац третий «прямое или опосредованное принуждение субъектов хозяйствования к вступлению в ассоциации...».

Абзац 7 – «предоставление отдельным субъектам хозяйствования или группам субъектов хозяйствования льгот или других преимуществ, ставящих их в привилегированное положение по отношению к конкурентам...». То есть ГСО перед другими охранными предприятиями.

Абзац 8 – «...субъектам хозяйствования или группам субъектов хозяйствования создаются неблагоприятные или дискриминационные условия деятельности по сравнению с конкурентами». Аналогичное объяснение.

Правда, все знакомо! И называется это – *антиконкурентные действия* органов власти. А часть 3 выше названного Закона гласит – «*совершение антиконкурентных действий органов власти... запрещается*».

В соответствии с Положением о Государственной службе охраны, ГСО сегодня является профессиональной, специализированной охранной организацией, которая действует на принципах самофинансирования, имеет разветвленную структуру коммерческих предприятий, оказывающих полный комплекс платных охранных услуг на договорной основе. Подразделения ГСО являются охранными предприятиями с государственной формой собственности. Целью их деятельности, является «предоставление услуг стоимостного характера, имеющих ценовое выражение». Они являются плательщиками налога на прибыль, и этим все сказано. По большому счету, направлена эта деятельность на получение прибыли (т. е. предпринимательство) или на достижение экономических, социальных и других результатов (некоммерческая) – роли не играет. И «заморочки» типа «публичное право», «неприбыльные учреждения», «некоммерческая деятельность» – все это от лукавого.

Ст. 7 Закона Украины «О милиции» гласит: «Милиция является единой системой органов, которая входит в структуру МВД», кроме прочих подразделений она включает и «милицию охраны». Как и вся милиция, (ГСО) -милиция охраны также должна содержаться за счет бюджета. И именно она обязана охранять на безвозмездной (!) основе «объекты, имеющие стратегическое значение». Так принято во всем мире, нигде нет «платной милиции». У нас все наоборот. Каким образом милиция охраны попала в хозрасчетную организацию ГСО, даже не входящую в структуру и численность МВД? Как в ГСО появились аттестованные работники милиции? На каком основании вооружены боевым огнестрельным оружием работники гражданской охраны ГСО и т. д. и т. п.? Более того, Конституция Украины, ст. 17, абзац 6 гласит: «На территории Украины запрещается создание и функционирование каких-либо вооруженных формирований, не предусмотренных законом!» Мы заявляем, что ни в одном законе Украины нет даже упоминания о ГСО!

Без законодательного решения этих вопросов ГСО, по сути, является незаконным вооруженным формированием. После всего вышеизложенного, о каком равенстве всех форм собственности, согласно Конституции, можно говорить?

Авторы обращают внимание на то, что (ГСО) заявляет **об исключительном праве правоохранительных органов осуществлять некоммерческую охранную деятельность (!?)**.

Мы предлагаем заинтересованному читателю сделать краткий экскурс в Украинское законодательство:

- ❖ ст.1 Закона Украины «О милиции» – «государственный вооруженный орган исполнительной власти»;
- ❖ Хозяйственный кодекс (ХК) Украины ст. 8 ч.1 «органы государственной власти... не являются субъектами хозяйствования»;
- ❖ ХК Украины ст. 52, ч. 3 «Не могут осуществлять некоммерческую деятельность органы государственной власти,... их должностные лица»;
- ❖ ХК Украины ст. 53, ч. 3. «В случае, если хозяйственная деятельность... юридического лица, зарегистрированного в качестве субъекта некоммерческого хозяйствования, приобретает характер

предпринимательской деятельности, к ней применяется положение настоящего кодекса и других законов, которым регулируется предпринимательство».

Что на практике? Сплошь и рядом аттестованные работники милиции и военнослужащие Внутренних войск осуществляют охранную деятельность по договорам, на платной основе. В том числе и за охрану общественного порядка, что само по себе является нонсенсом.

Требования Евросоюза, ВТО к странам-участницам исключают содержание правоохранительных органов государства за счет самофинансирования или каким-либо иным способом, кроме как за счет бюджета.

С принятием наших поправок к проекту данного Закона все должно стать на свои места. В стране существует рынок охранных услуг, на котором работают субъекты охранной деятельности с различными формами собственности, но с равными правами и обязанностями.

Говоря о специфике охранной деятельности, авторы упоминают ст. 6, ч. 8 законопроекта, в которой предлагается охрану субъектов хозяйствования государственного сектора экономики, осуществлять только государственными предприятиями, подразумевается – подразделениями ГСО при МВД Украины.

Подготовлен проект Перечня объектов, которые подлежат охране подразделениями ГСО при МВД по договорам. Планируется взять под охрану все (!) объекты, являющиеся государственной собственностью. Не надо ни маркетинга, ни продвижения услуг, ни кропотливой работы по увеличению продаж, и вообще, конкуренцию упразднить! Если это рыночная экономика, то что тогда монополизм? Предполагается предоставить заведомо одностороннее преимущество субъекту охранной деятельности с государственной формой собственности. Это противоречит Конституции и действующему законодательству. Мы должны сказать, что Постановлением КМ Украины, от 24.10.2007 г. №1251 внесены изменения в «Положение о ГСО» при МВД. Безусловно, единоличное право государства устанавливать порядок работы своих предприятий и организаций. Поэтому мы не будем обсуждать эти изменения. Но истины ради, упомянем об одном из них. Пункт 9 абзац 5 изложен в такой редакции: «Управления, отделы и подразделения охраны являются государственными учреждениями, которые осуществляет некоммерческую хозяйственную деятельность» (!??).

Таким образом, подразделения охраны, оказывающие платные услуги по договорам, несущие всю нагрузку по содержанию управленческого аппарата, поставлены, как и вся Государственная служба охраны, над рынком безопасности, выведены из него. На (ГСО) теперь не распространяются ни экономические законы, ни антимонопольное законодательство, да, наверное, вскоре и налоговое. И все это делается под лозунгом: «Да здравствует конкуренция!». Выводы, дорогие читатели и специалисты негосударственной Службы Безопасности – за вами.

Государственная и негосударственная СБ

Хотелось бы авторам высказать личное мнение о повсеместном употреблении термина «негосударственный» в контексте со словом «безопасность». «Безопасность народа – занятие государства», писал – английский философ Т. Гобс. Эта формула нашла свое отражение в законодательных

актах практически всех стран мира. В Украине осуществление мер по безопасности возложено на Президента, Кабинет министров, СНБО – и, соответственно, на их органы, отвечающие за данное направление.

Решая де-факто государственную задачу в общей системе безопасности, в то же время негосударственная Служба Безопасности (НСБ) добровольно сами выделяют себя из государства, берут часть государственных функций на себя. Чиновники, да и обыватель, очень негативно реагируют на термин «негосударственная СБ» (НСБ). Возникает вопрос, а чья тогда эта служба и выполняет ли она функции за соответствующие органы государства? Кто гарантирует качество оказываемых услуг – государственной и негосударственной служб?

По большому счету в государстве объективно не может быть двух систем обеспечения безопасности, тем более «негосударственной», государство, по определению, обязано решать все вопросы, связанные с обеспечением безопасности личности, собственности и предпринимательства. А частные СБ, оказывают ему помощь в рамках единой государственной политики. Есть единое правовое поле в рамках действующего законодательства и если НСБ – выполняют часть функций по обеспечению имущественной и личной безопасности, то они априори являются частью системы национальной безопасности. Правда, для того, чтобы это произошло, руководство страны должно официально признать эту реальность.

Предпринимались неоднократные попытки вынести проект Закона на обсуждение в Верховную Раду.

Первая – в 1999 г. Один из проектов прошел даже второе слушание, но был возвращен на переработку. Причина старая – разработчики пытались нарушить требования основного Закона – Конституции о равенстве всех форм собственности, представить необоснованные, незаконные привилегии одному участнику рынка перед другими.

Почему необходимо принятие данного Закона, а точнее – пакета Законов, включая Законы «Об оружии», «О детективной деятельности». Прежде всего, эти законы будут законодательной базой системы безопасности личности и предпринимательства. Практически НСБ частично выполняют государственные правоохранительные функции только в рамках договорных отношений с отдельными лицами. Обеспечение безопасности, в отличие от других видов деятельности, имеет свои особенности. С одной стороны, она осуществляется в целях защиты законных прав и интересов отдельных граждан и юридических лиц. С другой, целью создания ПБ является получение прибыли со всеми признаками предпринимательства. И не одна из этих составляющих не может быть приоритетной.

Осуществление любого вида деятельности требует ее законодательного обеспечения, тем более что НСБ являются предприятиями с особыми уставными задачами. И никакой подзаконный акт не сможет решить эти вопросы.

Организация, (создание) службы безопасности

В странах СНГ, России, Украины сложились негативные стереотипы к негосударственной службе безопасности, и при этом, многие понимают ее необходимость. Для исправления этих стереотипов необходимы целенаправленные усилия всех причастных к СБ специалистов, создание позитивного имиджа работника СБ, охраны и телохранителя, акцентирующих внимание на следующих позитивных моментах:

- ❧ работа в СБ, не временное занятие, а социально-позитивная деятельность;
- ❧ сотрудниками охраны, (личной охраны) могут быть люди, имеющие достаточный общеобразовательный уровень, (средне-специальное или высшее образование);
- ❧ профессиональный сотрудник СБ – это надежный специалист с перспективой служебного роста;
- ❧ при любом политическом климате страны, работник СБ всегда будет полезным и востребованным.

Эффективное функционирование службы безопасности предполагает предварительную проработку многих вопросов. Среди них особое значение приобретает проектирование оргструктуры службы безопасности и ее ресурсного обеспечения, т.к. без решения этих вопросов ее деятельность вообще невозможна. Собственно говоря, употребляемый нами многозначный термин «организация» среди многих значений имеет и такое, как создание нужной структуры и необходимых ресурсов, именно этот смысл раскрывается в главе.

Общеизвестно, что любое оргструктурное формирование создается для реализации определенных функций. Применительно к службе безопасности предприятия, эти функции определены в странах СНГ, России и Украины – по разному, и это необходимо учитывать в нормативно-правовых положениях Устава своего предприятия. Анализ этих функций позволяет утверждать, что для их реализации необходимо, как минимум, создать три подразделения службы безопасности: разведку, контрразведку и охрану. Разумеется, количественное соотношение работающих в них сотрудников будет различно, и оно носит объективный характер. Среди причин, определяющих неравномерное количество сотрудников в различных подразделениях службы безопасности, можно назвать финансовые возможности предприятия-учредителя, наличие или отсутствие охраняемых секретов, степень включенности в конкурентную борьбу и т.д. Более того, в практике некоторых служб безопасности встречаются случаи объединения двух детективных подразделений (разведка и контрразведка) в одну общую. Такое объединение, хотя оно и носит вынужденный характер, нельзя признать удачным. Основной причиной нежелательности такого объединения является то, что каждое подразделение службы

безопасности имеет свои специфические цели, задачи и функции, реализация которых, (поскольку они взаимно дополняют и не противоречат друг другу) позволяет значительно повысить эффективность службы безопасности в целом.

Законами также прямо предусмотрена должность руководителя службы безопасности, которая на практике трансформировалась в начальника службы безопасности (по-видимому, здесь сказался прошлый опыт деятельности в правоохранительных органах персонала службы безопасности). Совершенно очевидно, что если персонал службы безопасности по количеству большой, неизбежно встает вопрос о заместителях начальника службы безопасности. Их также должно быть не менее трех (по количеству подразделений службы безопасности), в крайнем случае, двух, если существует единая детективная служба.

Как правило, заместитель начальника службы безопасности является одновременно руководителем одного из подразделений и, в свою очередь, также имеет одного или нескольких заместителей. Не вызывает сомнений целесообразность создания таких подразделений, как канцелярия и бухгалтерия (в случае, если службу безопасности не обслуживает единая бухгалтерия предприятия-учредителя).

В крупных службах безопасности возможно введение должностей помощников (референтов) начальника. Следует отметить, что в маленьких (по количеству персонала) службах безопасности проектирование их оргструктуры на этом можно и закончить, утвердив его у руководителя предприятия-учредителя.

Иная ситуация складывается в крупных службах безопасности, где возникает необходимость создания штабных подразделений, т.к. начальники службы безопасности просто физически не способны на должном уровне выполнять такие управленческие функции, как анализ, планирование, контроль и т.д. Исполнение этих обязанностей помощниками положение дел не меняет, т.к. в этом случае возникает необходимость их повседневного руководства, что опять-таки не под силу начальнику службы безопасности и он вынужден будет назначить одного из них координатором деятельности других, а это по сути означает выполнение обязанностей начальника штаба. Следует отметить, что создание штаба в оргструктуре службы безопасности обычно вызывает возражение руководителей предприятия – учредителя и преодоление их нежелания является трудным делом.

Предложенная схема оргструктуры должна время от времени уточняться и пересматриваться.

Любая оргструктура, даже самая оптимальная, не сможет дать ожидаемых результатов, если ее не дополнить внутренними нормативными актами, регулирующими деятельность всех подразделений и сотрудников службы безопасности. Образно выражаясь, «кость» (оргструктура) должна обрести «мясо» (нормативными документами). Причем эти нормативные акты условно можно разделить на две группы – непосредственно относящиеся к деятельности самой службы безопасности и к деятельности других служб (подразделений, сотрудников) предприятия:

К **первой группе** относятся: Устав службы безопасности, Положения об отделах и штабе службы безопасности, Положения о группах и секторах службы безопасности, должностные инструкции сотрудников службы безопасности. Структура Устава службы безопасности нашими авторами

ранее уже рассматривалась, а структура положений об отделах и штабе будет изложена в последующих главах и приложениях.

Структура должностной инструкции должна включать следующие разделы: общие положения; функции; должностные обязанности; права, ответственность; взаимоотношения и связи по должности. Разработка этих нормативных актов идет последовательно, начиная с Устава до должностной инструкции, что позволяет охватить весь комплекс целей, задач и функций, решаемых службой безопасности.

Чтобы избежать дублирования этих целей, задач и функций рекомендуется составить таблицу по прилагаемой форме, заполнить пустующие графы формулировками целей, задач и функций и в случае их пересечения вновь переформулировать, избегая дублирования (как пример см. таблицу).

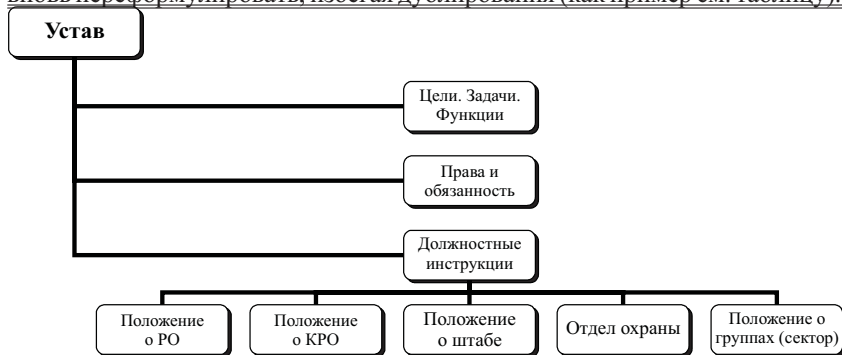


Таблица: Нормативные документы. Цели. Задачи. Функции.

Устав службы безопасности

Положение о разведывательном отделе

Положение о контрразведывательном отделе

Положение об отделе охраны

Положение о штабе

Положение о группе, отделении (секторе)

Должностная инструкция

Примечания:

- в должностных инструкциях цели не формулируются;
- при составлении таблицы приводится исчерпывающий перечень всех групп (секторов) и должностей.

Внесение корректив в Устав службы безопасности допускается только по согласованию с руководителем предприятия и органов внутренних дел по месту своего учреждения. Другие нормативные акты рекомендуется систематически обновлять (по крайней мере, один раз в год) и утверждать у начальника службы безопасности (в некоторых случаях у руководителя предприятия).

Вторая группа внутренних нормативных актов, обеспечивающих деятельность других сотрудников и служб подразделений предприятия-учредителя, включает в себя:

- 🔊 договор предприятия с партнером об обеспечении им мер безопасности коммерческой информации;

- 🔊 инструкцию для исполнителей работ и документов, содержащих коммерческую тайну;
- 🔊 обязательство о неразглашении коммерческой тайны;
- 🔊 перечень сведений, составляющих коммерческую тайну предприятия и основные требования к сотрудникам по ее защите;
- 🔊 перечень сведений, которые не должны разглашаться посторонним лицам в целях личной безопасности сотрудников, предприятия;
- 🔊 перечень должностных лиц, уполномоченных относить информацию к коммерческой тайне;
- 🔊 правила отнесения информации к коммерческой тайне и снятия с их носителей грифа конфиденциальности;
- 🔊 правила ведения секретного делопроизводства;
- 🔊 памятку работнику (служащему) о сохранении коммерческой тайны предприятия;
- 🔊 правила приема посетителей на предприятии;
- 🔊 правила внутреннего трудового распорядка и т.д.

Разумеется, все эти предполагаемые нормативные акты разрабатываются сотрудниками службы безопасности совместно с соответствующими службами предприятия, и после их утверждения руководством подлежат также совместному контролю за их исполнением. (Примечание: Общий перечень образцов документов, рекомендуемых для использования в деятельности службы безопасности, прилагается в приложениях).

Однако оптимальное оргструктурное построение и полное правовое обеспечение службы безопасности сами по себе не приведут к ее эффективному функционированию, если она не будет обеспечена соответствующими ресурсами. Продолжая образные сравнения, можно утверждать, что после того, как оргструктура обросла внутренне-нормативными документами, следует позаботиться о своих ресурсах.

Среди них первостепенное значение имеют финансовые ресурсы. Без финансового обеспечения деятельности службы безопасности бессмысленно вообще говорить о ее функционировании. Между тем, на практике эта истина подвергается иногда ненужной проверке (несвоевременная выдача зарплаты сотрудникам, задержка с оплатой заказа и т.д.), причем всегда с отрицательным результатом для предприятия - учредителя.

Поскольку служба безопасности не вправе самостоятельно зарабатывать деньги путем заключения договоров с другими клиентами, именно на предприятии-учредителе лежит обязанность финансирования ее деятельности. Но это не означает, что руководство службы безопасности должно занимать в этом вопросе пассивную позицию. Напротив, обоснованные текущие и прогнозные оценки в финансовых потребностях службы безопасности и основанные на них точные расчеты должны стать правилом, а не исключением. Финансовую политику службы безопасности определяют, конечно, ее руководители, но при этом активную помощь им должна оказывать бухгалтерская служба.

В функции этой службы входит: (первое)

- ❏ ведение табеля, учета рабочего времени;
- ❏ начисление зарплаты, премий и т.д.;

- ❖ учет выплат за различные услуги;
- ❖ перечисление денег;
- ❖ выдача сотрудникам их денежного содержания;
- ❖ оплата счетов и т.д.

Поскольку руководители службы безопасности не являются, как правило, специалистами в финансовых вопросах, наиболее целесообразно свое внимание сосредоточить им на некоторых ключевых моментах.

Во-первых, периодически проверять финансовое состояние службы безопасности с помощью приглашенных специалистов.

Во-вторых, открывать расчетные и текущие счета только в надежных банках.

В-третьих, добиваться такого уровня минимальной зарплаты персонала службы безопасности, чтобы у него не возникало соблазна увольняться (можно порекомендовать в связи с этим устанавливать в контрактах сумму зарплаты в иностранной валюте по курсу Центрального банка России на день его выдачи).

В-четвертых, установить поэтапное финансирование закупленных, (приобретенных) материально-технических средств, от наиболее необходимых, (например, оружие, спецсредства) до менее необходимых (например, канцелярские принадлежности и т.д.).

Наконец обратите внимание на то, что рационально и обоснованно использовать деньги из фонда поощрения и материальной помощи персоналу.

Не менее важное значение для руководителей службы безопасности имеет вопрос кадрового обеспечения ее деятельности. Работу эту условно можно разделить на два этапа.

На первом этапе происходит отбор кандидатов для работы в службе безопасности, их проверка, прохождение ими специальной подготовки и стажировка в должности. При отборе кандидатов особое внимание должно уделяться их образованию (помимо юристов, целесообразно приглашать на работу психологов, экономистов, финансистов и т.д.). Помимо проверки органами внутренних дел, не помешает и выяснение биографических и других, характеризующих личность кандидата, данных. Разумеется, это необходимо делать не во всех случаях, (излишней будет такая проверка, например, кандидата, которого хорошо и давно знает руководитель службы безопасности) и с письменного согласия кандидатов. Однако письменное согласие на проверку такого рода после зачисления кандидата в службу безопасности необходимо получать в любом случае.

Второй этап. Если в процессе проверки установлена пригодность кандидата для работы в службе безопасности, то его направляют на учебу в негосударственное образовательное учреждение, (за исключением лиц, имеющих стаж работы в оперативных или следственных подразделениях не менее трех лет). При этом особое внимание обращается на наличие лицензии у этого учреждения и качество программы обучения. После прохождения специальной подготовки и получения лицензии охранника или детектива, целесообразно организовать стажировку его в соответствующей должности, (согласно Законов, от 1 до 6 мес.) и лишь после этого решать вопрос об его зачислении на постоянную работу в службе безопасности или увольнении. Разумеется, такая возможность должна

быть предусмотрена в контракте, который подписывается после отбора кандидата.

После зачисления сотрудника на постоянную работу наступает этап закрепления его на работе в службе безопасности. Он состоит из повышения его профессионального уровня, проведения работы по укреплению трудовой дисциплины и законности, обеспечения правовой и социальной защиты.

Известно, что полученные специальные знания (даже если они превосходные) не всегда подкреплены соответствующими умениями и навыками. Поэтому закреплению и совершенствованию этих навыков у детективов и охранников на занятиях (при отсутствии организованной учебы в службе безопасности необходимо направлять их на курсы повышения квалификации) должно уделяться первостепенное внимание.

Весьма актуальными являются также вопросы о соблюдении трудовой дисциплины и законности, укрепления физического развития, здоровья, повышения культуры. К сожалению, на практике, иногда, наблюдается обратная картина. Определенная часть сотрудников совершает правонарушения, в т.ч. преступления, перестает уделять внимание спорту, в общении между собой, персоналом предприятия и его посетителями проявляет грубость и т.д. Можно в связи с этим с уверенностью утверждать, что в таких службах безопасности кропотливая работа по кадровому обеспечению сводится, по сути, к поспешному и формальному отбору кандидатов, проведению только инструктажей вместо систематического обучения и полному безразличию к их поведению после работы.

В основе такого поверхностного (вместо комплексного, ныне забытого) подхода к кадрам, по наблюдению наших авторов, лежат следующие причины:

- ❏ безразличие к судьбам сотрудников, нежелание части руководителей служб безопасности предметно заниматься воспитательной работой с подчиненными, которая, к тому же, если заниматься ею добросовестно, занимает много времени;
- ❏ отсутствие у некоторой части руководителей навыков работы с кадрами и т.д.

Устранение или нейтрализация этих причин возможна на основе внесения в должностные инструкции руководителей всех степеней конкретных обязанностей по работе с кадрами и установлению жесткого контроля за их соблюдением.

В сфере социальной защиты персонала службы безопасности необходимо соблюдать требование Законов по вопросам зачета трудового стажа и страхованию за счет средств предприятия-учредителя. С целью повышения эффективности правовой защиты сотрудникам службы безопасности следует неукоснительно добиваться привлечения виновных к ответственности в соответствии с законодательством за оказание им сопротивления, угрозы или насилия в связи с исполнением ими своих обязанностей. Заметим, что в связи с этим, необходимое знание Законов Вашей страны. Этот пробел легко устраним, если правильно применять уголовное и административное законодательство.

Полное и качественное обеспечение деятельности службы безопасности материально-техническими ресурсами – не только средство, но и усло-

вие повышения эффективности работы его сотрудников. Эти ресурсы условно подразделяются на следующие группы:

-  оружие и боеприпасы;
-  специальные средства;
-  служебные помещения различного характера (кабинеты, караульные помещения, оружейные комнаты, стрелковые тир, комнаты досмотра);
-  вспомогательная техника (автотранспорт, видео-, кино-, фото-техника, средства оперативной радио- и телефонной связи, компьютеры и т.д.);
-  средства предупреждения и защиты (охранно-пожарная сигнализация, сторожевые собаки, охранное освещение, телевидение т.д.);
-  средства обеспечения нормальной деятельности сотрудников, (обмундирование, мебель, канцелярские принадлежности, медикаменты, бланки документов, юридическая и специальная литература и т.д.).

Обеспечение оружием, боеприпасами, спецсредствами сотрудников службы безопасности регламентировано Законами и нормативными актами Правительства, МВД и Министерства финансов страны, на территории которой Вы работаете. В отношении обеспечения некоторых средств целесообразно использовать нормативы, имеющиеся в различных министерствах и ведомствах (количество служебных собак, оборудование и размеры стрелкового тира, наличие медикаментов, расчет различных видов охранно-пожарной сигнализации и т.д.).

Сложнее решить вопрос о необходимом количестве автотранспорта, целесообразности выделения охранникам обмундирования и т.д. Следует только помнить, что без обеспечения персонала службы безопасности этими средствами эффективность его работы значительно снижается. Кроме того, необходимо знать способы приобретения материально-технических средств. Часть из них можно получить только через органы внутренних дел (спецсредства, оружие, боеприпасы), другую часть самостоятельно, (средства связи, мебель и т.д.), а оставшуюся часть непосредственно от предприятия-учредителя (служебные помещения, охранное телевидение и освещение и т.д.).

Наконец, последнее по счету, но не по важности, обеспечение деятельности службы безопасности – это информационные ресурсы.

Прежде всего, следует определить потребность и объемы минимума информации, без которых функционирование службы безопасности вообще невозможно. Такую информацию можно условно разделить на **три блока**:

-  Среда функционирования предприятия;
-  Состояние безопасности внутри предприятия;
-  Внутриорганизационная деятельность службы безопасности, после чего в рамках каждого блока разработать перечень необходимых сведений.

Этот перечень не будет носить произвольный характер, если при его составлении руководствоваться одним принципом: любая информация реально должна «обслуживать», «работать» на реализацию, как минимум,

одной функции службы безопасности. Можно рекомендовать в этой связи включать в вышеуказанные блоки следующие сведения, которые, разумеется, не могут быть исчерпывающими.

В 1-й блок «Среда функционирования предприятия» возможно включение сведений о предприятиях-конкурентах, правоохранительных и контрольно-надзорных органах, рыночной конъюнктуре, криминогенной ситуации в районе месторасположения предприятия, нормативных актах, регулирующих деятельность предприятия-учредителя и т.д.

Во 2-й блок «Состояние безопасности внутри предприятия» целесообразно включить следующие сведения:

- состояние преступности среди персонала,
- наличие или отсутствие коммерческой тайны,
- источники (каналы) и суммы материального ущерба, наносимого предприятию,
- анализ насильственных преступлений, совершенных против его персонала,
- эффективность работы юрисконсульта (юридической службы),
- о сотрудниках предприятия, имеющих доступ к конфиденциальной информации, с корыстно-насильственной мотивацией, связанных с сохранностью товарно-материальных ценностей;
- о местонахождении и правилах работы с документацией, содержащей коммерческую тайну;
- о месторасположении и состоянии сохранности изделий (описания процесса), составляющих секрет предприятия и т.д.

Наконец, в **3-м блоке** «Внутриорганизационная деятельность службы безопасности» желательно иметь сведения о составе и структуре службы безопасности, перемещениях сотрудников, дисциплинарной практике, результатах проверок, состоянии законности и т.д.

Совершенно очевидно, что без надлежащей организации такого массива информации, удобной и практичной для использования, не обойтись. Идеальным вариантом в этом случае было бы создание информационной системы на базе компьютерной техники, однако, его создание требует определенных финансовых затрат. Поэтому на практике чаще всего встречается отражение и систематизация необходимой информации в письменных документах. К документам, составляемым в службе безопасности, относятся:

1) – организационные документы (устав, положение, должностные инструкции, штатное расписание, правила внутреннего трудового распорядка);

2) – правовые документы (законы, подзаконные акты, методические рекомендации по проблемам безопасности и т.д.);

3) – распорядительные документы (приказы, инструкции, указания, графики работы персонала и т.д.);

4) – информационно-справочные документы (протоколы, акты, справки, письма, докладные и объяснительные записки, телефонограммы, телеграммы, досье и т.д.);

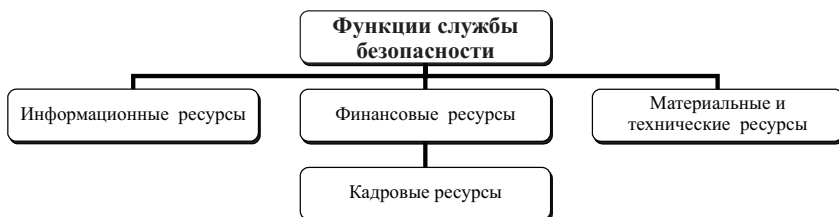
5) – договоры, трудовые соглашения;

6) – документы по личному составу (приказы по личному составу, трудовые книжки, материалы проверок по жалобам, графики отпусков и т.д.).

В результате правильно организованного документального отражения необходимых сведений достигается эффективное информационное обеспечение деятельности службы безопасности.

Разумеется, предоставление службе безопасности необходимых ресурсов осознается и его руководителями, и руководством предприятия-учредителя. Однако определение этих необходимых ресурсов на практике встречает значительные трудности. Связано это с отсутствием соответствующей методики расчета этих ресурсов.

В связи с этим, наши авторы предлагают поэтапный подход к определению необходимых ресурсов в деятельности службы безопасности. Схематично она может быть изображена следующим образом.



На **первом этапе** определяются те функции, реализация которых возлагается на службу безопасности. Такая работа проводится на уровне руководителей предприятия при помощи будущего начальника службы безопасности. В итоге составляется перечень четко сформулированных функций.

На **втором этапе** решаются одновременно две задачи.

Во-первых, определяется необходимое количество детективов и охранников для реализации каждой отдельной функции, их оргструктурное построение, целесообразность обучения и повышения квалификации и т.д.

Во-вторых, определяется объем, структура и содержание сведений, необходимых для реализации каждой функции.

Материально-технические потребности рассчитываются на основе уже установленных и утвержденных кадровых и информационных ресурсов. Финансовые же ресурсы определяются на (заключительном) этапе и с таким расчетом, чтобы они «покрывали» ранее определенные необходимые ресурсы.

Авторы прекрасно осознают, что такая методика, даже если она будет признана оптимальной, не найдет широкого распространения ввиду финансовых затруднений предприятия-учредителя. В связи с этим, перед будущими руководителями служб безопасности неизбежно встанет вопрос о расчете необходимых ресурсов при заранее зафиксированной сумме денег, выделяемых для обеспечения безопасности предприятия.

В таком случае, как представляется, необходимо вначале определить кадровые и информационные ресурсы, затем материально-технические средства и лишь потом составить перечень функций, которые могут быть обеспечены необходимыми ресурсами. Причем, производить такой расчет необходимо несколько раз, добиваясь полного одновременного расходо-

вания выделенных финансовых средств и максимального (при всех ограничениях) расширения перечня функций.

В деятельности некоторых служб безопасности получила распространение практика маневрирования ресурсами. Например, в случае нехватки финансовых средств и с целью удержания на необходимом уровне количества охранников, их труд на некоторое время становится мало оплачиваемым. Наоборот, если финансовых средств у предприятия хватает, то за счет внедрения охранно-пожарной сигнализации, других технических средств, происходит снижение (уменьшение) числа охранников. Подобные комбинации в распределении ресурсов могут помочь службе безопасности на некоторое время (поскольку носят вынужденный характер), однако признать их оптимальными нельзя. Вы сами должны четко осознавать свои задачи и сопоставлять их с финансовыми возможностями предприятия.

Следует напомнить, что профессиональная подготовка требует много времени, знаний и умений выполнять должностные инструкции, а также целого ряда других требований. Опыт – проходит с годами. Наши авторы стремятся разъяснить проблемы, стоящие перед теми, кто хочет стать профессионалом в негосударственной службе безопасности и дать необходимые рекомендации.

Задачи, положения и типовая структура СБ

Негосударственная служба безопасности, (далее СБ) создается для решения комплекса задач по обеспечению безопасности предприятия, банка, фирмы и помощи руководству в реализации его основных интересов.

К задачам СБ относятся:

-  своевременное выявление угроз и эффективное пресечение посягательств на законные интересы Предприятия с применением юридических, технических, организационных и других средств;
-  организация физической и технической защиты помещений и персонала Предприятия;
-  выявление возможных каналов утечки конфиденциальной информации, защита коммерческой тайны предприятия;
-  выявление возможных каналов утечки конфиденциальной информации, защита коммерческой тайны предприятия;
-  совершенствование системы безопасности Предприятия; организация взаимодействия с правоохранительными органами по вопросам обеспечения безопасности Предприятия;
-  постоянный сбор и своевременное предоставление полученной информации руководству для реализации интересов Предприятия.

В процессе своей деятельности СБ разрабатывает и осуществляет две взаимосвязанные подсистемы мер по обеспечению безопасности Предприятия.

Первая подсистема мер носит превентивный характер и призвана предупреждать, затруднять и ограничивать возможности проведения акций в отношении Предприятия со стороны любого недоброжелателя.

Вторая подсистема мер направлена на выявление и локализацию конкретных действий в отношении Предприятия.

Служба безопасности является структурным подразделением Предприятия, созданным на основе приказа руководителя Предприятия и действующем на основе **Положения о Службе безопасности**.

СБ подчиняется только руководителю Предприятия или лицу, которому руководитель Предприятия делегировал (постоянно или временно) свои права по руководству ее деятельностью.

Деятельность СБ строится на основе **Программы обеспечения безопасности Предприятия**, которая разрабатывается СБ (или привлеченными консультантами) в конце истекшего года на год наступающий и утверждается руководителем Предприятия. Об этой программе обеспечения, мы писали в предыдущей главе.

Типовая структура службы безопасности

Для решения поставленных задач в полном объеме СБ должна иметь примерную структуру, (см. таблицу)



Организацию СБ следует производить поэтапно, целесообразно начинать с создания Отдела безопасности и охраны Предприятия; в дальнейшем должен быть создан Отдел расследований, защиты коммерческой тайны и информационно-аналитической работы.

С активным ростом Предприятия и расширением стоящих перед СБ задач Отдел расследований, защиты коммерческой тайны и информационно-аналитической работы может быть разделен на два отдела.

Штатная структура и профессиональные требования к сотрудникам СБ

Начальник СБ (бывший работник СБУ, МВД, уволенный в запас кадровый военный, имеющий связи в правоохранительных органах, желательно с юридическим образованием. Очень желательно, чтобы сотрудник прошел обучение на факультете (курсах) подготовки менеджеров по безопасности).

1.) Отдел безопасности и охраны:

Начальник отдела – зам. начальника СБ (бывший военный или работник правоохранительных служб, имеющий опыт работы в охранных подразделениях).

Технический специалист (специалист с высшим техническим образованием, имеющий опыт работы (разработки, монтажа, эксплуатации) технических средств охраны);

Охранники, (везде хотят иметь специалиста в возрасте от 21 до 45 лет, но в каждом случае — есть исключение, которое решается руководителем СБ), законченное среднее (среднее-специальное) образование, несудимые, не имеющие связей с преступным миром, с хорошей физической подготовкой, желательны имеющие разряды по боксу, борьбе или другим видам спорта. Рекомендуются: уволенные в запас кадровые военные, младшего и среднего офицерского состава, прапорщики, сержанты сверхсрочной службы).

II.) Отдел расследований, защиты коммерческой тайны и информационно-аналитической работы:

Начальник отдела — (бывший работник МВД, СБУ, имеющий опыт работы по нескольким направлениям деятельности отдела, обязательно высшее техническое или гуманитарное образование, желательны имеющий связи в информационных агентствах и средствах массовой информации, опыт работы с СМИ. Подбирается из числа сотрудников Предприятия. Очень желательно, чтобы сотрудник прошел обучение на факультете (курсах) подготовки менеджеров службы безопасности);

Психолог — зам. начальника отдела по кадрам, (опытный специалист по работе с кадрами, имеющий диплом психолога, военного врача или преподавателя с данного направления);

Специалист по ведению служебных расследований (сотрудник, имеющий опыт оперативной работы в следственных подразделениях МВД или СБУ).

Специалист по обработке информации и формированию банков данных (сотрудник с высшим образованием, имеющий способности к аналитическому мышлению, систематизации);

Оператор-программист (профессиональный программист, имеющий опыт работы с базами данных. Если ПК фирмы объединены в локальную сеть, требуются навыки работы с сетью).

Функции подразделений службы безопасности

1. Отдел безопасности и охраны :

-  физическая охрана руководства Предприятия и некоторых главных специалистов;
-  физическая охрана офисов, территории объектов Предприятия и его филиалов, оборудования и продукции Предприятия, складских помещений и находящихся в них материальных ценностей;
-  сопровождение и охрана грузов, принадлежащих Предприятию;
-  охрана культурных и деловых мероприятий, проводимых Предприятием (выставки, презентации, банкеты);
-  обеспечение выполнения сотрудниками Предприятия установленных режимов;
-  физическое противодействие возможным акциям недоброжелателей в отношении Предприятия; установка, ремонт и обслуживание технических систем защиты объектов;
-  сбор и предоставление в Отдел расследований, защиты коммерческой тайны и информационно-аналитической работы информации о фактах, имеющих значение для обеспечения безопасности.

2.) Отдел расследований, защиты коммерческой тайны и информационно-аналитической работы:

-  физическая охрана руководства Предприятия и некоторых главных специалистов;
-  проведение служебных расследований по фактам краж, хищений материальных ценностей, ограблений и похищений сотрудников Предприятия;
-  учет персонала Предприятия, сбор информации о деловых и личных качествах каждого служащего, отслеживание опасных для Предприятия отклонений в поведении сотрудника, работа по проверке вновь поступающих на работу;
-  проведение мероприятий по защите каналов связи и противодействию технической разведке конкурентов;
-  контроль за обстановкой в коллективах подразделений Предприятия, проведение работ по созданию благоприятного микроклимата;
-  контроль и фиксация публичных выступлений, публикаций сотрудников Предприятия;
-  выработка рекомендаций по определению круга сведений, составляющих коммерческую тайну Предприятия, определению круга лиц, имеющих право доступа к коммерческой тайне, разработка и совершенствование правил пользования, хранения и уничтожения, системы защиты документов, содержащих конфиденциальную информацию;
-  сбор конфиденциальной информации о конкурентах, о структуре и особенностях рынка, предоставление в Информационно-аналитический отдел собранной информации.
-  сбор открытой информации о конкурентах, клиентах, деловых партнерах, состоянии и перспективах развития рынка;
-  сбор информации по вопросам обеспечения безопасности от других подразделений СБ;
-  аналитическая обработка полученной информации и систематический доклад ее руководству Предприятия;
-  организация надежного хранения полученной информации;
-  защита информационного банка от умышленного или неумышленного разрушения и утечки.

Практическая документация по созданию СБ.

“УТВЕРЖДАЮ”

Руководитель предприятия

“ — ” _____ 200_ года

ПОЛОЖЕНИЕ "О службе безопасности предприятия"

I. Общие положения

1.1. Служба безопасности (СБ) Предприятия создана для решения задач по обеспечению безопасности Предприятия с целью оказания помощи руководству Предприятия для реализации его основных интересов.

1.2. СБ в своей деятельности руководствуется законами РФ (Украины и т.д.), другими нормативными актами органов государственной власти и настоящим Положением. Она неукоснительно соблюдает законность и применяет не противоречащие законодательству силы, средства, формы и методы при безусловном соблюдении конституционных прав и свобод граждан. Деятельность СБ носит преимущественно упреждающий характер.

1.3. Деятельность СБ является одним из важнейших средств достижения основных целей Предприятия. Она строится на основе "Программы обеспечения безопасности Предприятия", которая разрабатывается СБ и утверждается руководителем Предприятия.

1.4. Общее руководство деятельностью СБ осуществляет руководитель Предприятия. Текущее руководство осуществляет начальник СБ, который ставит СБ задачи по добыванию необходимой информации, обеспечивает строгое соблюдение принципов и правил ведения этой работы, мер конфиденциальности и безопасности, взаимодействие на должном уровне с правоохранительными органами. Руководитель Предприятия организует кадровое, материально-техническое и финансовое обеспечение СБ, создает необходимые условия для ее эффективной работы.

II. Основные задачи СБ

2.1. Своевременное выявление угроз и эффективное пресечение посягательств на законные интересы Предприятия с применением юридических, технических, организационных и других средств.

2.2. Организация физической и технической защиты помещений и персонала Предприятия.

2.3. Выявление возможных каналов утечки конфиденциальной информации, защита коммерческой тайны Предприятия.

2.4. Совершенствование системы безопасности Предприятия.

2.5. Организация взаимодействия с правоохранительными органами по вопросам обеспечения безопасности Предприятия.

2.6. Постоянный сбор и своевременное предоставление полученной информации руководству для реализации основных интересов Предприятия.

III. Функции СБ

Для решения поставленных задач СБ осуществляет:

3.1. Административно-распорядительную функцию.

Она реализуется путем разработки, внедрения и поддержания в офисе Предприятия, его подразделениях и филиалах, торговых залах различных режимов безопасности, определения полномочий, прав, обязанностей и ответственности сотрудников Предприятия по вопросам безопасности, подготовки и проведения мероприятий по физической безопасности и сохранению коммерческой тайны.

3.2. Учетно-контрольную функцию.

Она обеспечивается путем организации своевременного обнаружения реальной и потенциальной угрозы деятельности Предприятия, оценки и контроля за источниками этой угрозы, налаживанием контроля за неблагоприятными для Предприятия ситуациями и факторами, ведение их учета.

3.3. Социально-кадровую функцию.

Она реализуется путем участия СБ в подборе, проверке и расстановке кадров, выявлении негативных тенденций в коллективах подразделений

Предприятия, в предупреждении и локализации возможных конфликтов, инструктаже и использовании как гласно, так и конфиденциально сотрудников Предприятия по вопросам своей компетенции, формировании у сотрудников чувства ответственности за обеспечение безопасности Предприятия.

3.4. Организационно-управленческую функцию.

Она реализуется путем организационного, материально-технического и технологического обеспечения безопасности, достижения уровня безопасности, соответствующего уровню развития Предприятия.

3.5. Методическую функцию.

Она реализуется путем внедрения на Предприятии позитивного опыта обеспечения безопасности, организации обучения сотрудников Предприятия, методической разработки решения возникающих проблем обеспечения безопасности.

3.6. Информационно-аналитическую функцию.

Она обеспечивается путем целенаправленного сбора, накопления, обработки, хранения и выдачи информации по вопросам безопасности руководства Предприятия и заинтересованным подразделениям.

IV. Силы и средства обеспечения деятельности СБ

4.1. К силам деятельности СБ относятся руководство и сотрудники СБ.

4.2. Средства обеспечения деятельности СБ включают в себя: материально-техническое обеспечение, информационное обеспечение, научно-методическое обеспечение.

4.3. Финансовое и материально-техническое обеспечение СБ осуществляется в соответствии с утвержденной Руководителем Предприятия Программой обеспечения безопасности Предприятия. Начальник СБ имеет в своем распоряжении определенные Программой финансовые и материально-технические средства, с помощью которых реализуется выполнение поставленных перед СБ задач. В случае возникновения потребности в дополнительном выделении средств, начальник СБ для решения этого вопроса обращается к руководителю Предприятия.

4.4. Информационное обеспечение СБ организуется и реализуется путем сбора подразделениями СБ информации, а также обязательного и инициативного направления в СБ информации другими подразделениями Предприятия по вопросам, связанным с обеспечением безопасности Предприятия. СБ разрабатывает и корректирует перечень информации, которая должна поступать из подразделений Предприятия, организует и контролирует ее поступление в базу данных. Сотрудники Предприятия вправе получать из базы данных информацию по вопросам безопасности Предприятия в рамках своей компетенции.

4.5. Научно-методическое обеспечение СБ осуществляется с использованием возможностей Предприятия, а также путем привлечения специализированных предприятий и организаций. В целях повышения квалификации сотрудников, СБ с разрешения руководителя Предприятия принимает участие в семинарах и конференциях по проблемам обеспечения безопасности коммерческих структур.

V. Начальник СБ.

5.1. Начальник СБ назначается на должность и освобождается от занимаемой должности по решению руководителя Предприятия.

5.2. Начальник СБ подчиняется непосредственно руководителю Предприятия и выполняет его указания, не противоречащие действующему законодательству.

5.3. Начальник СБ выполняет следующие функции:

- определяет штатную численность сотрудников СБ и представляет соответствующие предложения руководителю Предприятия;
- обеспечивает подбор и расстановку начальников подразделений СБ, а также руководителей СБ филиалов;
- производит текущее руководство и координацию деятельности подразделений СБ и руководителей СБ филиалов;
- обеспечивает через руководство Предприятия соответствующий условиям и требованиям обстановки уровень материально-технического снабжения СБ;
- создает условия для эффективного выполнения подразделениями и сотрудниками СБ своих функциональных обязанностей, повышения профессионального уровня сотрудников;
- обеспечивает выполнение СБ поставленной перед ней задач, исполнение распоряжений руководителя Предприятия в рамках ее компетенции;
- обеспечивает координацию деятельности всех подразделений Предприятия по вопросам безопасности;
- осуществляет взаимодействие СБ с правоохранительными органами по вопросам обеспечения безопасности Предприятия.

5.4. Начальник СБ имеет право:

- присутствовать на заседаниях Совета директоров Предприятия;
- иметь доступ к любой информации в отношении деятельности Предприятия;
- давать обязательные к исполнению указания руководителям подразделений Предприятия по вопросам безопасности;
- направлять своих сотрудников для участия в заседаниях и других мероприятиях любого подразделения Предприятия;
- устанавливать с сотрудниками Предприятия конфиденциальные отношения в целях обеспечения безопасности Предприятия;
- подбирать, представлять руководителю Предприятия к назначению или увольнению руководителей подразделений, филиалов и сотрудников СБ;
- выступать в качестве представителя Предприятия в отношениях с внешними организациями по вопросам обеспечения безопасности;
- проводить профилактические беседы с руководителями подразделений и сотрудниками Предприятия по вопросам безопасности;
- при наличии оснований снижать и/или отказывать в допуске конфиденциальной информации сотрудникам Предприятия;
- вносить руководителю Предприятия предложения о привлечении сотрудников, виновных в нарушении установленных режимов безопасности либо иного ущерба безопасности Предприятия к дисциплинарной и/или материальной ответственности;
- делегировать часть своих полномочий руководителям подразделений СБ для выполнения ими своих функциональных обязанностей.

VI. Организация работы СБ

6.1. Основой для работы СБ и ее сотрудников является принцип конфиденциальности, который предполагает сохранение в тайне некоторых методов ее деятельности. По согласованию с руководителем Предприятия в целях профилактики СБ информирует коллективы подразделений Предприятия о некоторых аспектах своей деятельности.

6.2. В своей работе СБ использует конфиденциальные связи. Они устанавливаются для получения информации о фактах враждебных акций конкурентов и криминогенных элементов в отношении Предприятия. Установление конфиденциальных связей производится с разрешения руководителя Предприятия. Их учет ведется начальником СБ.

6.3. При осуществлении своей деятельности СБ использует аппаратуру видео– и аудиозаписи, кино– и фотосъемки, технические и иные средств

ва, не причиняющие вреда жизни и здоровью граждан и окружающей среде, а также средства оперативной и телефонной связи.

6.4. При выполнении служебных функций, сопряженных с опасностью собственной жизни и здоровья, сотрудникам СБ разрешается использовать специальные средства, виды, порядок приобретения, учета, хранения и ношения которых определяется действующим законодательством Украины.

6.5. Сотрудникам СБ запрещается:

- скрывать от правоохранительных органов ставшие им известные факты готовящихся или совершенных преступлений;
- выдавать себя за сотрудников правоохранительных органов;
- собирать сведения, связанные с личной жизнью, политическими и религиозными убеждениями отдельных лиц;
- осуществлять видео– и аудиозапись, кино– и фотосъемку в служебных или иных помещениях без письменного разрешения руководства Предприятия или частных лиц;
- прибегать к действиям, посягающим на права и свободы граждан, ставящие под угрозу жизнь, здоровье, честь, достоинство и имущество граждан;
- фальсифицировать материалы или вводить в заблуждение руководство Предприятия;
- разглашать собранную информацию, использовать ее в каких-либо целях вопреки интересам Предприятия.

VII. Права Службы безопасности

7.1. Контролировать выполнение утвержденной руководителем Предприятия Программы обеспечения его безопасности.

7.2. Устанавливать официальные от имени Предприятия и конфиденциальные отношения с гражданами Украины, иностранными гражданами и лицами без гражданства в интересах обеспечения безопасности Предприятия.

7.3. Вести необходимые учеты и получать документальные материалы.

7.4. Проводить в оговоренных случаях проверку лиц, поступающих на работу на Предприятие.

7.5. Осуществлять проверку и иные мероприятия в пределах действующего законодательства в отношении организаций и частных лиц, проводящих против Предприятия противозаконную деятельность.

7.6. Использовать имеющиеся в распоряжении финансовые, материально-технические и иные средства.

7.7. Запрашивать, по согласованию с руководителем Предприятия, в государственных, кооперативных, общественных организациях и учреждениях сведения и материалы, необходимые для выполнения своих функций.

7.8. Устанавливать, по согласованию с руководителем Предприятия, в интересах обеспечения безопасности организации на использование конфиденциальной информации сотрудниками Предприятия, а также информации, передаваемой деловым партнерам и клиентам.

7.9. Вести в пределах своей компетенции деловую переписку с подразделениями и филиалами Предприятия, клиентами, деловыми партнерами и т.д.

7.10. Вести конфиденциальное делопроизводство.

VIII. Кадры Службы безопасности

8.1. Руководящий состав и сотрудники СБ подбираются, как правило, из числа лиц, имеющих высшее образование, а также опыт практической работы в правоохранительных органах, службы в ВС, не дискредитировавшие себя противоправными поступками, получившие необходимую специальную подготовку, способные по своим деловым, моральным и

физическим качествам выполнять работу по реализации возложенных на них функций.

8.2. Подбор и изучение кандидатов для зачисления в СБ производится начальником СБ.

8.3. Сотрудники СБ специализируются по функциональным направлениям деятельности. С санкции руководителя Предприятия отдельные сотрудники СБ могут направляться для решения поставленных задач в другие государственные и негосударственные предприятия и организации.

8.4. Профессиональная подготовка, переподготовка и повышение квалификации сотрудников СБ осуществляется в соответствующих специализированных учебных заведениях.

8.5. Начальник СБ и руководители ее подразделений обязаны выявлять и эффективно использовать возможности своих подчиненных для решения задач, поставленных перед СБ.

8.6. Заработная плата начальника и сотрудников СБ определяется штатным расписанием Предприятия. Оценка трудового вклада сотрудников СБ осуществляется на основе конечных результатов деятельности СБ и всего Предприятия. Руководители подразделений Предприятия вправе вносить предложения руководству СБ и Предприятия о поощрении сотрудников СБ за конкретные результаты работы по обеспечению безопасности.

IX. Отчетность и контроль деятельности СБ

9.1. СБ осуществляет организацию и контроль за внедрением и практической реализацией системы безопасности Предприятия, учет результатов своей работы. Критерием эффективной работы СБ является стабильная деятельность Предприятия по реализации своих основных целей и интересов.

9.2. Начальник СБ периодически отчитывается перед Руководителем Предприятия по вопросам, входящим в компетенцию СБ, а также несет ответственность за полноту и достоверность отчетной информации. Периодичность и форма отчетности определяется руководителем Предприятия.

9.3. Отчетность СБ осуществляется с целью организации эффективно управления обеспечением безопасности Предприятия, своевременного выявления и устранения недостатков.

9.4. В соответствии с законодательством Украины или на основании двухсторонних договоров, представителями соответствующих государственных органов может осуществляться проверка установленной на Предприятии системы безопасности. СБ содействует проведению этих проверок по требованию правоохранительных органов, при этом производя контроль за сохранением коммерческой тайны Предприятия.

X. Взаимодействие СБ со службами безопасности других организаций

10.1. СБ в необходимых случаях координирует свою деятельность и осуществляет взаимодействие со службами безопасности других организаций, специализированными предприятиями и правоохранительными органами в целях достижения согласованности действий в интересах успешного решения общих задач.

10.2. Взаимодействие строится на основе заключенных договоров и включает:

- обмен информацией;
- совместный анализ обстановки;
- совместное планирование деятельности по отдельным направлениям и в целом;
- взаимное использование имеющихся сил и средств;
- совместное проведение мероприятий;
- других совместных действий.

10.3. Предварительные планы совместных действий утверждаются руководителем Предприятия.

Начальник Службы безопасности
предприятия

" ____ " _____ 200_ года

фамилия

.....
“УТВЕРЖДАЮ”
Руководитель ПРЕДПРИЯТИЯ
“ ____ ” _____ 200_ года

Инструкция
“Сотрудникам службы безопасности
Предприятия по охране объектов”

1. Общее положение.

1.1. Настоящая инструкция разрабатывается в соответствии с государственными законодательными актами, нормами и инструкциями, применительно к странам СНГ, России или Украины, где будут учтены: правовая база, условия и правила осуществления предпринимательской деятельности по СБ, предоставлению услуг в охране коллективной и частной собственности, а также охране граждан, монтажу, ремонту, контролю и профилактическому обслуживанию средств охранной сигнализации и ряд других видов деятельности, которые будут разрешены в Уставе предприятия”.

1.2. Настоящая Инструкция определяет правила несения дежурства охранниками на объектах Предприятия.

1.3. Осуществление охраны на конкретном объекте регламентируется также Инструкцией об охране объекта.

II. Охранник дежурной смены

2.1. Охранник подчиняется начальнику Отдела безопасности и охраны.

2.2. Охранник обязан:

2.2.1. Бдительно нести дежурство на охраняемом объекте, неукоснительно выполнять требования действующего законодательства, служебных инструкций, приказов руководства, немедленно докладывать о всех чрезвычайных происшествиях на объекте.

2.2.2. Быть вежливым и тактичным при общении с клиентами и сотрудниками Предприятия, а в отношении нарушителей быть твердым и решительным.

2.2.3. Хорошо знать особенности охраняемого объекта, применяемые на нем технические средства охраны и противопожарной защиты.

2.2.4. Пресекать действия любых лиц, нарушающие нормальную работу Предприятия, удалять их за пределы объекта, а в случае необходимости, проводить задержание (о чем незамедлительно сообщить руководству и в территориальный орган внутренних дел).

2.2.5. Вести контроль за доступом сотрудников Предприятия и посетителей на охраняемый объект, в отдельные помещения, в рабочее и нерабочее время согласно установленных правил.

2.2.6. Осуществлять контроль за посетителями: следить за тем, чтобы сотрудники Предприятия не оставляли посетителей одних в помещениях хранения и выставления товарно-материальных ценностей;

- при необходимости вести их учет в Журнале посетителей, сопровождать их по объекту;

- обращать повышенное внимание на работников ремонтных служб и сферы обслуживания (электромонтеры, слесари, работники связи, посыльные и др.), обязательно проверять их документы;

- особое внимание уделять посетителям, проявляющим признаки нервозности и беспокойства (возможно наличие у них оружия, взрывных и подслушивающих устройств);

- при обнаружении забытых вещей посетителей сообщить об этом руководству

2.2.7. При обнаружении предмета, похожего на взрывное устройство:

- немедленно вывести людей и выйти самому из помещения, в котором находится предмет;

- не пускать в опасное помещение людей;

- сообщить руководству и в милицию;

- до прибытия милиции запрещается подвергать предмет механическим воздействиям, необходимо оберегать его от воздействия прямых солнечных лучей, любых источников тепла, влаги.

2.2.8. При обнаружении подслушивающего устройства сообщить руководству о находке. Взрывные и подслушивающие устройства могут быть замаскированы под любой бросовый (бумажный пакет, пачка сигарет, коробок спичек) и бытовой (авторучка, блокнот, наручные часы, пепельница) предмет.

2.2.9. При получении вещей и корреспонденции, доставляемой посылным:

- проверить удостоверяющие личность документы у доставителя;

- спросить о том, кому оно предназначается, сообщить адресату;

- записать данные доставителя, сделать пометку о характере предмета.

2.2.10. Исключить посещение объекта в ночное время лицами, не имеющими допуск на объект (в т.ч. родственниками, знакомыми, друзьями).

2.2.11. Осуществлять строгий контроль за порядком вноса и выноса материальных ценностей, находящихся под охраной; допускать вынос имущества и товарно-материальных ценностей только с письменного разрешения руководства или при наличии накладной (разрешение, накладная при этом остаются у охранника), если другой порядок выноса не предусмотрен на объекте.

2.2.12. Следить за постоянным обновлением перечня материальных ценностей, находящихся под охраной.

2.2.13. Бережно относится к техническим системам охраны объекта, средствам связи, специальным средствам, использовать их умело и только по назначению.

2.2.14. Иметь аккуратный внешний вид, соблюдать установленную форму одежды.

2.2.15. Неукоснительно соблюдать установленный график дежурства. В случае невозможности заступления на дежурство в установленное графиком время, – заблаговременно ставить об этом в известность начальника Отдела безопасности и охраны.

2.2.16. Во время несения дежурства постоянно находиться на охраняемом объекте.

2.2.17. Своевременно вносить коррективы в список телефонов руководства при их изменении.

2.2.18. Докладывать начальнику Отдела безопасности и охраны согласно установленных правил о:

- приеме-передаче дежурства;
- текущей обстановке на объекте;
- происшествиях на охраняемом объекте;
- фактах нарушения правил безопасности и системы охраны со стороны сотрудников Предприятия.

2.2.19. Уметь применять приемы рукопашного боя против нарушителей.

2.2.20. Уметь оказывать доврачебную помощь лицам, пострадавшим в результате несчастного случая, и т.д.

2.2.21. Умело взаимодействовать с нарядами милиции, участковыми, дворниками и сторожами.

2.2.22. Поддерживать чистоту и порядок на месте несения дежурства.

2.3. При заступлении на дежурство охранник обязан:

2.3.1. Проверить техническую укрепленность охраняемого объекта (наличие решеток на окнах помещений, работоспособность замков на дверях, наличие ключей от них, работоспособность дежурного освещения), целостность пломб и печатей (если они имеются).

2.3.2. Проверить исправность технических средств охраны (сигнализации, охранной видеосистемы и др.), средств связи и средств пожаротушения.

2.3.3. Проверить соответствие описи имущества, товарно-материальных ценностей на объекте их фактическому наличию на момент заступления на дежурство, принять их под охрану.

2.3.4. Проверить наличие всех документов в папке "Документация охраны" по описи. Документы из папки могут быть изъяты только руководством Предприятия. При изъятии документа из папки (в случае, если старый документ сразу не заменяется новым) об этом делается соответствующая запись в описи папки.

Категорически ЗАПРЕЩАЕТСЯ ознакомление с содержимым папки других лиц, кроме работников правоохранительных органов, а также копирование и изъятие любых документов из папки (в том числе работниками правоохранительных органов без санкции руководства).

2.3.5. Доложить начальнику Отдела безопасности и охраны о замечаниях по предыдущему дежурству и о заступлении новой смены.

2.4. При сдаче дежурства охранник обязан:

2.4.1. Подготовить документацию.

2.4.2. Проинформировать заступающую дежурную смену о положении на объекте, приходе и уходе охраняемых материальных ценностей, количестве сотрудников Предприятия и посетителей на объекте в момент передачи дежурства.

2.4.3. Проконтролировать проставление подписей заступающей сменой в документации.

III. Порядок несения дежурства на охраняемом объекте

3.1. Работнику охраны прибыть на дежурство за 15 минут до начала смены, быть отдохнувшим, иметь опрятный внешний вид.

3.2. Дежурство нести бодро, принимать все меры по предупреждению порчи, хищения, и нанесению материального ущерба охраняемому объекту.

3.3. Физическую силу и спецсредства применять лишь в случаях, если все другие меры предупреждения и убеждения оказались исчерпанными (применение физической силы и спецсредств без необходимости или их неприменение в необходимом случае наказывается в дисциплинарном порядке, вплоть до увольнения).

3.4. При применении газовых пистолетов, газовых баллончиков придерживаться Инструкции по правилам пользования и применения газового оружия;

- при применении резиновых палок запрещается нанесение ударов по голове, животу, ключичной области, суставам, половым органам;

- при применении наручников требуется один раз в два часа проводить проверку фиксации замков, чтобы не было сдавливания конечностей.

3.5. При несении дежурства работникам охраны ЗАПРЕЩАЕТСЯ:

3.5.1. Самовольно оставлять пост, даже на непродолжительное время, спать во время несения дежурства.

3.5.2. Являться на дежурство в нетрезвом состоянии, приносить и распивать спиртные напитки (в том числе с сотрудниками Предприятия).

3.5.3. Отвлекаться от несения дежурства, допускать на объект посторонних лиц (в том числе друзей и родственников работников охраны).

3.5.4. Использовать компьютеры, другую оргтехнику, оборудование Предприятия на охраняемых объектах без разрешения руководства этих объектов, а также технические средства охраны, спецсредства не по назначению, вести неслужебные разговоры по телефону.

3.6. При осуществлении пропускного режима работник охраны должен знать, что:

3.6.1. Документом, дающим право на вход-выход работников и других лиц на территорию объекта, является пропуск. Пропуска могут быть постоянными (для постоянных работников), временные и разовые. Руководство Предприятия обеспечивает работников охраны образцами указанных пропусков.

3.6.2. Для ввоза-вывоза грузов основанием является путевой лист и товарно-транспортная накладная. При пропуске автотранспорта работник охраны обязан проверить наличие у водителя пропуска, путевого листа, товарно – транспортной накладной, а также соответствие наименования и количества ввозимых (вывозимых) грузов данным указанным документов, тщательно осмотреть кабину водителя и другие места возможного укрытия похищенного.

При пропуске опломбированного груза работник охраны сверяет номер или оттиск пломбы с образцами.

3.7. При проведении личного досмотра на охраняемых объектах, работник охраны должен знать, что:

3.7.1. Досмотр может производиться только в случаях:

- при наличии у лица признаков совершения хищения в виде следов на одежде и вещах;

- когда очевидцы прямо укажут на данное лицо, как на совершившего хищение;

- при нарушении лицом пропускного режима;

- когда имеются показания технических средств (металлодетектора, сигнализации);

- когда лицо застигнуто в момент совершения хищения или непосредственно после его совершения.

3.7.2. О произведенном досмотре составить акт. (в 2-х экземплярах) в присутствии понятых или представителя администрации объекта, в котором отражаются результаты досмотра.

Акт подписывается всеми участниками. Второй экземпляр Акта вручается досматриваемому лицу.

3.7.3. В случае обнаружения кражи сообщить руководству.

3.7.4. Быть внимательным и вежливым, не допускать действий, унижающих достоинство осматриваемого лица, не разглашать сведения, связанные с производством досмотра.

IV. Действие охранника в экстремальной ситуации.

4.1. При нападении на объект (офис, рабочие помещения, склады) с целью проникновения в его помещения:

4.1.1. Немедленно блокировать все входы с помощью подручных средств или закрыть на замки, при блокировании входов задействовать сотрудников Предприятия, находящихся на объекте.

4.1.2. Доложить о происшествии начальнику Отдела безопасности и охраны (начальнику Службы безопасности, на соседний пост, руководству объекта), который информирует о случившемся органы милиции.

4.1.3. Привести в готовность средства самозащиты (газовый баллончик, резиновая палка, пневматическое оружие), подручные средства для их возможного применения.

4.1.4. Отразить нападение и задержать нападающих до прибытия подкрепления или наряда милиции, далее действовать согласно указаниям руководства.

4.1.5. Зафиксировать точное время происшествия, характерные приметы нападающих, чем вооружены, обстоятельства и события, о чем доложить начальнику Отдела безопасности и охраны.

4.2. При захвате заложников из числа работников предприятия:

4.2.1. Немедленно информировать о происшествии начальника Отдела безопасности и охраны.

4.2.2. Срочно сообщить о происшествии в милицию.

4.2.3. Вступить в переговоры с нападающими с целью получения максимума информации о них и мотивах их действий, максимально затягивая время с тем, чтобы дождаться подкрепления.

4.2.4. Выполнить, по возможности, все требования нападающих, не допуская действий, которые могли бы спровоцировать их и повлечь за собой опасность жизни заложников.

4.2.5. Регулярно докладывать об обстановке начальнику Отдела безопасности и охраны и выполнять все его указания.

4.3. При обнаружении предметов с признаками взрывного устройства:

4.3.1. Немедленно сообщить об этом начальнику Отдела безопасности и охраны.

4.3.2. Проинформировать об обнаруженном взрывоопасном предмете дежурного по районному военному комиссариату и дежурного по районному отделу внутренних дел.

4.3.3. Принять экстренные меры по выводу людей из помещения в безопасную зону.

4.3.4. Обеспечить охрану предмета до прибытия наряда милиции.

4.3.5. Собрать сведения о посетителях объекта для возможного установления лица, доставившего предмет в помещение;

4.3.6. В дальнейшем действовать в соответствии с указаниями начальника Отдела безопасности и охраны.

4.4. При поступлении на пульт сигнала о вскрытии помещения:

4.4.1. Блокировать все выходы из офиса.

4.4.2. Привести в готовность средства самообороны для возможного применения.

4.4.3. Немедленно известить начальника Отдела безопасности и охраны, обследовать визуально помещение, где сработала сигнализация.

4.4.4. При обнаружении признаков несанкционированного проникновения в помещение посторонних лиц действовать согласно п.4.1. настоящей Инструкции.

4.4.5. При отсутствии признаков вскрытия помещения, сигнализация включается охранником повторно с отметкой времени ее срабатывания в журнале приема-сдачи дежурства.

4.4.6. При невозможности включить систему охраны вызывать сотрудника, имеющего право вскрытия и сдачи данного помещения под охрану и в его присутствии вскрыть кабинет, проверить тщательность закрытия окон, форточек, дверей.

4.4.7. Доложить о положении дел начальнику Отдела безопасности и охраны.

4.5. Действия охранника в случае пожара, аварий и других чрезвычайных происшествий:

4.5.1. При необходимости – вызвать пожарную или аварийную службы (по телефонам, имеющимся на посту).

4.5.2. Принять необходимые меры к локализации пожара, сохранению материальных ценностей и документов, для чего, при необходимости, с разрешения начальника Отдела безопасности и охраны самостоятельно вскрыть соответствующие помещения.

4.5.3. Усилить наблюдение за объектом.

4.5.4. Поставить в известность начальника Отдела безопасности и охраны и действовать по его распоряжениям.

4.5.5. Вызвать работников объекта, отвечающих за помещения, где произошло происшествие.

4.5.6. Организовать, при необходимости, не ослабляя охрану объекта, эвакуацию материальных ценностей, приняв соответствующие меры по их сохранности.

Начальник Службы безопасности
предприятия

" ____ " _____ 200__ года.

(фамилия)



Охрана стационарных объектов

Частные (негосударственные) фирмы безопасности охраняют множество различных производственных объектов, торговых предприятий, офисов коммерческих фирм и банков, больницы, школы и высшие учебные заведения. Они же обеспечивают вооруженное сопровождение грузов и финансовых ценностей. Охранные фирмы вносят все возрастающий вклад и в обеспечение общественной безопасности. В текущем году силами негосударственных организаций безопасности задержано около 50 тысяч правонарушителей, в том числе по подозрению в совершении уголовных преступлений. Возможности "частников" все активнее используются в оперативно-профилактических мероприятиях, проводимых совместно с правоохранительными органами.

Эксперты отмечают, что охранные (и сыскные) организации решают сегодня большие социально-значимые задачи, связанные с трудоустройством и приобщением к гражданской жизни значительной части увольняемых в запас военных, сотрудников МВД, СБУ, ФСБ и других силовых структур. По некоторым оценкам, в данных организациях проходят социальную реабилитацию от 40 до 80 процентов ветеранов. Для многих из них – это единственное место, где можно найти реальное применение своему опыту и профессиональным навыкам.

Вместе с тем в своем развитии этот сектор услуг сталкивается с серьезными проблемами, одна из которых – недоверие к охранному бизнесу в обществе, в том числе и в правоохранительных органах. Не завершены процессы очищения этой сферы деятельности от криминальных элементов. Далеко не в полном объеме используется огромный потенциал негосударственных предприятий безопасности, способных вносить значительно больший вклад в борьбу с преступностью и обеспечение общественной безопасности. Это становится особенно актуальным на фоне возрастающей угрозы нашему обществу со стороны организованной преступности, террористов и экстремистских сил.

Но, несомненно, самым узким местом, сдерживающим развитие системы негосударственной безопасности, остается масса противоречий в законодательном поле стран СНГ, России и Украины. Подобное положение дел больше всего не устраивает охранные фирмы – тех, кто боролся с криминалом и создавал очаги цивилизованного охранного бизнеса, сложившиеся в последние годы в полноценную Систему негосударственной безопасности. В последнее время, при участии "частников" была проделана огромная работа по разработке различных поправок к законам и нормативным актам, однако потом работа затянулась и со временем совсем приостановилась.

Мы считаем серьезным упущением, – то обстоятельство, что целая отрасль экономики, каковой сегодня реально является негосударственная

система безопасности – не взяла на себя функцию координации отраслевых интересов, и не принимает активного участия в формировании государственной политики в этом направлении".

Необходимо рассмотреть вопрос о создании единого правового поля для всех субъектов охранной деятельности... вне зависимости от организационно-правовых форм, ведомственной принадлежности, формы собственности и т.д. Имеющиеся сегодня существенные различия в этом вопросе серьезно нарушают не только принципы добросовестной конкуренции, но и приводят к ненужному противостоянию, разобщению усилий по борьбе с единым врагом – преступностью.

Характеристика и виды стационарных объектов

Объектом охранной деятельности является защита имущества предприятия и физическая защита его персонала. Соответственно, элементами стационарного объекта охранной деятельности являются:

1. – весь комплекс производственных, складских, торговых и других помещений;

2. – отдельные здания, служебные комнаты и т.д., находящиеся внутри территории предприятия;

3. – транспортные средства, принадлежащие или арендуемые предприятием;

4. – участки, на территории которых имеются (размещены) материальные ценности;

– отдельные физические лица из числа персонала предприятия. Первые четыре элемента объекта охранной деятельности, обычно, в практической деятельности и литературе называют – охраняемые объекты. Они делятся на стационарные и подвижные объекты. В зависимости от размера охраняемого объекта и занимаемой площади они подразделяются на малые, средние, большие и сверхкрупные объекты.

№. Классификационные признаки	Виды охраняемых стационарных объектов
1. Режим работы персонала объекта.	1. Объект, персонал которого работает в одну смену. 2. Объект, сотрудники которого работают в двухсменном режиме. 3. Объект, персонал которого работает круглосуточно
2. Район расположения охраняемого объекта.	1. Объект, расположенный вне охраняемой зоны. 2. Объект в отдельно стоящем здании или занимающий часть другого помещения или территории. 3. Работа на удаленных объектах вахтовым способом (суммированный учет рабочего времени).

№. Классификационные признаки	Виды охраняемых стационарных объектов
3. Техническая укрепленность объекта.	1. Очень хорошо укрепленный объект, теоретически и практически не имеющий уязвимых мест. 2. Хорошо укрепленный объект, имеющий некоторое количество уязвимых мест, которые известны охране и в принципе могут контролироваться ее сотрудниками. 3. Слабо укрепленный объект, имеющий большое количество уязвимых мест, многие из которых охрана не способна контролировать.
4. Важность объекта.	1. Особо важные объекты с повышенной стоимостью (значимостью) материальных ценностей или опасностью охраняемых объектов. 2. Особо важные объекты. 3. Важные объекты. 4. Простые объекты. 5. Простые объекты с низкой стоимостью (значимостью) охраняемых материальных ценностей.

Система обеспечения безопасности объекта.

Система обеспечения безопасности объекта охранной деятельности строится на следующих принципах:

1.) Комплексность. Применение всех возможных средств защиты (должно быть согласовано с возможными видами потенциальных и реальных угроз, при этом средства защиты (т.е. средства предупреждения, обнаружения, отражения и ликвидации угрозы) должны функционировать как единый механизм защиты, взаимно дополняя друг друга.

2.) Эшелонирование. Это создание нескольких последовательных рубежей защиты таким образом, чтобы наиболее важная зона безопасности охраняемого объекта находилась внутри других зон.

3.) Равнопрочность. Необходимо, чтобы все участки всех рубежей, защищающих зону безопасности, были «равнопрочными» с точки зрения вероятности реализации угрозы.

4.) Разумная достаточность. Требуется выбора некоторого приемлемого уровня безопасности охраняемого объекта, при котором риск и размер возможного ущерба находились бы в разумных пределах.

5.) Непрерывность. В процессе функционирования системы обеспечения безопасности не должно быть перерывов в ее работе, которыми может воспользоваться правонарушитель.

Основной целью деятельности охранного подразделения является пресечение несанкционированного проникновения посторонних лиц на охраняемый объект и защита физической неприкосновенности охраняемых сотрудников предприятия.

Для достижения этой цели необходимо реализовать **следующие задачи:**

- 🔊 организации рациональной и эффективной службы охранников;
- 🔊 внедрения и эксплуатации комбинированных средств защиты;
- 🔊 организации профилактических мероприятий по пресечению несанкционированного доступа на охраняемый объект и т.д.

Достижение вышеуказанных целей и задач возможно на основе реализации следующих охранных функций:

- 🔊 защиты персонала предприятия от насильственных преступлений;
- 🔊 охраны имущества предприятия;
- 🔊 организации инженерно-технической защиты охраняемого объекта;
- 🔊 обеспечения порядка в местах проведения руководством предприятия массовых мероприятий;
- 🔊 устранения причин, порождающих, и условий, способствующих совершению преступлений в отношении собственности предприятия и совершению насильственных преступлений в отношении его персонала.

Классификация охраняемых стационарных объектов

Охраняемые стационарные объекты можно классифицировать следующим образом:

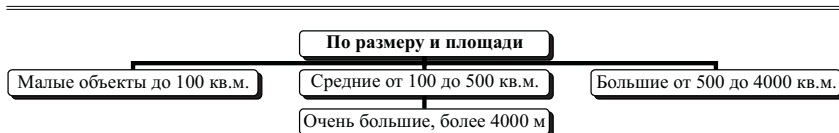
1. По размеру объекта, площади его территории:

а) малые объекты (до 100 кв. м) – квартиры, малые офисы, отдельно стоящие торговые палатки и ларьки, торговые точки, расположенные в пристройках зданий (например, в одной из проходных арок административного или жилого здания), в бывших служебных помещениях и т.д.;

б) средние объекты (от 100 до 500 кв. м) – крупногабаритные квартиры в домах улучшенной планировки, частные дома с надворными постройками и приусадебным участком, отдельно стоящие или примыкающие к другим зданиям офисы вместе со складами и производственными помещениями, крупные пункты обмена валюты, небольшие коммерческие банки, автостоянки вместимостью до 50-60 автомашин и т.д.;

в) большие стационарные объекты (от 500 до 4000 кв. м) – средние предприятия с численностью работающих до 300-400 человек, базы хранения продукции, крупные автомобильные стоянки, склады и т.д.;

г) очень большие стационарные объекты (площадью более 4000 кв. м) – крупные промышленные (акционированные) предприятия, фермерские хозяйства, крупные базы.



2. По режиму работы персонала объекта:

а) объекты, персонал которых работает в одну смену;

б) объекты, работающие в двухсменном режиме;

в) объекты, работающие круглосуточно.

3. По району расположения охраняемого объекта:

а) объекты, расположенные вне основной промышленной, производственной или охраняемой зоны, например, склад предприятия на железнодорожной станции, склад сырья (например, винматериала) на подъездных путях предприятия;

б) объекты в отдельно стоящих зданиях или занимающие часть другого помещения или территории, например, несколько комнат или квартир в доме, этаж или крыло здания, часть территории ярмарки):

- ❑ в производственной зоне;
- ❑ на охраняемой или вблизи от охраняемой территории;
- ❑ рядом с криминогенными объектами (рынки, рестораны, пивбары, вокзалы).

4. По технической укреплённости объекта:

а) очень хорошо укрепленные объекты, практически не имеющие уязвимых мест;

б) хорошо укрепленные объекты, имеющие незначительное число уязвимых мест, которые известны охране и контролируются ее сотрудниками;

в) слабо укрепленные объекты, имеющие значительное число уязвимых мест, многие из которых охрана не контролирует.

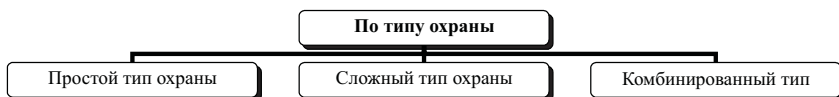
5. По типу охраны:

а) объекты с простым типом охраны (путем периодического обхода охраняемой территории без использования огнестрельного оружия и специальных средств);

б) объекты с усложненным типом охраны (сотрудники используют специальные средства и служебных собак, часть помещений на охраняемом объекте выведена на пульт централизованного наблюдения);

в) объекты с комбинированным типом охраны (для патрулирования объекта используется автотранспорт, охранники экипированы огнестрельным оружием и специальными средствами, используют собак, наиболее значимые помещения оборудованы средствами видеоконтроля территории объекта).

Эта классификация может быть использована для определения стоимости услуг частной охраны, для прогнозирования криминальных ситуаций на объекте. Для решения этих и других вопросов также следует учитывать вид товаро-материальных ценностей, находящихся на объекте приспособленность объекта для работы охраны.



Элементами технической защиты объектов являются:

1. Средства связи. Они должны обеспечивать связь как внутри охраняемого объекта, так и за его пределами. Во избежание нежелательных контактов охранников с криминальными элементами посты на объекте должны быть оборудованы только внутренней связью со старшим смены (или с начальником караула). Если же на охраняемом объекте только один пост, то его следует оборудовать как внутренней связью с участками или отделами предприятия (организации), так и внешней связью. В значительной степени негативных контактов охранников по телефону можно избежать за счет использования на объекте средств радиосвязи, переговоры по каналам которой легче контролировать.

2. Средства видеонаблюдения. С их помощью контролируется вход и выход с объекта лиц, въезд и выезд автотранспорта, выборочно отслеживаются отдельные лица, находящиеся на объекте, просматриваются внутренние помещения (в том числе закрытые).

3. Средства охранно-пожарной сигнализации. По экономическим соображениям охранная и пожарная сигнализация нередко объединяется и служит для выдачи сигнала тревоги в нерабочее время при попытках проникновения или возникновения пожаров на охраняемых объектах.

4. Освещение объекта охраны. Наличие достаточного освещения на объекте позволяет охране контролировать не только его территорию, но и прилегающую к нему местность. Правильно установленное на объекте электроосветительное оборудование должно обеспечивать малозаметное для постороннего наблюдателя движение охранника по территории объекта. В первую очередь освещаться должен не сам маршрут движения (обхода), а прилегающая к нему территория для того, чтобы охранник не превращался в живую мишень.

5. Ограждение периметра объекта.

6. Запретная зона. Запретная зона может быть расположена как по периметру объекта охраны, так и внутри объекта, вокруг участков с ограниченным доступом. Запретная зона может контролироваться как при помощи служебных собак, так и путем использования различных оптико-электронных, ультразвуковых, емкостных и радиоволновых датчиков.

7. Запорные устройства и замки. Имеющиеся на охраняемом объекте замки и запорные устройства должны обеспечивать плотное закрывание дверей и возможность правильного наложения пломб.

8. Контрольно-пропускные пункты (КПП). КПП на охраняемых объектах предназначены для пропуска людей, автомобильного транспорта, железнодорожных вагонов и платформ. На КПП должна быть "вертушка" с блокирующим ее механизмом, а двери надо оборудовать замками с дистанционным управлением с поста охраны.

9. Специально оборудованные места нахождения охранников.

К ним относятся:

- а) наблюдательные вышки;
- б) постовые будки;
- в) укрытия для проведения скрытого наблюдения за объектом и прилегающей территорией и для осуществления засады при задержании посторонних лиц, проникших на объект.

Являясь важным условием эффективности охраны объектов, техническая укрепленность прямо влияет на криминогенную обстановку на

объекте, особенно при наличии на нем значительных товаро-материальных ценностей. Соотношение технической укрепленности и случаев проникновения на охраняемый объект находится в пропорциональной зависимости.



Средства сигнализации в охране стационарных объектов

В настоящее время для охраны объектов очень широко используются технические средства. В зависимости от вида сигнализации они подразделяются на:

- ❑ технические средства охранной сигнализации;
- ❑ технические средства пожарной сигнализации;
- ❑ технические средства тревожной сигнализации.

На ряде объектов охранная и пожарная сигнализация по экономическим соображениям объединяется в одну систему, которая называется охранно-пожарной сигнализацией.

Охранно-пожарная сигнализация предназначена для выдачи сигналов тревоги в охраняемое (нерабочее) время при попытках проникновения или возникновения пожаров на охраняемых объектах.

Тревожная сигнализация предназначена для подачи сигналов тревоги при разбойных нападениях на сберегательные банки и на другие объекты и включается в действие персоналом путем воздействия на скрытно установленные датчики (кнопки, педали).

Тревожная и охранно-пожарная сигнализация подразделяются на автономную и централизованную. Автономная сигнализация предназначена для выдачи местных звуковых и световых сигналов тревоги у доверенных лиц, в помещениях общественных организаций и учреждений.

Централизованная сигнализация предназначена для выдачи сигналов тревоги на приборы, установленные в помещениях КПП, дежурных частей милиции или пунктов централизованной охраны.

В состав системы охранной сигнализации входят:

- ❑ средства обнаружения – датчики;
- ❑ средства передачи информации – каналы связи;
- ❑ средства приема и обработки информации;
- ❑ источники световых и звуковых сигналов.

Датчик – это устройство, устанавливаемое на объекте охраны, которое непосредственно воспринимает информацию о состоянии объекта и преобразует ее в величину, удобную для передачи по каналу связи.

Средства передачи информации обеспечивают перенос информации от датчика к средствам приема. В качестве каналов передачи информации с объектов охраны используются абонентские телефонные линии городских телефонных сетей, радиотрансляционные линии, электрические линии, специально проложенные кабели, а также радиоканалы.

Средства приема, обработки и воспроизведения информации осуществляют прием информации о состоянии объекта, обрабатывают результаты и выдают оперативную информацию о виде, месте и времени нарушения, если таковое имеется.

Источники световых и звуковых сигналов служат для выдачи сигналов тревоги в случае поступления к ним информации о наличии нарушения линий блокировки на охраняемом объекте.

В качестве источников световых и звуковых сигналов тревоги используются электrolампы, звонки громкого боя, сирены.

Принцип действия охранной сигнализации заключается в следующем. С помощью датчиков блокируются (то есть защищаются) окна, форточки, двери, стеклянные проемы и другие места возможного проникновения на объекте. Установка датчиков производится таким образом, чтобы при попытке проникновения посторонних лиц на охраняемый объект (то есть в момент открывания дверей, окон, разбития стекла и т.п.) изменялось нормальное состояние этих датчиков. Отдельные датчики соединяются между собой проводниками и подключаются к средствам приема и обработки информации. Последовательно соединенные датчики вместе с соединительными проводниками образуют электрическую цепь, называемую шлейфом или лучом блокировки. При попытке проникновения нарушителя на объекте изменяется состояние одного или нескольких датчиков, вследствие чего нарушается блокировка объекта: электрическая цепь (шлейф блокировки) либо размыкается, либо замыкается (в зависимости от вида установленных датчиков), система охранной сигнализации срабатывает и выдает сигнал тревоги.

Для повышения надежности охраны наиболее важных объектов (банки, кассы, места хранения оружия) сигнализация на них устанавливается в несколько рубежей, например, первый рубеж – наружный периметр, второй – места возможного проникновения на объект (двери, окна, форточки и т.п.), третий – внутренние помещения по объему, четвертый – непосредственно охраняемые предметы (сейфы, шкафы, ящики и т.д.). При этом каждый рубеж обязательно подключается к самостоятельной ячейке приемно-контрольного прибора с тем, чтобы при возможном обходе нарушителем одного из рубежей был выдан сигнал тревоги с другого.

Датчики по принципу действия подразделяются на следующие виды: электромеханические, тепловые, емкостные, ультразвуковые, опτικο-электронные, микроволновые. Как средство обнаружения информации о наличии нарушения блокировки охраняемого объекта, датчики в целом определяют возможности охранной сигнализации и надежность охраны объекта. Этим объясняются чрезвычайно жесткие требования, предъявляемые к ним, а также постоянное стремление к совершенствованию существующих и разработке новых конструкций.

Принцип действия **электромеханических датчиков** основан на восприятии механических воздействий, создаваемых нарушителем, и преобразовании этих воздействий в изменения параметров электрической цепи. Наиболее простыми из данной группы являются прямоконтактные датчики, воздействие на которые приводит к непосредственному замыканию или размыканию цепи. Эти датчики представляют собой выключатели нажимного действия (кнопочные устройства), применяемые для блокировки дверей, окон, форточек, люков и других открываю-

щихся конструкций. При открывании, например, двери происходит разрыв электрической цепи шлейфа блокировки.

В качестве проволочных датчиков используется тонкий провод диаметром 0,1-0,25 мм, алюминиевая фольга шириной 10-12 мм, а также токопроводящий состав "Паста". Проволока и фольга наклеиваются, а "Паста" наносится кистью на внутреннюю сторону легкоразрушаемых поверхностей (стекло, двери, легкие перегородки). При разрушении заблокированных конструкций происходит разрушение и датчиков, что приводит к разрыву цепи шлейфа блокировки.

Натяжные датчики представляют собой несколько рядов стальной проволоки, натянутой по периметру охраняемого объекта между вертикальными колоннами (стыковыми, промежуточными и сигнальными). В сигнальных колоннах установлены микровыключатели, которые срабатывают как при обрыве, так и при натяжении проволоки в момент раздвигания ее рядов при попытке нарушителя проникнуть на объект. Данное устройство может быть выполнено также в виде козырька над забором.

Магнитоуправляемые датчики применяются для блокировки окон, форточек, дверей, люков и состоят из магнитоуправляемого контакта – геркона (геркон – герметичная стеклянная капсула с запрессованными внутри нее нормально разомкнутыми контактами) и постоянного магнита. Если магнит поместить рядом с герконом, то его контакты под воздействием магнитного поля замкнутся. Геркон крепится обычно на дверной или оконной коробке, а магнит – на открывающейся конструкции так, чтобы при закрытой двери он находился рядом с герконом (на расстоянии не более 10-15 мм). При открывании двери или окна магнит удаляется от геркона и контакты последнего замыкаются, что вызывает сигнал.

Вибрационные датчики применяются для блокирования стеклянных и других легкоразрушаемых поверхностей (пластик, фанера и т.п.).

Контактные вибрационные датчики представляют собой устройства с подпружиненными контактами. При ударе по заблокированной поверхности возникают колебания и происходит кратковременное размыкание контактов датчиков, что приводит к разрыву электрической цепи и выдаче сигнала "Тревога".

Бесконтактные вибрационные датчики (**электромагнитные, пьезоэлектрические**) действуют по принципу преобразования механических колебаний, возникающих при попытке разрушения заблокированной поверхности, в электрические. Приемно-контрольные приборы регистрируют изменение параметров электрической цепи шлейфа блокировки и выдают сигнал тревоги.

Принцип действия тепловых датчиков основан на их способности фиксировать повышение температуры в помещениях выше определенной величины. При возникновении очага загорания чувствительный элемент датчиков (подпружиненные контакты, соединенные легкоплавким припоем; биметаллическая пластина) деформируется и размыкает контакты, разрывая тем самым электрическую цепь охранно-пожарной сигнализации.

Емкостные датчики применяются для блокирования мест возможного проникновения на объект (оконный, дверной проемы), отдельных предметов (сейф, металлический шкаф, ящик), а также для охраны объектов по периметру. Принцип их действия основан на регистрации изменения емкости антенны, вызванного приближением к ней какого-либо предмета,

человека. В качестве антенны используется обычный провод, металлический корпус сейфа, шкафа, другие металлические предметы.

Ультразвуковые датчики предназначены для блокирования помещений по объему и выдают сигнал тревоги как при появлении нарушителя, так и при возникновении пожара. Принцип их действия основан на регистрации изменения ультразвукового поля, вызванного появлением в охраняемом помещении человека или возникновении пожара.

Опτικο-электронные (инфракрасные) датчики подразделяются на две группы: активные и пассивные. Активные опτικο-электронные датчики применяются как для блокирования помещений (контроль подступов через витрины, оконные, дверные проемы; блокировка в помещении подходов к охраняемым участкам по периметру, припотолочных пространств слабоукрепленных складских помещений и т.п.), так и для охраны территории по периметру. С их помощью создается барьер из невидимых невооруженным глазом инфракрасных лучей, при пересечении которых выдается сигнал тревоги. Кроме того, датчики данной группы обнаруживают в помещении задымление, вызванное возникновением очага загорания, путем регистрации уменьшения прозрачности среды.

Пассивные инфракрасные датчики позволяют обнаруживать проникновение человека в контролируемую зону путем регистрации изменения интенсивности принимаемого инфракрасного излучения от движущегося объекта, а также возникновения пожара. Эти датчики используются для блокировки подступов к охраняемым участкам в закрытых отапливаемых и неотапливаемых помещениях.

Микроволновые датчики подразделяются на две группы:

- ▶ частотные;
- ▶ амплитудные.

Датчики первой из указанных групп обнаруживают проникновение человека в контролируемую зону путем регистрации доплеровского сигнала. Датчики второй группы регистрируют изменения напряженности поля на входе приемника. Микроволновые датчики позволяют формировать эллипсоидную форму зоны обнаружения для блокировки закрытых отапливаемых и неотапливаемых помещений, а также для блокировки периметра различных объектов. Предусмотрена возможность регулирования размеров зоны обнаружения и изменения ее пространственной ориентации.

Средства приема, обработки и воспроизведения информации, исходя из назначения и технических возможностей, подразделяются на: однолинейные и многолинейные приемно-контрольные устройства, и на аппаратуру централизованного наблюдения.

Для охраны объекта, все датчики на котором включены в один шлейф блокировки, используются однолинейные приемно-контрольные приборы.

При наличии на объекте нескольких обособленных помещений необходимо иметь соответствующее число шлейфов блокировки. В этом случае используются многолинейные приемно-контрольные устройства.

Такие приборы позволяют контролировать соответственно до 30-50 и более шлейфов. Предназначены эти приборы для приема тревожных сообщений либо от объектовых однолинейных приемно-контрольных приборов, либо непосредственно от датчиков, а также для включения местной

световой и звуковой сигнализации и передачи сигнала тревоги на пульт централизованной охраны. Используют их и в качестве пультов централизованного наблюдения за охраной объектов, расположенных на небольшой территории. Так, приемно-контрольный прибор "Буг", позволяющий контролировать до 60 шлейфов сигнализации, предназначен для автоматизированной охраны банков, торговых центров, гостиниц и других крупных объектов.

Для централизованного приема, обработки и воспроизведения информации с большого числа объектов охраны используются пульта и системы централизованного наблюдения. Выдаваемая информация отображается в виде акустических и оптических сигналов, а при наличии счетно-записывающих устройств регистрируется соответствующими приборами.

Пульта и системы централизованного наблюдения обеспечивают контроль состояния шлейфов блокировки на охраняемых объектах, взятие объектов под охрану и снятие с охраны, регистрацию нарушения шлейфов на охраняемых объектах с указанием номера объекта и характера нарушения. Имеется большое количество различных пультов, различающихся между собой по техническим характеристикам, емкости, конструктивному оформлению. Наибольшее распространение получили пульта централизованного наблюдения, позволяющие подключать до 100-120 объектов.

Приёмы осмотра и контроля охраняемого объекта

В практике охраны применяются следующие приемы контроля и осмотра охраняемого объекта;

1. Фронтальный осмотр объекта, при котором несколько охранников движутся в одном направлении до границы охраняемого объекта, а затем производят движение в обратную сторону.

2. Осмотр объекта навстречу друг другу, при котором охранники движутся от границы объекта к центру (точке встречи), после чего вновь расходятся в направлении периметра охраняемого объекта.

3. Концентрический и эксцентрический способ контроля и осмотра объекта, при котором один или два охранника движутся по спирали от центра охраняемой территории на периферию и наоборот.

4. Последовательный осмотр отдельных участков охраняемого объекта по сложной траектории в зависимости от планировки и конструкции объекта.

5. Выборочный осмотр участков объекта в зависимости от значимости хранимых товаро-материальных ценностей, наличия на объекте уязвимых мест.

6. Движение по объекту с постоянно меняющимся маршрутом применяется в сложных ситуациях для предупреждения нападения на охранника.

7. Движение по объекту с временными остановками и осмотром уязвимых мест и иных участков с закрытого поста (из засады).



Порядок приема стационарных объектов под охрану

Надежная охрана объекта невозможна без тесного сотрудничества фирмы с охраняемым предприятием или наличия своей службы безопасности.

Непосредственно перед сдачей объектов под охрану в их помещениях не должны оставаться посторонние лица. Проверка этого обстоятельства является обязанностью как клиента охраняемого предприятия, так и службы безопасности.

Клиент должен также следить, чтобы в помещениях, сдаваемых им под охрану, были выключены электрические и газовые приборы, чтобы окна были закрыты на внутренние защелки (задвижки), а двери – на замки или запорные устройства (с последующим навешиванием пломб, состояние которых должно проверяться охранниками). Образцы товаров и изделий следует убирать с витрин магазинов и ателье для меньшего привлечения к ним внимания хулиганов и ситуативных (случайных) преступников. Если товары и изделия все же оставляются в витринах, то на них должна быть составлена опись, подписанная клиентом и скрепленная печатью фирмы. Опись вместе с журналом приема и сдачи смены и другими документами хранится у охраны на посту.

Помещения, передаваемые под охрану, их крыша, потолки, стены, окна, пол (если есть подвал со слуховыми окнами) и двери должны находиться в исправном состоянии. Окна нижних этажей, по возможности надо оборудовать металлическими решетками, или ставнями с запорами. Освещение объекта и прилегающей к нему территории должно быть достаточным для возможности визуального контроля в темное время суток.

Особое внимание следует обратить на укрепление и дооборудование помещений касс и хранилищ, в которых находятся особо ценные товары. К этим помещениям предъявляются повышенные требования. Они заключаются в следующем:

а) помещения касс и хранилища ценностей должны быть изолированы от других служебных и подсобных помещений;

б) в многоэтажных зданиях помещения касс или хранилищ должны размещаться на промежуточных этажах, а в двухэтажных домах – на верхнем этаже;

в) в одноэтажных помещениях окна касс и хранилищ должны быть оборудованы металлическими ставнями (внутренними) либо заложены капитальной кладкой, двери должны быть металлическими либо обиты с двух сторон листовым металлом;

г) кассы и хранилища должны иметь капитальные стены, прочные перекрытия потолка и пола, а также надежные внутренние стены и перегородки;

д) с внутренней стороны помещений, в местах, доступных для проникновения извне (оконные проемы, дымоходы, вентиляционные каналы и шахты, тонкие перегородки и др.), необходимо установить металлические решетки;

е) данные помещения должны иметь сейфы для хранения денег и ценностей, которые прочно прикрепляются к стенам и полу;

ж) помещения касс и хранилищ должны блокироваться охранной сигнализацией с выводом ее на пульт, расположенный в комнате дежурной смены охраны, на КПП охраняемого объекта и т.д.;

з) в помещениях касс и хранилищ должны быть предусмотрены меры, предупреждающие использование преступниками в процессе посяательства на охраняемый объект электросверлильного и электрорежущего инструмента. К этим мерам относятся:

- ❖ использование в кассе и хранилище для освещения тока низкого напряжения (24,36 вольт);
- ❖ оборудование в кассе и хранилище скрытых розеток и выключателей, нахождение которых известно только ответственным за безопасность предприятия лицам и кассиру (ответственному за хранение);
- ❖ проведение электромонтажа таким образом, чтобы включение питания розеток и освещения производилось из соседнего, изолированного от кассы помещения или же из помещения, где находится дежурная смена охраны.

и) охраннику при выполнении им своих функциональных обязанностей на объекте запрещено:

- ❖ принимать под охрану объекты, не указанные в договоре, таблице поста, постовой ведомости;
- ❖ самостоятельно или по просьбе администрации объекта открывать или закрывать замки, запорные устройства, двери, окна, накладывать или снимать пломбы, печати; [в случае, если это диктуется производственной необходимостью (завоз товаров, внеплановая отгрузка), то составляется акт вскрытия (опечатывания) объекта, делается запись в книге приема объекта под охрану.];
- ❖ перемещать пожарный инвентарь и использовать его не по прямому назначению;
- ❖ выполнять работы, не связанные с охраной объекта (грузчик, посыльный, уборщик);
- ❖ допускать кого-либо на объект без согласования с руководством фирмы, администрацией охраняемого объекта, диспетчером частного охранного предприятия или его руководителем;
- ❖ передавать кому бы то ни было свое оружие и специальные средства, за исключением ответственного за хранение и выдачу,

утвержденного приказом руководителя охранного предприятия, с соответствующей отметкой в книге приема и выдачи вооружения и специальных средств;

- ❖ отключать сигнальные приборы, автономную сигнализацию, освещение на объекте, в том числе и при срабатывании сигнализации;
- ❖ уходить с поста (объекта) или отвлекаться от несения службы, спать на посту;
- ❖ самостоятельно передавать охрану объекта другим лицам, в том числе близким родственникам.

Защита персонала предприятия от насильственных преступлений.

Охранники службы безопасности защищают жизнь и здоровье двух групп персонала.

К первой группе относятся специально выделенные из персонала лица, в отношении которых совершенные насильственные преступления могут принести предприятию значительный экономический ущерб (руководители, кассиры и т.д.). Защиту этих лиц осуществляют специально выделенные из охранников – телохранители, они выполняют свои обязанности как на, – так и вне территории предприятия. Надо сказать, что широко распространенный термин «телохранитель» авторы считают не совсем удачными, т.к. и юридически, и фактически охране подлежат не только физическая неприкосновенность охраняемого лица («тело»), но и его личные вещи.

Ко второй группе относятся те сотрудники предприятия, чьи рабочие места расположены внутри охраняемого объекта. Следует отметить, что такую задачу перед охранниками не ставят, однако, в силу других их действий (пропускной режим, отсутствие допуска посторонних лиц, проверка посетителей и т.д.) такая стационарная охрана фактически осуществляется. Правда, здесь есть одно исключение: персоналу не гарантированы пресечения насильственных действий со стороны своих сослуживцев и это в вину охране не вменяется

Охрана имущества предприятия

Под имуществом понимается вещь или определенная совокупность вещей. Охране подлежат все материальные ценности предприятия, независимо от их местонахождения. В то же время существуют объекты первостепенной важности, охране которых уделяется особое внимание, так как именно они чаще всего подвергаются противоправному посягательству. Охране подлежат специально выделенные для этого стационарные и(или) передвижные объекты. К стационарным объектам относятся: помещения касс, склады и т.д., к передвижным – железнодорожные вагоны, автомобили, самолеты и корабли с грузом, принадлежащим предприятию. В отличие от защиты персонала предприятия здесь перед охранниками ставится другая задача – пресечь несанкционированный доступ к охраняемым материальным ценностям предприятия (следует оговориться, что такое разделение обязанностей труда охранников является условным и излагается из методических соображений, т.к. фактически охранники чаще всего выполняют одновременно обе функции).

Организация инженерно-технической защиты охраняемого объекта

Такая организация предполагает активное внедрение в деятельность охранного подразделения технических систем охраны и инженерно-технических средств защиты. К техническим системам охраны относятся:

- ❖ охранная сигнализация объектов;
- ❖ пожарная сигнализация;
- ❖ автоматизированный контроль доступа;
- ❖ комбинированные системы.

Кроме этого, уровень защищенности объекта повышается, если будут внедрены инженерно-технические средства защиты. Последние включают в себя:

- 1) – естественные и искусственные барьеры (водные преграды, заборы, ограждения, колюча проволока и т.д.);
- 2) – особые конструкции проходов, помещений, сейфов, хранилищ;
- 3) – планировка объекта, его зданий и помещений по зонам безопасности.

Обеспечение порядка в местах проведения руководством предприятия массовых мероприятий

Необходимость в обеспечении порядка возникает в случаях проведения представительских (выставки, ярмарки), культурно-оздоровительных (спортивные соревнования, концерты и т.д.) и служебных (конфиденциальные заседания правления, совещания руководителей и специалистов и др.) мероприятий. При этом должна быть обеспечена физическая безопасность персонала предприятия и приглашенных лиц, приняты меры к сохранности их личных вещей и автотранспорта, оборудования предприятия.

Устранение причин способствующих совершению преступлений против собственности предприятия

Профилактические мероприятия должны быть направлены на предотвращение двух групп преступлений. К первой группе – относятся преступления против личности. Ко второй группе – относятся преступления против собственности, подлежащие профилактическому воздействию, и определены спецификой деятельности охранного подразделения.

На основе утвержденных вышестоящим руководством целей, задач и функций охраны, формируется ее оргструктура. Целесообразно, по-видимому, в структуре отдела охраны создать следующие подразделения: охраны персонала, охраны стационарных объектов, охраны передвижных объектов, профилактики правонарушений, пропускного и внутриобъектового режима, инженерно-технической защиты, организации работы сторожевых собак, пожарной безопасности и др. В соответствии с функциональным предназначением этих подразделений их можно разделить на три группы:

- 1) – подразделения физической защиты;
- 2) – подразделения имущественной безопасности;
- 3) – подразделения, обеспечивающие деятельность первых двух групп.

Обязательным условием создания этих подразделений является значительное превышение общей численности групп физической защиты и имущественной безопасности над вспомогательным персоналом, (см. табл.)

№№ Наименование и подразделения	Задачи	Форма представления результатов работы
1. Отделение (группа, сектор) охраны персонала.	Обеспечение физической защиты отдельных категорий персонала от преступных посягательств.	Планы; схемы; отчеты; графики дежурств.
2. Отделение (группа, сектор) охраны стационарных объектов.	Пресечение несанкционированного проникновения посторонних лиц на охраняемые объекты.	Графики дежурств; акты (протоколы) задержания правонарушителей; журналы.
3. Отделение (группа, сектор) охраны передвижных объектов.	Пресечение несанкционированного проникновения на передвижной охраняемый транспорт.	Акты обследования транспортных средств; графики дежурств; журналы; акты приема-передачи охраняемого груза.
4. Отделение (группа, сектор) профилактики правонарушений.	Внесение предложений руководству предприятия по устранению причин, порождающих и условий, способствующих совершению правонарушений на охраняемом объекте.	Информационные письма; акты обследования объектов.
5. Отделение (группа, сектор) пропускного и внутриобъектового режима.	Обеспечение порядка вноса (выноса), ввоза (вывоза) материальных ценностей и входа (выхода) сотрудников предприятия и посетителей.	Журналы выдачи пропусков; графики дежурств; образцы пропусков и т.д.
6. Отделение (группа, сектор) инженерно-технической защиты.	Обеспечение постоянной эксплуатации инженерно-технических средств защиты объекта.	Акты обследования; журналы.
7. Информационно-аналитическое отделение (группа, сектор).	Анализ, оценка, обобщение сведений о деятельности охранного подразделения.	Аналитические записки; обзоры; справки.
8. Отделение (группа, сектор) организации работы сторожевых собак.	Организация постоянного (или систематического) применения собак.	Журнал дежурств; акты применения собак при охране объекта.
9. Отделение (группа, сектор) пожарной безопасности.	Предотвращение загораний и пожаров.	Акты; докладные записки; представления.

Эффективное функционирование охранного подразделения возможно только на основе всестороннего и полного его ресурсного обеспечения. Прежде всего, это касается технических средств. К ним принадлежат: различные охранные системы, оружие, спецсредства, автомототранспорт, средства связи, компьютеры, поисковые приборы, телевизионные системы, приборы наблюдения, спецоборудование и т.д. Общепринятым является деление технических средств охраны на средства обнаружения – (пожарная сигнализация, охранный видеонаблюдение, охранное телевидение и т.д.) и средства отражения и ликвидации – (оружие, спецсредства, средства индивидуальной защиты и т.д.).

Информационное обеспечение предполагает ведение учетов задержанных правонарушителей, ложных срабатываний сигнализации, суммы похищенных по вине охранников материальных ценностей, угроз или покушений на охраняемое лицо и т.д. Компьютерное обслуживание информационных потоков, циркулирующих в сфере деятельности охранного подразделения, в значительной степени повышает уровень его информационного обеспечения. В области материально-технического обеспечения особое внимание уделяют форменному обмундированию, мебели, различным формам бланков служебной документации, камерам хранения и т.д. Исключительно важное значение приобретает финансовое обеспечение деятельности охраны. Стремление экономить на зарплате охранников, покупке относительно дешевых, но малоэффективных технических средств, отсутствие системы материального стимулирования труда сотрудников охраны, в конечном счете может свести на нет все усилия по повышению эффективности их труда.

Неудовлетворительное финансовое обеспечение может также отрицательно сказываться на работе с кадровыми ресурсами. Такая работа предполагает отбор кадров, систематическое обучение (переобучение) охранников, налаживание действенной воспитательной работы по укреплению должной дисциплины и т.д. При полном ресурсном обеспечении своеобразную, цементирующую роль труда сотрудников охранного подразделения играет его правовое обеспечение – наличие положения об охранном подразделении, его секторах (группах), должностных инструкций, инструкций по организации пропускного режима, контрактов и т.д.

Способы охранной деятельности

Применительно к деятельности охраны применяется такой термин, как способ охранной деятельности. Он включает и такие методы детективной деятельности, как наблюдение, устный опрос, изучение документов, внешний осмотр строений и помещений применяются охранниками достаточно активно, разумеется, в рамках их полномочий. На практике чаще употребляется термин «способ», т.е. действие или система действий, применяемая при исполнении какой-либо работы. Отсюда можно выделить следующие основные способы действий охраны: патрулирование, несение постовой службы, сопровождение, применение служебных собак, пропускной режим и создание рубежей (зон) безопасности.

К числу факторов, влияющих на выбор способов охраны, относятся:

-  характеристика технической скрепленности охраняемого объекта;
-  наличие и характеристика охранно-пожарной сигнализации, охранного телевидения и охранного освещения;

- 🔊 природно-климатические условия местности, на которой расположен охраняемый объект;
- 🔊 наличие уязвимых мест в системе охраны объекта, которые в принципе могут стать известными потенциальным правонарушителям;
- 🔊 возможные способы проникновения на охраняемый объект;
- 🔊 режим и характер работы охраняемого объекта;
- 🔊 наличие на объекте материальных и финансовых ресурсов;
- 🔊 режим охраны объекта;
- 🔊 количественные и качественные характеристики охранного подразделения;
- 🔊 полнота ресурсного обеспечения сотрудников охраны.

Рассмотрим более подробно основные способы охранной деятельности.

Патрулирование заключается в систематическом обходе территории охранниками с целью пресечения несанкционированного доступа посторонних лиц на охраняемый объект. Применяется при охране стационарных объектов. Протяженность маршрута при пешем патрулировании составляет от 150 метров (пост – меньше 150 метров), но не более 1500 метров. Однако, если объект охраняется патрулем на велосипеде, мопеде, мотоцикле или лошади, то протяженность маршрута составляет 3-5 км, при использовании автопатруля – не более 6-8 км. Патрули могут выставляться для охраны участков территории непосредственно у охраняемого объекта и по периметру ограждения территории объекта. При патрулировании применяются следующие приемы контроля и осмотра охраняемого объекта:

1. Фронтальный осмотр объекта, при котором несколько охранников движутся в одном направлении до границы охраняемого объекта, а затем производят движение в обратную сторону.

2. Досмотр объекта навстречу друг другу, при котором охранники движутся от границы объекта к центру (точке встречи), после чего вновь расходятся в направлении периметра охраняемого объекта.

3. Концентрический и эксцентрический способ контроля и осмотра объекта, при котором один или два охранника движутся по спирали от центра охраняемой территории на периферию и наоборот.

Последовательный осмотр отдельных участков охраняемого объекта по сложной траектории в зависимости от планировки и конструкции объекта.

Выборочный осмотр участков объекта в зависимости от значимости хранимых товарно-материальных ценностей, наличия на объекте уязвимых мест.

Движение по объекту с постоянно меняющимся маршрутом применяется в сложных ситуациях для предупреждения нападения на охранника.

Движение по объекту с временными остановками и осмотром уязвимых мест

При выставлении патрулей необходимо обеспечить максимально полный контроль за охраняемым участком местности, возможность визуального контроля охранником хотя бы части участка другого патрулируемого маршрута (если он есть), возможность взаимопомощи других охранников

с соседних маршрутов, связь охранников друг с другом и дежурной частью службы безопасности.

Несение постовой службы. Охранник выполняет свои обязанности на ограниченном участке местности (на посту) с целью пресечения несанкционированного доступа посторонних лиц к охраняемому объекту. (Пост – это порученный охраннику участок территории, на которой расположен охраняемый объект, где он должен в течение определенного ему времени обеспечить к нему только санкционированный доступ согласно полученной инструкции). Применяется этот метод при охране как стационарного, так и передвижного объекта. Места, где обычно выставляются посты, – это контрольно-проходные и проездные пункты охраняемых объектов, внутренние помещения зданий, принимаемых под охрану, особо важные участки производств, отдельные цеха или отделы и т.д. При выставлении постов необходимо обеспечить максимально полный контроль за охраняемым зданием, помещением и связь охранников с дежурной частью службы безопасности.

Система “Диспетчер”

Авторы предлагают обратить внимание на надежную систему охраны “Диспетчер. Принцип работы этой системы охраны очень прост, а значит, надёжен и не требует длительного изучения, эта система уже работает в различных направлениях, там, где нужна надежная система оперативного контроля, например : охрана стационарного объекта, физическая охрана периметра, фиксация графика движения троллейбусного и автобусного парка, маршрутных такси, контроль за работой сотрудников охраны и службы безопасности на других направлениях. Рассмотрим принцип работы данной системы на примере работы службы охраны.

Руководитель или начальник службы безопасности предприятия разрабатывает оптимальные маршруты патрулирования охранниками территории предприятия. После этого, вдоль маршрута обхода на контрольных объектах крепятся специальные контрольные микропроцессоры – электронные метки. На компьютер устанавливается программное обеспечение “Диспетчер”, в которое заносятся номера электронных меток и приборов регистрации событий. Каждой метке в программе присваивается место установки: склад, сейф, офис, гараж и т.д. Аналогично заносятся номера ПРС (Иванов, Петров, Сидоров и т.д.). Далее каждому охраннику выдается прибор регистрации событий – ПРС. Проходя по маршруту, охранник подходит к каждому объекту, на котором закреплена метка и касается её ПРС. Таким образом, в ПРС переносится информация о времени обхода, когда и какой именно охранник был у конкретного объекта, например склада, фасада, крыльца и т.д. После необходимого количества обходов, как правило в конце смены, когда в памяти каждого ПРС уже содержится подробный отчет о выполнении своих обязанностей каждым сотрудником охраны, начальнику охраны, дежурному или другому ответственному лицу выдаётся устройство сбора данных – УСД. Он объезжает объекты, на которых установлена система “Диспетчер” и касанием УСД контактной площадки ПРС переносит информацию из памяти прибора в свою память, тем самым, очищая память прибора. Далее все очень просто. Начальник охраны или руководитель предприятия через адаптер подключает УСД к компьютеру и переносит данные из УСД в специальную программу анали-

за работы охраны “Диспетчер”. Программа выдает отчёт о работе по каждому охраннику индивидуально, в который входит: общее количество обходов за сутки, время начала и конца каждого обхода, его продолжительность, последовательность и точное время прохождения охранником контрольных объектов, (на которых установлены электронные метки). Более того, программа выдает не просто детальный отчёт о работе охраны, она сама показывает какой охранник, где и когда допускал нарушения относительно графика и маршрута обхода. Все результаты могут быть распечатаны и предоставлены самим охранникам для анализа своей работы. Остается только поощрить добросовестных охранников и наказать любителей поспать...

Хотим отметить, что система контроля работы охраны “Диспетчер” работает в круглосуточном режиме, поэтому есть возможность контролировать работу охраны даже в ночное время!

1. Некоторые актуальные проблемы службы охраны Каждый понимает, что работа охранников – это нелёгкий труд (если его добросовестно выполнять). На это есть масса причин – это и необходимость совершать обходы по зачастую довольно значительной территории, и работа при любых погодных условиях и в любое время суток, характер охраняемых объектов и сложные маршруты патрулирования и т.д. И таких факторов очень много. Понятно, что работоспособность любого человека в вечернее, и, тем более в ночное время, намного меньше, чем днём. И ни для кого не секрет, что большинство охранников пытаются решить эту проблему гениально просто – либо делать вместо 8 положенных обходов охраняемой территории в лучшем случае 2-3, либо вообще расположиться поудобнее на диване, и смотреть десятый сон. Более того, контроль со стороны руководства за работой охраны в ночное время либо просто невозможен, либо сильно ограничен, что является стимулирующим фактором, к мягко говоря “халтуре”, а по сути – невыполнению своих должностных обязанностей работниками охраны. А ведь именно ночью необходимость делать обходы территории стоит особо остро, так как известно, что большинство краж происходит собственно в ночное время. Что делать?

2. Решение проблемы с помощью системы Диспетчер Единственный верный способ значительно повысить эффективность работы охранников – установить надёжную автономную систему оперативного контроля за их работой. Причем необходимо, чтобы эта система была удобной и простой в применении, имела автономное питание, была устойчива к внешним воздействиям (агрессивным средам, механическим повреждениям и т.д.), не давала возможности работникам повлиять на результаты контрольных данных, что исключает их фальсификацию. Основной довод в пользу контроля охраны с помощью специальных устройств – однозначное определение эффективности работы персонала. После изучения отчета у начальника службы безопасности не просто колонки цифр, а объективная информация о добросовестности каждого сотрудника охраны. Система полностью фиксирует все нарушения:

-  если охранник вообще не делал обходов территории и объектов;
-  если охранник сделал меньшее количество обходов территории и объектов, чем установлено ему должностной инструкцией;
-  если охранник делал обход по сокращённому маршруту, пропуская охраняемые объекты;

 если было нарушено время обхода мимо конкретного объекта, интервал между обходами и т.д.

Прибор с точностью до минуты фиксирует прохождение охранником заданного объекта, который, в свою очередь, не имеет возможности каким-либо образом повлиять на результат считывания, а значит не сможет с имитировать обход, если он его не делал. Одновременно, система “Диспетчер” очень удобна, проста в работе, имеет автономное питание, устойчива к агрессивным средам, что немаловажно для климата наших стран.

Основные требования к режиму охраны объекта

Применение служебных собак. Заключается в использовании собак при охране стационарного или передвижного объектов с целью своевременного выявления лиц, стремящихся незаконно проникнуть на них и оповещения об этом охранников. Обычно применяют три варианта участия собаки в охране:

- 1) – на короткой привязи, непосредственно у охраняемого объекта;
- 2) – на блок-посту – по троссу, натянутому между деревянными столбами на всем протяжении и на ширину не менее 8-10 м.;
- 3) – без привязи при наличии ограждения вокруг охраняемого участка или объекта.

Выбор в пользу того или иного варианта зависит от различных характеристик объекта и наличия на нем уязвимых мест. Для использования в охране объектов рекомендуют следующие породы собак: восточноевропейская овчарка, кавказская овчарка, среднеазиатская овчарка, южно-русская овчарка, колли, доберман-пинчер, ротвеллер, дог, ньюфаундленд, боксер, московская сторожевая и другие.

Режим охраны – это установленный, обязательный для всех порядок жизнедеятельности охраняемого объекта, который формируется из внутриобъектового, противопожарного и пропускного режимов.

Внутриобъектовый режим – это выполнение распорядка дня и соблюдения общественного порядка на территории предприятия. Сотрудники охранного подразделения для поддержания внутриобъектового режима контролируют своевременную сдачу ключей от служебных помещений, требуют закрытия окон, форточек и дверей при окончании работы и т.д.

Противопожарный режим – это система мер, регламентирующих порядок обеспечения пожарной безопасности. Авторы обращают внимание, что в странах СНГ, России и Украины могут быть различия, где сотрудникам охраны разрешено выполнять только часть противопожарных мер по проектированию, монтажу и эксплуатационному обслуживанию средств пожарной сигнализации.

Пропускной режим – это установленный порядок контроля за перемещением персонала, посетителей, материальных и транспортных средств на охраняемом объекте. Пропускной режим включает в себя:

- 1.– порядок приема посетителей и выдачи пропусков;
- 2 – порядок пропуска посетителей и сотрудников предприятия;
- 3 – порядок пропуска транспортных средств и имущества;
- 4 – порядок документирования нарушений пропускного режима.

Применяется этот метод с целью не допустить перемещения на территории и внутри объекта лиц, не имеющих на это разрешения и для пресечения бесконтрольного ввоза и вывоза оружия, взрывчатых веществ, имущества и т.д. Обычно устанавливаются два вида пропускных докумен-

тов – удостоверения и пропуска, которые дают право прохода сотрудников и посетителей на предприятие, вноса (выноса), ввоза (вывоза) материальных ценностей. Пропуска для сотрудников предприятия и его посетителей могут быть разовыми, временными и постоянными. Для ввоза (вывоза) материальных ценностей используются материальные пропуска. Бюро пропусков осуществляет учет бланков удостоверений и пропусков, их оформление и выдачу. Сотрудники бюро пропусков ведут документацию по пропускному режиму, которая включает в себя:

-  дело с инструкциями по пропускному режиму и образцами подписей на материальные пропуска;
-  дело с приказами и распоряжениями по пропускному режиму;
-  дело с заявками на удостоверения, разовые, постоянные, временные и материальные пропуска;
-  дело с актами на уничтожение пропускных документов;
-  книга учета выдачи удостоверений и пропусков;
-  книга учета ежедневного расхода бланков разовых пропусков.

5 – журнал учета печатей и штампов предприятия.

Создание рубежей защиты и зон безопасности. Границы пространства, защищаемого от угрозы, называют рубежами защиты. Область пространства внутри замкнутого рубежа защиты принято называть зоной безопасности.

Рубежи защиты и зоны безопасности располагаются последовательно от забора вокруг территории охраняемого объекта до главного, особо важного помещения. Оптимальным считается создание шести рубежей (зон) безопасности. Для иллюстрации приведем пример расположения зон безопасности крупного предприятия.

Зона 1 – периметр территории предприятия.

Зона 2 – периметр здания предприятия.

Зона 3 – расположенные внутри здания представительские помещения для приема посетителей.

Зона 4 – расположенные внутри здания служебные кабинеты сотрудников.

Зона 5 – расположенные внутри здания кабинеты руководства, комнаты переговоров.

Зона 6 – расположенные внутри здания хранилища ценностей, сейфы, компьютерный банк данных.

При создании рубежей основное внимание следует уделять правильному расположению в зонах безопасности средств обнаружения угроз, чтобы на их преодоление потребовалось как можно больше времени. Каждый из приведенных способов достаточно результативен, однако эффективность деятельности охранного подразделения достигается лишь при их комбинировании, т.е. использовании всех способов. Вышеуказанные способы охранной деятельности лишь тогда способны выполнить свою роль, когда они органично вписаны в интегральную систему обеспечения физической безопасности предприятия (объекта). Такая система включает в себя следующие средства противодействия (защиты) от потенциальных и реальных угроз нарушения неприкосновенности охраняемого объекта:

- ❖ здания и инженерно-строительные препятствия, (мешающие действиям правонарушителя);
- ❖ технические средства, обеспечивающие обнаружение попыток несанкционированного проникновения на охраняемый объект и оценку их опасности;
- ❖ системы связи, обеспечивающие своевременную регистрацию (фиксацию) и передачу тревожной информации для ответных защитных действий в пункт управления охранного подразделения;
- ❖ сотрудники охраны, выполняющие ежедневно плановые и внеплановые охранные мероприятия;
- ❖ процедуры обеспечения физической безопасности, регламентирующие определенные защитные мероприятия, их направленность и управление ими. Представление о методах и источниках охранной информации можно получить из представленной ниже таблицы.

Человек	Документ	Изделие (процесс)
Опрос сотрудников предприятия о недостатках в охране имущества.	Изъятые охраной поддельные пропуска.	Ложное срабатывание охранной сигнализации.
Специалист, привлеченный к сотрудничеству для обследования состояния охраны и ее узких мест.	Составленный отделом кадров список уволенных сотрудников, не сдавших свои пропуска.	Предметы, находящиеся в зоне безопасности не допускается.
Гражданин, заявивший по своей инициативе об известном ему факте подготовки к покушению на имущество предприятия.	Поддельный или подложный перевозочный документ.	Изъятые в охраняемых местах подслушивающие и взрывные устройства.
Инструктажи сотрудников разведки и контрразведки службы безопасности и правоохранительных органов.	Ориентировки правоохранительных органов о разыскиваемых преступниках.	Приборы-ловушки.
Сообщения должностных лиц о возможных стихийных бедствиях (пожарах, наводнениях, землетрясениях и т.д.) или наблюдаемые непосредственно самими охранниками.	Список сотрудников предприятия, подозреваемых в совершении правонарушений.	Временно выведенные из строя средства связи и электроэнергетики.
Факты подготовки покушения криминальных элементов на охраняемое лицо или имущество предприятия, наблюдаемые непосредственно самими охранниками.		Повреждение систем жизнеобеспечения предприятия. Вывод из строя охранного телевидения и освещения. Состояние запирающих устройств.

**Образцы служебной документации
по охране стационарных объектов**

Для эффективного функционирования физической охраны на объектах, регламентации ее обязанностей в соответствии со спецификой объекта, разрабатывается служебная документация.

Разработка документов производится в соответствии с законодательными и нормативными актами Вашего государства, регулирующими вопросы безопасности предпринимательства и деятельности охраны.

На каждом объекте, где выставляется охрана, должен находиться перечень документов, в который входят:

1. Журнал дежурства охранников.
2. График дежурства охранников на месяц.
3. Инструкция по охране объектов.
4. Инструкция по охране труда и технике безопасности во время дежурства на объекте.
5. Табель поста.
6. Журнал приема под охрану ключей от кабинетов.
7. Журнал приема помещений на КМЕ (концентратор малой емкости).
8. Журнал распоряжений и указаний охране.
9. Приказ руководителя Предприятия "О правилах и трудовом распорядке дня для работников Предприятия".
10. Образцы подписей материально – ответственных лиц.
11. Образцы печатей, которыми опечатывался помещения.
12. Список руководства Предприятия и Службы безопасности, а также список материально ответственных лиц с адресом и домашним телефоном.
13. Список охранников с указанием места жительства и домашних телефонов.
14. Номера телефонов аварийных служб, скорой медицинской помощи, милиции, пожарных служб, ФСБ, СБУ.
15. Паспорт на офис предприятия.
16. Паспорт на место проживания руководителя предприятия

Инструкция охраннику-телохранителю по сопровождению руководителя на маршруте "работа-дом" (если эти услуги предоставляются) Все журналы должны быть пронумерованы и прошнурованы согласно установленным правилам. Документация должна храниться в папке под названием "Документация охраны". Папка должна содержать Опись документов, находящихся в папке, следующего вида:

(папка):

Документация охраны

№ п/п	Наименование документа	Дата изъятия	Подпись
1	Журнал дежурства охранников	22.10.2007	подпись
2	График дежурства охранников на месяц	10.01.2005	подпись
3	Журнал распоряжений и указаний охране	02.02.2006	подпись
4	...	...	...

Служба безопасности – залог успеха предпринимательства

При изъятии документа из папки об этом делается соответствующая запись в Описи документов. Документы из папки имеют право изъять только руководство Предприятия или Службы безопасности. При приеме-передаче дежурства дежурная смена обязана проверить наличие всех документов в папке. На каждом посту должна находиться также медицинская аптечка с инструкцией по применению.

1. Журнал дежурства.

Журнал дежурства позволяет осуществлять контроль за работой охранников, принимать соответствующие меры реагирования на выявленные недостатки внесена службы, закрепляет юридическую ответственность охранника за выполняемую работу. Журнал дежурства заполняется по следующей форме:

ЖУРНАЛ дежурства охранников по охране офиса Предприятия

№ п/п	Дата	Время заступления на охрану	Ф.И.О. и роспись охранника	Краткое содержание результатов дежурств за смену	Примечание
1	21.01.2007	8.00	Петров И.И. РОСПИСЬ	За время охраны офиса с 9:00 18.03.96 до 9:00 19.03.96 происшествий не зарегистрировано, с работник средств сигнализации на КМЕ не поступало. (РОСПИСЬ)	

2. График дежурства охранников на месяц

Ведение графика работы охранников позволяет контролировать суммарное время работы по охране, болезни, отпуску и др. невыходов, и, соответственно, начислять зарплату охранникам.

График имеет следующий вид:

ГРАФИК дежурств охранников по охране офиса предприятия
на _____ месяц 200__ г.

№ п/п	Ф.И.О. о охранника	Числа месяца										Отработано часов за месяц на посту	Роспись охранника об ознакомлении	Количество часов		
														по болезни	Отпуск	Другие невыходы
1	Петров И.И.	1	2	3	4	5	6	7	8	9	10	и т.д. до 31	Петров И.И. (РОСПИСЬ)			
2																

3. Табель поста

Табель поста предназначен для определения перечня наиболее важных помещений объекта и особых обязанностей охранников по их охране. В Табеле поста отражаются следующие вопросы:

- порядок приема поста под охрану;
- уязвимые места в помещении;
- почасовой график осмотра помещений во время их охраны;
- действия охранника при срабатывании средств охранной сигнализации;
- действия охранника при пожаре, затоплении и т.д.;
- порядок вскрытия помещений при чрезвычайных ситуациях.

Табель поста заполняется по форме:

“УТВЕРЖДАЮ”
Руководитель предприятия
 “_____” _____ **200_ г.**

ТАБЕЛЬ ПОСТА

по охране офиса предприятия по адресу: ул.Котельникова,35
 Время работы: рабочие дни с 18:00 до 9:00 суббота с 9:00 до 9:00
 воскресенье с 9:00 до 9:00 праздники с 9:00 до 9:00

№ п/п	Охраняемые помещения	Особые обязанности охранника	Примечание
1	Бухгалтерия	1.Получив сообщение о сдаче помещения от материально-ответственного лица или лица, назначенного приказом руководителя ответственным за сдачу помещения под охрану, охранник обязан: – прибыть лично к принимаемому помещению, – проверить закрытие оконных фрамуг и форточки на запирающие устройства, – исправность металлической решетки на окне, – целостность оконного стекла, отключение бытовых и офисных приборов; – совместно со сдающим включить средства охранной сигнализации в режим “охрана”, – закрыть входные двери на замок, опечатать установленной печатью дверь; – в помещении охраны принять в присутствии сдающего помещение на КМЕ путем постановки тумблера в режим “охрана”; – при получении с КМЕ подтверждения о взятии помещения под охрану произвести запись в журнале, поставить свою подпись	

		и подпись сдающего помещение. 2. Во всех случаях вскрытия помещения после постановки его под охрану составляется Акт, который при сдаче дежурства передается начальнику Отдела охраны и техзащиты. 3. Во время охраны помещения производить осмотр помещения путем осмотра целостности входной двери, прослушивание помещения через входную дверь. Периодичность осмотра: в 22:00, 23:00 1:00, 3:00 и 5:00. Результаты осмотра отражать в журнале охраны. 4. При срабатывании средств охранной сигнализации: – поставить переключатель КМЕ в режим “снятие с охраны”; – незамедлительно прибыть к помещению бухгалтерии, осмотреть входные двери прослушаться с целью выявления обстановки внутри помещения; – в случае обнаружения посторонних сообщить в милицию по тел: _____, начальнику Отдела охраны и техзащиты, и принять меры к задержанию преступников; – если целостность помещения не нарушена, перевести переключатель КМЕ в режим “охрана”; – в случае не взятия пультом помещения бухгалтерии под охрану, вызвать материально-ответственное лицо и в присутствии его вскрыть помещение с целью установления причин срабатывания сигнализации. Время срабатывания сигнализации регистрируется в Журнале приема помещений под охрану. 5. При возникновении возгорания в помещении бухгалтерии: – сообщить по тел: 01 в пожарную часть и руководству Предприятия о возгорании; – вскрыть помещение и принять меры по тушению пожара и эвакуации материальных ценностей в коридор офиса, а документации – в комнату охраны; – по прибытию пожарной команды записать фамилию старшего и номер машины, усилить охрану эвакуированных ценностей.	

		– по прибытию пожарной команды записать фамилию старшего и номер машины, усилить охрану эвакуированных ценностей. По окончании смены составить подробную докладную записку о происшедшем на имя руководителя Предприятия. 6. При посещении офиса в ночное время работником милиции с целью проверки, работник охраны обязан: – через стекло в дверях проверить удостоверение личности (Ф.И.О., должность, № удостоверения работника милиции); – выяснить причину посещения, из какого подразделения прибыл работник милиции, перезвонить в дежурную часть территориального органа милиции для получения подтверждения на данное лицо (например: <i>“Говорит Петров И.И., охранник предприятия, расположенной по адресу: _____”</i>). <i>Ко мне прибыл участковый инспектор Иванов И.И., удостоверение № __, подтвердите его работу в вашем управлении”).</i> – при получении подтверждения доложить руководителю предприятия по телефону о прибытии работника милиции и цели его посещения. Решение о допуске в офис работника милиции принимает руководитель Предприятия. 7. В случае проникновения в офис преступника, наряд милиции допускается в офис беспрепятственно. 8. При затоплении помещения бухгалтерии работник охраны обязан: – сообщить о случившемся руководителю Предприятия и по его указанию вскрыть помещение; – в случае необходимости эвакуировать документацию и материальные ценности в безопасное место; – вызвать аварийную службу водоканала. Допуск в офис работников водоканала аналогичен допуску пожарных. По окончании смены составить подробную докладную записку о происшедшем на имя руководителя Предприятия. 9. В ночное время имеют право посещения офиса руководитель Предприятия, его заместители, начальник Отдела охраны и техзащиты с целью проверки несения службы. Их допуск в офис осуществляется по удостоверениям.	
2	...	...	

Начальник Отдела охраны и техзащиты

(подпись)

4. Журнал приема под охрану ключей от кабинетов.

Журнал приема ключей необходим охранникам для осуществления контроля за сохранностью ключей. Ключи от помещений объекта сдаются охране по окончании рабочего дня. Ключи используются охраной для вскрытия помещений в нештатных ситуациях: в случае проникновения злоумышленников в помещения через окна, при пожаре, затоплении и других стихийных бедствиях.

Журнал приема ключей заполняется по следующей форме:

ЖУРНАЛ **приема под охрану ключей от кабинетов офиса предприятия**

Прием ключей						Выдача ключей				
№ п/п	Дата	Время	№ каб./ кол-во ключей	Ф.И.О. Сдал <i>Рос-пись</i>	Ф.И.О. Принял охран-ник <i>Рос-пись</i>	Дата	Время	№ каб./ кол-во ключей	Ф.И.О. охран-ник выдал <i>Р/ос-пись</i>	Ф.И.О. полу-чил <i>Рос-пись</i>
1	14.03.08г.	19.00	4/3	Петров И.И. <i>Роспись</i>	Сидоров С.С. <i>Роспись</i>	15.03.08г	9.00	4/3	Иванов И.И. <i>Роспись</i>	Петров И.И. <i>Роспись</i>

5. Журнал приема помещений на КМЕ (концентратор малой емкости)

Настоящий Журнал необходим охране для осуществления контроля за сдачей помещений под охрану с использованием средств охранной сигнализации, а также проверки работоспособности средств сигнализации.

Прием помещений (под охрану) на КМЕ						Вскрытие (снятие с КМЕ) помеще-ний			
№ п/п	Дата	Время	Наим. помеще-ния № ячей-ки на КМЕ	Ф.И.О. Сдал <i>Роспись</i>	Ф.И.О. Взятие на КМЕ охран-ник <i>Роспись</i>	Дата	Время	Ф.И.О. охран-ник Снятие с КМЕ <i>Роспись</i>	Ф.И.О. Вскрыл <i>Роспись</i>
1	14.03.06г.	19.00	Касса офи-са №2	Петров И.И. <i>Роспись</i>	Сидоров С.С. <i>Роспись</i>	15.03.06г	9.00	Сидоров С.С. <i>Роспись</i>	Петров И.И. <i>Роспись</i>
2	...	...	...	...	...	...	...	...	...

6. Журнал распоряжений и указаний охране

Журнал распоряжений необходим для осуществления контроля за выполнением охраной своих обязанностей и дачи дополнительных указаний.

Распоряжения и указания охране даются руководством Предприятия и Службы безопасности.

Журнал распоряжений необходим для осуществления контроля за выполнением охраной своих обязанностей и дачи дополнительных указаний.

Распоряжения и указания охране даются руководством Предприятия и Службы безопасности.

ЖУРНАЛ
распоряжений и указаний охране в офисе предприятия

№ п/п	Дата, время	Ф.И.О. должностного лица, дающего указания	Содержание указания, срок его выполнения, роспись дающего указания	Справка охранника по результатам исполнения указания	Примечание
1	21.01.2007 в 10.00	Сергеев В.И. генеральный директор	На 12:00 вызвать из дому гл. бухгалтера Курицину Н.И. РОСПИСЬ	Сообщено Курициной по телефону в 10:10 охранник Петров (роспись)	

7. Паспорт на офис предприятия

“УТВЕРЖДАЮ”
Руководитель предприятия
“___” _____ 200__ г.

Паспорт на офис предприятия

Офис предприятия расположен в г. _____

С фасадной стороны здания офиса проходит проезжая часть проспекта с интенсивным движением автотранспорта.

Между проезжей частью и зданием офиса проходит полоса насаждений шириной до 20 м, внутри полосы прожжена асфальтированная дорожка для пешеходов. С западной стороны здания офиса проходит. На противоположной стороне на расстоянии 30 м расположено одноэтажное здание кафе. С тыльной стороны здания офиса на расстоянии 35 м расположен 9-этажный жилой дом с двумя парадными, которые выходят в противоположную сторону от здания офиса.

Помещение офиса расположено на первом этаже 5-этажного жилого дома. В помещении офиса размещены восемь кабинетов, пять из которых окнами выходят в тыл здания (это кабинет зам. руководителя, бухгалтерии, коммерческого центра, технического центра, начальника охраны).

На фасадную сторону здания выходят окна кабинета руководителя, торгового центра. В помещении офиса всего имеется восемь окон (в каждом кабинете по одному окну, в торговом центре два), а также один вход со стороны. Двери входа двойные.

Стекла окон оклеены тонированной самоклеющейся пленкой.

Возле здания офиса на расстоянии 10 м от центрального входа оборудована стоянка для автотранспорта на 3 единицы.

Стоянка охраняется с помощью технических средств -телевизионной установки. Помещение офиса оборудовано средствами охранной сигнализации с выводом на пульт, который установлен в помещении охраны.

Вход в помещение офиса осуществляется через контрольно-пропускной пункт.

Служба безопасности – залог успеха предпринимательства

Решением (приказом) руководства фирмы в здание офиса установлен пропускной и внутри объектовый режим для работников фирмы, посетителей и клиентов.

Поддержание установленного режима возложено на Службу охраны.

Охрану здания офиса осуществляет:

– круглосуточный пост охраны (см. Схему расположения офиса предприятия “_____”, (Пост № 1) в количестве 1 единицы (3 охранника по-сменно);

– один 9-часовой пост (на Схеме Пост №2) в количестве 1 единицы в приемной по охране руководителя (на рабочем месте и при поездках.

Для работников охраны разработана и утверждена инструкция, регламентирующая действия охранника при обычном, усиленном режиме и в случаях возникновения нештатных ситуаций и чрезвычайных происшествий, взаимодействия работников охраны с правоохранительными органами (Приложение № 1). Экипировка работников охраны:

- палка РП(резиновая);
- наручники;
- газовый баллончик “Терен-1..”;
- радиостанция “Виола” или иного типа.

С работниками охраны два раза в месяц проводятся занятия по специальной подготовке, разработан план занятий (расписание), а также в спортивном зале проводятся занятия (еженедельно по вторникам и четвергам с 18.00 до 20.00) по общей физической подготовке, рукопашному бою, действию охранников в экстремальных условиях. Учет занятий ведется в специальном журнале.

Списки, адреса, номера телефонов и факсов, электронные адреса для связи: Руководитель фирмы Иван Иванович проживает по адресу _____, тел. _____, № автомобиля _____, группа крови I, резус- положительный. Рост 180 см, полного телосложения, волосы черные, нос прямой, глаза карие. Особая примета – возле правого уха на шее имеется родимое пятно круглой формы размер в диаметре 0,5 мм.

Близлежащий орган внутренних дел – городской отдел милиции № ____ тел: _____ - дежурный,

Медицинское учреждение: _____

Средства массовой информации: _____

К Паспорту прилагается Схема расположения офиса предприятия

Начальник Службы безопасности

(подпись)

“УТВЕРЖДАЮ”
Руководитель ПРЕДПРИЯТИЯ
“ — ” _____ **200_ года**

**Инструкция работнику охраны
по охране труда и технике безопасности**

I. Общие требования безопасности.

1.1. Работник охраны Предприятия при несении службы может использовать для обогрева электронагревательные приборы промышленного изготовления (утвержденные госпожнадзором), при этом соблюдать правила:

- электронагревательные приборы, должны быть с закрытой спиралью, изготовленные на предприятии и установлены на огнеупорных подставках, на безопасном расстоянии от стены и других элементов строительных конструкций;
- в процессе эксплуатации электроприборов запрещается подвешивать электропроводку на гвоздях, заклеивать ее обоями, применять провод с поврежденной изоляцией, самодельные предохранители, завертывать электролампы в бумагу или материн;
- самостоятельно производить ремонт электропроводки, выключателей и других электроприборов.

1.2. Работникам охраны во время несения службы на стационарном или обходном посту запрещается:

- исполнять работы, которые не предусмотрены инструкцией по несению службы на объекте;
- допускать на рабочее место (пост) лиц которые не имеют никакого отношения к работе, которая выполняется;
- оставлять пост, за исключением случаев оказания помощи в предотвращении правонарушений, потерпевшим при авариях на объекте, задержания преступника;
- уклоняться от безопасного маршрута движения при обходе территории охраняемого объекта;
- передавать посторонним лицам специальные средства защиты, оставлять их без присмотра;
- курить в не установленных местах, разрешать разведение огня, сожжения тары, производственных отходов вблизи объекта и на территории;
- использовать для осмотра транспорта приставные лестницы без крюков, другие подсобные предметы, осматривать его с подножки или колеса при работающем двигателе;
- проверять пропуски на право выезда (въезда) транспорта во время его движения;
- допускать посторонних лиц к управлению воротами с механизированным приводом;
- находиться в зоне проведения погрузочно-разгрузочных работ.

1.3. В случае заболевания во время работы, охранник должен доложить об этом начальнику Отдела безопасности и охраны.

II. Требования безопасности при заступлении на службу

2.1. Перед началом работы охранник заступающий на службу обязан:

– убедиться в наличии и исправности средств связи, сигнальных устройств, приборов ОПС, средств пожаротушения, электронагревательных приборов, освещения в ночное время;

– обойти маршрут безопасного движения по территории объекта (согласно разработанной схеме), во время гололеда маршрут посыпать песком с целью предотвращения травм от падения.

III. Требования безопасности во время несения службы.

3.1. Обход охраняемой территории, помещений осуществлять по разработанной схеме движения. Во время движения работник охраны должен соблюдать меры личной безопасности на опасных участках маршрута.

3.2. Выпуск транспорта с территории объекта производить в следующем порядке: осмотреть его, провести сверку соответствия груза с сопроводительными документами.

3.3. Во время управления механизированными воротами охранник обязан убедиться в отсутствии людей, транспорта в зоне движения створок ворот. Особую осторожность соблюдать при открытии немеханизированных ворот во время порыва ветра.

IV. Требования безопасности в аварийных ситуациях.

4.1. Работник охраны обязан незамедлительно доложить в пожарную службу по телефону 01, начальнику Отдела безопасности и охраны о пожаре, загорании, стихийном бедствии, которое возникло на объекте. О данном факте информируется и руководство объекта.

4.2. Соблюдая меры личной безопасности, работник охраны принимает меры по устранению возникшей опасности, и оказывает первую медицинскую помощь потерпевшим, предварительно вызвав машины скорой помощи (тел. 03).

V. После окончания несения службы работник охраны обязан:

5.1. Привести в порядок рабочее место.

5.2. Отключить электроприборы.

5.3. Доложить оперативному начальнику Отдела безопасности и охраны и о всех недостатках выявленных во время несения службы, а также принятых мерах по их устранению.

Начальник Службы безопасности

ПРЕДПРИЯТИЯ

“ ____ ” _____ 200_ года.

(фамилия)



Система охраны периметра

Предпроектное обследование при построении системы охраны периметра объекта

Авторы обращают внимание, что полученная информация и технический прогресс – очень изменчивые, поэтому в данной главе, мы даем только общее понятие. Система охраны периметра предприятия по типу используемого оборудования и стоящим задачам относится к системе охранной сигнализации объекта и ее построение должно отвечать требованиям нормативных и руководящих документов. Вместе с тем в составе СОП кроме технических средств охраны должны применяться инженерные средства, без которых некоторые задачи охраны периметра вообще не реализуемы. Согласно положениям и требованиям ГОСТов – создание системы охранной сигнализации на объекте должно вестись поэтапно, (мы приводим требование ГОСТов для России и просим читателя следить за возможными изменениями нормативных документов.) Для Украины, основные нормативные документы мы представили в конце главы – в приложении.

Авторы подчеркивают, что при этом обязательным этапом, должно быть предпроектное обследование состояния объекта охраны, оценка его готовности к установке инженерных и технических средств охраны (ИТСО). Итогом обследования является разработка заказчиком Технического задания для проектирования системы охранной сигнализации объекта. Предпроектное обследование объекта на предприятии проводится заказчиком (собственником) самостоятельно или с привлечением сторонних специалистов, компетентных в этой области. Наилучший эффект в работе при этом может быть достигнут при создании, (консультации) группы специалистов проектирования и монтажа охранной сигнализации с учетом охраны периметра Вашего объекта, последних технических новинок, возможностей и требований в этом направлении. Следите за изменениями и новинками.

Нормативные требования к построению системы охранной сигнализации

ГОСТ 26342-84	Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры.
ГОСТ Р 50775-95	Система тревожной сигнализации. Часть 1. Общие требования. Раздел 1. Общие положения (МЭК 839-1-1-88).
ГОСТ Р 50776-95	Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию (МЭК 839-1-4-89).
ОСТ 25 1099-83	Средства охранной, пожарной и охранно-пожарной сигнализации Общие требования и методы испытаний.
РД 25.952-90	Системы автоматические пожаротушения, пожарной, охранной и охранно-пожарной сигнализации. Порядок разработки задания на проектирование
РД 25.985-90	Комплексы, системы пожаротушения, технические средства охранной, пожарной, охранно-пожарной сигнализации. Термины и определения.
РД 78.143-92 МВД РФ	Системы и комплексы охранной сигнализации. Элементы технической укреплённости объектов.
РД78.145-93МВДРФ	Системы и комплексы охранной, пожарной и охранно-пожарной сигнализации. Правила производства и приемки работ.
РД 78.146-93 МВД РФ	Инструкция. О техническом надзоре за выполнением проектных и монтажных работ по оборудованию объектов средствами охранной сигнализации.
РД78.147-93МВДРФ	Единые требования по технической скреплённости и оборудованию сигнализацией охраняемых объектов.

Понятия “Концепция охраны периметра предприятия”

Разработка Концепции в ходе предпроектного обследования дает возможность на начальном этапе провести всесторонний анализ разнородных данных о состоянии сооружений и оборудования периметра территории предприятия, о самом предприятии и в концентрированной, удобной форме представить проектировщику СОП необходимый состав сведений в виде Технического задания. Сведения, содержащиеся в этом документе, должны способствовать: с одной стороны, грамотному построению системы охраны периметра, максимальной адаптации ее к условиям функционирования данного предприятия, а с другой – минимизировать затраты собственника на ее создание и последующую эксплуатацию. Кроме того, такой подход дает возможность повысить эффективность работы СОП путем объединения возможностей различных инженерных и технических средств (систем) охраны.

Концепция охраны периметра может являться самостоятельным документом в том случае, когда СОП на предприятии является доминирующей, а остальные системы (система объектовой сигнализации, система контроля и управления доступом, система охранного телевидения) входят в ее состав фрагментами. В противном случае разрабатываемые разделы “Концепции охраны периметра предприятия” должны входить в состав разделов общей Концепции охраны предприятия, дополняя их в части ее касающейся. Концепция представляет собой документ внутреннего использования, отражающий систему взглядов собственника на облик будущей системы охраны периметра и содержащий совокупность сведений, объединенных в следующие разделы:

1. Модель объекта охраны (модель периметра).
2. Модель угроз (в том числе модель нарушителя).
3. Тактика охраны периметра.

Модель периметра

Глава содержит сведения, характеризующие текущее состояние зоны периметра предприятия. Под зоной периметра понимается часть территории предприятия вдоль ее периметра (в виде кольца), ограниченная с внешней стороны внешним ограждением предприятия, а с внутренней стороны – внутренним ограждением, либо указателями ее внутренней границы.

В **состав зоны периметра** предприятия, как правило, входят контрольно-пропускные пункты, внешнее ограждение и зона отчуждения (ее ширина может достигать 3-х метров), а также расположенные в ней инженерно-технические средства охраны и освещения и т.п.

Собранные в разделе сведения должны способствовать грамотному подбору и построению СОП при эффективном использовании возможностей инженерных и технических средств, уже размещенных в зоне периметра, а также условиям его размещения на местности и порядку функционирования в рабочее и нерабочее время. Раздел документа представляется графической и текстуальной частью, (пояснительной запиской).

Графическая часть – это генеральный план распределенных на местности сооружений предприятия. Наряду с общим планом (при необходимости) могут создаваться и частные планы (схемы, чертежи), детализирующие отдельные его фрагменты. Например, чертежи развертки полотна ограждения, или чертежи ворот и калиток, входящих в линию ограждения, и т.п.

Генеральный план содержит графическое изображение (в масштабе);

- 👁 прилегающих к внешнему ограждению территорий (с указанием их характеристики и функционального назначения наиболее удобных мест для наблюдения и подходов нарушителя и т.п.);
- 👁 транспортных проездов и пешеходных маршрутов (при их наличии) вдоль внешней стороны периметра (с указанием их дистанции, протяженности, характеристики и интенсивности использования, а также принятых мер по повышению защищенности зоны периметра с этих сторон и т.п.);
- 👁 внешнего ограждения периметра (с указанием состояния и характеристики его строительных конструкций и др.);

- 👁️ зоны отчуждения (при ее наличии) и ее инженерно-технической оснащенности (с указанием ее состояния, мест установки и характеристик ИТСО и т.п.);
- 👁️ контрольно-пропускных пунктов (КПП), предназначенных для прохода персонала и проезда служебного транспорта (с указанием их состояния, возможностей и характеристики инженерно-технической оснащенности.);
- 👁️ инженерных указателей (внутреннего ограждения) вдоль внутренней границы зоны периметра (при их наличии);
- 👁️ зданий и сооружений на внутренней территории, имеющих охраняемое имущество (с показом взаимных удалений и их дистанций от внешнего ограждения, а также наиболее удобных путей и способов для проникновения в них нарушителя и т.п.);
- 👁️ трасс прохождения линий электропитания и внутренней связи вдоль зоны периметра (с указанием их характеристик и способа прокладки, а также возможных точек подключения и т.п.);
- 👁️ элементов системы освещения зоны периметра и территории предприятия (с указанием их состояния, возможности и характеристик и т.п.) и др. необходимые сведения.

В случае, когда фрагментом внешнего ограждения является внешняя стена здания, то дополнительно на плане указываются: «та часть ограждения, которая является внешней стеной здания (при этом характеризуются слабые места в ее инженерно-строительных конструкциях: оконные, дверные и другие проемы, способствующие доступу нарушителя на территорию предприятия); применяемые инженерные средства укрепления и их состояние (оконные решетки, жалюзи, стальные двери и т.п.) и технические средства охраны, др. необходимые сведения.

Пояснительная записка содержит, как правило, ту часть информации о зоне периметра, которая не может быть отражена на плане, но необходима для составления реалистичной модели периметра. Пояснительная записка должна начинаться с изложения:

- 👁️ необходимости создания (если СОП отсутствует) или модернизации (если существующая система уже не удовлетворяет текущим требованиям) системы охраны периметра;
- 👁️ цели, возлагаемой на СОП, и задач, которые она должна реализовать в ходе эксплуатации.

От того, какие цель и задачи поставлены перед создаваемой СОП, зависит ее конечный технический облик и финансовые затраты. Как правило, целью применения СОП является: своевременное оповещение сил охраны предприятия о факте несанкционированного проникновения через зону периметра нарушителя. Задачи, ставящиеся перед системой охраны периметра, уточняют и конкретизируют цель.

Таковыми задачами могут быть:

- 👁️ психологическое воздействие внешним видом на будущего нарушителя, созданием у него образа высокой защищенности и непреодолимости внешнего ограждения периметра (или незащищенности периметра в зависимости от выбранной тактики охраны);

- 👁 оповещение персонала предприятия о запретной для его пребывания (или опасной для его здоровья) зоне с внутренней стороны периметра;
- 👁 обнаружение (скрытное – при необходимости) факта (попытки) преодоления нарушителем зоны периметра;
- 👁 передача на пульт поста сил охраны сигнала о проникновении через внешнее ограждение нарушителя (фиксация места и времени проникновения);
- 👁 затруднение продвижения или блокирование (обездвиживание – при необходимости) нарушителя средствами инженерного ограждения (задержания) до прибытия наряда сил охраны и другие.

Вместе с тем, в пояснительной записке отдельными пунктами должны быть изложены:

- 👁 статистика нарушений установленного на предприятии режима (отмечается: время, место, способ и цели нарушения, а также размеры ущерба и тип нарушителя (если он задержан), его оснащенность и т.п.); анализ криминогенной обстановки в прилегающих к территории предприятия районах;
- 👁 физико-географическая характеристика местности (указывается перепад высоты внешнего ограждения, характеристика грунта и растительности прилегающих территорий и в зоне периметра и т.п.);
- 👁 климатические условия места размещения предприятия (приводится статистика колебаний температуры воздуха, метеосадков, силы и направлений ветра по сезонам) и другие необходимые сведения.

Кроме перечисленных выше, в разделе могут содержаться и другие необходимые для построения системы охраны периметра сведения. Итогом формирования сведений раздела является создание реалистичного описательного образа (модели) периметра в динамике его функционирования на фоне реальных условий его размещения на местности и воздействия объективных дестабилизирующих факторов

Модель угроз

Модель угроз представляет собой перечень возможных действий (целей и способов их достижения) нарушителя по преодолению зоны периметра распределенного объекта охраны. Под целью вторжения понимается конечная цель нарушителя, реализуемая им после преодоления зоны периметра. Их возможный спектр достаточно широк – от простой кражи, до террористических действий. Он прямо зависит от типа охраняемого имущества собственника. Определение целей вторжения на территорию предприятия, облика возможного нарушителя и наиболее вероятных сценариев его действий дает возможность сформировать требования к инженерно-техническим средствам системы охраны периметра, при реализации которых возможно ее эффективное противостояние.

Основная цель нарушителя в рассматриваемом варианте заключается в скрытном преодолении зоны периметра предприятия для получения не санкционированного доступа (НСД) к охраняемому имуществу собственника. Способ и время, затраченное им на преодоление зоны периметра, прямо зависят от его осведомленности о возможностях СОП предприятия, технической и физической подготовленности, а также от конечных целей вторжения. Для определения требуемого уровня защищенности перимет-

ра предприятия (способности его противостоять действиям нарушителя) необходимо формирование базовой модели нарушителя, на способности и возможности которого должна ориентироваться создаваемая СОП.

Такая модель наделяется максимальными для выбранного типа способностями и возможностями по преодолению зоны периметра. Созданная модель нарушителя принимается как базовая и относительно нее проходит разработка модели угроз. При формировании модели угроза рассматриваемом случае необходимо учитывать только те угрозы охраняемому имуществу предприятия, которые включают несанкционированное преодоление зоны его периметра нарушителем, обладающим возможностями сформированной его базовой модели.

Здесь полезными могут быть натурные испытания по количественной оценке возможностей нарушителя, например, времени преодоления внешнего ограждения заданной конструкции или зоны отчуждения, оборудованной инженерными средствами задержания, и т.п. При этом, как правило, исходя из принципа “хуже быть не может”, т.е. если созданная СОП в состоянии противостоять (обнаружить) нарушителя базовой модели, то она сможет противостоять всем типам нарушителей, обладающих меньшим уровне подготовленности по какому-нибудь параметру.

В ходе разработки модели угроз проводится оценка риска при том или ином варианте противодействия планируемой СОП вторжению нарушителя базовой модели с обозначенной целью вторжения. Согласно требований ГОСТов, **степень риска** – вероятностная величина, характеризующая невыполнение системой своей целевой задачи (например, обнаружения факта (попытки) проникновения на охраняемый объект) с учетом влияния опасных внутренних и внешних воздействий. Эти расчеты необходимы для выбора вида СОП (типа ИТСО ее реализующих), адекватной по затратам на ожидаемый ущерб от вторжения нарушителя, что предполагает реализацию принципа “экономичность”. Уровень риска предопределяет конечный выбор типа и количества инженерных и технических средств охранной сигнализации (обнаружения, приема-передачи, регистрации), типа передачи сигналов тревоги, способа их защиты от помех и т.п. Допускаемый СОП уровень риска должен учитывать не только возможную опасность по преодолению зоны периметра нарушителем, но и ее последствия. Завершающим этапом разработки модели угроз является формирование требований к возможностям будущей СОП в виде “списка сценариев действий” нарушителя базовой модели по преодолению зоны периметра, которые она должна выявить и блокировать. При этом необходимо учитывать возможные воздействия внешних и внутренних случайных факторов, которые могут способствовать достижению нарушителем своей цели – тактика охраны периметра

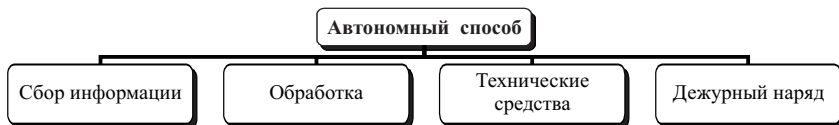
Тактика охраны объекта состоит из: выбора вида охраны, методов и средств ее реализации. В зависимости от результатов анализа данных рассмотренных выше моделей выбирается вид, структура и состав системы охраны периметра предприятия, соотношение инженерных и технических средств охраны. Определение тактики охраны периметра предприятия рекомендуется проводить в два этапа.

Первый этап. Вначале собственнику необходимо на основе выработанных разработчиками Концепции рекомендаций решить ряд стратегических задач, от варианта решения которых будет зависеть инженерно-технический облик СОП. При этом критерием для него долж-

на быть адекватность ожидаемых затрат на реализацию СОП возможному ущербу его имуществу, который повлечет НСД после проникновения через зону периметра нарушителя.

Таковыми задачами могут быть: – выбор вида охраны периметра предприятия, при этом определяется способ управления СОП:

1 – автономный: сбор, обработка информации от технических средств осуществляются в местном пункте наблюдения (в этом случае предприятие должно иметь наряд дежурных сил охраны для задержания нарушителя своими силами),



Варианты типовых моделей нарушителей

Категория	Тип нарушителя	Характеристика	Физпод-готовка	Знания о воз- можностях ТСО	Оснащенность	Примечание
1	Профессионал	Очень опасен. Способен добывать сведения об ИТСО, плакировать и готовить вторжение. Действует в одиночку, как правило, не интересуется материальными ресурсами. Опасается огласки.	Отличная	Высокие	Специальный набор средств, предназначенный для НСД, недоступен к свободному приобретению.	Тренируется государством и используется в его интересах. Защита от его проникновения – безнадежное дело, это по силам госструктурам.
2	Наемник (любитель)	Опасен. Способен на нелогичные действия, имеет зачатки плановости действий, может собирать сведения об ИТСО. Действует как в одиночку, так и группой. Интересует весь спектр целей вторжения.	Достаточная	Хорошие	Подобранный под за дачу НСД набор удовл., но усовершенствованных или самодельных средств.	Его услуги стоят дорого- цель его НСД на предприятие должна оправдывать затраты на его наем.

Служба безопасности – залог успеха предпринимательства

Категория	Тип нарушителя	Характеристика	Физпод-готовка	Знания о воз-можностях ИСО	Оснащенность	Примечание
3	Безработный (дилетант)	Умеренно опасен. Вторжение планируется на дилетантском уровне по сценарию героев популярных кинофильмов. Действует, как правило, а одиночку. Интересуют либо материальные, либо информационные ресурсы.	Удовлетворительная	Слабые	Бытовые средства, легко доступные для приобретения в магазине.	Остро нуждающийся в средствах – услуги его дешевы. Может преследовать свои цели по обогащению.
4	Бытовой (хулиган, наркоман, алкоголик)	Слабо опасен. Действует импульсивно, на основании обрывочных данных о возможной наживе. Действует как в одиночку, так и группой. Интересуют, главным образом, материальные ценности.	Плохая	Отсутствуют	Подручные средства (что под руку попало).	Совершает НСД из хулиганских целей, либо в целях обогащения. Услуги его очень дешевы.
5	Сотрудник предприятия	Опасен. Способен добывать сведения об ИТСО, планировать и готовить НСД, произвести саботаж ТСО Действует скрытно, в рабочее время, как в одиночку, так и группой. Интересуют материальные, информационные ресурсы, но малых размеров, позволяющих их пронос (провоз) через КПП.	Плохая	Высокие	Подобранный под задачу НСД набор доступных, но ворованных или самодельных средств	Остро нуждающийся в средствах. Его услуги стоят дорого – цель его НСД на предприятие должна оправдывать затраты на его наем и потерю работы. Либо преследует свои цели по обогащению.

2 – централизованный: сбор, обработка информации от технических средств осуществляются в местном пункте наблюдения, а для принятия решения по факту нарушения – информация транслируется на пункт централизованной охраны; (в этом случае для задержания нарушителя прибывает выездной наряд сил охраны);

- ⑤ определение количества рубежей охраны в пределах зоны периметра, а также вида охранных систем и типа технических средств сигнализации, предполагаемых к использованию на каждом из выделенных рубежей;

- 👁 решение о необходимости (либо отказе) оснащения зоны периметра инженерными средствами охраны;
- 👁 выбор вида системы контроля и управления доступом (СКУД) персонала (служебного транспорта) предприятия на территорию через КПП, а также способа технической ее реализации и типа технических средств, оптимально подходящих под условия деятельности предприятия;
- 👁 выбор места размещения и со здание условий для наряда сил охраны (при выборе этого варианта охраны), а также места размещения автономного (местного) пульта наблюдения;
- 👁 анализ возможностей имеющихся систем электропитания, связи и охранного освещения предприятия по обеспечению потребностей вы бранных видов охранных систем и типов технических средств сигнализации в составе планируемой СОП;
- 👁 оценка необходимости дальнейшего (после ввода в эксплуатацию) развития и наращивания СОП;
- 👁 оценка возможностей собственника предприятия по выделению финансовых и материальных средств на создание СОП на данный момент, а также на ее развитие в ближайшей и дальнейшей перспективе и т.п.

Результатом этой работы является оформление в разделе Концепции взглядов собственника (заказчика) на стратегический облик будущей СОП предприятия, оптимизированный под текущие условия его функционирования, разработанную выше модель угроз. При этом облик будущей СОП должен быть основан на финансовых и технических возможностях по ее реализации, как для настоящего момента, так и на ближайшую и дальнейшую перспективы развития предприятия.

На втором этапе осуществляется **детализация** принятых собственником стратегических решений, заключающихся:

1) – в планировании оптимального размещения рубежей на плане зоны периметра, оснащенных выиспользуемых для установки ТСО, либо создающих условия для задержания нарушителя (например, проволочные заграждения и т.п.);

- 👁 при прокладке дополнительных кабельных линий электропитания (ТСО и дополнительного освещения) и передаче извещений (изображения);
- 👁 при оборудовании мест размещения автономного (местного) пульта наблюдения за состоянием СОП предприятия, размещения наряда сил и средств группы охраны;
- 👁 подход позволяет грамотно составить техническое задание на проектирование системы охраны периметра предприятия, а в конечном итоге обеспечить собственнику охраняемого имущества надежную его защиту от несанкционированного доступа посторонних лиц, при этом оцениваются:

а) – возможность обеспечения работы ТСО вспомогательными системами и средствами (электропитанием, линиями связи и т.п.),

б) – необходимость наращивания возможностей сети электропитания и связи (оценка пути, способа и длины прокладки, трудовых и финансовых затрат вновь прокладываемых линий);

2) – в выборе варианта и процедур управления режимами для каждого спланированного рубежа зоны периметра предприятия, а также в выборе способа организации и типа средств передачи извещений от систем сигнализации в планируемой СОП;

3) – в оценке необходимости установки на КПП специального оборудования для досмотра людей и транспорта, контроля за вносом (выносом) и ввозом (вывозом) личных вещей и техники;

4) – в анализе проводимых строительных работ и их возможных объемов и затрат:

☉ при необходимости усилить слабые места в строительных конструкциях периметра инженерными средствами защиты;

☉ при строительстве дополнительных инженерных сооружений, при развертывании автоматизированной СКУД: оборудование точек прохода (проходной предприятия) и проезда транспорта, размещение оборудования контроля и бюро пропусков и т.п.;

5) – в оценке списочного состава сотрудников сил охраны по функциональным задачам, в планировании ее кадрового набора, а при необходимости – в организации его обучения (повышение квалификации);

б) – в выборе вида системы и типа технических средств оповещения дежурных сил охраны, руководства предприятия, а при необходимости – сотрудников предприятия о факте вторжения нарушителя и угрожающем их жизни развитии событий и т.п. (см. рис.)

Решение тактических задач при создании СОП в рамках разработки Концепции позволяет уйти от технических просчетов и выработать экономически приемлемый вариант защиты имущества от НСД нарушителя при вторжении его через зону периметра. Таким образом, разработка Концепции дает возможность заказчику (собственнику) провести квалифицированную оценку состояния периметра предприятия, выявить ключевые особенности в его расположении и применении, а также провести анализ возможных угроз охраняемому имуществу.



Раннее обнаружение нарушителя – задача ПСО

Информационной основой управления в современных автоматизированных системах физической защиты являются средства наружного и внутреннего (в помещениях) обнаружения нарушителей

Периметровые средства обнаружения (ПСО) обычно исполняют роль средств раннего наружного предупреждения, что обеспечивает для пользователя главное преимущество – исключение фактора внезапного нападения, выигрыш необходимого времени для организации реагирования сил охраны, обеспечение возможности пресечения преступной акции до ее реализации. Вместе с тем нет никаких технических ограничений на применение ПСО внутри крупногабаритных помещений (ангаров, складов, производственных корпусов и т.п.), если пользователя устраивают цена и внешний вид аппаратуры. Необходимо отметить, что ПСО, предназначенные для работы на открытом воздухе, обладают повышенной конструктивной и функциональной надежностью по сравнению с аппаратурой, предназначенной для эксплуатации в тепличных комнатных условиях, однако по этой же причине они обычно имеют и более высокую стоимость.

За многолетнюю историю эксплуатации в конструкциях ПСО практически опробованы все известные физические способы обнаружения. Создана масса оригинальных образцов, перечисление которых заняло бы немало места. Но, как показывают результаты эксплуатации, на практике преимущественно используется сравнительно ограниченное число физических способов обнаружения, типов и модификаций ПСО, поскольку в сложных климатических условиях России, Украины и других стран, многие образцы не выдержали испытаний климатом и временем. Поэтому, выбирая ПСО, следует внимательно изучить технические условия эксплуатации относительно требований стандартов, климатических условий района эксплуатации, рельефа местности и пространственной конфигурации рубежей физической защиты. Особое внимание следует уделить стыковочным параметрам аппаратуры по съему информации, электропитанию, способам автоматического, ручного и натурального контроля работоспособности. Обязательным условием эффективной защиты является анализ возможности сопряжения по пространству зоны обнаружения ПСО и формы охраняемого рубежа.

Как подойти к выбору?

Процесс выбора пространственной структуры периметровой системы, оптимального состава компонентов, способов энергоснабжения, съема и структуры обработки сигнальной информации для принятия решений и команд, управляющих силами реагирования и средствами инженерной физической защиты, осуществляемый в проектах создания СФЗ для крупных объектов, получил наименование “стадии и этапы разработки концептуального (технико-экономического) и рабочего (инженерного) проекта управления защитой”. Обычно в основе оптимального выбора лежат критерии “эффективность-стоимость” в двух альтернативах:

первая – получить заданную эффективность физической защиты (вероятность пресечения злоумышленных акций) и при этом минимизировать затраты на создание и эксплуатацию системы;

вторая – при ограниченных затратах создать периметровую систему, обладающую максимально возможной эффективностью. При оценке за-

трат следует помнить крылатую фразу: “Мы не настолько богаты, чтобы покупать дешевые вещи”, т.е. приобретая технику, следует помнить, что ПСО, в основном, рассчитаны на многолетнюю эксплуатацию, и прежде всего нужно осуществить оценку совокупных затрат стоимости аппаратуры, монтажа, пусконаладочных работ и эксплуатационных расходов (обслуживание, ремонт, срок службы, способы контроля работоспособности, регламенты обслуживания, потребление электроэнергии и многое другое). Очень часто высокая цена периметровой техники обуславливает ее высокую надежность и существенно более низкие затраты на инженерно-монтажные, пусконаладочные и эксплуатационные расходы, а в целом, – прямую экономию материальных и финансовых средств пользователя в процессе многолетней эксплуатации.

Что надо знать о компонентах ПСО?

Настоящий раздел охватывает практический перечень компонентов систем периметровой охраны, получивших широкое применение в практике физической защиты и охраны объектов России, Украины и стран СНГ. При этом авторы дают, только общее понятие и рекомендуют проводить консультации с техническими специалистами по актуальным новинкам “сегодняшнего дня”. Устойчивое место на рынке охранных технологий занимают радиотехнические средства обнаружения – РСО. Их отличительными особенностями являются объемная невидимая зона обнаружения, высокая устойчивость к биологическим помехам, воздействию дождя, ветра, тумана, изменению освещенности и солнечной радиации, грозovým разрядам, росе, инею, обледенению, промышленным и транспортным вибрациям, акустическим ударам и шумам, многим другим видам помех. К недостатку следует отнести наличие источников радиоизлучения. Вместе с тем уровень мощности радиоизлучения лучших образцов РСО сегодня не превышает долей милливатта при специальных видах модуляции, радиоизлучения, что весьма затрудняет возможность их обнаружения и обеспечивает полную безопасность обслуживания объекта.

К РСО принято относить однопозиционные и двухпозиционные радиолучевые средства обнаружения (ОРЛСО и ДРЛСО соответственно), кабельно-волновые и проводно-волновые средства обнаружения (КВСО и ПВСО соответственно). Оба – ОРЛСО и ДРЛСО работают обычно в диапазонах радиоволн не ниже дециметрового.

Зона обнаружения (30) имеет объемно-лучевую форму. Обнаружение осуществляется в пределах прямой радиолучевой видимости. Форма (30) определяется диаграммами направленного действия передающей и приемной антенн, и ее геометрические размеры зависят от уровня выставленной чувствительности приемника. КВСО и ДРЛСО работают, как правило, в дециметровом и метровом диапазонах радиоволн. В КВСО объемная (30) формируется вдоль “линии вытекающих волн” (ЛВВ), представленной специальными коаксиальными радиоизлучающими кабелями. Во внешней “оплетке” таких кабелей прорезаны радиопрозрачные отверстия, поэтому КВСО получили наименование “средства обнаружения на линиях вытекающих волн”. В ПВСО объемная (30) формируется между обычными проводными линиями, подвешенными над землей или над заградительными сооружениями. ОРЛСО обычно производится в трех вариантах:

1 – рубежные, предназначенные для блокирования линейного участка периметра;

2 – секторноплощадные – для блокирования секторной площадки, вплоть до круговой;

3 – универсальные – способные блокировать как линейные, так и секторноплощадные участки рубежа.

ДРЛСО представлено приемником и передатчиком, размещаемыми на противоположных сторонах участка рубежа. Для блокирования ломаных рубежей могут быть использованы специальные отражатели зеркального типа и затеняющие экраны. Высокая стабильность (30), автоматический контроль работоспособности, повышенная устойчивость к радиопомехам, пониженная мощность радиоизлучения и ряд других достоинств обусловили преимущественное применение ДРЛСО на периметрах стационарных объектов. К недостаткам следует отнести наличие двух позиций установки прибора. КВСО обычно представлены двумя радиоизлучающими кабелями, прокладываемыми параллельно под поверхностью грунта вдоль блокируемого рубежа. Возможен вариант, когда один из кабелей размещен на заграждении. ПВСО являются новым классом РСО, появившимся на рынке охранных технологий в начале XXI века, когда наконец-то была решена задача обеспечения помехоустойчивости и объемно-равномерной по чувствительности зоны обнаружения вдоль всей длины проводной линии, подвешиваемой над землей или над заграждениями вдоль рубежа.

Инфракрасные средства обнаружения (ИКСО)

Инфракрасные средства обнаружения (ИКСО) основаны на способности обнаруживаемых объектов поглощать, отражать и излучать электромагнитное поле инфракрасного (ИК) диапазона радиоволн. Разделяются на два класса: пассивные, регистрирующие ИК-излучение, и активные, основанные на прерывании ИК-луча.

Виброчувствительные средства обнаружения (ВСО)

Виброчувствительные средства обнаружения (ВСО) основаны на фиксации механических колебаний, вызываемых нарушителем при разрушении или преодолении заграждения. Следует выделить ВСО, работающие на основе дискретных чувствительных элементов (ЧЭ) или акселерометров и работающие на протяженных ЧЭ в виде специальных виброчувствительных кабелей с использованием пьезоэлектрических, трибоэлектрических, магнитоиндукционных, волоконно-оптических и других физических эффектов.

Сейсмо-акустические средства обнаружения (ССО)

Сейсмоакустические средства обнаружения основаны на фиксации звуковых колебаний инфракрасного (сейсмические) и звукового диапазонов частот. В качестве ЧЭ в различных типах ССО применяются микрофонные и геофонные датчики, объединенные в “косу” или трибоэлектрический кабель. Они представляют собой сложные наукоемкие устройства, использующие изощренные алгоритмы обработки и идентификации сигналов.

Магнитометрические средства обнаружения (МСО) – используются в двух случаях:

1 – для обнаружения э.д.с, наводимой при перемещении нарушителем электрического проводника в магнитном поле Земли;

2 – при проносе нарушителем намагниченного металлического предмета.

В первом варианте система электрических проводников размещается в качестве физического барьера, а во втором – используются флюктометры и специальные магниточувствительные кабели, заглубленные в грунт.

Емкостные средства обнаружения (ЕСО)

Емкостные средства обнаружения (ЕСО) относятся к приборам параметрического типа, контролирующим параметры электрической линии (емкость, индуктивность, проводимость). Принцип действия основан на обнаружении изменения электрической емкости линии при приближении к ней нарушителя. Многолетний опыт эксплуатации ЕСО показал, что эти средства в условиях работы на открытом воздухе наиболее эффективны, если выполнены на конструктивно жестких ограждениях (железобетонные плиты, кирпичные стены и т.п.), на которых чувствительный элемент представлен жестким конструктивом (например, электропроводом), установленным на изоляторах над полотном основного ограждения.

Обрывные средства обнаружения (ОСО)

Обрывные средства обнаружения (ОСО) относятся к приборам параметрического типа, контролирующим сопротивление замкнутой электрической цепи. Разрыв проводника или размыкание специального электромеханического контакта вызывают срабатывание прибора и сигнал тревоги. Созданы ОСО, позволяющие контролировать дальность до места обрыва микропроводника с точностью до 10 м на расстоянии до 1 км.

Системы охранной сигнализации (СОС)

Системы охранной сигнализации (СОС) стационарного типа формируются на стационарных объектах охраны путем оптимального выбора промышленных образцов СО, объединяемых в систему с помощью единой системы энергоснабжения, съема сигнальной информации с использованием аппаратуры сбора, обработки и документирования сигнальной охраны в составе специализированных пультов охраны и систем сбора, управления и контроля доступом (СКУД).

Быстроразвертываемые комплексы

Быстроразвертываемые (мобильные) комплексы средств охранной сигнализации, при кажущейся простоте решения технических задач, находили сравнительно ограниченное применение в практике охраны и из-за высокого энергопотребления аппаратуры и отсутствия малогабаритных средств радиосвязи. Достоинствами БКС-ОС являются: возможность быстрой организации сигнального рубежа, малые вес и габариты носимой оператором аппаратуры, длительная непрерывная работа (до 30 суток) от одного комплекта автономных источников питания, совместимость со стационарными СОС.

Периметровые системы телевизионного наблюдения

Телевизионные системы для видеоконтроля охраняемого периметра по своим особенностям можно разбить на несколько групп. В первую очередь следует учитывать жесткие требования к климатическому исполнению видеокамер, устанавливаемых на охраняемом рубеже, – температура и влажность, воздействие ветровых нагрузок. Эти проблемы в большинстве случаев могут быть решены применением специальных герметичных обогреваемых кожухов и кронштейнов для установки камер. Соответствующие жесткие требования также применяются и к поворотным устройствам.

Следующая проблема – работа видеокамер в условиях различной освещенности. Применение камер с повышенной чувствительностью может частично снять проблемы в условиях слабой освещенности, однако в днев-

ное время в этом случае необходимо применять специальные меры к исключению засветки камер.

В большинстве случаев проблема все же решается созданием системы освещения периметра, для чего могут использоваться инфракрасные или обычные прожекторы.

Характерная особенность любой периметровой системы – большое удаление видеокамер от регистрирующего оборудования, что порождает сразу две проблемы: передача видеосигнала и обеспечение видеокамер дистанционным электропитанием. Проблема транспортировки видеосигнала на большие расстояния может быть решена с применением устройств для передачи сигнала по витой паре и использованием различных промежуточных усилителей. Такие решения, к сожалению, ведут к снижению надежности системы и неизбежной потере качества изображения. Существуют специальные системы сбора видеоинформации на больших расстояниях по оптоволоконным линиям, однако стоимость таких систем высока.

Наибольшую эффективность система видеонаблюдения будет иметь, если видеокамеры сопряжены с охранными извещателями или снабжены детекторами активности. Это не совсем одно и то же, хотя в современных системах периметрового видеонаблюдения по показателям обнаружительной надежности и устойчивости работы к помеховым факторам детекторы движения приближаются к периметровым охранным извещателям. Конечно, речь идет не о встроенных в большинство мультиплексоров программных детекторах движения, а о специализированных устройствах, разработанных специально для решения задач периметровой охраны.

Системы сбора, обработки информации и приемно-контрольные пульты

Принципиально системы охранной сигнализации периметров – это, по сути, такие же системы охранной сигнализации, поэтому в качестве их могут применяться любые системы сбора и обработки информации на базе известных приемно-контрольных приборов. Особенно это справедливо для небольших по протяженности охраняемого рубежа и составу оборудования систем. Специфика периметровой охраны проявляется в следующих моментах:

- 👁 для средних и протяженных рубежей (более десятка линейных охранных зон) важно наглядное представление информации, поэтому наибольшее распространение получили системы, позволяющие графически на экране дисплея отображать план охраняемой территории, расположение охранных извещателей и размеры контролируемых ими зон;
- 👁 популярна схема сбора информации по интерфейсной линии (экономия кабеля), но в этом случае на самом периметре размещаются приемно-контрольные приборы малой емкости (до 4 шлейфов), к которым в первую очередь применяются повышенные требования по рабочей температуре и влажности;
- 👁 для систем периметровой охраны актуально совмещение систем сбора и обработки информации и дистанционного электропитания в одном комплексе.

Блоки и системы питания, включая дистанционное управление

Проблема электропитания – основная в системах охраны периметров.

Один вариант. Большинство периметровых извещателей имеет рабочее электропитание 10...30 В. Слаботочное питание в данном случае использовать проблематично, потому что падение напряжения в длинных линиях заставляет использовать медные силовые кабели с большим сечением жил (такое техническое решение мы лично признаем дорогим и некорректным). Применение для электропитания повышенного постоянного напряжения с понижением его с помощью различных самодельных устройств непосредственно в месте установки извещателя вряд ли можно рекомендовать для серьезных систем хотя бы из-за ограниченности такого решения.

Другой вариант – использование линий с питанием 220 В и применение на охраняемом рубеже специальных блоков питания с соответствующими температурными характеристиками. Однако в данном случае при кажущейся на первый взгляд простоте возникает проблема резервирования питания. Для ее решения можно использовать бензо- или дизельные агрегаты с автоматическим запуском, но тогда возникает другая проблема, а именно поддержки такого агрегата в постоянной готовности (использование источников питания типа ЛРЗ финансово неоправданно).

Именно поэтому для периметров протяженностью свыше 3 км применяются специализированные системы дистанционного электропитания, которые могут поставляться как отдельная система, либо находиться в составе комплекса периметровой охраны. Очень актуально наличие возможности дистанционно, с поста охраны изменять параметры настройки охранных извещателей (например, выбор чувствительности одного из нескольких алгоритмов обнаружения и т.п.) в зависимости от изменившихся условий, как помеховых, так и оперативных. Однако пока такие возможности реализованы лишь в отдельных системах зарубежного производства.

Специализированные запирающие устройства

Периметр всегда имеет точки прохода: ворота, калитки. Они, как и любые участки охраняемого периметра, должны надежно контролироваться, но при этом через них осуществляется доступ внутрь охраняемой территории. Для решения этого вопроса применяются специализированные запирающие устройства, которые могут быть механическими и управляемыми (электромеханическими).

Специальные заграждения и элементы конструкций

В настоящее время широко применяются различные средства усиления основного ограждения периметра: козырьки вертикальные и наклонные из сетки, колючей проволоки, армированной колючей ленты. Такие специальные заграждения имеют двойное назначение: создать препятствие для нарушителя при попытке преодоления ограждения через верх (соорудить преодоление с ходу) и создать условия для эффективной работы охрannого периметрового извещателя, например кабельного трибоэлектрического или виброакустического, чувствительный элемент которого размещен непосредственно на заграждении.

Специальные задерживающие устройства. Противотаранные устройства

Использование противотаранных устройств – неотъемлемая масть в мероприятиях по защите объектов повышенной важности. Они могут быть разнообразными по конструкции и классифицируются по своей останавливающей способности.

Спирали из режущей и колючей ленты

Объемные и плоские спирали из армированной колючей ленты позволяют создавать как простые механические, так и сигнализационные заграждения практически любой формы и площади. Предназначены для применения на крупных промышленных и иных режимных объектах повышенной опасности, а также военных объектах.

Вспомогательные системы

Дежурное освещение включается в ручном или автоматическом режиме при наступлении темного времени суток и обозначает для местности линию охраняемого периметра, а также создает условия для нормальной работы системы телевизионного наблюдения. Тревожное освещение, как правило, управляется системой охранной сигнализации и включает освещение того участка, на котором произошло нарушение, тем самым, создавая условия для наряда и воздействуя психологически на нарушителя. Кроме того, в комплекс технических средств охраны периметра могут быть включены система связи с нарядами, система звукового оповещения и др.

Помеховые факторы и нетрадиционные методы защиты периметра

В последнее время во многих издания нашего профиля достаточно часто обсуждаются технические средства охраны, предназначенные для защиты периметра объектов. Приводятся подробные характеристики различных типов ТСО, сравниваются между собой различные средства одного типа, предлагаются новинки и мы должны отметить тот факт, что есть очень хорошие, технические наработки. Не смотря на это, правильно выбрать подходящее средство очень не просто. Одними из самых важных характеристик средства являются стоимость, вероятность правильного обнаружения и вероятность ложных тревог. И если с первыми двумя, обычно, все понятно, то правильно оценить количество ложных тревог, которое будет выдавать то или иное средство, установленное на конкретном объекте, достаточно сложно. Коротко перечислим помеховые факторы, которые могут влиять на работу периметровых средств охраны, при этом в каждом конкретном случаи необходима консультация технического специалиста:

1. Климатические:

- температура в каждой стране – специфична, (например в России: от – 60 до + 60 °С);
- влажность; туман; дождь; гроза; снег; град; наледь; ветер; пыль; песок; солнечная радиация.

2. Фауна: – насекомые; птицы; животные.

3. Флора: трава; кусты; деревья.

4. Условия применения:

- дизайн периметра;
- перемещение вблизи периметра людей, животных, автомобилей, поездов и пр.;
- изгибы периметра по горизонтали и вертикали; характеристики грунта;
- характеристики заграждения (если оно есть);
- наличие луж, ручьев; неровности почвы; наличие или близость крупных предметов;
- близость различных коммуникаций.

5. Промышленные помехи:

- высоковольтные ЛЭП; радиостанции; сотовая связь; мощные электроустановки;
- электрофицированный транспорт;

Авторами перечислены далеко не все помеховые факторы. На специфических объектах их число может возрастать. Например, химически-активная среда, радиационное излучение и др. Естественно, на различные средства перечисленные факторы влияют по-разному. Например, насекомые, никак не влияющие на подавляющее большинство периметровых средств, могут существенно нарушать нормальную работоспособность инфракрасных приборов, закрывая телом чувствительный элемент или создавая непрозрачную паутину. Или зачем нужно знать характеристики грунта? Датчики с точной юстировкой, или определенным усилием натяжения, требуют прочных опор, что в условиях, например, вечной мерзлоты невозможно при обычной установке. Отдельно можно остановиться на собаках, которые появляются внутри или вблизи подавляющего числа охраняемых объектов, особенно где есть пункты питания. Даже объекты Заполярья, находящиеся за десятки и сотни километров от населенных пунктов, – не исключение. Подлезая под ворота и калитки, собаки проникают даже на очень серьезные объекты с трехрубежной системой охраны периметра. Чаше собаки перемещаются стаями, по несколько штук и способны вызвать сигнал тревоги практически у любого средства с зоной обнаружения примыкающей к земле ближе 0,5 – 0,7м. Без ограничения доступа животных в зону обнаружения эффективность охраны такими средствами будет сведена к нулю. Довольно часто основным “помеховым” фактором становится внешний вид охраняемого периметра, особенно для элитных объектов. В таких случаях приходится применять маскируемые или малозаметные средства обнаружения, которые обычно дороже.

Как правило, для объекта охраны существенными являются 5-7 помеховых факторов, не считая климатических. С учетом этих факторов осуществляют выбор средств обнаружения. У каждого средства есть свои “плюсы” и “минусы”, свои ограничения по применению. Как реагирует то, или иное средство на конкретную помеху знают его разработчики или опытные инсталляторы. В торговых организациях не всегда можно получить исчерпывающий ответ. Наиболее распространенными, традиционными, средствами для защиты периметра производственных хозяйственных объектов являются:

- ⑤ вибрационные, емкостные и инфракрасные средства, защищающие верх заграждения;
- ⑤ инфракрасные и радиолучевые средства, установленные на полосу отчуждения (КСП);
- ⑤ вибрационные средства, смонтированные на сетчатых заграждениях.

Наиболее уязвимыми, но более дешевыми являются инфракрасные средства обнаружения.

Обычно в таком порядке строятся 3-х рубежные системы охраны периметра. На менее важных объектах применяется какой-нибудь один вариант, иногда два. Список перечисленных средств достаточно широк и выбор их зависит, в том числе, от финансовых возможностей заказчика.

Необходимые условия применения указанных вариантов:

для 1-го – добротный, прочный забор, отсутствие примыкающих веток деревьев;

для 2-го – выровненная, без ям и бугров полоса отчуждения вдоль периметра шириной 3-6 метров, отсутствие на ней деревьев, кустов и высокой травы;

для 3-го – наличие качественного сетчатого ограждения, отсутствие примыкающих к нему деревьев, кустов и высокой травы.

Очень часто к защите периметра может относиться защита ворот и калиток, крыш и стен зданий, переходов трубопроводов и коммуникаций над, и под ограждением, водостоки и др. В каждом таком случае может потребоваться свой, нетрадиционный подход к поставленной задаче. Особый подход нужен к защите периметра дачных и коттеджных участков. Одним из основных требований к средствам обнаружения является сохранение соответствующего дизайна участка. Поэтому сразу отпадают средства связанные с возведением дополнительных козырьков или ограждений. Если не брать во внимание дорогих экзотических, преимущественно импортных, устройств, требующих соответствующей инженерной подготовки и обслуживания, то наиболее приемлемыми здесь являются **инфракрасные, радиолучевые и радиоволновые средства**.

Основное отличие этих средств – рабочая частота, и соответственно длина волны излучаемого сигнала. Известно, чем короче длина волны, тем проще организовать направленность приемо-передающих антенн, и соответственно узкую зону обнаружения. В то же время, если объект сравним с длиной волны или много больше, то, попадая в зону обнаружения, может оказывать существенное влияние на параметры принимаемого сигнала, амплитуду и фазу. Чем больше объект, тем больше влияние при прочих равных условиях. Таким образом, **для инфракрасных средств**, с длиной волны, составляющей сотые доли миллиметра, туман, пыль, дождь, снег уже являются существенными помеховыми факторами, с которыми борются, используя различные алгоритмы обработки сигналов. Другим видом помех являются пролетающие птицы, падающие листья и т.п., влияние которого удастся уменьшить, используя двух и более лучевые средства. В связи с большим количеством помеховых факторов, современные инфракрасные средства используют микропроцессорную обработку сигналов.

К **радиолучевым** относят миллиметровые, сантиметровые и дециметровые средства, с соответствующими длинами волн излучаемого сигнала, хотя последние имеют достаточно широкую зону обнаружения. Чем больше длина волны, тем меньше влияние на параметры входного сигнала вышеперечисленных факторов, в этом случае существенное преимущество имеют дециметровые средства. Однако, за счет слабой направленности, максимальная длина блокируемого одним средством участка не превышает обычно 50-100 метров, существуют ограничения по перемещению вблизи зоны обнаружения людей и транспортных средств, близкому расположению больших кустов и деревьев.

Еще меньше реагируют на внешние помехи **радиоволновые** средства обнаружения с длиной волны метрового диапазона. Остаются незамеченными не только птицы, но и мелкие животные. Растительность, кусты и деревья могут находиться непосредственно в зоне обнаружения. Однако, остаются некоторые ограничения по перемещению транспорта вблизи зоны обнаружения. Выше приведены общие физические аспекты сигналообразования для радиотехнических средств обнаружения. Их реакция на эфирные, промышленные помехи и другие особенности зависят от структуры, схемотехники, алгоритмов обработки и вариантов применения конкретного средства. Нет средств, работоспособность которых не зависит ни от каких помеховых факторов.

Необходимо учитывать, что воздействие большинства помех носит вероятностный характер. Конкретное событие для данного объекта может происходить раз в год, или раз в минуту. Можно привести некоторые примеры. Если средство будет реагировать на проезд автомобиля, а случается это раз 8 месяц, то с этим можно смириться. Если средство реагирует на пролет птиц всего лишь один раз из десяти, а таких пролетов несколько сот в сутки, его установка недопустима. Если помехи происходят днем, когда средство снято с охраны и отсутствуют вечером и ночью, то ими можно пренебречь. Частый случай, когда средство устанавливается на забор между двумя соседними дачными участками и может реагировать на подход с внешней стороны.

В случае, когда с внутренней стороны периметра по тропе наряда перемещается часовой, и средство охраны его обнаруживает, информация, получаемая оператором, является только полезной и не относится к разряду ложных тревог. Когда средство срабатывает по сравнительно редкому известному событию, например открывание ворот, включение поливальной установки и т.п., это можно учесть.

Понятно, что трудно сделать правильный выбор средства охраны периметра, не обладая необходимой полной информацией об объекте. С учетом всех полученных сведений определяют подходящий тип средств обнаружения и варианты их установки. Затем, сравнивая тактико-технические, стоимостные и пр. характеристики, выбирают конкретные средства. В конце 90-х, радиотехнические средства обнаружения дециметрового диапазона начали использовать в качестве радиолучевых для охраны периметра, а на начало 2008 года мы уже имеем более современные радиотехнические средства.

Этим объясняется **высокая универсальность применения** таких средств в нетрадиционных вариантах защиты периметра. С их помощью можно организовать как протяженную, так и необходимую объемную зону обнаружения. Они могут перекрывать крыши, проемы, окна, внешние лестницы зданий и сооружений, блокировать трубопроводы и другие металлоконструкции, выходящие за периметр. При установке не требуется юстировка, нет высоких требований по жесткости крепления блоков, допускаются колебания до нескольких сантиметров. При защите периметра допускаются большие перепады неровностей почвы, высота травы и

снежного покрова, чем у других радиолучевых средств, отсутствуют “мертвые” зоны. Каждый охраняемый объект индивидуален. Трудно предусмотреть заранее все возможные особенности. Необходимые консультации и советы по конкретному объекту, можно получить у разработчиков средств охраны.

Заграждения – как элемент комплекса технических средств охраны периметра

Заграждение в составе комплекса технических средств охраны (КТСО) выполняет роль преграды, изменяющей условия передвижения нарушителя по направлению к охраняемому объекту. Все периметровые средства обнаружения (извещатели), устанавливаемые вблизи или на заграждении, можно разделить **на 3 категории**:

1. Осуществляющие сигнализационное блокирование *непосредственно* заграждения, которое в процессе вторжения подвергается механическим деформациям;

2. Осуществляющие сигнализационное блокирование некоторой зоны пространства (зоны обнаружения) *вблизи* заграждения;

3. Реагирующие как на деформации заграждения, так и на изменение физического поля вблизи него, вызванного нарушителем.

В первом случае требуется, чтобы преодоление его нарушителем сопровождалось возникновением каких-либо полезных сигналов в конструкциях заграждения, которые бы надежно дискриминировались от помех, вызванных различными природно-климатическими и промышленными факторами, также непосредственно воздействующими на заграждение.

Во втором случае необходимо, чтобы заграждение так изменяло параметры движения нарушителя (например, уменьшало скорость или изменяло направление движения в нужную сторону), чтобы его обнаружение было достоверным на фоне помех.

В третьем случае к заграждению предъявляются и те, и другие требования. Заграждение представляет собой физический барьер – вид ограждения, препятствующий свободному входу нарушителя на территорию объекта. Как нам представляется, в настоящее время попытки построения эффективного КТСО периметра любого объекта без устройства заграждения обречены на неудачу по нескольким причинам:

- ❖ высокий (не снижающийся) уровень криминализации населения;
- ❖ низкий правовой уровень имущественных отношений, отсутствие права владения и применения оружия при посягательстве на собственность, в том числе земельную;
- ❖ заграждение, с одной стороны, “отсекает” большую часть животных, которые являются существенным помеховым фактором, а также случайных прохожих и т.д., с другой стороны, не позволяя потеряться играющим детям или домашним животным;
- ❖ заграждение является весомым психологическим фактором для потенциального нарушителя;
- ❖ заграждение препятствует быстрому отходу нарушителя.

Все заграждения в зависимости от назначения можно **разделить на 4 типа:**



Видимость сквозь заграждение определяется конструкцией, выбираемой заказчиком в соответствии с его пониманием безопасности и эстетики.

В России, Украине и странах СНГ – традиционно наиболее распространенными являются сплошные (непрозрачные) заграждения. К преимуществам таких заграждений отнесем:

- возможность скрытного передвижения людей по объекту, особенно вблизи заграждения с внутренней стороны (например, реакция охраны на сигнал тревоги);
- скрытность установки средств обнаружения (СО) во внутренней части периметра;
- затруднение визуального сбора информации о характере производственной деятельности объекта, составе и тактике действия подразделения охраны.

Недостатками заграждения являются высокая стоимость и трудоемкость возведения, а также обратная непрозрачность – для наблюдения изнутри за перемещениями или действиями людей с внешней стороны периметра. Впрочем, для объекта с периметром более 300...500 м, когда дальность наблюдения (до границы участка) превышает 50 м, последний недостаток является общим и может быть устранен при использовании системы теле наблюдения, освещения, (или ИК-подсветки). Прозрачные заграждения (например, сеточные, решетчатые) относительно дешевле, трудоемкость на их возведение значительно ниже, однако они не обеспечивают вышеописанной скрытности.

Вместе с тем, при рассмотрении заграждения как элемента комплекса технических средств охраны, необходимо учитывать следующие соображения. По мнению экспертов ряда фирм-производителей, средств охраны периметров, в том числе – Израиль, наиболее эффективным заграждением являются так называемые “мягкие” заборы, выполненные из различных металлических сеток, проволоки или армированной колючей ленты. Любое воздействие на такой забор с целью преодоления (перелаз, разрушение полотна забора, подкоп) неизбежно приводит к колебаниям полотна заграждения. В настоящее время существует целый арсенал кабельных извещателей, способных преобразовать эти колебания в сигнал тревоги.

Высота заграждения является важным параметром, который определяет его проходимость (путем перелаза), время преодоления, опасность падения, которой подвергает себя нарушитель наверху. В принципе, чем она больше, тем лучше, – по этой причине не рекомендуются заграждения высотой менее 1,5 м, которые могут быть преодолены прыжком. С другой

стороны, заграждения высотой свыше 4 м (известны примеры высотой до 6 м), уже практически ничего не прибавляя с точки зрения охранных качеств, выглядят не эстетично, требуют дополнительного конструкционного усиления ввиду возрастания парусности. В целом, высота заграждения должна определяться разумным компромиссом между охранной функцией и эстетикой.

Полоса отчуждения. Из вышесказанного следует, что проектирование и изготовление заграждения, возводимое на периметре охраняемого объекта, должно проходить при участии и под контролем специалистов в области периметровой охраны. В конце главы обращаем внимание на важное обстоятельство, зачастую игнорируемое при построении КТСО – **полосу грунта шириной до 3 м**, примыкающую к заграждению с внутренней стороны периметра объекта, которую назовем **полосой отчуждения**. Она предназначена для возможной установки периметрового СО (в том числе и в грунт) и формирования зоны обнаружения, что накладывает ограничения на посадку деревьев, кустов, а также на перемещение людей в этой зоне. Ее необходимость обусловлена тем, что:

1. Деревья и кусты в непосредственной близости от заграждения оказывают существенное помеховое влияние на любое периметровое СО, (при ветре, дожде, снегопаде, неконтролируемом отращивании ветвей);

2. Крупные деревья дают дополнительную возможность нарушителю преодолеть рубеж (по стволу);

3. “Непрозрачные” деревья и кусты делают неработоспособными многие виды СО (например, радиотехнические, активные ИК);

4. Перемещения людей и собак вблизи заграждения могут вызывать ложные тревоги, что приводит к необходимости в дневное время выключать периметровые СО, чем может воспользоваться нарушитель.

Если полоса отчуждения по каким-либо причинам не может быть сформирована, а вдоль заграждения с внутренней стороны растут деревья, то, как показывает практика, это приводит к невозможности эффективной защиты периметра от вторжения подготовленных нарушителей. Возможным становится только сигнализационное блокирование заграждений от отдельных видов преодолений “нормальным” нарушителем при некотором снижении потенциальных характеристик средств обнаружения.

Автономные и быстро развертываемые системы

Для современных систем охраны периметра – характерно большое количество разнообразных используемых принципов и конструкций. Такие системы дают возможность в короткое время организовать охрану периметра даже на неподготовленных территориях. В последние годы заметный интерес проявляется к автономным охранным системам, которые можно оперативно развернуть в полевых условиях. Для таких систем в ряде случаев используют беспроводные датчики с автономным питанием. Американские фирмы выпускают быстро разворачиваемые системы с использующую двухпозиционные радиолучевые датчики. Сменные антенны обеспечивают выбор оптимальных геометрических параметров чувствительной зоны. Выбор частоты модуляции передатчиков позволяет устранить межзональные помехи. Системы питаются от аккумуляторных батарей, которых хватает на 190 часов работы. Для передачи сигналов тревоги используется радиопередатчик, подключаемый к выходу приемного

блока комплекта. В портативных и быстро разворачиваемых системах охраны используют:

- 👁️ датчики типа СВЧ лучевые;
- 👁️ пассивные инфракрасные датчики;
- 👁️ радиолучевые системы, или двухпозиционные датчики ;
- 👁️ радиоволновые системы;
- 👁️ системы с вибрационно-чувствительными кабелями и сенсорными кабелями;
- 👁️ универсальные системы Classik 2000 с автономным питанием и геофонными сенсорами;
- 👁️ очень много других, более современных технических новинок, (в каждом конкретном случае – Вам необходима консультация с техническими специалистами по охране периметра).

Мы дадим общее понятие о работе специальной универсальной системы. Каждый датчик такой системы снабжен встроенным источником питания и объединен с миниатюрным радиопередатчиком сигналов тревоги. Приемная станция контролирует до 100 датчиков. Каждый датчик обеспечивает зону чувствительности средней длиной 30 м, комплект с 24-мя датчиками позволяет защитить периметр протяженностью до 750 м. В корпусе каждого датчика установлен радиопередатчик **сигналов тревоги** с радиусом действия не менее 300 м. Встроенная в датчик литиевая батарея обеспечивает работу датчика в течение нескольких лет.

Наведенного примера и всего сказанного, вывод в том, что периметральная охранная система должна быть надежной, экономичной, помехозащищенной и малозаметной. Специфика (как российских так и стран СНГ) – условий эксплуатации накладывает дополнительные требования, связанные с колебаниями температуры, сильными ветрами, снегопадами, метелями, градом и т.п. Если учитывать также и экономические ограничения отечественных заказчиков, то выбор периметральной системы часто становится весьма непростым делом. Очевидно, что из множества современных периметральных охранных систем невозможно выделить одну, которая была бы универсальной и наилучшей - во всех точках зрения. При выборе и проектировании системы охраны необходимо учитывать множество факторов - рельеф местности, топографию объекта, конструкцию и материал ограды, окружающие условия, промышленные помехи, организацию службы охраны и др. Поэтому системные интеграторы должны хорошо ориентироваться в имеющемся разнообразии выпускаемых систем, учитывать их особенности и специфику применения в условиях Вашей страны.

Ложные тревоги охранной системы периметра

Тема вибрационных извещателей, поднята нами в качестве иллюстрации, для раскрытия общих взглядов и подходов к обеспечению достоверности обнаружения нарушителя, может быть отнесено к любому другому классу периметровых извещателей. Развитие разработки и производства периметровых извещателей делает актуальным, необходимостью выработки единых подходов к оценке их эффективности или содержанию их потребительских свойств. Мы неоднократно акцентировали, что вы-

данная информация как и денежная политика стоимости товара, со временем претерпевают очень сильные изменения. Следите за информацией.

... Итак, как получить сигнал тревоги с первичного преобразователя, сегодня понятно многим, при этом любой кабель связи, обладающий трибоэлектрическим эффектом, может стать чувствительным элементом вибрационного извещателя. Не вдаваясь в физические дебри, и не повторяя выше сказанное, мы должны подчеркнуть, что принцип формирования сигнала в кабелях связан с тем, что при изменениях геометрии кабеля происходят локальные перераспределения электрических зарядов в его структуре, что в свою очередь вызывает протекание микротоков, которые и улавливаются специальными усилителями. Существуют специально изготовленные кабели, **обладающие рядом преимуществ:**

- 👁️ отсутствие (максимальное снижение) уровня собственных трибоэлектрических шумов позволяет “безнаказанно” повышать чувствительность усилителя, т.е. делать извещатель более чувствительным без увеличения количества ложных тревог, вызванных внутренними шумами;
- 👁️ специальное проектирование кабелей позволяет учесть особенности их эксплуатации, поэтому такие кабели, как правило, значительно тоньше и гибче, чем неспециальные, а также допускают практически любой угол изгиба.

Кроме того, существуют специальные кабели с защитной металлизированной оплеткой, предохраняющие чувствительный элемент от повреждений. Вместе с тем, такие кабели имеют значительно большую погонную стоимость, чем неспециальные. Это конечно ниже, чем стоимость виброакустических кабелей (Великобритания), однако даже при этом стоимость защищаемого периметра извещателем с таким чувствительным элементом выходит за границу \$50,00, что тяжело переваривается большинством отечественных заказчиков. Для извещателей, которые используют неспециальные кабели с “паразитным” трибоэффектом, единственным преимуществом является низкая стоимость кабелей. При этом уровень собственных трибошумов весьма значителен и, что более важно, случаен: он зависит от партии кабеля, использованных при изготовлении материалов, технологии производства и т.д. Парадоксально, но в данном случае высокая чувствительность усилителя не является преимуществом: все равно нельзя поднять чувствительность извещателя выше уровня собственных шумов в трибокабеле. Поэтому демонстрация высокой чувствительности системы в лабораторных условиях (различного рода “шумов”), в которых отсутствуют помеховые факторы, в избытке присутствующие при открытой установке, не должна вводить в заблуждение специалистов. Получение сигналов первичным преобразователем – кабельным чувствительным элементом вибрационного извещателя – в обоих случаях одинаково: кабель должен быть жестко связан со средой, на которую оказывает воздействие нарушитель, преодолевающий контролируемый рубеж. В качестве такой среды могут быть:

- 👁️ полотно ограждения из гибких металлических материалов: сетки, колючей проволоки, спирали АКЛ, листового металла и т.п.
- 👁️ полотно ограждения из твердых металлических решеток, стены зданий, бетонные ограждения;

👁️ грунт.

Первичный преобразователь сформировал сигнал, усилительный каскад отработал усиление, и что же дальше?.. А вот здесь техника в общем-то заканчивается, и начинается нечто иное. Вернее, вместе с техническими аспектами обработки сигнала и превращения его в достоверное сообщение о нарушителе появляются некоторые вопросы, имеющее отношение к концепции построения периметровых извещателей и всей системы охраны объекта в целом. Ведь понятно, что на извещатель может оказывать воздействие не только нарушитель... (но и многочисленные помеховые факторы, чем, собственно, и “славятся” периметровые извещатели). И зачастую сигнатура воздействия на ограждение, например, порывов ветра, падающих с дерева веток, взлет и посадка птиц поразительно похожи на воздействие нарушителя при перелазе.

Периметровый охранный извещатель имеет две основные характеристики, составляющие его, так сказать, потребительскую сущность:

- 1) – вероятность обнаружения,
- 2) – устойчивость к помехам.

Простыми словами, он должен обнаруживать нарушителя и не обнаруживать все остальное: снег, ветер, ветки деревьев, птиц и животных, электромагнитные наводки, и т.д. и “п. Эти характеристики взаимосвязаны: они имеют смысл только вместе. Разбить эту фразу на две независимые половинки просто невозможно: каждая из них будет лишена всякого смысла, потому что не даст никакой информации о потребительских свойствах извещателя. Никому не нужна система обнаружения с вероятностью обнаружения нарушителя 0,98, если каждые 10 минут от нее поступают ложные тревоги, точно так же не нужна система, не реагирующая на преодоления нарушителем, но имеющая очень высокую наработку на ложный сигнал тревоги!

И вот тут-то и начинаются странности: ни в одном техническом документе на эти извещатели нет характеристики. Все дело в том, что до сих пор производители и “эксплуататоры” не могут (а, возможно, и не хотят) договориться, что это такое и как это измерять. А кому-то, например, недобросовестным производителям просто на руку эта неразбериха терминов и понятий, позволяющая преследовать какие-то цели, к безопасности объектов отношения не имеющие. Существуют некие, иногда очень хорошие, отраслевые стандарты, и продолжают существовать другие целые отрасли и структуры, которые демонстративно эти стандарты игнорируют (“негоже нам руководствоваться стандартами чужой отрасли, там никто ни в чем не разбирается”). Например, довольно исчерпывающе термины и понятия, а также методики их оценки определяются в документе, разработанном в СНПО “Элерон”, РТМ LU164-85 “Руководящий технический материал: оценка основных тактико-технических характеристик средств обнаружения”. Реалии сегодняшнего дня требуют более современных подходов в решении этих вопросов.

Зачастую на всякого рода испытаниях или показах ограничиваются только проверкой чувствительности (вероятности обнаружения) извещателя. Срабатывание системы от первого же касания проверяющего (или косога взгляда) обычно оказывает неизгладимое впечатление на всякого рода ангажированных или некомпетентных представителей заказчика, но не имеет ничего общего с понятиями “охранная система” и “безопасность

объекта”, так как при этом, как правило, о помехоустойчивости вообще говорить не приходится. __Итак, что такое “ложное срабатывание охранной системы” и к каким последствиям приводит большое количество этих самых ложных срабатываний, гениально показал частный детектив Саймон Дермотт, (герой Питера О’Тулла) в фильме “Как украсть миллион”. Запуская из укромного места детскую вертушку, которая в полете воздействовала на лучи активного инфракрасного извещателя, он добился нескольких тревог за ночь. Вертушка, подобно бумерангу, каждый раз возвращалась к нему, охранники не могли установить причину тревоги, в результате чего система охраны была признана неисправной и отключена.

Таким образом, еще в 1966 году американский режиссер Уильям Уайлдер показал всему миру, что **частые ложные тревоги охранной системы эквивалентны ее неработоспособности!** Но даже сегодня находятся “специалисты”, обманывающие себя (а чаще заказчика), уверяя, что ничего страшного в ложных тревогах нет! Главное – чтобы нарушителя обнаружили, а по ложным тревогам охранники как-нибудь побегут. Это ошибка, долго они не будут бегать. Большое количество ложных тревог способно поставить крест на авторитете любой охранной системы на любом объекте. Возникает – “привыкание”, за которым следует – “игнорирование”, а затем – “отключение” за ненадобностью. А сколько нужно этого – “большого количества”?

Авторы утверждают, что если на объекте случается 1 ложная “сработка” тревоги в сутки, то это можно считать приемлемым. При этом необходимо сказать:

- 👁️ протяженность периметра роли особой не играет, если по тревогам действует одна и та же смена охраны;
- 👁️ для охраны совершенно безразлично, упала ли это шапка снега на ограждение, подул ли сильный ветер или под ограждением протиснулась собака, по размерам сопоставимая с нарушителем.

Для среднего периметра участка протяженностью 1 км и более, контролируемого одним извещателем, наработка 100 м. на ложный сигнал тревоги на один участок (извещатель) должна составлять не менее 240 час. Если периметр 5 км – требования к извещателям резко возрастают и их наработка должна составлять 600-1200 часов. Таким образом, чем длиннее периметр, тем надежнее должен быть извещатель. Общепринятые европейские представления о периметровых извещателях соответствуют величине 720 часов (или 1 месяц). __На 5 км прибор с наработкой 240 часов даст общую наработку системы на ложную тревогу 4,8 часа, т.е. 5 тревог в сутки. И это, при идеально смонтированном ограждении и правильной установке приборов. И вот тут встает во весь рост вопрос: а что такое вообще ложная “сработка” (ложный сигнал тревоги), так называемый “ложняк”? На сегодняшний день ни один нормативный документ не содержит четкого определения, что дает возможность предлагать самые фантастические интерпретации.

Адекватное определение, на наш взгляд, такое: любой сигнал тревоги, не связанный с преодолением охраняемого рубежа нарушителем или сотрудником охраны в качестве проверки, является ложным. Самое нелепое определение мы слышали совсем недавно от одного компетентного сотрудника очень уважаемого ведомства: любой сигнал тревоги от любого воздействия на ограждение не является ложной тревогой, так как извеща-

тель должен обнаруживать любое воздействие. Иначе как же он обнаружит нарушителя? Без слов !

Три подхода борьбы с ложными тревогами

Итак, как же бороться с ложными тревогами. Вот тут-то и хочется перейти к описанию возможных способов, исходя из имеющихся на рынке безопасности средств. В настоящее время на рынке периметровых вибрационных извещателей присутствуют в виде технических воплощений три различных, достаточно ярко выраженных подхода.

Итак, **подход первый**. Ограничить обработку сигнала только аналоговой частью, выставив порог превышения сигналом некоего фиксированного уровня. Принцип обработки сигнала, по информации производителя: “В БОС происходит фильтрация и усиление сигнала и, в случае превышения порогового значения, – формирование тревожного извещения з виде размыкания контактов реле и свечения индикатора”. Существует, и некая регулировка накопления таких превышений, но ею пользоваться, мы не рекомендуем: *“Режим накопления сигнала рекомендуется применять в исключительных случаях, только при необходимости обнаружения серии повторяющихся сигналов”*. (Извещатель охранный периметровый – три-бозлектрический Тюрза-035П”. Руководство по эксплуатации ФРKM.425160.035-01 РЭ 2005г.). У такого подхода есть безусловное преимущество – отсутствие какой, бы то ни было адаптации к изменяющимся условиям эксплуатации исключает возможность ухищренного преодоления системы путем зашумления извещателя. Нарботка на ложный с сигнал тревоги по определению не может быть высокой, что особенно ярко проявляется на длинных периметрах охраны.

Подход второй. Ввести цифровую процессорную обработку поступающих от усилительного каскада сигналов, обрабатывая максимально возможное количество информационных признаков, и на этом пытаться отделить ложные сигналы от сигналов тревог. Возможность точной (фиксированной) настройки извещателя по нескольким информационным признакам (не только порогового превышения) под конкретное ограждение позволяет в несколько раз повысить помехоустойчивость извещателя по сравнению с предыдущим случаем и исключить жесткую зависимость повышения чувствительности и возрастания количества ложных тревог.

Вместе с тем, извещатель не может самостоятельно изменить настройки при изменении внешних условий эксплуатации, например, сезонной смены направления и силы ветра, смены типа и интенсивности атмосферных осадков и т.п., и в процессе эксплуатации извещатель предполагает сезонные подстройки для обеспечения заявленных характеристик.

Подход третий (Galdor-Secotec, Израиль). Вводится цифровая процессорная обработка сигнала, обрабатывается максимально возможное количество информационных признаков, но при этом исключается фиксирование параметров. То есть жестко задаются не значения параметров, а интервалы, в которых эти параметры могут изменяться автоматически процессором при изменении внешних условий. Характерный пример – извещатель “Мультисенсор MS-018B”. В данном случае чувствительный кабель, закрепленный на ограждении или установленный з грунт, используется и для анализа внешней обстановки, т.е. постоянно происходит процесс анализа внешнего шума. Такой подход позволяет при построении систем периметровой охраны реализовать **следующие функции:**

а) – дистанционную, с поста охраны, настройку извещателей;
б) – сохранение, хранение и загрузку в извещатель файлов настройки для конкретных типов ограждений и грунтов, что значительно сокращает время настройки;

в) – введение совместного (коррелированного) анализа внешнего шума от всех извещателей системы или флангов одного извещателя, что значительно повышает помехоустойчивость системы в целом.

Такого типа извещатель может быть построен, только с применением специально изготовливаемого кабеля с пониженным уровнем трибоэлектрических шумов, что вкупе с высокоинтеллектуальной обработкой сигналов обуславливает довольно высокую стоимость комплекта. Практика показывает, что все три подхода к созданию вибрационных извещателей с кабельным чувствительным элементом имеют право на существование. Вместе с тем, при синтезе периметровых охранных систем необходимо понимать возможности, а значит, и область применения различных подходов к обеспечению помехоустойчивости системы, а так же учитывать все выше перечисленные факторы.

Следите за новинками по охранной сигнализации и системах видео наблюдения – ведущих производителей: Commax, TVS, Acula, Ebelco, Fighter, Hyudai telecom и консультируйтесь с специалистами.

В качестве примера, мы продемонстрируем несколько новинок систем видеонаблюдения от Samsung Techwin по состоянию на конец 2007 и начало 2008 г.г.

Новинки систем видеонаблюдения

В июне 2007 года на украинский рынок систем видеонаблюдения, пришёл известный гигант данной отрасли – Samsung Techwin. Эта компания является подразделением всемирно известного концерна Самсунг. Она была основана в 1977 году и занимается, в частности, производством высокотехнологичного оборудования для систем видеонаблюдения. Любопытно отметить, что первыми клиентами Самсунг были представители силовых структур, всегда предъявляющие повышенные требования к качеству аппаратуры. Завоевав доверие военных и полицейских, специалисты компании вышли и на гражданский рынок. Сочетание высоких функциональных возможностей оборудования Самсунг с его исключительной надежностью (вот где сказались годы сотрудничества с армией!) и демократичными ценами помогло корейской фирме быстро занять главенствующее положение на мировом рынке систем видеонаблюдения. Но этот успех не заставил компанию почитать на лаврах, напротив, стремясь упрочить свои позиции, она непрерывно совершенствует технологии, чтобы сделать продукцию еще более эффективной и в то же время доступной.

Специалисты Самсунг резонно полагают, что для достижения этой цели они должны постоянно немного опережать общий уровень развития отрасли. Последним на сегодня результатом такого подхода стала новая линия камер, официальный релиз которой состоялся совсем недавно. В Украине она появится уже в этом 2008 году, так что самое время ознакомиться с некоторыми из новинок корейской компании. По состоянию на 2008 год, наши авторы представят читателю:

1.) Вне зависимости от света, SIR-4150 – это высококачественное устройство, призванное обеспечить исключительно четкую картинку вне

зависимости от места установки – будь то склад, производственное помещение, двор или магазин.

Камера оснащена инфракрасными светодиодами, что позволяет ей видеть и различать объекты в полной темноте (с уровнем освещения 0 лк) и давать картинку высокой четкости в любое время суток. Этому способствует и возможность автоматически убирать инфракрасный фильтр, иными словами, аппарат имеет все необходимое оборудование для полноценной работы в режиме «День/Ночь».

К преимуществам SIR-4150 также относится использование SSNR. Данная технология эффективно убирает шумы и позволяет получать более качественный сигнал из светочувствительного элемента камеры, так что едва ли у пользователя возникнут нарекания на картинку при работе с данным устройством. На высоком уровне находятся и показатели надежности SIR-4150. Камера имеет уровень защиты IP-65, что говорит о ее высокой водо- и пыленепроницаемости, а также наличии солнцезащитного козырька. В сочетании с высокой четкостью картинки вне зависимости от уровня освещения и наличием 3,8—9,5 мм варифокального объектива для гибкой настройки угла обзора это делает SIR-4150 одной из самых привлекательных новинок 2008 года от Самсунг.

2.) Высшая лига видео наблюдения – камера SNH-735.

Первое, на что обращаешь внимание при знакомстве с камерой SNH-735 – ее впечатляющее разрешение – 560 ТВЛ в цветном и 700 ТВЛ в черно-белом режиме. В основе функционала SHC-735 лежат последние технологии обработки изображений от Samsung. В данном случае речь идет о такой интересной инновации, как SV-IV – представителя четвертого поколения цифровых обработчиков сигналов серии Super Vision. Это патентованная Самсунгом технология визуализации и настраиваемой обработки изображения с элементами трехмерного подавления шумов видеочастоты. Ее использование заметно повышает качество картинки и эффективно компенсирует переотраженный свет. Также SV-IV делает возможным наблюдение при низком (вплоть до 0,0004 лк) освещении. При этом четкость изображения практически не страдает.

Как и подобает камере премиум-класса, SHC-735 обладает целым набором «умных» функций, таких, как интеллектуальное обнаружение движения. При этом, используя последние достижения науки и техники, создатели SHC-735 не забыли о таких само собой разумеющихся вещах, как режим «День/Ночь» и компенсация встряски.

Подумали разработчики камеры и об удобстве потребителя – упрощение эксплуатации и многоязычное меню делает возможным установку SHC-735 рядовым пользователем практически любой страны мира.

И это лишь малая толика возможностей, которыми обладает это устройство. Так что оптимизм представителей Самсунг (они заявили, что выход SHC-735 призван укрепить лидерские позиции компании на рынке камер премиум-класса) вполне объясним и оправдан.

3.) На шаг вперед – сетевые технологии, сетевая PTZ – камера SNP 3300.

Еще одной примечательной новинкой 2008 года есть сетевая PTZ – камера SNP 3300 – с 30-кратным увеличением. В пользу правоты данного утверждения говорит многое. Например, то, что в SNP-3300 используется чип SV III DSP – еще одна технология, запатентованная Самсунг. Ее главное преимущество – способность обеспечивать сверхвысокую чувст-

вительность: отчетливую и яркую картинку удается получить даже при очень низком освещении (до 0,0006 люкс). Впечатляет и разрешение камеры (520 ТВЛ в цветном режиме), и возможности 128 предустановок. Наличие режима «День/Ночь» и различные аксессуары для удобной установки на условиях заказчика по низкой цене на этом фоне выглядят приятным бонусом.

Немаловажным (и очень актуальным для нашего рынка) преимуществом данной новинки представляется возможность ее использования с уже существующими аналоговыми камерами, поскольку SNP-3300 имеет аналоговый байонетный коннектор на выход в добавку к сетевому выходу.

Но и это еще не все. Камера обладает функцией Wed Viewer и 16-канальным ПО комплексного управления, связанным с серией iPOLIS. Используя Wed Viewer, за изображением, поступающим с камеры, могут одновременно следить в режиме реального времени до 20 пользователей вне зависимости от их местоположения – ведь Интернет в наше время уже почти вездесущ. А по комплексного управления Network Mapadeq предоставляет триплексную систему, делающую возможными удаленный контроль, хранение, наблюдение и воспроизведение для всех сетевых продуктов Самсунг. И это существенный шаг вперед в плане повышения производительности сети.

4.) Купольный High-tech, камера SIR-4250, обращает на себя внимание купольная камера SIR-4250 с

оборудованными инфракрасными прожекторами. Разработчики утверждают, что их творение будет успешно работать в любое время суток (в том числе в полной темноте), поддерживать протокол RS-485 и обладать высокой (до 0,005 лк) чувствительностью. Повысить четкость изображения – призвана SSNR. Ну а наличие встроенного 3,8-9,5мм варифокального объектива и отличное разрешение (520 ТВЛ в цвете), похоже, станут общими отличительными особенностями большинства камер новой линии Самсунг, в том числе и SIR-4250.

Купольная WDR-камере сверхвысокого разрешения SID-560, способна давать четкую картинку, до 560 ТВЛ-линий в цветном режиме и до 700 – в черно-белом, дополнительно имеет встроенный 3,8-9,5 мм варифокальный объектив, многоязычное меню, стабилизатор цифрового изображения и работает в режиме «День/Ночь». Качество ночного изображения будет повышено продвинутым SSNR II. Как видим, специалисты Самсунг верны себе, продолжая делать упор на высокое качество изображения, максимальное разрешение и обеспечение комфортной работы с камерой любому пользователю вне зависимости от его региональной принадлежности и навыков работы с подобной аппаратурой.

5.) «Пегас-06» – охранно-пожарная сигнализация представлена ООО «Аргус-Информ», которая является разработчиком пультового оборудования и ППКОП. В настоящее время, данное оборудование эксплуатируется в 16 областях Украины, как Государственной службой охраны, так и коммерческими структурами, выполняющими функции по наблюдению за состоянием средств охранной или пожарной сигнализации на объектах и их обслуживанию. С вступлением в силу стандарта ДСТУ EN-54, возникла необходимость приведения параметров ППК к требованиям европейских норм. В связи с этим была разработана группа ППКП «Пегас -06», которая предназначена для:

- ❑ контроля состояния зон охрано-пожарной сигнализации; обеспечения обмена данными с пунктом централизованного наблюдения (ПЦН) по абонентской телефонной линии с импульсным или тональным (DTMF) набором телефонного номера в протоколах 20 BP5 (2 300 Гц, Data-1 800 Гц) 4/2 нерасширенный формат, Contact-ID, «Гриффон-DTMF», по каналу GSM в протоколах «Гриффон-01», «GSM DTMF»;
- ❑ обеспечения контроля обрыва телефонной линии и передачи соответствующего извещения на ПЦН;
- ❑ автоматического переключения на резервный канал при повреждении или перегрузке основного;
- ❑ формирования тестовых извещений по каналу связи GSM.

Все ППКП имеют встроенный импульсный источник питания, отвечающий современным требованиям, позволяющий подключать до 14 четырехпроводных извещателей в каждую из 8 зон, имеют световую и звуковую индикацию сигналов «Пожар» и «Неисправность». Программирование приборов выполняется с помощью ПЭВМ.

6.) Новая эра интегрированных систем оповещения.

На сегодняшний день ни один крупный новый или реконструируемый объект не может быть сдан в эксплуатацию без охранно-пожарной системы оповещения и эвакуации людей (сокращенно СО). Тип и функции данной системы определяются нормативными документами (ДБН В. 1.1—7—2002) и указываются в «Предписании» или специально разработанной «Концепции», но не секрет, что эти системы используются в охранном комплексе. В случае пожара или другой чрезвычайной ситуации СО должны управлять эвакуацией людей путем автоматического включения световых указателей и подачи заранее записанных сообщений в различные зоны по специально разработанному алгоритму. В «мирное» время эти системы используются в охране стационарных объектов на – все 100%, при этом выполняют дополнительные функции: трансляцию музыки, информационно-рекламных объявлений, громкоговорящую связь для вызова персонала и др. Особенно сложными в реализации СО являются системы для крупных объектов с большим скоплением людей, например, крупные спортивные объекты, метрополитены, многоэтажные торговые, развлекательные и выставочные центры. Эти объекты требуют комплексного подхода и применения лучшего оборудования с высокой степенью надежности и максимальной функциональностью.

Этим требованиям полностью отвечает система оповещения и управления эвакуацией людей при пожаре нового поколения Дупасорд ProMatrix. Построенная на основе нового матричного процессора Дупасорд Р64, программной оболочки IRIS-NET и центрального процессора системы оповещения DPM 4000 эта система обеспечивает самые смелые и сложные инженерные решения. Новый цифровой процессор Дупасорд Р64 включает в себя матрицу 32х32, модули аналоговых и цифровых входов и выходов, виртуальные модули динамических обработок и органов управления, реализованные на внутреннем и опциональном внешнем DSP процессорах. Несколько матричных процессоров Р-64 могут объединяться в единую цифровую систему по протоколам IRIS-Net и COBRA – Net. Передача управляющих и звуковых сигналов между компонентами системы осуществляется в цифровом виде с минимальной за-

держкой, это позволяет строить распределенные звуковые системы с большим удалением частей системы друг от друга, дистанционно управлять стойками усилителей с процессорным управлением, что очень актуально при озвучивании крупных объектов. При этом постоянно осуществляется полный контроль технического состояния компонентов системы, линий, усилителей мощности и громкоговорителя.

7.) Октопус – беспроводная передача сообщений. Целесообразность или необходимость применения беспроводной системы сигнализации «ОКТОПУС» определяется пятью группами факторов:

А). Нормативные. Ряд существующих руководящих документов регламентируют применение беспроводных систем сигнализации. Прежде всего они касаются специальных объектов. Например, «Інструкція з організації охорони державних музеїв, історично-культурних, заповідних та інших важливих об'єктів...» Кроме того, там же (п. 4.20 инструкции) рекомендуется использовать радиоканальные средства сигнализации с целью обеспечения скрытности охраны объекта.

Б). Экономические. Стоимость прокладки шлейфа с учетом цены кабеля в среднем в пересчете на одну проводную пару составляет от 500 до 1 000 грн. и более на 100 м прокладки. Средняя стоимость беспроводного шлейфа той же длины с использованием удлинителя «ОКТОПУС» составляет 150-300 грн. Экономическая целесообразность очевидна, (цены на начало 2008 г.).

В). Безопасность. Мировые тенденции в технике и строительстве усугубляют требование безопасности людей в качестве главного критерия. Данные современных исследований по факторам возникновения, распространения и тяжести последствий пожара указывают на кабельную продукцию как на один из основных источников риска. Это привело к ужесточению требований ДБН к кабельным изделиям, (распространение горения, токсичность и т. д.) Беспроводные системы дают радикальное решение этой проблемы путем исключения кабеля из системы сигнализации.

Г). Тактические. Имеются в виду случаи, когда использование проводного шлейфа невозможно или ограничено по соображениям тактики построения системы сигнализации. Например, когда охраняемая зона находится вне помещения или объект состоит из нескольких помещений или, как упоминалось выше, требуется обеспечить скрытность сигнализации и т. д.

Д). Эстетические. Эту группу факторов можно оставить без комментариев, они очевидны. Удлинитель радиоканальный «ОКТОПУС» (осьминог) представляет собой комплект из приемного устройства и передающих модулей количеством от 1 до 8. Приемник удлинителя подключается к входу одной из зон стандартного ППК и, по сути, является адресным расширителем на 8 беспроводных зон. В приемнике имеется также выход «саботаж», который может подключаться к 24-часовой зоне ППК. Он активируется при попытке нарушения целостности приемника, передатчика, извещателя, а также при попытках саботажа или нарушениях в канале связи. Питание приемника осуществляется от ППК. К передатчику удлинителя может подключаться стандартный извещатель, либо группа извещателей. Передатчик может работать также автономно в режиме беспроводного магнитоконтактного извещателя.

Авторы задают простой вопрос заинтересованному читателю, “может ли полководец рассчитывать на победу, если его армия не вооружена и не обучена”. Ответ – нет. В негосударственной системе безопасности, (НСБ) – развитие и успех охранных подразделений напрямую зависят от технического оснащения, транспорта, вооружения, экипировки, средств связи, уровня подготовленности персонала и человеческого фактора. По поводу технического обеспечения, авторы рекомендуют следить за новинками и консультироваться со специалистами по интересующим направлениям. Технический прогресс не стоит на месте.

Оборона Вашего дома

Первый рубеж обороны Вашего дома – это входная дверь, именно через нее в дом проникают преступные элементы. Давайте поговорим о замках на дверях и выборе взломостойкого механизма. Для начала посмотрим, что говорят об этом нормативные акты. Сегодня в Украине действуют два стандарта по замкам: ДСТУ Б.В.2.6—1—95 «Замки и защелки для деревянных дверей. Типы и основные размеры» (что касается металлических дверей, то тут стандартов нет) и ДСТУ Б В.2.6—13—97 «Изделия замочные и скобяные. Общие технические условия».

Пункт 3.4 ДСТУ Б.В.2.6—13—97 гласит, что движущиеся детали изделий должны фиксироваться в крайних, а по необходимости, в промежуточных положениях. Это легко проверить путем нажатия на засов (ригель) замка в открытом или промежуточном положении. Далее говорится о том, что конструкция изделий (замков) должна обеспечивать возможность демонтажа, регулирования и, по необходимости, смазывания трущихся деталей в процессе эксплуатации.

Последнее замечание очень важно при использовании многонаправленных замков, ибо, в случае чего, необходимо будет нарушать обшивку и декоративное оформление двери. Исключения составляют лишь дорогие экземпляры дверей, где для этого предусмотрен специальный лючок.

Кстати, о дверях. «Дверной» стандарт ДСТУ Б В.2.6—11—97 говорит, что дверь должна закрываться замком, который обеспечивает замыкание минимум в трех направлениях.

Если речь идет о так называемых цилиндрических замках, необходимо обратить внимание на то, чтобы замок комплектовался защитной фурнитурой, которая бы защищала цилиндрический механизм от вандальных посягательств. Речь идет прежде всего о специальных, (термообработанных или армированных) материалах запорного устройств бронированных накладках, оберегающих замок от попыток механического взлома. защите от высверливания цилиндра замка. Последняя может достигаться путем установки подвижных элементов в передней части замочной скважины, которые будут просто вращаться вместе со сверлом взломщика.

О типах замков. Например, отраслевой стандарт Государственной службы охраны МВД Украины гласит о том, что двери должны комплектоваться двумя замками разных типов которые необходимо устанавливать так, чтобы расстояние между их ригелями было минимум 300 мм.

О защитной фурнитуре. Следует обратить внимание, чтобы она крепилась на стяжных винтах. Причем качественные образцы имеют три стяжных винта. Третий винт расположен приблизительно на половине длины накладки. Но в этом случае придется выбирать подходящий замок со сквозным отверстием для этой стяжки. В случае применения совмеще-

нии фурнитуры она сама в некоторой степени защищает корпус замка. Но фурнитура может быть и на одной планке, и раздельная. В этом случае корпус замка оставляет открытым доступ к замку путем высверливания через полотно двери. В этом случае рекомендуем устанавливать замок, который имеет накладную защитную пластину на корпусе замка.

Предложение рынка Украины

Условно замки можно разделить по следующим характеристикам:

1. По способу замыкания: нормально открытые и нормально закрытые.

2. По типу замыкающего механизма:

-  сувальдные;
-  цилиндровые;
-  магнитные.

3. По принципу действия:

-  механические;
-  Электромеханические;
-  электрические.

Авторы предлагают ознакомиться с современными тенденциями развития замков.

Сувальдные замки. Прежде всего, следует отметить тенденцию к увеличению секретности замка. Однако есть одно «но». Увеличение секретности – это увеличение числа «сувальд». Число сувальд приводит к увеличению толщины замка. В таком случае его не всегда можно установить в некоторые двери. Дополнительно к этому вводятся конструктивные ухищрения, призванные снизить вероятность вандального воздействия и взлома с помощью инструментов. Также применяются конструктивные особенности, призванные снизить риск открытия замка с помощью манипуляций (отмычек). Например, наличие специальных зацепов-ловушек на зубцах сувальд.

Цилиндровые замки. В развитии этого класса замков также просматривается увеличение секретности, применение цилиндрических механизмов, сертифицированных на высокий уровень секретности, на стойкость к воздействию факторов окружающей среды, факторов вандального взлома. При установке цилиндрических механизмов необходимо устанавливать защитные броненакладки, которые защищают цилиндры от различных, в том числе и вандальных, воздействий.

В обоих типах замков широко применяют так называемые «тяги», которые, с одной стороны, обеспечивают дополнительные точки замыкания, а с другой стороны способны управлять так называемыми «девиаторами», которые по сути являются автономными запирающими устройствами.

Последние новинки – это установка замков, принцип работы которых основан на передаче информационного кода через твердые предметы (например, дверь). При этом на лицевой стороне двери отсутствуют какие-либо видимые признаки замка (замочная скважина и пр.). Поэтому снаружи не видно, где установлен замок, и установлен ли он вообще. А отсутствие замочной скважины и сохранение целостности дверного полотна

позволяют применять эти замки для контроля доступа в полностью изолированные и экранированные комнаты. Такой механизм может как блокировать дверь, так и препятствовать работе самого замка путем блокировки тяги. Это сводит на «нет» попытку открыть дверь даже при наличии родного ключа. По состоянию на 2008 год, авторы предлагают ознакомиться с некоторыми марками взломостойких замков, представленных на украинском рынке. Мы все время повторяем, технический прогресс не стоит на месте, следите за новинками, (см. таблицу основных марок взломостойких замков, представленных на украинском рынке в 2008 г. Приложение).

Сегодня уже применяются замки, которые имеют возможность посылать сигнал, отображая состояние ригеля (открыто/закрыто). При подключении GSM-модема этот сигнал можно получать и на мобильный телефон. А с помощью мобильного телефона в свою очередь можно и управлять самим замком. Плюс еще использовать ряд дополнительных функций. Например, включать свет в коридоре одновременно с открытием замка.

Авторы обращают внимание на то, что применяются различные типы электронных замков, которые работают от кода, радиобрелка, отпечатка пальца и пр. Но для обеспечения надежного сопротивления усилиям взломщика они также должны быть снабжены вандало-защищенным корпусом и усиленными запорными устройствами. Кроме того, такие замки в обязательном порядке, комплектуются блоком автономного питания. При выборе замка в первую очередь необходимо обратить внимание на марку. Насколько она известна (в мире, а не на ближайшем рынке), какова репутация данной фирмы. Необходимо помнить, что хорошие вещи не могут стоить дешево. Лучше приобретать замки в специализированном салоне, где вам смогут его правильно установить и предоставить полный комплекс дальнейшего сервисного обслуживания, поддерживать гарантию. Не стоит покупать замки китайского производства и турецкие замки с крестообразным ключом. То есть покупать их можно, но не следует их устанавливать на металлические входные двери, надеясь обеспечить безопасность вашего имущества. Надо понимать, что какая бы прочная дверь не была, если замок в ней некачественный, то степень ее защиты равна степени защиты этого замка. Всегда надо измерять по «самому слабому звену».

Если вы решили потратиться на металлическую дверь, то не поспешите на замок. Ведь качественный замок не только защитит от возможных попыток взлома или от манипулирования отмычками, но и будет хорошо работать долгие годы. И наоборот, нет необходимости ставить высококлассный замок на некачественные двери. Необходимо также иметь надежную фурнитуру, которая бы обеспечивала не только хороший внешний вид, но и защиту самого механизма замыкания. Только соблюдая все эти условия, можно будет говорить о надежности и взломостойкости вашего замка и обороны Вашего дома.

Приложение

Основные марки взломостойких замков, представленных на украинском рынке (2008 г.)

Марка замка	Knock N'Lock	Mult-T-Loк Interactive, Mult-T-Loк Integrator	Сандер Рубин; Гранит; Кремень; Вальмет; Алмаз	Guard, Guard Millennium, M15 RED LINE	New Cambio Facile	ABLOY PROTEC	Керберос
Производитель	E-Loк Technologies (Израиль)	Mult-T-Loк (Израиль)	Эльбор (Россия)	Эльбор (Израиль)	CISA (Италия)	ABLOY (Финляндия)	Заказ замка – собственная модель (Россия)
Тип замка	Электромаг. для дверей, сейфов	Цилиндровые замки (накладные, врезные, навесные, штильеры)	Сувальные врезные и накладные	Сувальные и штильерные комбинированные	Врезной механический	Мех. замки штиль-на, штильеры	Механический сувальдный (врезные, накладные)
Класс защиты	Класс D высокой безопасности (VDS, Германия, UL, CHA)	2 (высокий) класс стойкости ко взлому по ДСТУ EN 1303	4 класс (по российскому стандарту)	4 класс (по российскому стандарту)	6-уровневая сертифицированная	Более 5 млн	4 класс (по российскому стандарту)
Стойкость к взлому	Кольцо кода 16"	6 (высокий) класс стойкости по ДСТУ EN 1303	Более 3 млн серийных	Более 3 млн серийных	Более 244 млн	2 млрд комбинаций	Более 5 млн
Настройка ключа	Нет ключа, сканеры и др. устройства	Система MODULAR (вместе с замком)	–	–	–	–	–
Количество точек захвата	Стандарт – 1	4-стороннее	3-стороннее (до 6 ригелей)	3-стороннее (до 6 ригелей)	4 ригеля + 2 дол. точки захвата	Система MODULAR (поддается штильеру)	1 точка (2 ригеля и 16 мм)
Материал запорной планки	Нержавеющая сталь	Никелированная сталь	Никелированная сталь	Никелированная сталь	Никелированная сталь	Никелированная сталь	Никелированная сталь
Валет ригелей из двери	Исполнит. механизм на соленоиде	В замке (от 25 мм)	40 мм	40 мм	37 мм	В завыт. от корпуса замка (от 20 мм)	40 мм
Примоголосие к силовой нагрузке	На разрыв – 1 500 кг (стеклокомпозит – до 4,5 т)	6 (высокий) класс по ДСТУ EN 1303. Работоспособен при давлении до 10 т	–	–	От 600 до 1000 кг боковой нагруз.	Работоспособен при давлении до 300 кг	Работоспособен при давлении до 300 кг
Защита корпуса	Не уязвимая к срезу	Повышенная прочность корпуса, усиленные пластины – от разрыва, протектор из 3 мм. закал. стали, ХР-пласта в корпусе (от разрыва штильера)	Корпус из минеральной пластины 2,5 мм. Бронир. пластины. Термообр. вставка в термостекле. Термообр. защитный ригель	Корпус из минеральной пластины 2,5 мм. Бронир. пластины. Термообр. вставка в термостекле. Термообр. защитный ригель	Оцинкованная сталь, бронированные пластины и накладки	От высверливания (14-кл. штильер из закаленной стали). Корпус штильера из закаленной стали	От высверливания (стойка замка с закаленным валом, штильером). Бронир. пластины
Защита механизма от взлома	Отсутствие любых наружных элементов – лишь защита от взлома и выламывания	Защита от манипуляции (отмечки) и башинга	Блокир. зубцы и I-фиксатор; пятый зуб, кодовый ключ, вращ. з-на, лопатки паза на зубях, сквозной микроканал	Блокир. зубцы и I-фиксатор; пятый зуб, кодовый ключ, вращ. з-на, лопатки паза на зубях, сквозной микроканал	Центральное расположение нарезки ригеля препятствует взлому сдвиганием	Стойкость к открытию отмычкой	Ложные паза на сувальдах (против отмычки)
Антикриминальные свойства	Нержавеющая сталь. Не подвержена коррозии из-за погодных факторов	Класс С (высокий) корпуса и штильера – от коррозии, коррозионная стойкость по ДСТУ EN 1303	Стойкость к коррозии, стойкость к воздействию агрессивных сред, стойкость к воздействию щелочей	Стойкость к коррозии, стойкость к воздействию агрессивных сред, стойкость к воздействию щелочей	Перекоррозийный механизм, не влияющий на замену всего замка	Стойкость к коррозии (температ. нет. 1-30 С° ... + 60 С°)	Гарант. 100 лет
Дополнительные секреты	–	Панельный кодиратор ключа (от неслуха, копирования)	Защита от неслуха, считывания кода ключа	Защита от неслуха, считывания кода ключа	Количество секретных штильеров 6-14	2-система штильер-пружина (штильер пружин в штильере)	Гарант. 100 лет
Крыление запорной планки	От 180 у.е.	От 70 у.е. (Interactive ®) до 40 у.е. (Integrator®)	4 штильера	4 штильера	На штильерах или в штильерах	На штильерах или в штильерах	Гарант. 100 лет
Стойкость, у.е.	От 180 у.е.	От 70 у.е. (Interactive ®) до 40 у.е. (Integrator®)	от 20 у.е.	от 20 у.е.	от 120 у.е.	от 120 у.е.	Гарант. 100 лет
Особенности	Замок на основе беспробойной перфорации ригеля (пусть срез, по перфорации ригеля, замок не сломается, а сломается через материал ригеля)	Комбинир. или корпуса и ригельный пуш-бтер, по перфорации ригеля, замок не сломается, а сломается через материал ригеля	Отсутствие смещения тг и стержня относительно корпуса замка	Отсутствие смещения тг и стержня относительно корпуса замка	Расстояние между датчиками и межкомарные (повышенная газоустойчивости)	Дополнительные секреты: только в сериальных центрах ABLOY (перезаправка)	Гарант. 100 лет

Технічні засоби захисту

Проектування і монтаж охоронної сигналізації з урахуванням охорони периметра Вашого об'єкта, можливостей і вимог в цьому напрямку для України. В складі системи охорони периметра, крім технічних засобів охорони, повинні застосовуватися інженерні засоби, без яких деякі завдання охорони периметра взагалі не виконані. Згідно з положеннями і вимогами ГОСТів – створення системи охоронної сигналізації на об'єкті повинно вестися поступово з урахуванням вимог Вашої країни. Для українських підприємств і фахівців по роботі з технічними засобами охоронної, охоронно-пожарної сигналізації корисно знати, хоча б базові особливості українського законодавства, застосовані до цього виду діяльності. Потрібно бути дуже обережним в відношенні Закону України “Про інформацію” від 02.10.92 № 2657-XII.

Автори все час підкреслюють, що технічний прогрес, інформація і нормативні вимоги, мають властивість – змінюватися. Зацікавленому читачеві, ми пропонуємо ознайомитися з нижче перерахованими документами. Слідкуйте за змінами.

1. Закон України “Про державні оборонні замовлення” від 03.03.99 № 464-XIV.

2. Закон України “Про державну таємницю” від 21.09.99.

3. Закон України “Про науково-технічну інформацію” від 25.06.93.

4. Закон України “Про друковані засоби масової інформації (преси) в Україні” від 16.11.92.

5. Постанова Верховної Ради України “Про Концепцію (основу державної політики) національної безпеки України” від 16.01.97 №3/97-ВР.

6. Постанова Кабінету Міністрів України “Про Положення про порядок видачі суб'єктам підприємницької діяльності спеціальних дозволів, (ліцензій) на здійснення окремих видів діяльності від 17 травня 1994 р. № 316.

8. Постанова Кабінету Міністрів України Про затвердження “Порядку організації та забезпечення режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях” від 02.10.03 № 1561-12.

9. Постанова Кабінету Міністрів України “Про заборону використання бюджетних коштів для закупівлі імпортованих товарів” від 04.06.96 №611.

10. ДСТУ 3859-99. Засоби інженерно-технічного укріплення та захисту об'єктів. Терміни та визначення.

11. ДСТУ 2273-93. Система стандартів безпеки праці. Пожежна техніка. Терміни та визначення.

12. ДСТУ 2624-94. Зв'язок телефонний. Системи сигналізації. Терміни та визначення.

13. ДСТУ 2860-94. Надійність техніки. Терміни та визначення.

14. ДСТУ 2861-94. Надійність техніки. Аналіз надійності. Основні положення.

15. ДСТУ 2864-94. Надійність техніки. Експериментальне оцінювання та контроль надійності. Основні положення.

16. ДСТУ 2874-94. Система оброблення інформації. Бази даних. Терміни та визначення.

17. ДСТУ 1.0-93. Державна система стандартизації України. Основні положення.

18. ДСТУ 78.11.001—98. Укріпленість об'єктів, що охороняються за допомогою пультів централізованого спостереження Державної служби охорони. Загальні технічні вимоги.

19.ГОСТ 26342-84. Система показателей качества продукции. Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры.

20.ГОСТ 27990-88. Система показателей качества продукции. Средства охранной, пожарной и охранно-пожарной сигнализации. Общие технические требования.

21. ГОСТ 4.188-85. Система показателей качества продукции. Средства охранной, пожарной и охранно-пожарной сигнализации. Номенклатура показателей.

22. ГОСТ В 2.902-68 „ Система разработки и постановки на производство военной техники. Единая система конструкторской документации

23.ГОСТ В 20.39.308-76. Комплексная система общих технических требований. Аппаратура, приборы, устройства и оборудование военного назначения. Общие технические требования, методы контроля и испытаний. Конструктивно-технические требования.

24. ГОСТ В 20.57.304-76. Комплексная система общих технических требований. Аппаратура, приборы, устройства и оборудование военного назначения. Общие технические требования, методы контроля и испытаний. Методы оценки соответствия требованиям по надежности.

25. ГОСТ В 20.57.306-76. Комплексная система общих технических требований. Аппаратура, приборы, устройства и оборудование военного назначения. Общие технические требования, методы контроля и испытаний.

26. ГОСТ В 20.57.310-76. Комплексная система общих технических требований. Аппаратура, приборы, устройства и оборудование военного назначения. Общие технические требования, методы контроля и испытаний;

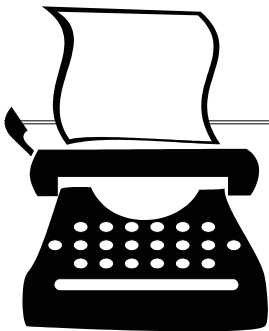
27. ГОСТ В 23226-78. Порядок разработки программ и методик испытаний опытных образцов изделий. Система разработки и постановки.

28. ГОСТ 21.001-77. Система проектной организации для строительства. Общие положения.

29. ДБН А. 2.2-3-97. Склад, порядок розроблення, погодження та затвердження проектної документації для будівництва.

30. СНИП 3.05.06-85. Электротехнические устройства.

Інструкція про категорії військових об'єктів та єдині вимоги щодо їх обладнання технічними засобами охорони: _____ Введена в дію наказом Міністра оборони України від 04.12.95 № ***.



Контрольно-пропускной режим на предприятии

Построение надежной системы безопасности, предприятия, фирмы сложный и многогранный процесс. Одним из немаловажных факторов обеспечения надежной защиты того или другого объекта есть организация и поддержка определенного контрольно-пропускного режима (КПР).

Контрольно-пропускной режим – это специальный режим организационно-правовых ограничений и правил, которые устанавливают порядок пропуска через контрольно-пропускные пункты, в отдельные дома (помещение) сотрудников объекта, посетителей, транспорта и материальных средств.

Основная цель контрольно-пропускного режима – обеспечение нормативных, организационных и материальных гарантий выявления, предупреждение и прекращение посягательств на законные права предприятия, его имущество, интеллектуальную собственность, производственную дисциплину и охраняемую информацию.

Естественное создание надежного контрольно-пропускного режима требует известных затрат. Однако, если внимательно оценить все отрицательные факторы, влияния на деятельность фирмы, эти затраты не кажутся настолько большими, так как обеспечивают стойкое экономическое движение фирмы и сводят к минимуму возможные потери. И вдобавок процесс создания системы контрольно-пропускного режима может быть растянут во времени, с учетом материальных возможностей фирмы и ее деятельности на рынке. Принципиально важным условием для реализации задуманного есть анализ ситуации и разработка программы действий, которая разрешит избежать шараханий и лишних затрат.

Организация контрольно-пропускного режима отличается определенной сложностью. Дело в том, что механизм осуществления контрольно-пропускного режима направлен на применении “запретов” и “ограничений” в отношении одних субъектов, которые пересекают границы охраняемых объектов, домов (помещений), для обеспечения прав и интересов других (фирмы и ее персонала). Такой механизм регулирования правоотношения в сфере предпринимательства должен быть безупречный из позиции требований действующего законодательства и учета Вашей страны. В книге мы будем рассматривать основные направления создания контрольно-пропускного режима на предприятии в общем плане:

- 1.) методика определения и оценка исходных данных;
- 2.) разработка мероприятий и нормативных документов;
- 3.) оборудование контрольно-пропускных пунктов;
- 4.) образец перечня необходимой документации на посту.

Организация контрольно – пропускного режима предприятия (КПР)

Контрольно-пропускной режим является неотъемлемой частью общей системы обеспечения безопасности фирмы. Контрольно-пропускной режим (как и вся система безопасности) должен отвечать действующему законодательству, устава фирмы, предприятию, а также другим нормативно-правовым актам, которые регулируют деятельность организации.

1.) Основные цели контрольно-пропускного режима сводятся к следующему:

- 👁 защита законных интересов прав фирмы, поддержка стойкости порядка внутреннего управления;
- 👁 сохранение собственности фирмы, ее рационального и эффективного использования;
- 👁 оказывать содействие росту прибылей фирмы;
- 👁 достижение внутренней и внешней стабильности предприятия;
- 👁 сохранение коммерческих секретов и прав интеллектуальную собственность.

2.) Требования к организации контрольно-пропускного режима предприятия:

- 👁 обеспечение санкционированного прохода сотрудников и посетителей, ввоз (вывоз) продукции и материальных ценностей, ритмической работы предприятия;
- 👁 исключать незаконный проход лиц на охраняемые территории и в отдельные дома (помещение), бесконтрольный въезд (выезд) транспортных средств;
- 👁 своевременное выявление угроз важным интересам фирмы, причин и условий благоприятному нанесению фирме материального и морального убытка, ее нормальному функционированию и развитию;
- 👁 формирование надежных гарантий поддержки организационной стабильности внешних и внутренних связей фирмы, отработка механизма оперативного реагирования на угрозы и отрицательные тенденции в развитии;
- 👁 прекращение посягательств на законные интересы фирмы, использование юридических, экономических, организационных, социально-психологических, технических и других средств в выявлении и ослаблении источников угрозы ее безопасности.

3.) Система обеспечения. Контрольно-пропускной режим можно определить как:

а – систему обеспечения нормативных, организационных и материальных гарантий выявления;

б – предупреждение и прекращение посягательств на законные права предприятия, его имущество, интеллектуальную собственность, производственную дисциплину, технологическое лидерство, научные достижения и охраняемую информацию;

в - совокупность организационно-правовых ограничений и правил пропуска, которые устанавливают порядок, через контрольно-пропускные пункты сотрудников объекта, посетителей, транспорта и материальных ценностей.

4.) Нормативные гарантии состоят в толковании и реализации норм права с учетом Вашей страны, выяснение границ их действий, в формировании необходимых правоотношений, и обеспечении правомерной деятельности подразделов и работников фирмы по поводу ее безопасности использования ограничительных мер, применением санкций к физическим и юридическим лицам, которые посягают на законные интересы фирмы.

А.) Организационные гарантии формируются путем разработки, построения и поддержки высокой трудоспособности общей организационной структуры управления процессом выявления и подавления угроз деятельности фирмы, использование эффективного механизма стимулирования ее оптимального функционирования, которое отвечает подготовке кадров.

Б.) Материальные гарантии формируются за счет выделения и использование финансовых, технических, кадровых, интеллектуальных, информационных и других ресурсов фирмы, которые обеспечивают своевременное выявление, ослабление и подавление угрозы, предотвращение и локализацию возможного убытка, и создание благоприятных возможностей и условий деятельности фирмы. Данные гарантии наполняют нормативные и организационные меры безопасности практическим содержанием, создают реальную основу развития культуры безопасности фирмы.

5.) Основные мероприятия контрольно-пропускного режима разрабатываются службой безопасности и утверждаются руководителем фирмы и оформляются инструкцией о контрольно-пропускном режиме. Ответственность за организацию контрольно-пропускного режима возлагает на начальника службы безопасности. Практическое осуществление контрольно-пропускного режима возлагает на охрану (контролеров, охранников по КПП), работники которой должны знать установленные на объекте правила контрольно-пропускного режима, которые действуют документы по порядку пропуске на объект (из объекта) сотрудников и посетителей, ввоза (вывоза) товарно-материальных ценностей. Контрольно-пропускной режим может быть установлен как в целом по объекту, так и в отдельных корпусах, домах, отделах, хранилищах и других специальных помещениях.

6.) Требования по контрольно-пропускному режиму должны быть доказаны в обязательном порядке к каждому сотруднику объекта. Все рабочие и служащие объекта обязаны соблюдать их. По каждому случаю нарушения контрольно-пропускного режима должно проводиться административное расследование.

Обязанности охраны по контрольно-пропускному режиму определяется в инструкции и в должностных обязанностях контролеров контрольно-пропускных пунктов.

Подготовка исходных данных для разработки контрольно-пропускного режима

Предпринимательство и запрет (ограничение) – по своей природе противоречивое. Искусство разработчика контрольно-пропускного режима заключается именно в том, чтобы найти умное соединение запрета (ограничений) и интересов предпринимательской деятельности фирмы.

Разработка мероприятий и нормативных документов контрольно-пропускного режима начинается с определения исходных данных. Оценивая исходные данные, разработчик определяет основные положения инструкции о контрольно-пропускном режиме. Наши авторы целесообразно предлагают следующую последовательность определения и оценки исходных данных.

1. **Организационная структура** фирмы, местоположения его отдельных элементов и характер производства (деятельности) на них. Выяснение этих вопросов разрешает решить следующие практические задачи:

- 👁 выделить объекты, площадки, дома, помещения на которые необходимо организовать контрольно-пропускной режим;
- 👁 определить характер контрольно-пропускных пунктов (КПП) для пропуска сотрудников, транспортных средств.

2. Провести оценку “суточного объема” потоков транспортных средств, грузов, материальных ценностей и людей (персонала фирмы и посетителей) проходящих через КПП и в отдельные дома (помещение). Только на основе оценки реального состояния мест пропуска можно оценить пропускную способность действующих КПП и привести ее в соответствие с задачами основного производства на объекте. Такая оценка разрешит выбрать оптимальный вариант автоматизации и контроля прохода, проезда на охраняемые территории.

3. Выделить на территории (по степени важности) категории объектов, транспортных средств и грузов, а также категории лиц, которые пересекают установленные границы. Для достижения четкости в определениях предлагается помещение и территорию объекта классифицировать в зависимости от условий доступа и степени защищенности на шесть категорий режимности (“зон безопасности”)

Классификация категорий режимности

Авторы предлагают шесть категорий режимности, которые способны охватить практически все варианты функционального назначения служебных помещений. Кроме того, Вы должны дать четкий ответ на вопрос, которые нужно сделать действия при организации контрольно-пропускного режима и разработке исходной документации по оборудованию объекта техническими средствами охраны. Приведение помещений в соответствие требованиям категорий режимности помогает регламентировать и обосновать:

- 👁 условия доступа сотрудников предприятия и посетителей на объект, определить общедоступного, закрытого и ограниченного доступа объекты, дома, помещение;
- 👁 предложения администрации предприятия по изготовлению оптимального варианта разрешительного порядка пропуска лиц, транспортных средств и материальных ценностей на объект;
- 👁 наличие и вид физической охраны;
- 👁 виды используемых технических средств для обеспечения безопасности.

Разработка инструкций пропускного режима

Пропускной режим является неотъемлемой частью общей системы охраны предприятий. Практическое решение этих вопросов оформляется в виде “Инструкции о пропускном режиме”. Указанная инструкция должна определять систему организационно-правовых охранительных мер, которые устанавливают разрешительный порядок (режим) прохода (проезда) на объект (из объекта) и может включать:

1. Общие положения. В этом разделе указывается:

- нормативные документы, на основании которых составлялась инструкция;
- определение контрольно-пропускного режима и цель его установления;
- на кого возлагает руководство пропускным режимом, практическое его осуществление;
- санкции к нарушителям контрольно-пропускного режима;
- требования к оборудованию разных помещений.

2. Порядок пропуска сотрудников предприятия, откомандированных лиц и посетителей через контрольно-пропускные пункты. В этом разделе рекомендуется:

- пересчитать все КПП и их назначение, описание, расположение и установить их единую нумерацию;
- изложить требования к оборудованию КПП;
- установить порядок прохода сотрудников и посетителей на территорию объекта;
- определить права и основные обязанности контролеров КПП;
- установить помещение, где запрещается принимать посетителей и представителей посторонних организаций.

3. Порядок допуска на объект транспортных средств, вывоза продукции, документов и материальных ценностей. В этом разделе указывается:

- порядок допуска на территорию объекта (из объекта) автотранспорта;
- въезд и стоянка на территории объекта транспорта, который принадлежит сотрудникам на правах личной собственности;
- порядок пропуска автомашин посторонних организаций, которые прибыли с грузом в адрес объекта в рабочее и нерабочее время;
- порядок вывоза (ввоза) товарно-материальных ценностей;
- правила оформления документов на вывоз (вынос) материальных ценностей из территории объекта.

4. Виды пропусков, порядок их оформления. В этом разделе определяется:

- виды пропусков, их количество и статус;
- описание пропусков;
- порядок оформления и выдачи пропусков;
- общая замена и перерегистрация пропусков;
- мероприятия при потере пропуска сотрудником.

5. Обязанности должностных лиц по поддержке контрольно-пропускного режима.

6. Учет и отчетность, порядок хранения пропусков, печатей.

В зависимости от структуры предприятия и характера его деятельности инструкция может содержать и другие разделы.

Виды пропусков

Для допуска на предприятие, в отдельные помещения, как правило, устанавливаются несколько видов пропусков. Это могут быть: постоянные, временные, разовые и материальные пропуска. Образцы бланков пропусков разрабатываются администрацией объекта (службой безопасности). По своему внешнему виду и содержанию пропуска должны отличаться друг от друга и иметь защитные свойства. Все виды пропусков, за исключением материальных, оформляются и выдаются бюро пропусков (или другим подразделом) по письменным заявкам. Виды пропусков определяются в зависимости от специфики предприятия.



1.) Постоянные пропуска выдаются сотрудникам объекта, принятым на постоянную работу, а так же работникам других организаций, закрепленных для постоянного обслуживания объекта. Постоянные пропуска могут делиться на группы, их количество и назначения определяется инструкцией о контрольно-пропускном режиме. Постоянные пропуска могут сохраняться как на руках у сотрудников объекта, так и в кабинах на КПП. Постоянные пропуска лиц, которые убывают из объекта на продолжительное время (отпуск, болезнь, командировка и т.п.), кажутся на хранение в бюро пропусков (отдел кадров), а при оставлении таких пропусков в кабине, на ячейке (где сохраняется пропуск) делается соответствующая оценка. Пропуска уволенных из работы уничтожаются установленным порядком.

2.) Временные пропуска выдаются лицам работающим по контракту, который находится на временной работе, прикомандированных к предприятию и сохраняются, как правило, на КПП. Срок действия и порядок оформления временных пропусков определяется инструкцией о контрольно-пропускном режиме.

Временные пропуска могут быть с фотографией и без фотографии. Временные пропуска без фотографии действительные только при предъявлении документа (подтверждающий личность.)

3.) Разовые пропуска (для посетителей и клиентов) выдаются на один человека и только для разового посещения предприятия и его подразделов. Пропуск оформляется и действительный при наличии документа личности. Разовые пропуска должны периодически меняться по цвету бланков и других отличительных признаков. Разовый пропуск выдан водителю транспортного средства может служить одновременно и разовым пропуском для транспорта. Разовый пропуск действительный для входа на территорию объекта или его подраздела в режиме определенного времени. Контроль за посещением предприятия по разовому пропуску осуществляется с помощью оценки на оборотной стороне пропуска, где указывается

время посещения, заверенное подписью лица посетителя, который принял.

Разовый пропуск изымается на посту контролером, при выходе посетителя из объекта иάζεται в бюро пропусков. О лице, которое не вышли из объекта по истечению указанного срока действия пропуска, контролер докладывает начальнику стражи (очередному по КПП) для принятия мер по выяснению причин задержки. Фамилии лиц, которые посетили объект по разовому пропуску могут записываться в специальную книгу учета.

4.) Материальные пропуска для вывоза (выноса) товарно-материальных ценностей выдаются администрацией предприятия. Срок действия пропуска определяется инструкцией о контрольно-пропускном режиме. Материальные пропуска должны изыматься на КПП и казаться в бюро пропусков.

Образцы действующих пропусков должны находиться на КПП. Для обучения работникам охраны выделяется необходимое количество образцов пропусков.

Контрольно-пропускной пункт. (КПП)

Для организации пропускного режима на предприятии оборудуются контрольно-пропускные пункты. Оборудование КПП должно обеспечивать необходимую пропускную способность и возможность тщательной проверки пропусков, документов у проходящих лиц, обзора всех видов транспорта, перевозка грузов и удовлетворять следующим требованиям:

- 👁️ исключать возможность несанкционированного проникновения через КПП на объект (из объекта) людей и транспортных средств;
- 👁️ оказывать содействие сокращению времени на проверку документов, обзор транспорта и материальных ценностей;
- 👁️ оказывать содействие исключению (сведения к минимуму) ошибок охранника при пропуске людей и транспорта;
- 👁️ обеспечивать меры безопасности охранника при обзоре транспортных средств;

Все виды КПП должны быть оборудованы необходимыми видами связи и тревожной сигнализации для вызова резерва охраны. На КПП рекомендуется располагать внутренний телефон и список телефонов администрации предприятия.

КПП для прохода людей

Для контроля лиц проходящих на объект и в отдельные дома (помещение) строятся КПП. Каждое человеческое КПП рекомендуется оборудовать: комнатой для охраны, комнатой для обзора граждан, камерой хранения, гардеробом, турникетом с фиксирующими устройствами-запорами.

Размещение помещений определяются проектами и зависит от средств механизации, автоматизации КПП и особенностей предприятия. В контрольно-пропускном зале устраиваются проходы, которые оборудуются техническими средствами охраны и физических барьеров. В комплект оборудования, как правило, входит:

- 👁️ средства механизации, автоматизации, системы контроля доступа;
- 👁️ физические барьеры (ограждение турникеты, калитки);
- 👁️ основное и резервное освещения;
- 👁️ средства связи и тревожной сигнализации;

 системы видеоконтроля.

Как средства контроля доступа могут употребиться разные турникеты. Турникеты предназначены для управления потоками людей и регулирования входа (выхода). В последнее время наиболее широкое распространение получили электромеханические турникеты. Эти турникеты, в отличие от громоздких и неудобных в управлении механических, легко управляются из пульта охранника и могут работать в составе автоматизированной системы контроля доступа.

При выборе турникета нужно знать, как они бывают “нормально открытые” и “нормально закрытые”. “Нормально открытые” турникеты (например, раздвижные, которые до недавнего времени были установлены в русском метро) в мировой практике употребляются довольно редко. Они могут ударить проходящий человека и не разрешают осуществлять эффективный контроль.

Для осуществления надежного контроля чаще употребляются “нормально закрытые” турникеты:

роторные турникеты - "вертушки", турникеты-триподы и калитки.

1.) Калитки применяются для управления потоками людей – организации – организации свободного прохода в одну сторону (на вход или выход) и запрета прохода в другую. Калитки широко употребляются в магазинах, аэропортах, вокзалах. Применение калиток для контроля доступа – неэффективно, это связано с тем, что калитки не разделяют поток людей по одному, так как после открытия калитки через нее могут пройти несколько человек. Калитки могут устанавливаться для организации свободного выхода, в то время как контроль входа доверяют триподам или “вертушкам”.

2.) Турникеты-триподы с тремя планками, которые преграждают, есть одним из наиболее оптимальных средств для осуществления контроля санкционированного прохода. Триподы имеют современный элегантный вид и легко монтируются. Триподы разрешают осуществлять эффективный контроль доступа, так как разделяют поток людей по одному, обеспечивая при этом высокую пропускную способность. Триподы могут применяться в системах электронных проходных, в том числе в условиях большого потока людей. Для предотвращения возможности подлезть под планки турникета или перепрыгнуть через них, на турнике рекомендуется устанавливать специальные датчики, которые срабатывают при попытке несанкционированного прохода.

3.) Роторные турникеты - "вертушки" применяются в тех случаях, когда необходимо полное перекрытие зоны прохода. Они могут быть разными по высоте, от поясных - до турникетов в полный рост, которые конструктивно похожи на вращающейся дверь.

Автотранспортные КПП

В состав автотранспортного КПП входит: обзорная площадка и служебные помещения.

1.) **Обзорная площадка** назначается для обзора автомобилей при их выезде. Обзорные площадки могут располагаться, как на территории предприятия, так и за ее пределами, на местности, непосредственно связанной с основными воротами КПП.

Обзорная площадка должна отвечать следующим требованиям:

- 🔊 иметь достаточную площадь для размещения транспорта, который оглядывается, технические средства для обеспечения нормальных условий работы охранника;
- 🔊 исключать возможность несанкционированного проникновения на объект (из объекта) людей и транспортных средств;
- 🔊 обеспечивать при установленной интенсивности движения, в любое время пор и года, обзор автомобильного транспорта и перевезенных грузов;
- 🔊 быть изолированной от других сооружений, которые не имеет отношения к охране объекта и оборудованию КПП;
- 🔊 обеспечивать меры безопасности охранника при выполнении своих обязанностей.

Размеры обзорной площадки устанавливаются в зависимости от габаритов транспорта и перевезенных грузов. Более детально на эту тему мы поговорим на семинарских занятиях

Автотранспортные КПП могут оборудоваться светофорами, весами для взвешивания автомобилей, обзорной ямой или эстакадой для обзора грузов, механизированными устройствами для автоматического открытия и закрытия ворот с фиксаторами.

Обзорные площадки по периметру оборудуются физическими барьерами и рубежом сигнализации. Площадки, как правило, выгораживаются забором из металлической сетки или декоративной решетки высотой до 2,5 метров. На площадке оборудуются основные и вспомогательные механизированные ворота. Основные ворота устанавливаются на линии основного ограждения объекта, а вспомогательные на противоположной стороне обзорной площадки. Вместо ворот могут применяться механизированные шлагбаумы. На автомобильных КПП употребляются ворота с ограничением, (и без ограничения) габаритов по высоте. По конструкции они могут быть распашными или раздвижными (выдвижными). Распашные ворота должны оборудоваться фиксаторами.

Для регулирования движения транспорта, который проходит через проезды обзорных площадок КПП могут применяться двухсекционные светофоры с линзами красный и зеленый цвета.

В состав электромеханического оборудования КПП для автомобильного транспорта обычно включаются:

- 🔊 электродвигатели, повод ворот;
- 🔊 конечные выключатели, автоматического отключения электродвигателей при полностью закрытых и открытых створках ворот;
- 🔊 магнитные пускатки электродвигателей;
- 🔊 электрооборудование светофоров;
- 🔊 кабельные, силовые линии.

Групповой распределительный щит (щит управления) может устанавливаться в помещении КПП, а при отсутствии дома КПП в специальном металлическом шкафу непосредственно на обзорной площадке.

2.) Служебные помещения. Об этом вопросе очень много написано в практических пособиях других авторов.

Допуск сотрудников и посетителей на объект

Проход сотрудников и посетителей на территорию объекта, в специальные подразделения, (помещения) и назад осуществляется по установленным на объекте пропускам, через контрольно-пропускные пункты. Пропуск должен быть основным документом, который дает право на проход.

Допуск откомандированных (посетителей) проводят по временным, разовым пропускам в установленные и указанные в пропуске часы, в исключительных случаях по утвержденным начальником службы безопасности спискам с предъявлением документов, которые удостоверяют личность.

Представители средств массовой информации допускаются на объект на общих основаниях в сопровождении представителей администрации.

В нерабочее время, выходные и праздничные дни допуск сотрудников на объект должен быть ограничен и вырабатываться по предыдущим заявкам (спискам) руководителей подразделов, завизированными начальником службы безопасности, с предъявлением постоянного пропуска. На предприятиях со сменным режимом работы к пропуску могут выдаваться специальные вкладыши изменяемости.

Дежурные специальных служб объекта (электрики, сантехники, работники связи и т.д.), что работают посменно, допускаются на территорию объекта в нерабочее время, в выходные и праздничные дни по спискам, подписанным начальниками соответствующих служб и утвержденными начальником службы безопасности.

На основании действующего законодательства и решение администрации отдельные категории лиц пользуются правом прохода на объект без пропуска, при предъявлении служебного удостоверения, это:

-  работники прокуратуры;
-  работники милиции по территориальности своей работы;
-  инспектора работы, котлонадзора, энергонадзора по территориальности своей работы;
-  должностные лица и отдельные категории работников санитарно-эпидемической службы органов здравоохранения, которые осуществляют санитарный надзор.

Категории лиц что имеют право прохода на объект без пропуска (по служебным удостоверениям) должны быть четко указанные в инструкции о контрольно-пропускном режиме.

С целью осуществления пропускного режима на территории объекта и в его структурных подразделениях приказом начальника предприятия утверждается перечень категорийных подразделов (помещений), хранилищ. В этих помещениях устанавливается специальный режим и повышенная ответственность за его соблюдение работниками этих подразделов.

Допуск в эти помещения осуществляется строго по списку, согласованному со службой безопасности. Прием посетителей посторонних организаций и предприятий, как правило, максимально ограничивается.

Во всех помещениях категорийных подразделений должны быть вывешенные в застекленных рамках списки работников, которые имеют допуск в эти помещения. Все помещения по окончании работ оглядываются очередными по подразделам и лицами, ответственными за их противопожарное состояние. Электричество и электронагревательная аппаратура обесточивается, окна и форточки закрываются, двери запираются на за-

мок и печатаются. По окончании рабочего дня, оборудованные охранительной сигнализацией категорийные помещения, спецхранилища и др. объекты закрываются и печатаются ответственными лицами этих подразделов. Помещения сдаются под охрану. Представитель охраны проверяет сигнализацию в присутствии работников, которые сдают помещение. Ключи от этих помещений в печатанных пеналах сдаются под расписку начальнику охраны.

Получение ключей, раскрытие помещений, оборудованных охранительной сигнализацией, делают люди, которые имеют допуск на право раскрытия этих помещений с предъявлением постоянного пропуска. Списки лиц, которые имеют право открывать (закрывать) указанные помещения с указанием номеров печатей, которыми печатаются помещения и номеров служебных телефонов, составляются и подписываются начальником подраздела и утверждаются начальником службы безопасности.

Все лица, которые стараются пройти через КПП без предъявления пропуска или по чужому, неправильно оформленному пропуску, пронести на объект (из объекта) запрещенные предметы, задерживаются и передаются в службу безопасности предприятия. По каждому факту задержки начальник охраны или старший охранник по объекту представляет служебную записку о нарушении пропускного режима.

Допуск на территорию предприятия транспортных средств, вывоз материальных ценностей

Допуск на территорию (из территории) предприятия транспортных средств, которые принадлежат предприятию, разрешается при предъявлении водителем личного пропуска со специальным шифром или транспортным пропуском и дорожным листом. Грузчики и сопроводительные лица, которые вытекают с транспортом, пропускаются через КПП на общих основаниях.

Все транспортные средства при проезде через КПП подвергаются обзору. Въезд и стоянка на территории предприятия транспорта, принадлежащим сотрудникам на правах личной собственности разрешается по специальным спискам.

Автомашины посторонних организаций, которые прибыли с грузом в адрес предприятия в рабочее время, допускаются на территорию по служебным запискам с обзором на автотранспортному КПП.

Въезд машин на территорию предприятия разрешается штатным водителем в сопровождении представителя администрации (грузополучателя).

Железнодорожный транспорт и обслуживающие его бригады пропускаются на предприятие по пропускам установленного образца, по спискам или в другом порядке установленным инструкцией о пропускном режиме. Для пропуска и обзора железнодорожного транспорта от подраздела охраны выделяется обзорная группа.

Опломбированные вагоны и контейнеры, пропускаются через КПП послу их внешнего обзора, если отражения пломб отвечают отражениям в сопроводительных документах или накладных. В случае несоответствия отражений, выявление проломов вагона (контейнера) или обрыва пломбы вагон (контейнер) подлежит раскрытию и обзору в присутствии представителей администрации и железные дороги.

Вывоз и вынос готовой продукции и других материальных ценностей из территории объекта осуществляется по материальным пропускам установленного образца.

Убедившись в правильности оформления документов и их полному соответствию с указанными ценностями, охранник оставляет на КПП пропуск, ставит на пропуске дату и время вывоза груза, расписывается и дает разрешение на вывоз материальных ценностей.

Все документы что вывозят (выносят) из предприятия материальные ценности регистрируются в бюро пропусков по книге учета и течения на следующий день передаются в бухгалтерию. Бланки всех видов материальных пропусков изготавливаются типографским способом и сохраняются в бухгалтерии, выдаются в подразделы предприятия по служебным запискам. Документы на вывоз (вынос) материальных ценностей должны быть выписанные только на (и) количество груза (мест, весы и т.п.), что может быть вывезено (вынесено), действительные только на дату, указанную в разрешительном документе.

Строительные и древесные отходы, макулатуру, металлолом, металлическую стружку рекомендуется вывозить из территории предприятия по накладной, как материальные ценности. Вывоз из территории объекта разного мусора, земли и снега может производиться без оформления документов, но с обязательной регистрацией на автотранспортном КПП.

Контроль за транспортными средствами, которые въезжают (выезжают) с территории предприятия, рекомендуется проводить в следующей последовательности.

Работник охраны, убедившись в правильности оформления сопроводительных документов должен удостовериться в соответствии наименования и количества ввезенного (или что вывозят) груза с данными, что указанные в сопроводительных документах, а также проверить скрытые места транспортного средства (которые могут употребиться для разворывания). С этой целью он осматривает транспортное средство и груз, используя специальную обзорную площадку, эстакаду. Материальные ценности на транспортном средстве должны быть положенные в определенном порядке, удобном для контроля. При пропуске опломбированных (опечатанных) грузов охранник сверяет пломбы (печати) с указанными данными в накладных, после чего, когда нет ни каких сомнений в соответствии количества и наименование груза, разрешается въезд или выезд автотранспорта. Материальные пропуска, товаротранспортные накладные регистрируются охранником в книге учета, (отдельно на ввезенные и вывезенные грузы,) в строгом соответствии с порядком их поступления.

Основные признаки возможного нападения на объект охраны

1. Обнаружение лиц, проявляющих повышенный интерес к работе фирмы и СБ:

-  использующих слуховые окна чердаков, окна подъездов, квартир, кафе, магазинов для ведения наблюдения за фирмой;
-  делающих попытки в различных инстанциях получить документацию о планировке помещений и объектов фирмы;
-  фиксирующих сотрудников, здания и территорию фирмы с помощью видеоаппаратуры;
-  пытающихся проникнуть на территорию фирмы без разрешения;

🔊 ведущих наблюдение за сотрудниками фирмы;

🔊 изучающих отходы деятельности фирмы.

2. Появление в окружении сотрудников фирмы лиц из преступной среды, пытающихся завести с ними знакомство, расспрашивающих о делах фирмы.

3. Обнаружение неестественного поведения людей вблизи фирмы:

– длительное время ведущих ремонтные, геодезические работы и не называющих своей организации;

– выдающих себя за корреспондентов радио, телевидения;

– устраивающих переносные торговые точки рядом с фирмой на малоплодном участке.

4. Длительное пребывание автомобилей рядом с фирмой.

5. Обнаружение фактов прослушивания телефонов фирмы и ее сотрудников, а также радиозакладок в помещениях.

6. Выход из строя сигнализации, связи, освещения и т.п.

7. Появление подозрительных людей в милицмейской форме, работников ремонтных служб и пожарной охраны, отказывающихся сообщить место своей службы.

8. Проверка действий СБ путем разбивания окон, создания пожароопасных и аварийных ситуаций на территории фирмы и прочих нестандартных ситуаций.

Отметив такие факты, необходимо предпринять меры по повышению безопасности фирмы:

❖ оценить ситуацию и принять решение: противостоять преступникам самостоятельно или обратиться в правоохранительные органы за помощью;

❖ усилить дежурные смены охранников, охрану руководителей фирмы и членов их семей;

❖ организовать взаимодействие с правоохранительными органами и СБ соседних фирм;

❖ уточнить боевые расчеты и провести с ними тренировку;

❖ проверить работу сигнализации, связи, запорных устройств;

❖ уменьшить объем ценностей, находящихся в фирме;

❖ усилить средства защиты при несении службы;

❖ уменьшить интенсивность перемещений охраняемых лиц и членов их семей.

Немаловажным остается вопрос взаимодействия с правоохранительными органами. Необходимость организации взаимодействия обуславливается следующими основными причинами:

1. недостаток сил и средств для выполнения задач стоящих перед охраной;

2. нехватка необходимой информации, как у охраны, так и в правоохранительных органах и т.д.

Взаимодействие необходимо обязательно организовывать на период проведения различных массовых мероприятий. В ходе проведения таких мероприятий необходимо четкое разделение функций между милицией и охраной.

Критерии эффективности работы охранного подразделения

Основными критериями эффективности работы охраны: **1.)** – есть степень защищенности от не санкционированного проникновения на охраняемый объект; **2.)** – степень обеспечения физической безопасности охраняемых лиц. Первый и второй критерий раскрывается с помощью ниже приведенной таблицы.

1.) Степень защищенности от преступного проникновения на объект: - сумма похищенного имущества по вине охраны; - количество пресеченных попыток проникновения на охраняемый объект; - количество случаев задержки сотрудников за вынос похищенного имущества; - количество лиц задержанных и привлеченных к уголовной ответственности; - количество лиц задержанных и привлеченных к административной ответственности.		2.) Степень обеспечение физической безопасности: - количество отвергнутых покушений на жизнь охраняемого лица; - количество прекращенных насильственных преступлений против охраняемого лица; - количество пресеченных действий преступников против родственников охраняемого лица; - количество задержанных лиц при попытке совершение преступления против сотрудников предприятия; - количество реализованных преступниками покушений на охраняемое лицо;

Типовой перечень документов, находящихся на КПП. (Для России)

1. Журнал учёта ввоза-вывоза-выноса товаро-материальных ценностей (ТМЦ) и служебной документации.
2. Журнал приёма и сдачи дежурства.
3. Журнал учёта принятия объектов под охрану.
4. Журнал учёта досмотра работников предприятия.
5. Журнал учёта по правонарушителям.
6. Журнал учёта посетителей.
7. Журнал учета приема ключей под охрану (на усмотрение администрации).
8. Журнал распоряжений и указаний по охране.
9. Журнал выдачи и регистрации временных пропусков.
10. Журнал выдачи и регистрации разовых пропусков и учета посетителей.
11. Рабочий журнал охранников дежурной смены.
12. Журналы регистрации первичного(вступительного) инструктажа по вопросам охраны труда (ТБ).
13. Журналы регистрации инструктажей по вопросам охраны труда.
14. График дежурств (постовая ведомость) охранников на посту №1 (КПП).

15. Копия приказа о закреплении материально-ответственных лиц по сдачу товарно-материальных ценностей под охрану.

16. Копия приказа «О мерах по усилению пропускного и внутреннего объектового режима на территории ООО «название предприятия» с приложением – подписи ВСЕХ работников Предприятия (касается прикомандированных и подрядных организаций).

17. Внутренний приказ на право проведения досмотра работниками Службы охраны.

18. Копия РАСПОРЯЖЕНИЯ „О скоростном режиме всех транспортных средств на территории ООО «название предприятия» с приложением – подписи ВСЕХ водителей (касается прикомандированных и подрядных организаций).

19. Образцы подписей материально ответственных лиц.

20. Образцы подписей должностных лиц, уполномоченных давать разрешение на вход(въезд), внос(вынос) ТМЦ на территорию Предприятия та вынос (вывоз) ТМЦ и служебной документации за пределы его территории.

21. Образцы печатей(пломб), которыми опечатываются служебные и складские помещения.

22. Должностная инструкция Начальника Службы охраны.

23. Должностная инструкция охранника.

24. Функциональные обязанности Начальника Службы охраны.

25. Функциональные обязанности охранника

26. Функциональные обязанности охранников при осуществлении патрулирования объекта в ночное время.

27. Копия Коллективного Договора или (ПРАВИЛ внутреннего трудового распорядка) в части касающаяся внутреннего трудового распорядка работы Предприятия его режима и характера труда .

28. Правила проведения досмотра в соответствии с « Инструкцией о пропускном режиме Предприятия», утвержденная Руководителем Предприятия.

29. «Инструкция о пропускном режиме на территории Предприятия»

30. Инструкция по охране труда и технике безопасности во время дежурства, (нахождения) на объекте (для охранников и Начальника Службы охраны), согласованная с Главным специалистом по охране труда.

31. Образцы всех видов пропусков ,товарных и товарно –транспортных накладных, иных сопроводительных документов на товарно-материальные ценности и служебную документацию, дающих право на их вывоз(ввоз).

32. Правила противопожарной безопасности на Предприятии (для личного состава охраны в соответствии с должностью).

33. Инструкция Первичного инструктажа « О мерах пожарной безопасности ООО «название предприятия».

34. Правила оказания первой медицинской помощи лицам с признаками нарушения дыхания , остановки сердца, в результате внезапного заболевания или травмы).

35. Опись имущества на посту охраны №1 (КПП).

36. Табель поста.

37. Расчет наряда смены поста №1 при происшествиях (при нападении на пост, при стихийных бедствиях, при пожаре на объекте или помещении охраны, при проникновении посторонних лиц на объект)

38. Бланк «Протоколов официальных визитов (проверок)» представителей контролирующих органов, приложение к «Журналу регистрации проверок» (в соответствии с Указом №.... или (Законом №.....) с учетом Вашей страны и особенностей нормативно-правовых документов.

39. Перечень лиц, не подлежащих досмотру.

40. Перечень лиц, беспрепятственного пропуска (допуска) на охраняемый объект.

41. Перечень автотранспорта, имеющего право на беспрепятственный въезд-выезд на охраняемую территорию.

42. Перечень автотранспорта, не подлежащего досмотру при въезде-выезде с территории.

43. Список всех работников (служащих) Предприятия по подразделениям.

44. Номера телефонов аварийных городских служб, скорой медицинской помощи, милиции, пожарной и ФСБ...

45. Список адресов и телефонов руководителей Предприятия.

46. Список адресов и телефонов работников Службы охраны Предприятия.

47. Список материально-ответственных лиц с адресом и домашним (мобильным) телефоном.

48. .Положение о Службе охраны и тех. защите Предприятия.

49. „Правила оказания первой медицинской помощи”, (Приложение к инструкции).

50. ОБРАЗЕЦ „ ЗАЯВЛЕНИЕ на выдачу разового пропуска”

51. ОБРАЗЕЦ „ ЗАЯВЛЕНИЕ на выдачу временного пропуска”

52. ПАМЯТКА для личного состава охраны о „ПОРЯДКЕ ПРОВЕДЕНИЯ ИНСТРУКТАЖЕЙ ДЛЯ РАБОТНИКОВ” „ИНСТРУКТАЖЕЙ ПО ВОПРОСАМ ОХРАНЫ ТРУДА”..

53. ПАМЯТКА для личного состава охраны „Пропускные документы, их виды и порядок оформления”

**Типовой перечень документов, находящихся на КПП.
(Для Украины)**

ПЕРЕЛІК ПАПКИ “СЛУЖБОВА ДОКУМЕНТАЦІЯ СЛУЖБИ ОХОРОНИ”			
№п/п	Найменування документу	Дата виділення	ПІДПИС
ЖУРНАЛИ (книги)			
1	ЖУРНАЛ № 1 обліку прийому та передачі чергування		
2	ЖУРНАЛ № 2 обліку та реєстрації ввезення/вивезення, внесення/винесення ТМЦ і службової документації через КПП		
3	ЖУРНАЛ № 3 обліку та реєстрації прийому об’єктів під охорону від уповноважених (згідно наказу) посадових осіб		
4	ЖУРНАЛ № 4 видачі та реєстрації разових перепусток та обліку відвідувачів		
5	ЖУРНАЛ № 5 обліку видачі та реєстрації тимчасових перепусток		
6	ЖУРНАЛ № 6 обліку проведення особистого огляду, огляду речей, які виносяться через КПП		
7	ЖУРНАЛ № 7 обліку наказів, розпоряджень та вказівок по організації охорони		
8	ЖУРНАЛ № 8 обліку та реєстрації правопорушень, виявлених на території охороняемого об’єкту		
9	ЖУРНАЛ № 9 для запису службових поміток, які стосуються організації охорони під час чергування		
10	ЖУРНАЛ № 10 реєстрації інструктажів з питань охорони праці		
11	ЖУРНАЛ № 11 вступного інструктажу з питань охорони праці		
12	ЖУРНАЛ № 12 обліку зберігання особистих речей;		
Закони України про працю, внутрішні нормативні документи, які регулюють трудові відносини працівників підприємства (включаючи охорону)			
13	КОДЕКС ЗАКОНІВ про працю УКРАЇНИ (глава III, IV, V, X, XI)		
14	Адміністративне законодавство України глава 20.ст.264,ст.265 ”Особистий огляд і огляд речей”, ”Вилучення речей і документів”		

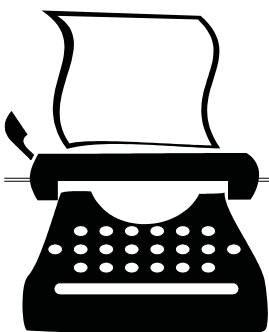
15	Копія „ПРАВИЛ ТРУДОВОГО РОЗПОРЯДКУ” стосовно: режиму роботи, тривалості робочого часу і його використання, порядку прийняття та звільнення працівників, відповідальності за порушення трудової дисципліни працівниками підприємства (включаючи працівників Служби охорони).		
16	Копія наказу № 24 від 06.06.2005 р. „Про заходи по зміцненню перепускного режиму і внутрішнього об’єктового режиму на території ТОВ “_____”.		
17	Копія НАКАЗУ № _____ від „_____” _____ 200_ р. „Про створення Служби охорони та технічного захисту на правах структурного підрозділу підприємства”		
18	Копія НАКАЗУ № _____ від „_____” _____ 2005 р. „Про закріплення матеріально -відповідальних посадових осіб на право передачі ТМЦ (о”єктів) під охорону.		
19	Положення про Службу охорони та технічного захисту ТОВ “_____”.		
20	Оригінал „Інструкції про про перепускний режим на території ТОВ „_____”, затверджена керівництвом.		
21	Копія РОЗПОРЯДЖЕННЯ №25 від 06.06.200_ р., „Про швидкісний режим всіх транспортних засобів на території ТОВ “_____”.		
ДОКУМЕНТАЦІЯ ПО ТЕХНІЦІ БЕЗПЕКИ на ПІДПРИЄМСТВІ			
22	Інструкція з охорони праці начальника Служби охорони та технічного захисту ТОВ “_____”, затверджена керівництвом та погоджена з Головним спеціалістом по охороні праці.		
23	ПАМ"ЯТКА для особового складу охорони про „ПОРЯДОК ПРОВЕДЕННЯ ІНСТРУКТАЖІВ ДЛЯ ПРАЦІВНИКІВ” „ІНСТРУКТАЖІ З ПИТАНЬ ОХОРОНИ ПРАЦІ”.		
24	Інструкція з охорони праці охоронника ТОВ “_____”, затверджена керівництвом та погоджена з Головним спеціалістом по охороні праці.		
25	Інструкція №1(копія) з питань пожежної безпеки для всіх підрозділів підприємства , затверджена наказом директора ТОВ “_____” №11 від 05.09.2_____ р.		

Служба безпеки – залог успеха підприємництва

26	„ПРАВИЛА надання першої медичної допомоги особам з ознаками порушення дихання, зупинки серця, у разі раптового захворювання чи травми”, ДОДАТОК до ІНСТРУКЦІЇ .		
27	Загальна Інструкція для особового складу з охорони праці та техніки безпеки під час чергування на об’єкті;		
СЛУЖБОВА ДОКУМЕНТАЦІЯ ПО БЕЗПОСЕРЕДНІЙ ОРГАНІЗАЦІЇ ОХОРОНИ НА ОБ’ЄКТІ			
28	ПОСАДОВА ІНСТРУКЦІЯ начальника начальни-ка Служби охорони та технічного захисту ТОВ “ _____ ”		
29	ФУНКЦІОНАЛЬНІ ОБОВ’ЯЗКИ начальника служ-би охорони та технічного захисту ТОВ “ _____ ”		
30	ПОСАДОВА ІНСТРУКЦІЯ охоронника поста №1(КПП)		
31	ФУНКЦІОНАЛЬНІ ОБОВ’ЯЗКИ охоронників по-ста №1(КПП) по пропуску людей і автомобільно-го транспорту		
32	ПОСАДОВА ІНСТРУКЦІЯ охоронника поста №2(піший патруль)		
33	ФУНКЦІОНАЛЬНІ ОБОВ’ЯЗКИ охоронника поста №2(піший патруль) при здійсненні парулювання		
34	Загальна Інструкція особовому складу Служби охорони та технічного захисту по організації ,по-рядку несення служби та дій в екстремальній ситу-ації при охороні об’єктів підприємства.		
35	Графік чергування (Пособна відомість) охорон-ників поста №1(КПП)		
36	Графік чергування (Пособна відомість) охорон-ників поста №2(піший патруль)		
37	Перелік (списки) посадових осіб, що мають право на пересічення меж «Об’єкту» без догляду; (дода-ток №1)		
38	Перелік(списки) автотранспортних засобів, з ука-занням реєстраційних номерів, які мають право на проїзд КПП без огляду (додаток №1)		
39	Перелік (списки) посадових осіб, які мають право безперешкодного відвідування території підприємства (додаток №1)		
40	Перелік(списки) автотранспорту ,який має право безперешкодного заїзду-виїзду на територію підприємства (додаток №1)		

41	Зразки підписів посадових осіб, що уповноважені згідно НАКАЗУ № _____ від „_____” _____ 2005 р. „ Про закріплення матеріально -відповідальних посадових осіб на право передачі ТМЦ (о’єктів) під охорону”. (додаток №2)		
42	Зразки підписів посадових осіб, що уповноважені надавати дозвіл на вхід (в’їзд, внесення (ввезення) ТМЦ на «Об’єкт», та винесення (вивезення) ТМЦ та службових документів за його межі; (додаток №2)		
43	Зразки штампів, печаток, пломб, якими візуються супроводжувальні ТМЦ або службові документи; (додаток №2)		
44	Зразки усіх видів перепусток, товарних та товарно-транспортних накладних, інших супроводжувальних ТМЦ документів;		
45	ПАМ’ЯТКА для всього особового складу охорони „ПРАВИЛА та порядок проведення під час несення служби огляду речей і особистого огляду працівників підприємства”, згідно „Інструкції про про перепускний режим на території ТОВ „_____”, затверджена керівництвом.		
46	ПАМ’ЯТКА для особового складу охорони „Перепускні документи, їх види та порядок оформлення”		
47	Перелік (опис) майна на посту охорони №1 (КПП).		
48	ЗРАЗОК „ЗАЯВКА на видачу разової перепустки”		
49	ЗРАЗОК „ЗАЯВКА на видачу тимчасової перепустки”		
50	Табель поста.		
51	Послідовність дій особового складу охорони чергової зміни у випадку: нападу на пост,пожежі на об’єкті або приміщенні охорони,проникнення сторонніх осіб на об’єкт, стихійного явища		
52	Бланк „Протоколу офіційних візитів (перевірок) представників контролюючих органів”,додаток до «Журналу реєстрації та перевірок» (згідно Указу № 817/98 від 23.07.98 р. “О некоторых мерах по дерегуляции предпринимательской деятельности”, ст.7) та затвердженому Наказом Державного комітету України з питань розвитку підприємництва №18 від 10 серпня 1998р.		
53	Перелік працівників підприємства (стосується прикомандированих та підрядних організацій)по підрозділам, ознайомлених з внутрішніми нормативними документами по охороні.		

54	Списки номерів телефонів міських аварійних служб:пожежної,швидкої допомоги,МНС,райвідділу УМВС та райвідділу УСБУ в _____ області, управління Служби безпеки та інших служб.(додаток №3)		
55	Списки адреси та номерів телефонів керівників підприємства.(додаток №3)		
56	Списки адреси та номерів телефонів особового складу .Служби охорони підприємства..(додаток №3)		
57	Списки адреси та номерів телефонів матеріально -відповідальних посадових осіб на право передачі ТМЦ (о"єктів) під охорону.(додаток №3)		
58	Папка з матеріалами особистих справ працівників Служби охорони та технічного захисту ТОВ " _____ "		
59	Схема закріплення території для підтримки чистоти та порядку.		
60	Схема тех.укріплення об'єкту.		
61	Схема безпечного переміщення під час патрулювання території в темний час доби.		
62	Схема розташування автотранспорту на охороняємій території .		
63	Схема екстренного евакуювання автотехніки з охороняємої території у випадку виникнення пожежі		
<i>Начальник служби безпеки</i>		<i>(підпис)</i>	



Защита коммерческой тайны предприятия

В современных условиях в нашей стране проблема коммерческой безопасности предприятия, банка, фирмы является очень актуальной, потому что без нее невозможно обеспечить безопасность бизнеса вообще.

В данной главе авторы тему : « Защита коммерческой тайны предприятия» предлагают рассмотреть на примере работы банковского учреждения (предприятия), в дальнейшем – банк.

Наши авторы неоднократно подчеркивают, что несмотря на очевидность особой значимости защиты предпринимательской деятельности,

проблема ее обеспечения не стала приоритетной для большинства бизнесменов стран СНГ, России, Украины. Об этом свидетельствует отсутствие соответствующих служб безопасности примерно у половины коммерческих фирм, низкие расходы банков и фирм на их содержание, а также недостаточная компетентность значительной части первых лиц в сложных вопросах безопасности себя и своих структур, наличие у них криминальной, (в т.ч. «беловоротничковой») «крыши», а также преступный характер определенной части негосударственных предприятий.

Предприниматель, не знакомый с этой проблематикой, не может считать себя в полной мере подготовленным для работы в условиях рыночной экономики, когда законодательная база «хромает на две ноги», а коррупция рождает борьбу между субъектами рыночных отношений.

Выпускник любого ВУЗа, где бы он ни начал работать, везде и всегда будет сталкиваться с проблемами безопасности предпринимательской деятельности, (защиты коммерческой тайны). Данную главу, наши авторы решили начать с информационно-аналитической работы службы безопасности банка, фирмы, необходимой для обеспечения безопасности предпринимательской деятельности с учетом прогнозирования возможных преступлений в бизнесе. Так как война умов в бизнесе и банковском деле уже вступила в решающую фазу, данная книга будет в значительной мере удовлетворять требованиям предпринимателей, и будет им «настойчивой книгой», чтобы обезопасить себя, свою деятельность. Начнем с самого простого и выделим 7 основных понятий:

Коммерческая тайна – информация, которая 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.

Банковская тайна – разнovidность коммерческой тайны, которая заключается в том, что банки стремятся скрыть сведения о своих операциях с целью закрепить за собой высокие прибыли.

Канал утечки информации – вариант технологии несанкционированного доступа к информации.

Способы защиты информации – действия по выявлению возможных каналов утечки информации, оценке степени опасности каждого реально-го канала, локализации (подавлению) опасных каналов и контроль за надежностью защитных мероприятий по сохранению информации.

Конкуренты – фирмы, организации, учреждения, отдельные граждане, которые сознательно противодействуют достижению банком, фирмой основных целей либо стремятся нанести прямой ущерб их деятельности.

Кредитоспособность – наличие предпосылок для получения кредита, способность возратить его.

Платежеспособность – способность и возможность физического или юридического лица оплатить свои долги.

Роль руководства банка в обеспечении безопасности

Служба безопасности банка, фирмы в лице ее начальника подчиняется непосредственно первому лицу предприятия. Прерогативой руководителя банка, фирмы по обеспечению безопасности руководимой им структуры является решение следующих вопросов

- 👁️ разработка стратегии деятельности службы безопасности;

- 👁 указание основных направлений в обеспечении безопасности предприятия;
- 👁 утверждение нормативных актов, разработанных службой безопасности;
- 👁 дача распоряжений начальнику службы безопасности по разработке аналитических документов, связанных с исследованием различных аспектов обеспечения безопасности предприятия;
- 👁 издание на основе анализа этих документов соответствующих распоряжений по совершенствованию обеспечения безопасности предприятия;
- 👁 привлечение начальника службы безопасности к ведению деловых переговоров с солидными клиентами, потенциальными партнерами и их изучение;
- 👁 обеспечение службой безопасности защиты кредитной политики банка и иных финансово-кредитных предприятий;
- 👁 привлечение службы безопасности к участию в подборе сотрудников банка, фирмы;
- 👁 дача распоряжений по использованию службы безопасности в процессе обучения персонала предприятия по вопросам безопасности;
- 👁 утверждение структуры службы безопасности;
- 👁 выделение финансовых средств для деятельности службы безопасности;
- 👁 организация совета безопасности предприятия под руководством первого лица банка, фирмы;
- 👁 создание механизма управления предприятием в чрезвычайных ситуациях («тревожный» комитет);
- 👁 оценка эффективности деятельности службы безопасности и др.

Чтобы успешно руководить службой безопасности предприятия, предприниматели должны быть компетентны в вопросах обеспечения безопасности, ибо от этого прежде всего зависят как состояние защищенности предпринимательских структур, так и их личная безопасность.

Первое лицо предприятия в своей деятельности должно руководствоваться рядом аксиом:

- 1.) «Безопасность – это наука, которую надо изучать и развивать, это искусство, которое надо постигать, это культура, которую надо воспитывать у бизнесмена»;
- 2.) «Всякий бизнес только тогда чего-нибудь стоит, когда он надежно защищен»;
- 3.) «Опасность легче упредить, чем с ней бороться»;
- 4.) «Основа успеха в бизнесе – своевременно полученная, правильно и умело использованная информация»

Потенциальная и реальная угрозы безопасности предпринимательских структур существуют в отношении их персонала, помещений, оборудования, материальных ценностей, наличных денег, информации. Угрозы персоналу банков, фирм могут осуществляться в форме нападений, шантажа, вымогательства, похищений руководителей, сотрудников и членов их семей, убийств. Угрозы помещениям, оборудованию и материальным

ценностям выражаются в их повреждениях, захватах, поджогах, минировании, обстрелах, взрывах. Угрозы в отношении информации заключаются в ведении промышленного шпионажа.

Промышленный шпионаж против банков и фирм

Структуры, занимающиеся промышленным шпионажем в отношении своих конкурентов – банков, фирм и других коммерческих организаций, стремятся добыть информацию прежде всего по следующим вопросам:

- 👁 стратегия и планы развития;
- 👁 финансовые прогнозы, отчеты и положение;
- 👁 маркетинг;
- 👁 условия оказания услуг;
- 👁 характеристика производимой и перспективной продукции;
- 👁 партнеры, клиенты и содержание договоров с ними;
- 👁 организационная структура;
- 👁 система безопасности, в первую очередь средства защиты конфиденциальной информации и т.д.

В процессе ведения промышленного шпионажа применяются следующие способы:

- 👁 использование внедренных в банк, фирму агентов;
- 👁 привлечение к сотрудничеству служащих банков и фирм;
- 👁 сманивание сотрудников, обладающих ценной конфиденциальной информацией;
- 👁 выведывание;
- 👁 подкуп ведущих специалистов и иных сотрудников;
- 👁 ложное приглашение сотрудников на работу с проведением с ними бесед для получения конфиденциальных сведений;
- 👁 ведение наблюдения за объектом и его сотрудниками;
- 👁 подслушивание переговоров с помощью технических средств;
- 👁 похищение необходимых документов;
- 👁 тайное фотографирование объекта, его сотрудников и документов;
- 👁 добывание информации через партнеров, клиентов, особенно пострадавших по вине конкурента;
- 👁 получение информации через коррумпированных сотрудников государственных структур;
- 👁 копирование документов;
- 👁 подделка документов, печатей, ключей и т.д.

Подготовки и совершения преступных акций против предпринимательских структур

Основными объектами преступных посягательств криминальных элементов являются коммерческие банки. Главную угрозу для банков и фирм представляют нападения. Эти преступные акции с точки зрения организации и осуществления делятся на 4 этапа:

- 1 – информационно-разведывательный,
- 2 – подготовительный,
- 3 – проведение нападения,

4 – сокрытие следов.

В процессе информационно-разведывательного этапа криминальные элементы для добывания сведений знакомятся с банком, изучают его персонал и сотрудников службы безопасности, устанавливают доверительные отношения с лицами, посещающими банк в силу служебных обязанностей, анализируют деятельность банка по всем направлениям. Для знакомства с банком криминальные элементы осуществляют следующие действия:

1.) Информационно-разведывательный этап:

- 👁 открытое посещение банка якобы для установления деловых контактов, возможного трудоустройства;
- 👁 посещение банка под видом сотрудников милиции, телефонной станции, энергонadzора и т.д. (в таких случаях используют поддельные документы);
- 👁 фотографирование, кино- или видео съемку банка с различных позиций для определения уязвимых мест;
- 👁 изучают необходимую литературу и документацию о банке, и проходящих через него коммуникаций: (электро-водо-тепло-газовые и другие).

Кроме того, используют скрытое наблюдение за банком для изучения режима его работы, клиентуры, порядка следования машин инкассации, доставки и отправки грузов; конфиденциальные связи, а также современные технические средства.

В процессе изучения персонала банка выясняют образ жизни, связи, моральные качества, материальное положение и особенности отдельных лиц. Полученные сведения используют для склонения их к сотрудничеству посредством подкупа, шантажа, запугивания. Изучение сотрудников службы безопасности банка ведется параллельно с выяснением режима охраны и пропуска (техническая оснащенность, наличие оружия). Потенциальные преступники стремятся добыть материалы, компрометирующие руководителей службы безопасности, при необходимости оказать на них психологическое давление – запугать, а в отдельных случаях – совершают убийства. Установление доверительных отношений с представителями налоговой администрации, пожарной охраны и их подкуп позволяют преступникам получать интересующую их информацию о банке, что облегчает не только совершение нападения или иного преступления, но и установление криминальной «крыши» над банком.

2.) На подготовительном этапе преступники совершают следующие действия:

- 👁 разрабатывают план нападения на банк;
- 👁 создают преступную группу, распределяют среди участников обязанности, обеспечивают их безопасность;
- 👁 приобретают оружие, взрывчатые вещества для проникновения на объект, автотранспорт, организуют наблюдение в различное время суток;
- 👁 разрабатывают маршрут выдвижения и сосредоточения участников группы;
- 👁 разрабатывают схему управления действиями участников группы;

- 👁️ трудоустраивают отдельных членов преступной группы в банк в качестве охранников;
- 👁️ приобретают документы и форму сотрудников правоохранительных органов, муниципальных служб и т.д.;
- 👁️ тренируют группу к предстоящему нападению в условиях, приближенных к реальным;
- 👁️ проверяют реагирование службы безопасности и прежде всего охраны банка на различные ситуации (попытки проникновения на объект, срабатывание системы сигнализации, стрельба, драки, автомобильные аварии вблизи него).

3.) На этапе проведения нападения на банк преступники осуществляют:

- 👁️ сбор участников группы и уточнение порядка их действий согласно плану;
- 👁️ скрытое выдвижение группы к банку;
- 👁️ отвлечение внимания службы безопасности и персонала посредством организации аварий, драк и т.д.;
- 👁️ проникновение на объект скрытно либо открыто с помощью взлома, взрыва, тросов, лебедок, через двери, окна, проходы, лазы.

Для дезорганизации действий охраны и персонала банка преступники применяют такие средства психологического воздействия, как взрывпакеты, звуковые автоматические свистки, ослепляющие в темное время фонари;

- 👁️ вынос и вывоз награбленного ценного оборудования, имущества и наличности;
- 👁️ уход и отъезд преступников с места совершения преступления. Ограбление обычно совершается за 1-3 минуты.

4.) Этап сокрытия следов включает следующие действия:

- 👁️ реализация преступно добытых материальных ценностей;
- 👁️ сокрытие исполнителей преступления;
- 👁️ вложение добытых средств в бизнес;
- 👁️ противодействие службе безопасности, государственным правоохранительным органам в расследовании преступления посредством сокрытия его следов, уничтожения ненадежных исполнителей и др.

По имеющимся данным, 85 % коммерческих предприятий, не использующих услуги служб безопасности и охранных структур, подвергаются преступным воздействиям со стороны криминальных элементов и конкурентов. Анализ ограбления банков, в частности их кассовых зон, свидетельствует о том, что нападения на охраняемые кассовые зоны завершались удачно для преступников в 39 случаях из 100, а на неохраняемые – в 89 случаях. Применительно к ограблениям фирм показатели выглядят так: более 50 % нападений совершено на объекты со свободным допуском персонала и клиентов; 25 % нападений – на объекты с пассивными ограничениями и неохраняемыми заграждениями; 20 % – на объекты с охраняемыми заграждениями; 5 % – на объекты с усиленным режимом охраны.

На основании анализа характера угроз безопасности предпринимательской деятельности, изучения практики и тенденций действий криминальных элементов, службы безопасности организуют свою деятельность, задействуют систему безопасности банков и фирм, вырабатывают адекватные меры противодействия.

Структура, функции, цели и задачи службы безопасности банка

С учетом характера и масштабов деятельности банка, фирмы, анализа потенциальных и реальных угроз их безопасности со стороны криминальных элементов и конкурентов, а также финансовых возможностей руководство предпринимательской организации определяет структуру и численность службы безопасности. Служба безопасности крупного предприятия состоит, как правило, из следующих подразделений: оперативного, добывания коммерческой информации, информационно-аналитического, режима и охраны, защиты электронно-вычислительной техники и каналов связи.

Основные функции оперативного подразделения:

- 👁️ обеспечение безопасности руководства, главных специалистов и других сотрудников банка, фирмы;
- 👁️ обеспечение безопасности объектов, территории, оборудования и продукции фирмы;
- 👁️ контроль за соблюдением действующих в банке, фирме режимов;
- 👁️ выявление фактов подготовки различных акций в отношении банка, фирмы, их сотрудников и клиентов со стороны криминальных элементов и конкурентов;
- 👁️ противодействие этим акциям;
- 👁️ контроль за обстановкой в коллективах подразделений банка, фирмы;
- 👁️ сбор и представление в информационно-аналитическое подразделение службы безопасности данных о фактах, имеющих значение для обеспечения безопасности предприятия;
- 👁️ связь со средствами массовой информации;
- 👁️ контроль за научными и иными публикациями сотрудников банка, фирмы.

Основные функции подразделения добывания коммерческой информации сводятся к получению следующих сведений:

- 👁️ о криминальных элементах в местах и районах расположения банка, фирмы и проживания их руководителей и персонала;
- 👁️ о конкурентах банка, фирмы и потенциальных клиентах;
- 👁️ о конъюнктуре рынка в соответствующих регионах и странах;
- 👁️ об обстановке в тех регионах и странах, где банк, фирма планируют выйти на рынок.

Подразделение службы безопасности также занимается постоянным изучением партнеров и клиентов, с которыми заключены кредитные и иные договоры на крупные суммы, и проводит мероприятия по созданию благоприятных условий для выхода банка, фирмы на рынок. Вся добытая информация представляется в информационно-аналитическое подразделение службы безопасности.

Основные функции информационно-аналитического подразделения:

- 👁️ сбор информации по вопросам обеспечения безопасности банка, фирмы от подразделений службы безопасности;
- 👁️ переработка этой информации в соответствии с разработанной и заложеной в информационную систему структурой;
- 👁️ выдача имеющейся в базе данных информации по требованию руководства предприятия и службы безопасности;
- 👁️ исследование поступающей в базу данных информации и представление первому лицу банка, фирмы аналитических обзоров и иных документов;
- 👁️ защита базы данных от умышленного или неумышленного разрушения и утечки накопленной в ней информации к криминальным элементам и конкурентам;
- 👁️ организация координации и взаимодействия с другими базами данных банка, фирмы и с разрешения их руководства – с банками данных партнеров и информационных центров.

Основные функции подразделения режима и охраны:

- 👁️ разработка и реализация режимов физической охраны (руководства банка, фирмы и некоторых главных специалистов, персонала и клиентов, объектов, территории, оборудования, продукции, перевозок финансовых средств, сырья, продукции);
- 👁️ контроль за выполнением сотрудниками установленных в банке, фирме режимов;
- 👁️ физическое противодействие возможным акциям криминальных элементов и конкурентов в отношении руководства, персонала, клиентов, объектов, наличности;
- 👁️ взаимодействие с государственными правоохранительными органами в вопросах обеспечения физической безопасности банка, фирмы;
- 👁️ сбор и представление в информационно-аналитическое подразделение сведений о фактах, имеющих значение для обеспечения безопасности банка, фирмы.

Основные функции подразделения защиты электронно-вычислительной техники и каналов связи:

- 👁️ выявление технических каналов утечки конфиденциальной информации и возможных фактов ведения криминальными элементами и конкурентами технической разведки против банка, фирмы;
- 👁️ предотвращение утечки конфиденциальной информации посредством технических средств и каналов;
- 👁️ применение технических средств для добывания сведений о конкурентах и др.;
- 👁️ предоставление в информационно-аналитическое подразделение информации о выявленных угрозах безопасности банка, фирмы со стороны криминальных элементов и конкурентов с использованием технических средств.

Цели, задачи и принципы обеспечения безопасности банка

Цели обеспечения предпринимательской деятельности вытекают из главных направлений деятельности предприятия, потенциальных и реальных угроз внешнего и внутреннего характера экономического состоянию банка, фирмы и реализации их основного жизненного интереса – получению стабильной прибыли. Целями обеспечения безопасности предпринимательской деятельности являются:

- 👁️ устранение внешних и внутренних угроз экономическому благополучию банка, фирмы;
- 👁️ обеспечение благоприятных условий реализации основных интересов, закреплённых в их учредительных документах.

Задачи обеспечения безопасности предпринимательской деятельности:

- 👁️ обеспечение реализации законных прав и интересов банка, фирмы, сотрудников;
- 👁️ сохранение интеллектуальной и материальной собственности банка и фирмы;
- 👁️ своевременное выявление реальных и потенциальных угроз жизненно важным интересам банка, фирмы;
- 👁️ вскрытие внутренних причин и условий, способствующих нанесению банку, фирме, их сотрудникам материального, психологического и иного ущерба;
- 👁️ разработка и реализация механизма оперативного реагирования на возникающие угрозы и негативные тенденции в развитии обстановки в отношении банка, фирмы;
- 👁️ сбор, анализ, оценка и представление руководству банка, фирмы информации по всем направлениям деятельности службы безопасности;
- 👁️ предотвращение проникновения в структуру криминальных элементов;
- 👁️ противодействие техническому проникновению на предприятие субъектов противоправной деятельности;
- 👁️ физическая и техническая охрана банков, фирм, их территории и транспорта;
- 👁️ участие в формировании и укреплении положительного имиджа банка, фирмы среди партнеров, клиентов, общественности и населения;
- 👁️ локализация или ослабление вредных последствий в связи с неправомерными действиями физических и юридических лиц в отношении банка, фирмы.

Для достижения целей и задач обеспечения безопасности предпринимательской деятельности предполагается соблюдение следующих принципов создания и функционирования системы безопасности законности, экономической целесообразности, профессионализма, координации и взаимодействия, ответственности, конфиденциальности.

Основными критериями **оценки качества** работы службы безопасности банка, фирмы являются стабильность функционирования предприятия и получение им гарантированных прибылей. Таким образом, для качественной работы службе безопасности необходимо:

- 👁 выявлять, предотвращать и пресекать насильственные посягательства на жизнь и здоровье сотрудников;
- 👁 не допускать утечки и разглашения сведений, составляющих коммерческую тайну, и утраты важных документов и изделий;
- 👁 сохранять материальные ценности и финансы;
- 👁 своевременно выявлять попытки несанкционированного проникновения криминальных элементов на объект в преступных целях,
- 👁 предупреждать чрезвычайные происшествия.

Исходя из целей и задач обеспечения безопасности деятельности банка, можно определить основные объекты защиты, а также силы и средства, используемые службой безопасности.

Объекты защиты, силы и средства службы безопасности банка

Объекты защиты службы безопасности:

- 👁 руководители, ведущие специалисты, рядовые сотрудники банка, фирмы;
- 👁 конфиденциальная информация;
- 👁 материально-технические ценности, финансовые средства.

Силы и средства службы безопасности:

- 👁 ее руководители и сотрудники;
- 👁 конфиденциальные связи из числа граждан Украины, иностранцев и лиц без гражданства;
- 👁 специальные технические средства (оптические приборы, кино-, фото-, видеоаппаратура, средства связи, электронно-вычислительная техника, транспорт);
- 👁 средства информационного обеспечения (справочные учеты и информационные системы);
- 👁 денежные средства.

Главным звеном системы обеспечения безопасности предпринимательской деятельности являются мероприятия, осуществляемые службой безопасности банка, фирмы. Комплекс мероприятий, перс-численных в планах, принято называть системой мер обеспечения безопасности банка, фирмы.

Комплекс мер по обеспечению безопасности банка, (предприятия, фирмы)

Меры по обеспечению безопасности предпринимательской деятельности условно можно разделить на две группы:

А) – Первая, это меры общего обеспечения безопасности;

Б) – Вторая, это меры, направленные непосредственно на предотвращение противоправных действий субъектов угроз. Мероприятия первой группы направлены на предупреждение, затруднение и ограничение возможности продления противоправных действий в отношении банка, фирмы со стороны неустановленных злоумышленников. Поэтому они являются превентивными, носят предупредительный характер и осуществляются гласно. Мероприятия второй группы предназначены для выявления, локализации и недопущения конкретных акций криминальных элементов и конкурентов в отношении банка, фирмы. Они проводятся негласно.

Наши авторы выделили **первую группу мер** общего обеспечения безопасности банка, (предпринимательской деятельности фирмы):

1. Введение в банке, фирме различных режимов безопасности, разработку инструкций по обеспечению режима конфиденциальности, физической охране объектов, сохранности коммерческой тайны и др.

2. Гласный контроль за исполнением установленных на объектах режимов.

3. Противодействие легальной промышленной разведке со стороны субъектов угроз. В этой связи рекомендуется:

- 👁️ “составить легенду” о характере и месте производства интересующей конкурентов продукции;
- 👁️ использовать средства массовой информации для доведения до конкурентов и других субъектов угроз выгодной предприятию информации о его деятельности, продукции и т.д.;
- 👁️ применять маскировку производства или изделий для сокрытия их истинного назначения.

4. Противодействие технической разведке субъектов угроз. В этих целях рекомендуется:

- 👁️ периодически применять приборы для выявления электронных закладок во всех помещениях и особенно в местах проведения переговоров, а также проверять состояние линий и средств связи;
- 👁️ готовить помещения, в которых планируется проведение переговоров и совещаний, (из таких помещений должны быть удалены все электронные и электрические приборы, в них не должно быть окон, выходящих на улицу, и неконтролируемых стен; помещение должно быть экранировано, или на время переговоров, совещаний в нем должны работать приборы, создающие общее фоновое излучение (магнитофон, радиоприемник);
- 👁️ перед и после переговоров, совещаний помещение должно тщательно проверяться электронными средствами.

5. Защиту средств связи с использованием следующих способов:

- 👁️ установка на объектах банка, фирмы автономных и защищенных средств связи – телефонных подстанций и т.д.;
- 👁️ применение специальных шифрующих устройств к телефонам и персональным ЭВМ для кодирования передаваемой информации; использование оптико-волоконных средств связи, которые исключают излучение вовне.

6. Предупредительно-профилактическое воздействие на сотрудников банка, фирмы, имеющее целью добиться выполнения ими установленных на предприятии режимов. Нарушение этих режимов, а также совершение отдельными сотрудниками преступлений бывают обусловлены различными причинами. Важными факторами, способствующими снижению риска нарушений установленных режимов и совершения преступлений, являются:

- 👁️ правильный подбор персонала и создание на предприятии здорового морально-психологического и этического климата, (в этой связи важно изучать и по мере возможности перенимать с учетом русского и украинского менталитета, японский, американский и иной передовой зарубежный опыт создания в коммерческих

структурах соответствующей атмосферы патриотизма, гордости, соблюдения фирменного кодекса чести, преданности фирме);

👁 адекватная моральная и материальная оценка результатов труда и уровня компетенции сотрудников;

👁 знание и соблюдение сотрудниками основных требований установленных на предприятии режимов.

7. Применение мер административного принуждения экономического и морального характера. К экономическим мерам относятся: понижение в должности; снижение зарплаты; лишение определенных материальных льгот; увольнение с работы. Моральные меры воздействия могут быть следующими: беседы с руководством предприятия; перевод в менее комфортные условия работы; не приглашение на переговоры, встречи, симпозиумы и т.д.

Вторая группа мер, непосредственно направленных на предотвращение противоправных действий субъектов угроз предпринимательской деятельности, осуществляется с использованием конфиденциальных связей отдельных сотрудников банка, фирмы и обычно включают в себя:

1. Конфиденциальный контроль за состоянием обеспечения безопасности предприятия, прежде всего за поддержанием его персоналом установленных режимов. Добытые службой безопасности сведения доводятся до первого лица предприятия для ознакомления и устранения обнаруженных недостатков и нарушений посредством издания соответствующих приказов, дачи устных распоряжений.

2. Конфиденциальный контроль за обстановкой в коллективах подразделений банка, фирмы (этому направлению деятельности уделяется особое внимание в японских компаниях). Служба безопасности предприятия должна отслеживать происходящие в коллективе процессы, знать их причины и принимать участие в их локализации под руководством первого лица. Обстановка в коллективах напрямую связана с обеспечением сохранности коммерческой тайны и иными аспектами безопасности банка, фирмы. Поэтому вопросам отбора, подготовки, выдвижения и увольнения кадров необходимо уделять больше внимания, чем засекречиванию информации.

3. Выявление возможных каналов утечки конфиденциальных сведений. В этой связи служба безопасности должна добывать информацию о характере устремлений субъектов угроз по отношению к банку, фирме и их сотрудникам, а также о степени осведомленности криминальных элементов, конкурентов, иных юридических и физических лиц о предприятии.

4. Выявление и проверка сотрудников банка, фирмы подозреваемых в работе на криминальные элементы и конкуренты.

5. Предупредительно-профилактическое воздействие на сотрудников, нарушивших установленные на предприятиях режимы, через конфиденциальные связи.

6. Обеспечение безопасности руководителей, ведущих специалистов и рядовых сотрудников банка, фирмы, выезжающих за рубеж, с целью предотвратить привлечение их к сотрудничеству иностранными специальными службами, недопущения их дискредитации. До выезда за рубеж сотрудники банка, фирмы должны пройти правовую, страноведческую и психологическую подготовку.

7. Проникновение к конкурентам. Это наиболее сложное направление в деятельности службы безопасности. Оно предполагает наличие высокого уровня профессионализма.

8. Конфиденциальное расследование по фактам утраты документов сотрудниками банка, фирмы. В таких случаях служба безопасности обычно выясняет следующие вопросы: каким образом пропал документ (украден, передан, уничтожен); какую информацию о банке, фирме содержал документ (степень конфиденциальности и важности информации, объем деформации, время значимости информации); какие опасные для банка, фирмы действия могут предпринять субъекты угроз на основании данной информации и в течение какого времени. Исходя из этого, служба безопасности предпринимает действия по компрометации исчезнувшего документа и канала утечки информации посредством дезинформирования документа и канала.

9. Конфиденциальное расследование чрезвычайных происшествий, похожих на акции вредительства со стороны криминальных элементов и конкурентов. В процессе расследования важно убедиться, имеют ли отношение к чрезвычайному происшествию субъекты угроз. Если такие предположения подтверждаются, то служба безопасности проводит прежде всего следующие мероприятия:

- ❑ добывается официального расследования чрезвычайного происшествия государственными правоохранительными органами;
- ❑ компрометирует причастную к чрезвычайному происшествию структуру на основе данных официального расследования.

10. Розыск пропавших сотрудников банка, фирмы. В таких случаях служба безопасности должна выяснить следующие вопросы: каким образом и когда исчез сотрудник (погиб, захвачен преступниками в качестве заложника, уехал в неизвестном направлении, перешел к конкурентам); какое положение занимал на предприятии пропавший сотрудник; какой информацией о банке, фирме он располагал. Если в ходе расследования установлено, что сотрудник перешел к конкурентам, то проводятся мероприятия по компрометации его и известной ему информации. В случае захвата сотрудника преступниками в качестве заложника с помощью управления по борьбе с организованной преступностью предпринимаются необходимые действия по его освобождению.

11. Конфиденциальный контроль за пожаро-взрыво-опасными участками, а также контроль за переговорами по открытым каналам связи, почты.

Подготовка к кризисной ситуации предполагает прежде всего создание специального «тревожного» комитета (в составе вице-президента, начальника службы безопасности, руководителей отдела кадров, юридического, финансового) по установлению контактов с общественностью и средствами массовой информации и др. «Тревожный» комитет разрабатывает план мероприятий превентивного характера на время кризисной ситуации и после нее: отдел кадров совместно со службой безопасности должны особое внимание уделять проверке и контролю за принимаемыми на работу сотрудниками. При этом в первую очередь необходимо изучать деловые и личные качества тех категорий лиц, которые осведомлены о распорядке дня и местопребывании первого руководи-

теля (к ним относятся секретари, помощники, референты, водители и другие).

К превентивным мероприятиям относятся:

- 👁️ постоянный контроль за формированием и поддержанием бесконфликтных отношений между руководителями и рядовыми сотрудниками; поддержание контактов с фирмами, специализирующимися на улаживании конфликтных ситуаций в коллективах;
- 👁️ возможная эвакуация персонала с предприятия и вывоз материально-технических ценностей и документов; координация действий службы безопасности и государственных правоохранительных органов.

При возникновении кризисной ситуации, вызванной, например, нападением преступников на банк, фирму, взрывом, поджогом, служба безопасности обязана:

- ❖ немедленно включить сигнал тревоги;
- ❖ попытаться предотвратить уход преступников с объекта;
- ❖ срочно уведомить местные государственные правоохранительные органы о чрезвычайном происшествии;
- ❖ сохранить улики совершенного преступления;
- ❖ оказать содействие в срочной доставке раненых и пострадавших в ближайшую больницу с обязательным учетом их полных установочных данных и адресов;
- ❖ предотвратить уход с предприятия присутствовавших при чрезвычайном происшествии сотрудников до прибытия представителей государственных правоохранительных органов, за исключением раненых и потерпевших;
- ❖ не допускать на территорию и в помещение банка, фирмы посторонних лиц, кроме сотрудников государственных правоохранительных органов;
- ❖ исключить сообщения в средства массовой информации до окончания следственных действий и без консультаций с адвокатом;
- ❖ провести с использованием заранее разработанной и размноженной анкеты опрос сотрудников банка, фирмы о преступниках, направлении их побега, использованных ими средствах транспорта.

После завершения чрезвычайного происшествия служба безопасности обязана подготовить для первого лица и органа милиции информацию с указанием следующих данных:

- ❖ вовлеченные в чрезвычайное происшествие лица (сотрудники предприятия, клиенты, свидетели преступления, случайные прохожие с указанием их фамилий и адресов);
- ❖ сведения о преступниках (приметы, тактика действий, используемое оружие и специальные средства, транспорт, направление побега);
- ❖ результаты чрезвычайного происшествия;
- ❖ сведения о сотрудниках охраны предприятия (из состава службы безопасности, подразделений милиции или вневедомственной охраны органов внутренних дел);

- ❖ информация о раненых и потерпевших лицах, состояние их здоровья, оказании им первой медицинской помощи, об адресах больниц, куда они направлены на стационарное лечение.

Особенности работы службы безопасности банка

Банки были, есть и будут в числе наиболее вероятных объектов нападения преступных групп. Наши авторы в очередной раз напоминают любознательному читателю о том, что необходимо учитывать правовые требования Вашей страны в особенностях работы службы безопасности банка. В настоящее время, на основополагающих нормативных документах, мы попытаемся раскрыть, определяющие правовые аспекты деятельности ведомственных банковских охранных структур Украины, (следите за изменениями в Законах):

- ❖ **«О национальном Банке Украины»** (№67Э-Х1V от 20.05.1999 г.);
- ❖ **«О банках и банковской деятельности»** (№2121-111 от 07.12.2000 г.);
- ❖ **Постановление НБУ №134 от 28.03.2001 г.** «Об утверждении Инструкции о требованиях к организации охраны учреждений банков Украины»;
- ❖ **Приказы МВД Украины:** №112 от 28.02.1994 г. «О внесении изменений и дополнений в Приказ МВД Украины от 30 августа 1993 года №534 «О выполнении постановления Кабинета Министров Украины от 10 августа 1993 г. №615 «О мерах по усовершенствованию охраны объектов государственной и других форм собственности», №812 от 22 декабря 1993 г. «Об утверждении состава комиссии по вопросам рассмотрения материалов и выдачи лицензий субъектам предпринимательской деятельности, которые предоставляют услуги по охране государственной, коллективной и частой собственности, монтажу, ремонту и профилактическому обслуживанию средств охранной сигнализации» и №1030 от 25.11.2002 г. «Об утверждении Инструкции об организации охраны учреждений банков ГСО при МВД Украины».

Исходя из требований ст.43 Закона Украины «О банках и банковской деятельности» на руководителя банка возложена ответственность за организацию нормальной и эффективной работы, в рамках закона, вверенного учреждения направленную «на пользу банка и клиентов».

Согласно п. 1.2 Инструкции (Постановление НБУ №134 от 28.03.2001 г.) на учреждения банков, в лице их руководителей, возложены обязанности по обеспечению надежной охраны. В соответствии с этим и п.1.3. Инструкции банки организуют внутреннюю безопасность за счет личной службы охраны, которая создается в установленном законодательством Украины порядке.

Учреждения банков имеют право использовать комбинированные варианты охраны с участием, как личной службы охраны банка, так и других субъектов охраны – подразделений МВД Украины и специализированных охранных подразделений.

Руководитель банка или уполномоченное им лицо, согласно п.1.10. Инструкции, при задействовании личной охраны банка или совместно с представителями подразделений МВД или специализированных охранных подразделений определяет комплекс задач и вырабатывает меры по их реализации, направленные на обеспечение безопасности банковского учрежде-

ния, и несет персональную, предусмотренную законодательством Украины, ответственность за данное направление работы (п.1.15 Инструкции).

Кроме общережимных охранных мероприятий банки в лице руководителей, согласно ст.61 Закона Украины «О банках и банковской деятельности» несут специфическую обязанность по сохранению банковской тайны. Выполнение данной задачи влечет за собой ряд упреждающих мероприятий со стороны личной охраны банка, так как столь конфиденциальная и ответственная работа не делегируется другим субъектам охраны банка.

На основе изложенных требований нормативных документов по вопросу банковской безопасности видно, что данный участок работы в силу своей специфичности представляет собой сложный комплекс предупредительно-профилактических мер и требует как постоянного контроля со стороны руководителя банка за его деятельностью, так и постоянного соответствующего кадрового, финансового и материально-технического обеспечения.

Немаловажное значение в работе банковской безопасности играет решение вопроса по взаимодействию с властными структурами, правоохранительными органами и коммерческими предприятиями. По данному направлению в банковских учреждениях работают целые подразделения численностью от 5 до 10 сотрудников.

При ознакомлении с работой многих банков было установлено, что решение банковской безопасности во всех нами изученных банках не отдано «на откуп» третьих лиц – субъектов частнопредпринимательской охранной деятельности.

Во-первых, в результате пробелов в законодательстве отсутствует гарантия выполнения, последними, основной задачи банковских услуг – **сохранения банковской тайны**.

Во-вторых, из-за специфики предоставляемых услуг на субъекты частнопредпринимательской деятельности не распространяются как внутрибанковские нормативные документы, относительно охранной деятельности так и другие законодательные документы, предусматривающие строгое подчинение и ответственность по вопросам банковской безопасности.

В-третьих, из-за отсутствия Законов Украины «Об оружии», «О частной детективной службе» и других подобных законодательных актов, законодательством Украины не предусмотрена выдача лицензий на охранную деятельность физическим лицам, т.е. в филиалах банка частные лица, зарегистрированные как частные предприниматели, не имеют права заниматься охранной деятельностью в банковских учреждениях.

Согласно, существующего законодательства для охраны ценностей, банки обязаны привлекать Государственную службу охраны, (ГСО). Привлечение Государственной службы охраны с учетом возможностей МВД обеспечивает достаточную надежность охраны, но в тоже время ведет к большим финансовым расходам со стороны Банков. Организации, умеющие считать свои деньги, будут стремиться либо снизить расходы, либо стараться создавать свои охранные структуры, в том числе и влиять на изменение законодательства в этой сфере. Согласно информации Ассоциации украинских банков только за последние три года расходы на охрану подразделениями государственной службы охраны выросли в 2-3 раза, а их часть в общей сумме небанковских операционных расходов возросла

до 16%. Подтверждением этому являются требования подразделений Государственной службы охраны к банкам увеличить в 1,5-2 раза стоимость услуг по охране учреждений банков. Кроме этого, Государственная служба охраны не берет на себя материальной ответственности за ущерб, нанесенный вследствие осуществления охранных услуг на ненадлежащем уровне.

Поэтому, для недопущения подобной монополии на рынке охранных услуг и обеспечения надежной охраны банковских средств и ценностей был разработан проект по внесению изменений в Закон Украины «Про банки и банковскую деятельность» (касательно охраны имущества банков и клиентов, а именно ст. 47-1). Принятие данного проекта приведет к уменьшению расходов на осуществление охранных услуг; появлению конкуренции на рынке обеспечения вооруженной охраны в Украине; а уменьшение банковских расходов приведет к уменьшению стоимости услуг для клиентов банков и росту отчислений в Государственный бюджет Украины.

Как было сказано выше, банки, как и предприятия, создают комиссии по осмотру объектов банка применительно к организации охраны собственными силами (ведомственной охраной). Результаты работы комиссий оформляются актом, в котором определяется состояние объектов и даются рекомендации по организации их охраны: виду охраны, количеству постов охраны, мерам по созданию искусственных барьеров, препятствующих доступу в банк и т.п. На основании акта разрабатываются необходимые меры охраны и разрабатывается Дислокация – документ, в котором указывается порядок охраны объектов банка техническими средствами и физическими силами. Основным нормативным актом банка по вопросам охраны является приказ об утверждении инструкции о пропускном и внутри-объектовом режиме, а также режиме функционирования и охраны кассового узла. Этим документом предусматривается порядок доступа персонала, клиентов, акционеров и посетителей в банк, порядок сдачи под охрану помещений, противопожарные мероприятия, порядок действий в чрезвычайных ситуациях и т.п. Кроме того, в банках разрабатываются так называемые кризисные планы, которые согласовываются с местными органами МВД.

Одной из основных проблем, которую придется решать службе безопасности банка, будет проблема сохранения банковской тайны. Правила по соблюдению банковской тайны разработаны в соответствии с требованиями статей 7, 57, 66 Закона Украины «О Национальном банке Украины», статей 60, 61, 62 Закона Украины «О банках и банковской деятельности», статьи 30 Закона Украины «О предприятиях в Украине», Уголовного кодекса Украины и Кодекса об административных правонарушениях, других законов Украины, определяющих требования по защите и сбережению информации и документов, которые содержат банковскую тайну, их выдаче по письменным запросам уполномоченных на это органов государственной власти. Ниже приводим примерную инструкцию по сохранению банковской тайны.

Особенности сохранения банковской тайны

Сотрудники банка обязаны обеспечивать сохранность информации, которая содержит банковскую (коммерческую) тайну, с целью недопущения ее незаконного разглашения и нанесения в результате этого матери-

ального или морального ущерба своим вкладчикам, кредиторам и другим клиентам.

В филиалах и отделениях организовать специальное делопроизводство с документами, которые содержат банковскую (коммерческую) тайну и применять технические средства для недопущения несанкционированного доступа к электронным и другим носителям информации, которые содержат банковскую тайну, с учетом требований этой инструкции.

Сотрудникам необходимо отражать в договорах и соглашениях между банком и клиентом предупреждение о сохранении банковской тайны и ответственности за ее незаконное разглашение или использование.

При составлении договора или соглашения клиент банка, который является владельцем информации, содержащей банковскую тайну, имеет право дать банку письменное разрешение на раскрытие банковской тайны.

Филиалы и отделения обязаны ограничить доступ к информации, которая содержит банковскую тайну, путем составления необходимого перечня лиц из числа сотрудников банка, а также третьих лиц, которые при исполнении своих функций или предоставлении услуг банка могут получить информацию, которая составляет банковскую тайну.

Руководителям подразделений или уполномоченных ими лицам определить служащих из состава персонала банка, которые имеют право доступа к информации, которая содержит банковскую тайну.

Служащие банка при поступлении на должность или при получении права доступа к информации, которая содержит банковскую тайну, подписывают обязательство про сохранность банковской (коммерческой) тайны.

Служащие обязаны включать предупреждение о сохранности информации, которая содержит банковскую тайну и ответственность за ее незаконное разглашение или использование, в договора и соглашения с частными лицами и организациями, которые при выполнении своих функций или при предоставлении услуг банка непосредственно или опосредованно, получили такую информацию.

Частные лица и организации, которые при исполнении своих функций, получении или передаче услуг банка непосредственно или случайно получили информацию, которая содержит банковскую тайну, обязаны не разглашать эту информацию и не использовать ее в свою пользу или в пользу третьих лиц.

I. Сохранность и защита тайны

1.1. В целях обеспечения сохранности банковской тайны руководители подразделений обязаны организовать специальное делопроизводство с документами, которые содержат банковскую тайну, ввести порядок подготовки, обработки, учета, сохранения, использования и уничтожения документов, дел, публикаций, в том числе электронных документов и других материальных носителей информации, которые содержат банковскую тайну. Документам, содержащим банковскую тайну, присваивается гриф «Банковская тайна» (ВТ), на предприятиях «Коммерческая тайна» (КТ).

На бумажных документах, которые содержат информацию, являющуюся банковской тайной, в правом верхнем углу первой страницы, а для публикаций – на титульном листе ставится гриф «ВТ» («КТ»). Необходимость фифа «ВТ» определяется руководителем филиала или уполномоченными на это лицами.

1.2. Банк самостоятельно определяет перечень ведомостей и информации, которые составляют банковскую тайну, который должен соответствовать статье 60 Закона.

1.3. Служащие банка несут ответственность за надлежащую сохранность, правильность ведения, составления, обработку, учет, хранение и использование документов с грифом «БТ».

2. Получение, размножение (копирование), рассылка (отправка) и учет документов.

2.1. Получение и отправка документов, которые содержат банковскую тайну, может осуществляться:

А – в бумажном виде или на электронных носителях с обязательным сопроводительным листом через предприятия связи (курьерской, фельдшерской почтой и т.п.) в соответствии с установленными правилами работы таких предприятий или представителем банка;

Б – в электронном виде каналами электронной связи, которые обеспечивают надежную защиту от несанкционированного доступа к информации.

Запрещается получать и отправлять документы с грифом «БТ» с использованием факсимильной связи или другими каналами связи, которые не обеспечивают защиты информации.

2.2. Получение и учет (регистрация) входящей и исходящей корреспонденции и информации с грифом «БТ», которая предоставляется на электронных носителях или в электронном виде, осуществляется подразделениями банка или служебными лицами, которые ведут учет документов в банке. При этом проверяют количество страниц и экземпляров документа, а также наличие приложений или информации в электронном виде, указанном в сопроводительном листе.

Текстовые документы, которые получены по каналам электронной связи, отпечатываются.

В случае отсутствия в конвертах документов или приложений к ним составляется акт в двух экземплярах, один из которых высылается отправителю. В случае отсутствия информации на электронных носителях, указанных в сопроводительном листе, или в электронном виде, которая поступила по каналам электронной связи, информация с грифом «БТ» на учет не берется, о чем уведомляется отправитель.

Документы с грифом «БТ», которые поступили ошибочно, возвращаются отправителю или пересылаются адресату в порядке установленном этими Правилами.

2.3. Регистрации подлежат все входящие, исходящие и внутренние документы с грифом «БТ». Они учитываются по количеству страниц, а издания (книги, журналы, брошюры, проекты планов, планы и другие материалы, составленные в брошюры) – по количеству экземпляров.

Входящие документы регистрируются в день их получения, исходящие и внутренние – в день подписания (утверждения). Входящие, исходящие, нормативные, распорядительные и другие внутренние документы с грифом «БТ» регистрируются вместе с другими документами согласно установленного порядка делопроизводства.

2.4. Исходящие документы с грифом «БТ» после подписи регистрируются служебным лицом. К регистрационному номеру исходящего документа с грифом «БТ» обязательно указывается знак «БТ».

2.5. Руководители подразделений или служебные лица банка, которые осуществляют размножение (копирование) документов с грифом

«БТ», обязаны обеспечить конфиденциальность информации, которая содержится в документах. Информация о размножении (копировании) документа с грифом «БТ», в том числе и по требованию служебных лиц Национального банка, подлежит учету в специальном журнале, в который заносятся данные о документе, количестве экземпляров, цели размножения (копирования) и т.п.

2.6. Печать документов с грифом «БТ» осуществляется в подразделениях банка с обязательным нанесением грифа на документы. На обратной стороне каждого экземпляра документа обязательно указывается количество отпечатанных экземпляров, фамилия исполнителя, который печатал документ, дата его печати.

2.7. Рассылка (отправка) документов с грифом «БТ» осуществляется в установленном в банке порядке.

В случае необходимости отправки бумажного документа с грифом «БТ» по нескольким адресам составляется расчет рассылки, в котором по каждому адресу проставляются номера экземпляров документа.

2.8. Отправляемые документы, дела и публикации с грифом «БТ» на бумаге, могут вкладываться в конверты или паковаться таким образом, чтобы исключить возможность доступа к ним.

На упаковке или конверте указываются адреса и названия получателя и отправителя, номера вложенных документов и ставится фиф «БТ».

3. Формирование исполненных документов в дела и их хранение

3.1 Документы с грифом «БТ» после их отработки (исполнения) формируются в дела согласно номенклатуры дел в соответствии с порядком делопроизводства, установленного в банке.

3.2. Передача информации «БТ» электронной почтой или в режиме оп-line проходит только в защищенном виде с контролем целостности и обязательным подтверждением о ее поступлении с электронной подписью получателя и с использованием средств защиты.

3.3. Печать документов с грифом «БТ» в технологических АРМ осуществляется согласно технологическим схемам работы соответствующих АРМ банка. На отпечатанных документах проставляется гриф «БТ», и они учитываются согласно требованиям, как и при учете бумажных документов.

В случае формирования данных на электронном носителе прилагается сопроводительный лист с грифом «БТ», в котором указываются данные по содержанию носителя.

3.4. Получение информации из баз данных технологических АРМ нестандартными способами запрещается.

3.5. Программные модули передаются и учитываются на электронных носителях информации с обязательным сопроводительным листом с грифом «БТ».

3.6. Листинги программ защиты информации, которые содержат банковскую тайну, должны храниться на защищенных серверах.

3.7. Формирование архивов в электронном виде осуществляется согласно технологическим схемам обработки документов. Архивы хранятся на серверах или внешних носителях в защищенном виде при соблюдении контроля целостности информации во время работы с документами из архивов.

Открытие банковской тайны

1. Общие требования открытия банковской тайны

Филиалы и отделения обязаны открывать информацию, которая содержит банковскую тайну:

- 1) по письменному запросу или с письменного разрешения владельца такой информации;
- 2) по письменному требованию суда или по решению суда;
- 3) органам прокуратуры Украины, СБУ, МВД – по их письменному требованию в отношении операций по счетам конфетного юридического лица или физического лица – субъекта предпринимательской деятельности за конкретный промежуток времени.

Информация, которая содержит банковскую тайну, владельцем которой является банк, раскрывается банком Национальному банку или уполномоченным им лицам, которые осуществляют функции банковского надзора или валютного контроля, третьим лицам при получении или предоставлении услуг банком, или по письменному требованию уполномоченных государственных органов, которые в соответствии с законом имеют на это право.

Письменный запрос или разрешение клиента об открытии информации, которая содержит банковскую тайну, и владельцем которой он является, составляется в произвольной форме или может быть оформлено отдельным условием в договоре (соглашении) между банком и клиентом.

Письменный запрос (разрешение) юридического лица – клиента банка в произвольной форме должен быть изложен на фирменном бланке, подписан руководителем или уполномоченным им лицом и скреплен печатью юридического лица.

Письменный запрос (разрешение) физического лица – клиента банка в произвольной форме подписан этим лицом, подпись физического лица должна быть заверена руководителем подразделения банка или уполномоченным им лицом и скреплена печатью банка или заверена нотариально.

Письменное требование государственного органа на получение информации, которая содержит банковскую тайну, должно содержать необходимые реквизиты, предусмотренные частью второй статьи 62 Закона, а именно:

- 1) письменное требование государственного органа должно быть изложено на бланке установленной формы, который отвечает требованиям нормативно-правовых актов Украины;
- 2) иметь подпись, скрепленную гербовой печатью, руководителя или его заместителя (исполняющего обязанности);
- 3) содержать предусмотренные Законом основания для получения соответствующей информации с указанием конкретной нормы закона (статья, часть, пункт, подпункт);
- 4) содержать ссылку на норму закона, в соответствии с которыми государственный орган имеет право на получение такой информации, с указанием конкретной нормы закона (статья, часть, пункт, подпункт);

В соответствующим образом оформленном требовании государственного органа должны быть указаны названия конкретного юридического или физического лица, календарный промежуток времени, за который требуется информация по операциям и счетам. Информация предоставляется только по вышеуказанным и соответствующим образом оформленным документам.

Руководители имеют право отказать в раскрытии информации, которая содержит банковскую тайну, если по своей форме требование соответствующего государственного органа не отвечает Закону.

Руководители обязаны предоставлять справки по счетам (вкладам) в случае смерти их владельца лицам, определенным владельцем счета (вклада) в завещании, государственным нотариальным конторам или частным нотариусам, иностранным консульским представительствам в делах наследства по счетам умерших владельцев счетов.

Справка оформляется в произвольной форме и должна содержать информацию о наличии счета (вклада) и остатке средств на день предоставления справки.

2. Размеры раскрытия информации, которая содержит банковскую тайну

2.1. Руководители подразделений обязаны раскрывать информацию, которая содержит банковскую тайну в размерах, установленных Законом.

Подразделения обязаны раскрывать информацию, которая содержит банковскую тайну, в отношении конкретного юридического или физического лица – клиента банка по письменному требованию органов государственной власти в размерах, определенных в письменном разрешении владельца соответствующей информации или решением (требованием) суда.

Подразделения банка обязаны раскрывать информацию, которая содержит банковскую тайну, касательно операций по счетам конкретного юридического или физического лица – субъекта предпринимательской деятельности за конкретный промежуток времени по письменному требованию уполномоченных и указанных в статье 62 Закона органов государственной власти.

Подразделения не имеют права отказывать в предоставлении или выдаче документов или их копий, а также других дел, которые требует следователь во время выемки, и которые определены в постановлении следователя.

Документы на бумажных носителях, которые находятся в документообороте или архиве банка, и которые содержат банковскую тайну, предоставляются уполномоченным государственным органам в копиях, заверенных в установленном порядке делопроизводства, если это требуется уполномоченным государственным органом.

2.2. Подразделения обязаны раскрывать информацию, которая содержит банковскую тайну, или дать мотивированный ответ про невозможность предоставления соответствующей информации в течение 10 рабочих дней со дня получения требования.

В случае, когда подготовка информации требует больше времени, подразделения обязаны сообщить об этом письменно лицу или государственному органу, который обратился с требованием о предоставлении информации, и указать срок предоставления информации, которая содержит банковскую тайну.

Информация, которая содержит банковскую тайну, предоставляется адресату в письменном виде, на электронных носителях информации или в электронном виде с выполнением требований этой Инструкции.

2.3. Подразделениям банка запрещается предоставлять информацию о клиентах другого банка, даже если они указаны в документах, договорах и

операциях клиента, если это не определено в разрешении клиента или решении (требовании) суда.

В случае предоставления информации в отношении операций по счетам конкретного юридического или физического лица – субъекта предпринимательской деятельности за конкретный промежуток времени подразделения обязаны предоставлять информацию по движению средств на счету клиента без указания наименований, реквизитов счета и других данных отправителя этих средств и их получателя (контрагентов), которые могут быть как клиентами других банков, так и клиентами нашего банка, если это не предусмотрено Законом.

2.4. Подразделения имеют право предоставлять общую информацию, которая составляет банковскую тайну, другим банкам в размерах, необходимых при получении кредитов, банковских гарантий с обеспечением требований в отношении их несанкционированного разглашения.

2.5. Выемка документов, которые составляют банковскую тайну, проводится только с санкции прокурора или его заместителя и в порядке, согласованном с руководителем соответствующего учреждения.

Выдача и осмотр документов, которые содержат данные, содержащие банковскую тайну, проводятся с соблюдением требований этих Правил в части сохранения и защиты банковской тайны.

2.6. При выемке могут быть изъяты лишь те предметы и документы, которые имеют значение для дела, а также ценности и имущество обвиняемого или подозреваемого с целью обеспечения гражданского иска или возможной конфискации имущества.

Все документы и предметы, которые подлежат конфискации, следователь должен предъявить понятым и другим присутствующим лицам и перечислить в протоколе выемки или в приложенном к нему описи. В необходимых случаях изъятые предметы и документы должны быть на месте выемки упакованы и опечатаны.

Соответственно к подпунктам б) пункта 4 статьи 12 Закона Украины «Об организационно-правовых основах борьбы с организованной преступностью», сотрудники специальных подразделений по борьбе с организованной преступностью органов внутренних дел и СБУ по постановлению и с санкции соответствующего прокурора, а в неотложных случаях – с последующим уведомлением прокурора в течении суток, при угрозе уничтожения, укрытия или утери предметов и документов, которые могут быть использованы в раскрытии и расследовании преступной деятельности, имеют право изымать предметы и документы с составлением соответствующего акта. Копия акта изъятия вручается руководителю или представителю подразделения банка.

2.7. При изъятии оригинала документа или его копии об этом делается соответствующая запись в протоколе выемки или акта изъятия.

Представитель подразделения банка имеет право обратиться к лицу проводящему выемку или изъятие оригинала документа, с просьбой дать возможность изготовить копию этого документа, которая заверяется руководителем учреждения (заместителем) и главным бухгалтером, а также лицом проводящим изъятие. Изготовленная копия документа прикладывается к другому экземпляру протокола выемки или акта изъятия, который вручается представителю банковского учреждения.

При выемке или изъятии копии документа, оригинал которого содержит информацию на электронных носителях (в частности, при переносе

такой информации на бумагу), копия такого документа заверяется руководителем учреждения (заместителем) и главным бухгалтером, о чем делается соответствующая запись в протоколе выемки или акте изъятия. В случае необходимости, в подразделениях банка изымаются, с соблюдением требований уголовно-процессуального законодательства Украины и этих Правил, электронные носители информации, с которых работникам банка с разрешения лиц, которые проводят выемку или изъятие, предоставляется возможность скопировать необходимую для обеспечения работы банка информацию и другие электронные носители информации.

Учреждение не несет ответственность за достоверность данных и информации, которая содержится в оригиналах документов, которые созданы (подготовлены) без его участия или присланы по его адресу.

IV. Ответственность за нарушение правил хранения, защиты и раскрытия банковской тайны

1. Ответственность за нарушение правил хранения и защиты информации, которая содержит банковскую тайну. Лица нарушившие правила хранения и защиты информации, которая содержит банковскую (коммерческую) тайну, несут ответственность согласно законодательства Украины (статьи 231, 232 УК).

За нарушение подразделениями банка правил хранения и защиты информации, которая содержит банковскую тайну, могут быть применены меры воздействия Национальным банком Украины.

2. Ответственность за нарушение порядка раскрытия информации, которая содержит банковскую тайну.

Лица, виновные в нарушении порядка раскрытия и использования банковской тайны, несут ответственность в соответствии с законами Украины. Незаконное разглашение или использование информации, которая является банковской тайной, лицом, которому эта информация стала известна в связи с исполнением профессиональных или служебных обязанностей влечет за собой административную ответственность в соответствии со статьей 164-11 Кодекса Украины об административных правонарушениях.

В случае утечки информации, которая содержит банковскую тайну, из органов, которые уполномочены осуществлять банковский надзор и валютный контроль, а также от третьих лиц, которым соответствующая информация стала известна вследствие профессиональной или служебной деятельности, и причинения в результате этого убытков банку или его клиентам, убытки, в том числе компенсация морального ущерба, возмещаются виновными лицами в порядке, установленном законодательством Украины. Одним из видов охраны банка – является охрана перевозки денег, ценностей и прочее. Основным документом для использования в повседневной деятельности есть Инструкция №1 по организации эмиссионно-кассовой работы в учреждениях банков Украины утвержденная постановлением Правления Национального банка Украины от 07.09.93 г., согласно которой в банках устанавливается соответствующий порядок работы кассовых узлов, действий охраны и работников касс в случае непредвиденных ситуаций, а также порядок транспортирования и охраны наличных средств и ценностей.

Инкассация денежных средств

Охрану инкассации могут осуществлять подразделения УГСО, соответствующие органы НБУ, в отдельных случаях – подразделения инкассации коммерческих банков, перечень которых определяет НБУ. Наши авторы подчеркивают то, что специалистов УГСО на всех не хватит, т.к. они в первую очередь обслуживают наиболее солидных клиентов, да и процент оплаты от перевозимой суммы устанавливают немалый.

Поэтому представляется важным, чтобы те лица, которые даже периодически бывают связаны с перевозкой денег и ценностей, представляли себе содержание деятельности инкассаторов, знали те правила безопасности, которые необходимо соблюдать в этой работе. Доставка денег в банк лишь часть функций, которые возлагаются на инкассаторов. В современных условиях они решают более широкий круг задач, а именно:

- 👁️ доставка выручки торгующих организаций в банковское учреждение;
- 👁️ доставка денежной выручки из торговых точек коммерческой структуры в ее офис для последующей сдачи в банк;
- 👁️ доставка денег из банка в офис фирмы, например, для последующей выдачи заработной платы сотрудникам;
- 👁️ перевозка денег из банка в место приобретения товара, под покупку которого берется банковский кредит;
- 👁️ доставка денежных и валютных средств из банка в обменный пункт и обратно;
- 👁️ доставка денежных средств из резервных фондов и подкреплений наличности из подразделений Национального банка Украины в расчетно-кассовые центры и операционные кассы коммерческих банков.

Даже исходя из этого, далеко не полного перечня, видно, что это не только задач и решать их могут далеко не все. В современных условиях сумма оплаты за перевозку денег и ценностей колеблется в пределах от 3-5 до 15-20% перевозимой суммы или суммы страховки (оценки) перевозимых ценностей. Имеют место и более высокие проценты оплаты услуг инкассаторов, например, при перевозке денег и ценностей в другие регионы.

При исполнении своих служебных обязанностей охранник (инкассатор) должен быть одет в специальную форму. Исключением из этого правила являются случаи зашифрованной перевозки денег и ценностей с их маскировкой под груз, не представляющий большой ценности. Для зашифрованной перевозки используются специальные схемы изменения маршрута следования и времени перевозки. Для усиления режима безопасности перевозки могут использоваться демонстративная погрузка, соответствующие извещения клиента (который заранее обо всем предупрежден) и другие элементы дезинформирующего характера.

В фирме, занимающейся перевозкой денег и ценностей или по роду деятельности связанной с периодическим совершением подобных операций, должен быть заведен журнал регистрации рапортов и докладных записок. В случае, возникновения нестандартных и криминальных ситуаций во время несения службы охранник обязан сообщить об этом рапортом или докладной запиской, оставить себе копию документа и проследить за тем, чтобы его доклад был зафиксирован в вышеуказанном журнале. В про-

цессе исполнения своих функциональных обязанностей инкассатору запрещается:

- 👁 совершать действия, не связанные с инкассацией и перевозкой ценностей;
- 👁 разговаривать с посторонними лицами в момент остановки автомашины или отходить от него;
- 👁 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 соответствующих статьях которые мы приводили выше. Вместе с тем представляется небезынтесным 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 инкассаторы должны:
- 👁 по данному факту сообщить дежурному по инкассации и дежурному территориального органа внутренних дел;
- 👁 до прибытия на место происшествия работников банка и милиции остаться на месте и обеспечить сохранность ценностей.

Представляется, что в зависимости от ситуации последнее правило может выполняться различным образом. Например, если существует угроза подвергнуться повторному нападению, то бригаде инкассаторов имеет смысл либо не останавливаться после применения оружия, либо немедленно уехать с того места, где было нападение на инкассаторов. Но в любом случае необходимо сообщить о случившемся – дежурному по инкассации и в милицию.

Оказание помощи пострадавшим преступникам должно быть в прямой зависимости от степени вероятной угрозы жизни инкассаторов и сохранности перевозимых ими денег и ценностей. По существующим правилам спецавтомобиль инкассаторов не останавливается при возникновении по пути следования различных криминальных и иных негативных ситуаций, например, при дорожно-транспортном происшествии с участием других автомобилей. Инкассаторы должны следовать своим

маршрутом и обязаны лишь сообщить по радиосвязи о случившемся дежурному по инкассации.

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.

Обеспечение должного режима безопасности инкассации не возможно без тесного взаимодействия с органами внутренних дел.

В процессе взаимодействия службы инкассации и милиции решаются следующие задачи:

А.) оборудование тревожной и охранной сигнализацией помещений для хранения денежных средств, автотранспорта, оружия и боеприпасов;

Б.) оформление разрешений инкассаторам на ношение, перевозку, хранение, использование и применение огнестрельного оружия и боеприпасов к нему;

В.) прикрытие силами милиции объектов инкассации и маршрутов транспортировки денег и ценностей;

Г.) сопровождение автотранспорта инкассаторов, перевозящего крупные суммы денег и значительные объемы ценностей. Аналогичный подход имеет место и за рубежом. Там для транспортировки крупных денежных сумм, особо редких и ценных музейных экспонатов и других ценных бумаг, дорогостоящих вещей и предметов, организуются полицейские эскорты;

Д.) организация связи между дежурными частями службы инкассации и милиции, а также отработка ее четкости и надежности;

Е.) оперативный обмен информацией между службой инкассации и милицией;

Ж.) проведение совместных учений, в ходе которых отрабатываются стандартные схемы взаимодействия инкассаторов и милиции, а также негативные ситуации, которые могут возникнуть в процессе инкассации и перевозки денежных средств и ценностей.

План прикрытия объектов и маршрутов инкассации разрабатывается ежегодно и хранится в дежурных частях милиции и инкассации. План прикрытия и графики выездов на объекты инкассации имеют гриф «для служебного пользования» и с ними не могут знакомиться лица, не имеющие отношение к инкассации.

Для обеспечения должного режима безопасности, возможности своевременного получения помощи служба инкассации информирует дежурную часть территориального органа внутренних дел о следующих обстоятельствах:

- 👁 о начале и окончании инкассации;
- 👁 об изменении маршрута и времени прибытия к объекту инкассации;
- 👁 об инкассации вновь открытых и не внесенных в план прикрытия объектов;

- о прекращении инкассации отдельных объектов в связи с их ликвидацией, реорганизацией и т.д.

В случае необходимости доставки крупных сумм денег в банк из резервных фондов, а также при необходимости подкрепления наличности в расчетно-кассовых центрах милиция информируется не позже, чем за 2 дня до проведения транспортной операции. Любое изменение графика доставки (заезда) должно согласовываться не позже, чем за 5-6 часов.

При необходимости доставки средств из резервных фондов или подкреплений наличности в другую область милиция производит сопровождение инкассаторов по своей территории (в пределах области), а затем передает их машину (машины) милицейскому эскورتу (сопровождению) из другой области.

Отработанная практикой схема инкассации денежной выручки в предприятиях и организациях выглядит следующим образом:

- один из инкассаторов является старшим бригады, а другой – сборщиком;
- при сборе сумок с денежной выручкой старший инкассатор и водитель автомашины охраняют собранную выручку и наблюдают за работой сборщика;
- если инкассация осуществляется двумя сотрудниками, то обязанности старшего выполняет водитель.

Перед выездом инкассатору-сборщику выдается доверенность на право инкассации, явочные карточки, печать участка инкассации с обозначением номера маршрута. Старший бригады инкассации получает порожние сумки.

К каждой сумке представителем инкассируемого предприятия или организации прилагается три экземпляра препроводительной ведомости. Станция железной дороги прилагает комплект препроводительных ведомостей в количестве четырех экземпляров.

Инкассатор-сборщик перед принятием сумок с выручкой предъявляет:

- удостоверение личности с фотокарточкой;
- доверенность на получение денежной выручки;
- явочную карточку.

В явочной карточке представитель предприятия или организации делает соответствующую запись. Инкассатору-сборщику запрещено делать отметку в явочной карточке.

При приеме сумки с денежной выручкой инкассатор-сборщик проверяет:

- а.) исправность сумки;
- б.) правильность опломбирования сумки и целостность шпагата, ясность отиска печати и его соответствие образцу;
- в.) соответствие номера сумки номеру в явочной карточке, накладной и копии препроводительной ведомости;
- г.) наличие подписей должностных лиц предприятия или организации на накладной;
- д.) соответствие суммы выручки, указанной в явочной карточке, записям в накладной и копии препроводительной ведомости, а также соответ-

ствие суммы цифрами и прописью, указанной в накладной и копии препроводительной ведомости.

После проверки инкассатор-сборщик передает должностному лицу предприятия или организации порожнюю сумку, расписывается на копии препроводительной ведомости, ставит на ней дату и печать.

При приеме двух и более сумок инкассатор-сборщик проверяет количество сумок и общую сумму выручки по записям в накладной и копии препроводительной ведомости на каждую из принимаемых сумок.

Старший бригады инкассаторов принимает у сборщика полные сумки и выдает порожние. Важным обстоятельством, которое не должно забывать лица, занимающиеся перевозкой денег и ценностей, является то, что накладная на принятую сумку с денежной выручкой и явочная карточка остаются у инкассатора-сборщика.

Правила и приемы безопасности при инкассации денежных средств

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 достаточное освещение и обогревательные устройства;

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

Для перевозки денег и ценностей аренда стороннего транспорта запрещена. Это допустимо лишь в случае долгосрочной аренды автомашины, при условии ее специального переоборудования и нахождения под постоянным контролем арендующей ее фирмы.

Во время инкассации денежных средств и перевозки ценностей запрещено курение. Это связано как с угрозой возникновения пожара в автомобиле, так и с некоторыми физиологическими реакциями, возникающими у курильщика.

Как уже было сказано выше, во время инкассации запрещается проезд и провоз 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 предприятия и организации, не связанные с денежными операциями.

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

- 👁️ захламлинные подъездные пути;
- 👁️ близко прилегающие к маршруту криминогенные объекты;

- 👁 темные коридоры;
- 👁 неосвещенные дворы;
- 👁 смежные организации, не имеющие отношения к инкассируемому объекту, через которые должен проходить инкассатор-сборщик;
- 👁 отсутствие удобной стоянки для автомобиля инкассаторов.

Важным правилом безопасности инкассации является обязанность представителя предприятия или организации встречать инкассатора с деньгами и ценностями при выходе его из автомобиля и провожать инкассатора 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.

По существующим правилам инкассаторский автомобиль должен подъезжать к «черному» входу инкассируемого объекта. От лиц, связанных с перевозкой денег и ценностей, требуется особая бдительность в начале и в конце маршрута следования. Каждый инкассатор и сопровождающий должен знать, что первые и последние 100 метров маршрута наиболее опасны, поэтому в начале и в конце пути требуется максимальная концентрация внимания. Во многих странах разрабатываются рекомендации по улучшению режима безопасности перевозки денег и ценностей.

По мнению специалистов, для повышения надежности операций по перевозке необходимо:

- 👁 иметь бронированные автомобили для перевозки ценностей;
- 👁 оснащать автомашины, используемые для транспортировки, современными техническими средствами защиты;
- 👁 усовершенствовать систему подбора персонала сопровождения и охраны;
- 👁 повысить качество планирования операций;
- 👁 тщательно подбирать сотрудников, имеющих отношение к планированию и проведению операций по перевозке денег и ценностей;
- 👁 хорошо продумать маршрут и время операции;
- 👁 ввести идентификационные удостоверения для сопровождающих;
- 👁 обеспечивать четкую договоренность между отправителем и получателем ценного груза о способах и условиях транспортировки (когда, где, кто и кому передает груз);
- 👁 использовать средства радиосвязи и устройства автоматического окрашивания денег при попытке ограбления. Немаловажное значение для повышения уровня профессионального мастерства, играют специальные учебные занятия, которые должны

периодически проводиться с сотрудниками службы инкассации и теми лицами, из числа работающих в коммерческих структурах, которые по роду своей деятельности изредка привлекаются к перевозке денег и ценностей.

**Документы, закрепляющие право предприятия
на коммерческую тайну**

Для создания правовых основ защиты конфиденциальной информации на 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 ее сохранности».

❖ «Предприятие обязано: обеспечить сохранность коммерческой тайны».

2. Разработать “Перечень сведений, составляющих коммерческую тайну предприятия”.

3. Дополнить “Коллективный договор” следующими требованиями:

а) – Администрация предприятия 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”.

4. При заключении трудовых соглашений (контрактов) с сотрудниками Предприятия внести пункт об обязанности сотрудника сохранять коммерческую тайну Предприятия.

5. При взятии на должность сотрудников, работа которых будет связана с конфиденциальной информацией, подписывать Обязательство о неразглашении коммерческой тайны.

**«Перечень сведений, составляющих
коммерческую тайну предприятия»**

“Перечень сведений, составляющих коммерческую тайну Предприятия” – это свод конкретный сведений коммерческого характера Предприятия, подлежащий защите. Он является юридическим документов, дающим право Предприятию в установленном законодательством порядке (в том числе через судебные органы) требовать возмещения понесенных материальных потерь или упущенной выгоды в случае, если предусмотренные “Перечнем” сведения были разглашены, переданы или утрачены лицом (юридическим или физическим), которому они были доверены.

Состав “Перечня”:

Менеджмент:

- применяемые оригинальные методы управления Предприятием;
- подготовка, принятие и исполнение отдельных решений руководства Предприятия по коммерческим, организационным и иным вопросам;

- факты проведения, цели, предмет и результат совещаний и заседаний органов управления Предприятия;
- планы расширения или свертывания различных направлений деятельности Предприятия, их технико-экономические обоснования;

Финансы:

- балансы Предприятия;
- бухгалтерские книги управления;
- информация о кругообороте средств Предприятия;
- финансовые операции Предприятия, инвестиции;
- состояние банковских счетов;
- уровень доходов Предприятия;
- долговые обязательства Предприятия;
- состояние кредита Предприятия;
- уровень заработной платы сотрудников.

Маркетинг:

- применяемые Предприятием оригинальные методы изучения рынка;
- результаты изучения рынка, содержащиеся в оценках состояния и перспектив развития рыночной конъюнктуры;
- рыночная стратегия предприятия;
- применяемые Предприятием методы сбыта, способы стимулирования сбыта;
- методики расчета, структура и уровень цен на предлагаемые товары, размеры скидок;
- сведения об эффективности коммерческой деятельности Предприятия;
- систематизированная информация о конкурентах;
- систематизированная информация о внутренних и зарубежных заказчиках, подрядчиках, поставщиках, потребителях, покупателях, компаньонах, спонсорах, посредниках и клиентах;
- сведения о подготовке и результатах проведения переговоров с деловыми партнерами Предприятия;
- сведения, условия конфиденциальности которых установлены в договорах, контрактах, соглашениях и других обязательствах Предприятия.

Безопасность:

- состояние системы безопасности Предприятия (организация охраны, система сигнализации, режимы и т.д.);
- организация защиты коммерческой тайны Предприятия;
- информация, составляющая коммерческую тайну предприятий-партнеров, переданная на доверительной основе.

***Приложение:** авторы книги предлагают для более детального ознакомления с вопросами защиты коммерческой тайны предприятия и разработки внутренних нормативных документов предприятия обратиться к практическим работкам, которые изложены в приложении, (раздел I).*

ПРИКАЗ № _____
« ____ » _____ 20 ____ г.

О введении в действие Положения о коммерческой тайне Предприятия и правилах ее сохранения, и создании Комиссии по вопросам коммерческой тайны

Руководствуясь действующим законодательством стран СНГ, Украины (России, Беларуси...) в целях защиты сведений, составляющих коммерческую тайну предприятия

ПРИКАЗЫВАЮ:

1. Ввести в действие Положение о коммерческой тайне предприятия и правилах ее сохранения.

2. Создать постоянно действующую Комиссию по вопросам коммерческой тайны в составе:

Председатель Комиссии _____

Члены Комиссии _____

3. Комиссии приступить к работе с « ____ » _____ 20 ____ г.

4. Возложить на Комиссию следующие задачи:

сбор предложений от подразделений предприятия о сведениях, которые могут быть отнесены к коммерческой тайне предприятия и подлежат защите от утечки;

изучение поступающих предложений, их обобщение и оценка, систематизация и разработка "Перечня сведений, составляющих коммерческую тайну предприятия".

5. Руководителям структурных подразделений предприятия с учетом Положения "О коммерческой тайне Предприятия и правилах ее сохранения" провести оценку коммерческих и иных планов, структуры цен, обзоров рынка, внутренней информации и т.п. к « ____ » _____ 20 ____ г. представить в комиссию предложения по установленной форме ("Служебная записка") о внесении в "Перечень" сведений, которые целесообразно считать конфиденциальными.

6. Председателю Комиссии: обеспечить контроль за своевременным поступлением материалов от руководителей структурных подразделений; представить "Перечень" мне на утверждение к « ____ » _____ с.г.

7. _____ в десятидневный срок ознакомить с настоящим приказом членов комиссии и руководителей структурных подразделений (по списку), участвующих в подготовке сведений для "Перечня".

Руководитель Предприятия

(фамилия)

“УТВЕРЖДАЮ”
Начальник Службы безопасности

(фамилия)

(дата)

**Должностная инструкция Начальника Отдела расследований,
защиты коммерческой тайны и информационно-аналитической
работы.**

I. Начальник Отдела расследований, защиты коммерческой тайны и информационно-аналитической работы отвечает за:

- проведение розыскных и следственных мероприятий;
- выявление возможных каналов утечки информации;
- техническую защиту информации;
- проведение работы с персоналом Предприятия по вопросам защиты коммерческой тайны;
- контроль за документооборотом и публикациями Предприятия;
- взаимодействие с правоохранительными органами по вопросам обеспечения безопасности деятельности Предприятия;
- сбор информации из открытых источников и отделов Службы безопасности;
- качественную обработку и анализ поступающей информации;
- надежное хранение информации;
- своевременную выдачу информации из банка данных;
- подготовку официальных материалов о деятельности Предприятия для публикации в источниках массовой информации;
- техническое и программное обеспечение деятельности подчиненного отдела.

II. Начальник Отдела расследований, защиты коммерческой тайны и информационно-аналитической работы обязан:

1. Проводить оперативно-розыскные и следственные мероприятия в случае похищений сотрудников Предприятия с целью шантажа или выкупа, обнаружения краж, хищений имущества и материальных ценностей, принадлежащих Предприятию и его сотрудникам.

2. Осуществлять контроль за обстановкой, проводить мероприятия по созданию благоприятного климата в коллективах подразделений Предприятия.

3. Проводить мероприятия по конфиденциальному выявлению и проверке сотрудников Предприятия, подозреваемых в работе на конкурентов или криминогенные элементы.

4. Проводить служебные расследования фактов утечки информации, нарушений персоналом Предприятия действующих норм и правил внутренней безопасности.

5. Вести работу по выявлению возможных каналов утечки информации и принимать меры по закрытию этих каналов.

6. Разрабатывать систему доступа сотрудников фирмы в различные помещения, к различным информационным ресурсам. Вести контроль за соблюдением сотрудниками действующих на Предприятии режимов.

7. Проводить работы по выявлению подготовки различных акций в отношении Предприятия со стороны конкурентов и преступных элементов, и противодействовать этим акциям. Незамедлительно сообщать начальнику

Службы безопасности о всех фактах, угрожающих безопасности Предприятия.

8. Вести регулярный сбор открытой и конфиденциальной информации о:

- а) деятельности клиентов и деловых партнеров Предприятия (финансовое положение, коммерческие и иные возможности по развитию дела, стратегические планы и т.д.);

- б) деятельности конкурирующих фирм;

- в) деятельности государственных контролирующих органов;

- г) структуре, возможностях и особенностях рынка как внутри страны, так и за рубежом по направлениям, являющимся сферой интересов Предприятия.

9. Вести сбор информации о деятельности конкретных предприятий и частных лиц по указанию руководства Предприятия и начальника Службы безопасности.

10. Проводить учебно-практические занятия с персоналом Предприятия по вопросам безопасности.

11. Оказывать помощь другим подразделениям Предприятия в подборе кадров.

12. Тесно взаимодействовать с МВД, Службой безопасности Украины, прокуратурой, специализированными предприятиями и организациями при осуществлении возложенных на подчиненный Отдел функций.

13. Контролировать состояние трудовой дисциплины штатных сотрудников подчиненного Отдела, создавать условия для повышения ими своего профессионального уровня.

14. Осуществлять контроль за учетом конфиденциальных документов в подразделениях и филиалах Предприятия.

15. Совместно с Отделом безопасности и охраны осуществлять доставку особо важных документов нарочными.

16. Осуществлять цензуру выходных документов Предприятия, предназначенных для широкого опубликования, на предмет наличия в них конфиденциальной информации (пресс-релизы, материалы для публикации в прессе, выступления работников Предприятия на выставках, семинарах и презентациях).

17. Вести учет, обеспечивать надежное хранение, регулярное техобслуживание и правильную эксплуатацию специальных и технических средств, находящихся в распоряжении Отдела расследований, защиты коммерческой тайны и информационно-аналитической работы.

18. Осуществлять сбор открытой информации из средств массовой информации по установленным направлениям.

19. Производить сбор информации, поступающей от отделов Службы безопасности, а также других подразделений Предприятия.

20. Вести регистрацию и обработку поступающей информации путем структурирования и кодирования в соответствии со структурой накапливаемой информации.

21. Обеспечивать архивирование и надежное хранение информации в папках дел и электронных базах данных.

22. Производить выдачу информации по запросам руководства Предприятия, начальника Службы безопасности, руководителей подразделений и сотрудников Предприятия в соответствии с имеющимися у них допусками к информации;

23. Вести статистическую обработку информации, регулярно в установленные сроки выдавать аналитические обзоры, прогнозы о состоянии и развитии рынка, деятельности конкурентов, принятии или отмене законодательных актов и т.д.

24. Незамедлительно сообщать начальнику Службы безопасности о всех фактах и тенденциях, угрожающих безопасности Предприятия.

25. Готовить официальные материалы о деятельности Предприятия для распространения в средствах массовой информации.

26. Обеспечивать своевременное обновление и модернизацию технических и программных средств.

27. Производить подбор и обучение кадров, контролировать состояние трудовой дисциплины штатных сотрудников подчиненного отдела.

28. Проводить мероприятия по сохранению коммерческой тайны, технической защите информации, циркулирующей в отделе.

29. Вести учет, обеспечивать надежное хранение, регулярное техобслуживание и правильную эксплуатацию технических средств, находящихся в распоряжении отдела.

30. Принимать участие в работе Комиссии по вопросам коммерческой тайны Предприятия.

*Начальник Отдела исследований,
защиты коммерческой тайны
и аналитической работы
ПРЕДПРИЯТИЯ*

“ ____ ” _____ 200_ года. (фамилия)

Приложение к 1 книге

ТИПОВОЕ ПОЛОЖЕНИЕ О КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И ЗАЩИТЕ КОММЕРЧЕСКОЙ ТАЙНЫ 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение является базовым документом и устанавливает единые требования обращения конфиденциальной информации в ООО «_____».

Положение разработано с целью предотвращения нанесения возможного экономического ущерба ООО «_____», ее ЗАКАЗЧИКАМ со стороны юридических или физических лиц, вызванного их неправомерными или неосторожными действиями путем безвозмездного присвоения чужой информации или разглашения коммерческой тайны.

1.2. Под **коммерческой тайной** следует понимать не являющиеся государственными секретами сведения, связанные с организацией охраны объектов ЗАКАЗЧИКОВ: дислокацией постов, маршрутов патрулирования, задействованных сил и средств, оснащенностью объектов техническими средствами охраны и другой деятельностью в области проведения научно-исследовательских, информационно-аналитических работ, а также с его технологической информацией, управлением, кадрами и финансами, разглашение (передача, утечка) которых может нанести ущерб интересам охраны.

1.3. К **сведениям, составляющим коммерческую тайну**, относятся несекретные сведения, предусмотренные “Перечнем сведений, составляющих коммерческую тайну предприятия”, вводимым в действие настоящим Положением (Приложение 1).

1.4. **Коммерческая тайна является собственностью ООО «_____».** *Если коммерческая тайна является результатом совместной деятельности, с другими предприятиями, основанной на договорных началах, то она может быть собственностью двух сторон. Это обстоятельство должно быть закреплено в договоре.*

1.5. **Конфиденциальная информация** – документированная информация, содержащую коммерческую тайну, персональные данные и иную охраняемую законом тайну, а также любые документы, содержащие гриф степени конфиденциальности.

1.6. **Конфиденциальный документ** – зафиксированная и определенным образом оформленная на бумаге или содержащаяся в файлах и подчиненная особому делу производства, имеющая реквизиты или другие признаки, позволяющие идентифицировать принадлежность документа к предприятию или его деятельности.

1.7. Под **разглашением коммерческой тайны** имеются в виду противоправные, умышленные или неосторожные действия должностных или иных лиц, способствующему преждевременному, не вызванному служебной необходимостью, открытому опубликованию сведений, подпадающих под эту категорию, а также их передача по открытым техническим каналам или обработка их на незащищенных ЭВМ.

1.8. Под **открытым опубликованием** вышеуказанных сведений следует понимать публикацию материалов в открытой печати, передача по

радио и телевидению, оглашение на международных, зарубежных конференциях, совещаниях, симпозиумах, при открытой защите диссертаций и при других публичных выступлениях, свободная рассылка, вывоз материалов за границу или передача их в любой другой форме конкурирующим либо иностранным фирмам, организациям или отдельным лицам вне сферы прямых служебных обязанностей.

Возможность и необходимость открытого опубликования этих сведений, а также их объемы, формы и время опубликования определяются директором или его первым заместителем 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 в деятельности охранных фирм.

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

1.9. Передача информации сторонним организациям, не связанным со специальной службой охраны прямыми служебными контактами, должна регулироваться договорными отношениями, предусматривающими обязательства и ответственность пользователей, включая возмещение материальных затрат на представление информации и компенсации за нарушение договорных обязательств.

1.10. Предоставление коммерческой информации представителям служебных, ревизионных, налоговых и следственных органов, депутатам, органам печати, радио и т.д. регулируется соответствующими отдельными инструкциями.

1.11. Тиражированные документы и издания с грифом содержащие коммерческую тайну рассматриваются как материалы, содержащие сведения ограниченного распространения.

1.12. Ответственность за обеспечение режима при работе с грифованными материалами, своевременную разработку и осуществление необходимых мероприятий по сохранению коммерческой тайны возлагается на директора, его заместителей по направлениям, а также руководителей структурных подразделений и начальников охран объектов. Ответственность за организацию и осуществление защиты коммерческой тайны, и проведение постоянного контроля за ее соблюдением возлагается на его службу безопасности.

Служба безопасности принимает меры по сохранению коммерческой тайны путем: максимального ограничения доступа к ней лиц; физической сохранности документов, содержащих такие сведения; обработки информации с соответствующим грифом секретности на ПЭВМ; внесения требований по конфиденциальности конкретной информации в договоры с ЗАКАЗЧИКАМИ и других мер по решению руководства предприятия.

1.13. Защита коммерческой тайны предусматривает:

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

1.13.2. Систему допуска сотрудников охраны, командированных и частных лиц к сведениям, составляющим коммерческую тайну;

1.13.3. Порядок работы с документами имеющие гриф секретности;

1.13.4. Обеспечение сохранности документов, дел и изданий с грифом секретности;

1.13.5. Обязанности лиц, допущенных к сведениям, составляющим коммерческую тайну;

1.13.6. Принципы организации и проведения контроля за обеспечением режима при работе со сведениями, составляющими коммерческую тайну;

1.13.7. Ответственность (перечень санкций) за разглашение сведений или потерю документов, содержащих коммерческую тайну.

1.14. Контроль за осуществлением учета, размножения, хранения и использования документов, дел, изданий и иной информации с грифом секретности возлагается на службу безопасности.

1.15. Контроль за неразглашением сведений, содержащихся в документах, делах, изданиях и тому подобной информации с грифом секретности, осуществляется службой безопасности.

2. СТЕПЕНИ КОНФИДЕНЦИАЛЬНОСТИ.

ПОРЯДОК ОПРЕДЕЛЕНИЯ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ

2.1. Настоящим Положением устанавливается четыре степени секретности (конфиденциальности) документов:

ПЕРВАЯ – особо секретно;

ВТОРАЯ – совершенно секретно;

ТРЕТЬЯ – секретно;

ЧЕТВЕРТАЯ – для служебного пользования.

Степень секретности указывается при создании документа в правом верхнем углу листа (файла). Определение грифа секретности производится на основании Перечня (Приложение 1) и в соответствии с п. 1.2 настоящего Положения; на документе – исполнителем и должностным лицом, подписывающим его, а на издании – автором (составителем) и руководителем, утверждающим к печати.

2.2. Срок действия коммерческой тайны, содержащейся в информации, определяется в каждом конкретном случае исполнителем или должностным 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 конкретный гриф секретности, а на документах и изданиях, кроме того, – номера экземпляров. Гриф секретности 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 дается разметка, в которой указываются: количество отпечатанных экземпляров, регистрационный номер, фамилия исполнителя, его телефон, дата, срок действия коммерческой тайны, фамилия машинистки.

2.4. Решение вопроса о снятии грифа секретности возлагается на создаваемую в установленном порядке специальную комиссию в составе представителей службы безопасности и соответствующих структурных подразделений, оформляется актом произвольной формы и утверждается директором или его первым заместителем. В акте перечисляются дела, с которых гриф секретности снимается. Один экземпляр акта вместе с делами передается в архив, а на дела постоянного хранения – в государственный архив.

На обложках дел гриф секретности погашается штампом или записью от руки с указанием даты и номера акта, послужившего основанием для его снятия. Аналогичные отметки вносятся в описи и номенклатуру дел.

3. СИСТЕМА ДОПУСКА РАБОТНИКОВ И ПОРЯДОК ОБРАЩЕНИЯ С ДОКУМЕНТАМИ, СОСТАВЛЯЮЩИМИ КОММЕРЧЕСКУЮ ТАЙНУ

Допуск к работе с конфиденциальными документами и носителям информации

3.1. Допуск работников охраны к сведениям, составляющим коммерческую тайну, осуществляется директором, его первым заместителем, руководителями структурных подразделений и начальниками охран объектов.

Руководители структурных подразделений, начальники охран объектов и служба безопасности несут ответственность за подбор кадров, допускаемых к сведениям составляющие коммерческую тайну, и 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 производственные секреты охранной деятельности, допускаются работники, в том числе находящиеся на испытательном сроке, обладающие необходимыми деловыми и нравственными качествами, гарантирующими надежность охраны коммерческой тайны которые:

- а) ознакомлены под роспись с настоящим Положением;
- б) занимают должности указанные Перечне документов содержащие коммерческую тайну;
- в) подписавшие соответствующие обязательства в службе безопасности.

3.3. Запрещается допускать к работе с секретными документами других лиц, кем бы они не являлись, без письменного разрешения (приказа, распоряжения) директора.

3.4. Допуск сотрудников к работе с делами, книгами, папками и другими материалами содержащие коммерческую тайну, производится в соответствии с оформленным на внутренней стороне обложки разрешительным списком за подписью директора или его первого заместителя, а к отдельным документам – согласно указаниям, содержащимся в резолюции директора или его первого заместителя.

Командированные и частные лица допускаются к ознакомлению и работе с документами и изданиями с грифом секретности с письменного разрешения директора или его первого заместителя, при наличии письменного запроса организаций, где они работают, с указанием темы и объема выполняемого задания, а также предписания на выполнение задания и соответствующего документа о допуске к секретной информации.

3.5. Выписки из документов и изданий, содержащих секретные сведения, производятся в тетрадях, имеющих такой же гриф, которые после завершения задания высылаются в адрес заинтересованной организации.

Создание конфиденциальных документов.

3.6. Документы, содержащие конфиденциальную информацию изначально грифуются по признаку предусмотренным Перечнем (Приложение 1). Любой документ, являющейся при написании конфиденциальным, соз-

дается лично или под непосредственным наблюдением руководителя структурного подразделения. При использовании черновиков после завершения работы над секретным документом они должны быть уничтожены либо сданы для уничтожения. При возникновении сомнения относительно статуса конфиденциальности документа руководитель структурного подразделения должен обратиться в службу безопасности за разъяснениями.

3.7. Конфиденциальные документы создаются только в рабочее время и только на рабочем месте.

3.8. Создаваемые документы, над которыми работа еще не закончена, должны храниться таким же образом, как и готовые. Включение конфиденциального фрагмента из другого документа в создаваемый, делает новый документ конфиденциальным.

3.9. Конфиденциальные документы запрещено вторично использовать под черновики других документов, для копирования на обратной стороне и другой работе, которая может послужить причиной утечки секретной информации.

Учет, порядок выдачи, размножения, уничтожения и хранение конфиденциальных документов.

3.10. Документы, содержащие коммерческую тайну, подлежат обязательной и немедленной регистрации в канцелярии. Они должны иметь реквизиты, предусмотренные п.п. 2-3, и гриф секретности.

3.11. Учет документов и изданий с грифом секретности ведется в Журнале регистрации конфиденциальных документов или на карточках, отдельно от учета другой несекретной корреспонденции. Листы журналов нумеруются, прошиваются и печатаются. Издания, которые не подшиваются в дела, учитываются в Журнале инвентарного учета. Движение документов и изданий с грифом секретности должно своевременно отражаться в журналах или карточках.

3.12. На каждом зарегистрированном документе, а также на сопроводительном листе к изданиям с грифом секретности проставляется штамп, в котором указывается регистрационный номер документа и дата его поступления.

3.13. Конфиденциальное делопроизводство регламентируется отдельной Инструкцией о делопроизводстве и номенклатуре дел.

3.14. Лицо, не зарегистрировавшее документ, несет за это ответственность. Незарегистрированный документ является источником утечки конфиденциальной информации.

3.15. На документах, передаваемых зарубежным гражданам, гриф секретности не проставляется. Материалы, полученные от иностранцев, маркируются грифом секретности графитным карандашом. В тексте документов и его реквизитах дополнительно могут оговариваться права на информацию, порядок пользования ею, сроки ограничения на публикацию и др.

Отсутствие грифа секретности и предупредительных оговорок в тексте и реквизитах означает свободную рассылку и предполагает, что автор информации или должностное лицо, подписавшее документ и санкционировавший ее распространение, предусмотрел все возможные последствия свободной рассылки и несет за это всю полную ответственность.

3.16. Дела и издания с грифом секретности выдаются исполнителям и принимаются от них под расписку в Карточке учета выдаваемых дел и изданий

3.17. Вся поступающая в охрану корреспонденция с грифом секретности принимается работником канцелярии. Вскрытие секретных конвертов (пакетов) производится директором или его первым заместителем. Регистрация данной корреспонденции осуществляется канцелярией. При регистрации проверяется количество листов и экземпляров документов и изданий, а также наличие приложений, указанных в сопроводительном письме. В случае отсутствия в конвертах (пакетах) документов содержащих коммерческую тайну или приложений к ним составляется акт в двух экземплярах, один из которых направляется отправителю. Регистрации подлежат все входящие, исходящие и внутренние документы, а также издания имеющие гриф секретности. Такие документы учитываются по количеству листов, а издания (книги, журналы, брошюры) – поэкземплярно.

3.18. Тираж издания с грифом секретности, полученный для рассылки, регистрируется под одним входящим номером в Журнале учета и распределения изданий. Дополнительно размноженные экземпляры документа (издания) учитываются за номером того же документа (издания), о чем делается отметка на размноженном документе (издании) и в учетных формах. Нумерация дополнительно размноженных экземпляров производится от последнего номера ранее учтенных экземпляров.

3.19. Документы с грифом «Особо секретно», «Совершенно секретно», «Секретно», «Для служебного пользования» после исполнения группируются в отдельные дела. Хранение различных по статусу документов в одном номенклатурном деле – ЗАПРЕЩАЕТСЯ. Правила такой работы предусматриваются номенклатурами дел по секретному делопроизводству. В номенклатуру дел в обязательном порядке включаются все справочные картотеки и журналы на документы и издания с грифом секретности.

3.20. Секретные документы в зависимости от производственной необходимости допускается приобщать в дела отдельно или вместе с другими документами по одному и тому же вопросу.

В случае, когда в службе (подразделении) образуется большое количество одних и тех же видов документов и дел (приказы, инструкции, сводки и т. п.) с грифом секретности и без этого грифа, целесообразно предусмотреть обособленное формирование в дела. При этом в графе номенклатуры к номеру дела с секретными документами добавляется соответствующий гриф секретности.

При пополнении дела документом с повышенным грифом секретности, данное дело получает повышенный гриф секретности, который соответствует грифу приобщенного к нему документа. Соответствующие изменения вносятся в номенклатуру дел.

3.21. На охраняемых объектах, где образуется небольшое количество секретных документов, номенклатурой дел может предусматриваться заведение одного дела, которому присваивается соответствующий гриф секретности. Срок хранения такого дела устанавливается директором на основании решения постоянно действующей комиссии.

3.22. Запрещается изъятие из дел или перемещение документов с грифом секретности 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.

3.23. Выданные для работы дела с грифом секретности подлежат возврату в канцелярию или уполномоченному службы безопасности в день

получения. Отдельные дела с грифом секретности с разрешения директора, его первого заместителя или начальника службы безопасности могут находиться у исполнителя в течение срока, необходимого для выполнения задания, при условии полного обеспечения их сохранности.

3.24. Передача документов, дел и изданий с грифом секретности другим сотрудникам, имеющим допуск к ним, производится только через канцелярию или службу безопасности.

3.25. По окончании календарного года, все номенклатурные дела, в которых содержатся сведения с коммерческой тайной, просматриваются экспертной комиссией полностью и, в случае необходимости, принимается решение о перегруппировке документов либо выделение их в отдельное дело.

В случае перегруппировки документов и выделение их в отдельное дело, это дело получает самостоятельный заголовок и дополнительно включается в общую номенклатуру дел.

3.26. Обработка информации с грифом секретности производится на учетных и защищенных ПЭВМ.

3.27. При пользовании открытой радиосвязью, мобильными телефонами запрещается передавать сведения, имеющие гриф секретности. Не допускается передача сведений через незащищенную модемную связь и телефаксы. Они могут передаваться исключительно по закрытым техническим каналам или открытой телетайпной связью с проставлением на документах и телеграммах штампа «Серия П». При пользовании проводной связью запрещается указывать должности адресатов-отправителей, разрешается указывать только телеграфные адреса и фамилии отправителей и получателей.

3.28. Печатание материалов с грифом «Особо секретно», «Совершенно секретно», «Секретно», «Для служебного пользования» производится в канцелярии или в структурных подразделениях под контролем их руководителей.

3.29. Отпечатанные и подписанные документы с грифом секретности вместе с их черновиками и вариантами передаются для регистрации сотруднику канцелярии, осуществляющему их учет. Черновики и варианты уничтожаются тем же сотрудником с подтверждением факта их уничтожения с записью на копии исходящего документа: «Черновик (варианты) уничтожен». Подпись.

3.30. Копирование (размножение) допускается только с письменного разрешения директора или его первого заместителя. Количество копий определяется исходя из служебной необходимости. Копия конфиденциального документа является конфиденциальной. В скопированном конфиденциальном документе под статусом секретности ставится штамп «Копия № _____. Всего копий _____».

3.31. Учет размноженных документов и изданий осуществляется по-экземплярно в Журнале регистрации конфиденциальных документов.

3.32. Размножение документов и изданий с грифом секретности в типографиях, на множительных аппаратах сторонних организаций производится с разрешения директора или его первого заместителя и под контролем службы безопасности.

3.33. По окончании размножения документов в полиграфических учреждениях, набор должен быть разобран, а печатные формы аннулирова-

ны, о чем составляется акт за подписями представителя службы безопасности и работника полиграфического учреждения.

3.34. Рассылка документов и изданий на охраняемые объекты с грифом секретности осуществляется на основании подписанных директором или его первым заместителем разнарядок с указанием учетных номеров отправляемых экземпляров. Рассылка производится канцелярией под контролем службы безопасности.

3.35. Отправляемые документы, содержащие секретные сведения, должны быть помещены в конверты либо упакованы. Все без исключения отправляемые конверты должны быть прошиты и опечатаны. На упаковке (конверте) указываются адреса и наименования получателя и отправителя, номера вложенных документов с добавлением отметки «Коммерческая тайна». Отправка секретных документов производится только нарочным или через управление специальной связи в Донецкой области.

3.36. Снятие копий (рукописных, машинописных, микро- и фотокопий, электрографических и др.), а также осуществление выписок из документов и изданий с грифом секретности производятся сотрудниками с разрешения директора или его первого заместителя. Снятие копий для сторонних организаций с документов и изданий с грифом «Особо секретно», «Совершенно секретно», «Секретно», «Для служебного пользования» делается на основании письменных запросов с разрешения тех же должностных лиц. Соответствующие отметки вносятся в описи и номенклатуры дел.

3.37. Запрещается выносить документы, дела и издания с грифом «Особо секретно», «Совершенно секретно», «Секретно», «Для служебного пользования» из служебных помещений для работы с ними на дому, в гостиницах и т.д. В необходимых случаях директор или его первый заместитель могут разрешить исполнителям или сотрудникам вынос из здания документов с грифом секретности для их согласования, подписи и т.п. в организациях, находящихся в пределах одного города.

3.38. Лицам, выезжающим на другие территории, запрещается иметь при себе в пути следования документы, дела или издания с грифом «Особо секретно», «Совершенно секретно», «Секретно». Эти материалы должны быть направлены заранее в адрес организации по месту командировки сотрудника, как правило, заказными или ценными почтовыми отправлениями, а также с курьерами предприятия.

3.39. При смене сотрудников, ответственных за учет и хранение документов, дел и изданий с грифом секретности, составляется по произвольной форме акт их приема – сдачи, который утверждается директором или его первым заместителем.

3.40. По окончании сроков хранения конфиденциальных документов или в связи минованием их надобности, секретные документы подлежат уничтожению. Все документы, подготовленные к уничтожению, хранятся у сотрудника, ответственного за их сохранность до момента передачи на уничтожение.

3.41. Уничтожение документов производится любым способом, в результате которого документ приходит в состояние, когда его невозможно даже частично восстановить (сжигание, измельчение или уничтожение специальными механическими устройствами).

3.42. Уничтожение массивов документов производится специально создаваемой комиссией, назначаемой приказом директора и состоящей,

как правило, из работника канцелярии, руководителя структурного подразделения имеющего отношение к уничтожаемым документам и сотрудника службы безопасности.

3.43. При уничтожении составляется акт, в котором указывается состав комиссии, перечень уничтоженных документов и копий. Акт, подписанный всеми членами комиссии, утверждается директором или его первым заместителем. Акты уничтоженных документов сдаются в архив канцелярии.

3.44. Документы, дела и издания, имеющие гриф секретности должны храниться в служебных помещениях в надежно запираемых и опечатываемых металлических сейфах (шкафах, хранилищах), при этом должны быть созданы надлежащие условия, обеспечивающие их физическую сохранность.

3.45. За организацию хранения конфиденциальных документов отвечает руководитель структурного подразделения, а на охраняемых объектах начальники охран.

3.46 Конфиденциальные документы должны храниться в папках – регистраторах с соответствующими пояснительными надписями, включая также Журналы регистрации. Первым листом в каждой папке должен быть перечень находящейся в ней документов.

3.47. Порядок работы с конфиденциальной информацией размещенной в средствах ПЭВМ и магнитных носителях устанавливается отдельными нормативными документами по защите конфиденциальной информации в информационных системах.

3.48 Сейф (металлический ящик) с конфиденциальными документами должен быть постоянно закрыт на ключ, а в нерабочее время опечатан. По окончании рабочего дня опечатыванию подлежат и служебные помещения, в которых хранятся конфиденциальные документы.

3.49. В каждой службе (подразделении) должен быть один комплект ключей от сейфов. Второй комплект ключей хранится в сейфе директора или его первого заместителя в специальном пенале, который опечатывается руководителем службы (подразделения).

3.50. Запрещается хранение конфиденциальных документов вне специально оборудованных мест. Лицо, нарушившее специальный порядок хранения, несет за это ответственность.

4. ОБЯЗАННОСТИ ЛИЦ, РАБОТАЮЩИХ С ИНФОРМАЦИЕЙ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ ПРЕДПРИЯТИЯ

4.1. Лица, допущенные к работам, документам и к сведениям, составляющим коммерческую тайну, несут персональную ответственность за соблюдение ими установленного на предприятии режима. Прежде чем получить доступ к закрытой информации с грифами «особо секретно» и «совершенно секретно», они должны изучить требования настоящего Положения и другие нормативные документы, определяющие защиту коммерческой тайны, сдать зачет на знание установленных требований и передать в службу безопасности соответствующее личное письменное обязательство.

4.2. Лица, допущенные к работам, документам и к сведениям, составляющим коммерческую тайну, ОБЯЗАНЫ:

4.2.1 Строго хранить коммерческую тайну, ставшую им известной по службе или работе либо иным путем, пресекать действия других лиц, которые могут привести к ее разглашению. О таких фактах, а также о других

причинах или условиях возможной утечки коммерческой тайны немедленно информировать непосредственно начальника и службу безопасности.

4.2.2 В течение договорного периода не использовать известную коммерческую тайну для своих личных целей, а также не заниматься без соответствующего разрешения руководства любой деятельностью, которая в качестве конкурентного действия может нанести ущерб предприятию, являющемуся собственником секретных сведений.

4.2.3 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.

4.2.4 При составлении документов со сведениями, составляющими коммерческую тайну, ограничиться минимальными, действительно необходимыми сведениями; определять количество, экземпляров документов в строгом соответствии с действительной служебной необходимостью и не допускать рассылки их адресатам, к которым они не имеют отношения.

4.2.5 На черновиках документов проставлять соответствующий ограничительный гриф и другие необходимые реквизиты. Передавать их для печатания только с письменного разрешения директора или его первого заместителя.

4.2.6 После получения отпечатанных документов проверить их наличие, сличить эти данные с записями в журнале и расписаться (с указанием даты) за получение отпечатанных документов и черновиков, после чего учесть в канцелярии или у уполномоченного службы безопасности.

4.2.7 Получать документы с грифом секретности лично в канцелярии или у уполномоченного службы безопасности. Своевременно знакомиться с полученными документами и разборчиво расписываться на них с указанием даты ознакомления.

4.2.8 Поступившие документы с грифом секретности своевременно направлять для приобщения к делу с соответствующими отметками об исполнении (номер дела, дата исполнения, подпись) и резолюцией директора или его первого заместителя.

4.2.9 Сдавать в канцелярию или службу безопасности исполненные входящие документы, а также предназначенные для рассылки, подшивки в дело, уничтожения и взятия на инвентарный учет под расписку в журнале учета.

4.2.10 Иметь внутреннюю опись документов с грифом «секретно» и немедленно вносить в 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.

4.2.11 По окончании работы с документами имеющие гриф секретности своевременно возвращать их в канцелярию или службу безопасности.

4.2.12 Об утрате или недостатке документов с грифом секретности, ключей от сейфов, личных печатей немедленно сообщать в службу безопасности.

4.2.13 При увольнении, перед уходом в отпуск, отъездом в командировку своевременно сдать или отчитаться перед канцелярией или службой безопасности за все числящиеся документы.

4.2.14 Знакомить представителей других учреждений с документами с грифом «Особо секретно», «Совершенно секретно», «Секретно», «Для служебного пользования» только с ведома начальника службы безопасности и при наличии письменного разрешения директора или его первого заместителя; лично знакомиться – с разрешения 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.

4.2.15 Документы с грифом секретности 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.

4.2.16 По первому требованию канцелярии, службы безопасности предъявлять для проверки все числящиеся и имеющиеся документы с грифом секретности; представлять по требованию начальника службы безопасности устные или письменные объяснения о нарушениях установленных правил выполнения работ с грифом секретности, учета и хранения секретных документов, а также о фактах разглашения сведений с грифом «Особо секретно», «Совершенно секретно», «Секретно», «Для служебного пользования», утраты документов, содержащих такие сведения.

5. ОРГАНИЗАЦИЯ ПРОВЕДЕНИЯ КОНТРОЛЯ ЗА ОБЕСПЕЧЕНИЕМ РЕЖИМА СОБЛЮДЕНИЯ КОММЕРЧЕСКОЙ ТАЙНЫ

5.1. Контроль за обеспечением режима секретности при работе с материалами с содержанием коммерческой тайны осуществляют служба безопасности предприятия и руководитель структурного подразделения.

5.2. Контроль за обеспечением режима при работе со сведениями, составляющими коммерческую тайну, осуществляется в целях изучения, анализа и оценки фактического состояния сохранности секретов, выявления недостатков и нарушений режима в работе с секретными материалами, установления их причин и выработки необходимых предложений.

5.3 Комиссия для проверки обеспечения надежности работы, с материалами имеющие гриф секретности комплектуется из опытных и квалифицированных работников в составе не менее трех человек, имеющих доступ к этой работе. Участие в проверке не должно приводить к необоснованному увеличению осведомленности проверяющих.

5.4. Проверки обеспечения режима при работе с материалами с грифом «Особо секретно», «Совершенно секретно», «Секретно», «Для служебного пользования» проводятся не реже одного раза в год в офисе охраны и не реже одного раза в квартал на охраняемых объектах комиссиями на основании решения, подписанного директором или его первым заместителем.

5.5. Проверки проводятся в присутствии руководителя службы (подразделения охраны) которое проверяется.

5.6. 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.

5.7. По результатам проверок составляется акт (справка) с отражением в нем состояния режима при работе с секретными материалами, выявленных недостатков и нарушений, предложений по их устранению. С актом после утверждения его директором или первым заместителем под подпись знакомится руководитель службы и начальники охран объектов.

5.8. Об устранении выявленных в результате проверки недостатков и нарушений в режиме при работе с секретными материалами и реализации предложений руководитель службы (начальник охраны объекта) в установленные комиссией сроки сообщает начальнику службы безопасности.

5.9. В случае установления факта утраты документов, дел и изданий с грифом «Особо секретно», «Совершенно секретно», «Секретно», «Для служебного пользования» либо разглашения содержащихся в них сведений немедленно ставятся в известность директор, его первый заместитель и начальник службы безопасности. Для расследования таких фактов приказом директора назначается комиссия, заключение которой утверждается директором, создавшим данную комиссию. На утраченные документы, дела и издания с грифом «Особо секретно», «Совершенно секретно», «Секретно», «Для служебного пользования» составляется акт. Соответствующие отметки вносятся в учетные документы. Акты на утраченные дела постоянного хранения после их утверждения директором или его первым заместителем по истечении срока передаются в архив для включения в дело фонда.

6. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОММЕРЧЕСКОЙ ТАЙНЫ

6.1. Утрата документов, содержащих сведения коммерческой тайны, представляет собой выход (в том числе и временный) документов из владения ответственного за их сохранность лица, которому они были доверены по службе или работе.

6.2. Нарушения режима при работе с материалами, имеющими гриф секретности, могут быть вызваны нарушениями требований настоящего Положения, которые могут привести к разглашению секретных сведений, утрате Документов, содержащих коммерческую тайну.

6.3. За хищение, утрату и преднамеренное уничтожение документов, дел и изданий с грифом секретности, за разглашение сведений, содержащихся в таких материалах, а также за нарушение требований настоящего Положения виновные лица привлекаются к ответственности в установленном порядке.

ИНСТРУКЦИЯ ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

1. ОБЩИЕ ПОЛОЖЕНИЯ.

1.1. Настоящая Инструкция определяет основные требования к системе защиты конфиденциальной информации (КИ) предприятия.

1.2. Организация и технология доступа к конфиденциальной информации, категорирование информации, обработка, хранение, и уничтожение конфиденциальных документов основываются на изложенных ниже положениях.

1.3. Организация и ведение делопроизводства документов, содержащих КИ, возлагается на специально сектор обработки документов с грифом “конфиденциальная информация”. Помещение, где будет располагаться сектор обработки документов должно быть оборудовано металлическими шкафами или сейфами, для хранения конфиденциальных документов.

1.4. Выполнение требований Инструкции является обязательным для всех исполнителей, допущенных к КИ.

1.5. Настоящая инструкция разработана в соответствии на основе нормативных актов, нормативно-методических документов по делопроизводству и архивному делу Российской Федерации, а также на основе организационно-распорядительных документов по обеспечению сохранности конфиденциальной информации предприятия.

1.6. Сотрудники предприятия обязаны:

- строго хранить в тайне сведения, отнесенные к конфиденциальной информации, ставшие ему известными при выполнении своих обязанностей;

- выполнять требования приказов, инструкций и положений по обеспечению сохранности конфиденциальную информацию;

- работать только с теми сведениями и документами, содержащими конфиденциальную информацию предприятия, к которым они получили доступ в силу своих должностных и функциональных обязанностей;

- знать какие конкретно сведения подлежат защите (согласно Перечню сведений, составляющих конфиденциальную информацию предприятия строго соблюдать правила пользования ими;

- не использовать конфиденциальную информацию в своих личных целях, не заниматься без разрешения руководства любой деятельностью, которая может нанести ущерб предприятию.

- в случае попытки посторонних лиц получить от сотрудника сведения о конфиденциальной информации немедленно сообщить об этом в отдел по защите конфиденциальной информации;

- сохранять конфиденциальную информацию организаций и частных лиц, с которыми предприятие имеет деловые отношения;

- в случае увольнения все носители конфиденциальной информации предприятия, которые находились в распоряжении сотрудника в связи с выполнением им служебных обязанностей, передать соответствующему должностному лицу или руководителю подразделения;

- об утрате или недостатке носителей конфиденциальной информации, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов, личных печатей и о других фактах, которые могут привести к разглашению конфиденциальную информацию, а также о причинах и условиях

ях возможной утечки сведений, немедленно сообщать руководителю подразделения и в отдел по защите конфиденциальной информации.

1.8. Руководство предприятия вправе знакомиться в полном объеме со всеми сведениями, составляющими конфиденциальную информацию, руководители структурных подразделений – по всему кругу задач, возложенных на них лично и на руководимые подразделения, остальные сотрудники – в рамках их функциональных обязанностей, а также данных руководством поручений.

1.9. При подготовке и проведении заседаний Руководства предприятия, совещаний и других форм коллективного обсуждения служебных вопросов, Председательствующий или, по его поручению, ответственный работник определяет круг приглашенных на каждый из вопросов и определяет процедуру совещания, создавая условия, исключающие возможность разглашения конфиденциальной информации.

1.10. Руководители предприятия и его структурных подразделений принимают меры по максимальному ограничению возможности ознакомления с конфиденциальной информацией сотрудников, которым по роду выполняемых обязанностей она не требуется.

2. КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ

2.1. Вся информация предприятия, составляющая конфиденциальную информацию (в соответствии с Перечнем сведений, составляющих конфиденциальную информацию предприятия) и содержащаяся в документах или на других носителях, подлежит установлению на неё грифа “конфиденциально” (“К”);

2.2. Каждый разрабатываемый или используемый в подразделении документ или программный продукт рассматривается начальником подразделения на предмет присвоения ему категории конфиденциальности.

2.3. Решение об изменении (снятии) категории с документа принимает должностное лицо, подписавшее (утвердившее) данный документ. О принятии такого решения информируются все держатели документа и на документе делаются соответствующие пометки.

3. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

3.1. Разглашением сведений, составляющих конфиденциальную информацию, признается не вызванное интересами предприятия, умышленное или неосторожное действие либо сообщение, в результате которого такие сведения стали известны посторонним лицам.

3.2. Под утратой документов, содержащих сведения конфиденциальную информацию понимается выход (в том числе и временный) документов из владения ответственного за их сохранность лица, которому они были доверены по работе, являющийся результатом нарушения установленных правил обращения с ними, вследствие чего эти документы стали или могут стать достоянием посторонних лиц.

3.3. Под иными нарушениями режима конфиденциальности (утрата удостоверений, пропусков, ключей от сейфов и помещений, личных печатей, нарушения правил работы с документами и другими носителями конфиденциальной информации) понимаются нарушения, которые могут привести к разглашению конфиденциальной информации, утрате документов, содержащих конфиденциальную информацию.

3.4. Разглашение конфиденциальную информацию, утрата ее носителей, передача третьим лицам, публикация без согласия предприятия, нару-

шение режима при работе с носителями конфиденциальной информации, а также использование для занятий любой деятельностью, которая в качестве конкретного действия может принести ущерб предприятию, влечет административную, гражданско-правовую, уголовную и иную ответственность в соответствии с действующим законодательством.

3.5.. Решение о привлечении к ответственности принимается руководством предприятия по предложению руководителя подразделения.

В необходимых случаях для оценки нанесенного вреда предприятию либо для выяснения других существенных обстоятельств организ с уется служебная проверка.

4. СИСТЕМА ДОСТУПА СОТРУДНИКОВ К СВЕДЕНИЯМ СОСТАВЛЯЮЩИМ “КИ”

Система доступа к конфиденциальным документам – это совокупность установленных положений, обеспечивающих обоснованный и правомерный доступ исполнителей к необходимому им для производственной деятельности объему документов, сведений, содержащих конфиденциальную информацию.

Целями системы доступа к конфиденциальным документам являются:

- ❖ обеспечение исполнителей всеми необходимыми для работы конфиденциальными сведениями;
- ❖ ограничение круга лиц, допускаемых к конфиденциальным документам;
- ❖ исключение излишнего или несанкционированного ознакомления с конфиденциальными сведениями;
- ❖ повышение ответственности руководителей и исполнителей всех категорий за обеспечение сохранности сведений, составляющих конфиденциальную информацию;
- ❖ усиление контроля со стороны сотрудника предприятия за обоснованностью доступа к конфиденциальным документам и изделиям.
- ❖ Разрешение на доступ исполнителя к сведениям, составляющим конфиденциальную информацию, дается соответствующим должностными лицами при выполнении следующих условий:
- ❖ при наличии приказа о приеме на работу или назначении на должность;
- ❖ при оформлении обязательства о сохранении и неразглашении работником сведений, составляющих конфиденциальную информацию;
- ❖ при изучении вновь принятым (назначенным на должность) работником требований нормативных документов по обеспечению сохранения конфиденциальной информации. После изучения указанных требований, руководитель подразделения с вновь принятым (назначенным на должность) работником проводит собеседование.

Любое разрешение на ознакомление с конфиденциальными документами и любое фактическое ознакомление с ними необходимо оформить в письменном виде. Ознакомление с документом фиксируется распиской исполнителя на самом документе (при оперативном ознакомлении исполнителя), и на карточке разрешении (при постоянном или длительном пользовании).

Работники предприятия могут получать разрешение на доступ к сведениям, составляющим конфиденциальную информацию, только в пределах своих должностных обязанностей и в объеме действительно необходимом им для выполнения своих обязанностей.

Руководители предприятия, его структурных подразделений несут персональную ответственность за правомерность выдаваемых ими разрешений на доступ исполнителей к сведениям, составляющим конфиденциальную информацию, а также исполнители, работающими с конфиденциальными документами, при нарушении порядка обращения и хранения с ними.

4.1. КРУГ ЛИЦ, ИМЕЮЩИХ ПРАВО ДАВАТЬ РАЗРЕШЕНИЕ НА ДОСТУП К КОНФИДЕНЦИАЛЬНЫМ ДОКУМЕНТАМ

4.1.1. Разрешение на доступ к документам с грифом «Конфиденциально» дает только руководитель предприятия.

4.1.2. Временно исполняющие обязанности, в том числе и заместители руководителя предприятия, пользуются всеми правами в объеме, предусмотренными настоящей Инструкцией для лица, должность которого замещается.

4.2. ПОРЯДОК ОФОРМЛЕНИЯ РАЗРЕШЕНИЯ НА ДОСТУП К КОНФИДЕНЦИАЛЬНЫМ ДОКУМЕНТАМ

4.2.1. Доступ к конфиденциальным документам производится только на основе письменного разрешения соответствующего руководителя.

4.2.2. Разрешение на доступ к конфиденциальным документам оформляется в следующем виде:

- резолюция руководителя на документе;
- указание об исполнении документа и фамилия исполнителя в содержании распорядительных документов (приказов, распоряжений, указаний);
- карточка-разрешение выдачи документа (дела);
- требование на выдачу документов (для архивных дел).

4.2.3. Исполнитель документа (если он продолжает работать по той же тематике) и лица, визировавшие и подписавшие документ, допускаются к нему без специального разрешения.

4.2.4. Если исполнитель допускается только к части документа, к отдельным документам дела, в разрешении должны указываться пункты, учетные номера документов или листы дела, к которым допускается исполнитель, а лицо, ответственное за учет, обработку и хранение конфиденциальных документов (сотрудник предприятия) принимает необходимые меры, исключающие ознакомление с другими частями документа (дела).

4.2.5. В случае отсутствия исполнителя (командировка, отпуск, болезнь) его документами имеют право пользоваться руководитель структурного подразделения, в котором он работает, или по письменному разрешению последнего – другие исполнители того же подразделения, имеющие отношение к указанным документам. Из сейфа документы в отсутствие исполнителя изымаются в установленном порядке комиссией с составлением акта.

4.2.6. Доступ к поступившим конфиденциальным документам осуществляется на основе резолюции соответствующего руководителя на самом документе или на сопроводительном письме. С сопроводительного

письма резолюция переносится на документ и заверяется подписью лица, ответственного за учет, обработку и хранение конфиденциальных документов (сотрудника) с указанием даты.

4.2.7. Доступ к изданным конфиденциальным документам осуществляется в соответствии с резолюцией на документе, указанием об исполнении документа (см. п. 4.2.2.), а в необходимых случаях в соответствии с карточкой-разрешением.

4.2.8. Доступ исполнителей к делам осуществляется согласно спискам в номенклатуре дел с грифом «Конфиденциально», утвержденным руководителем предприятия. Из номенклатуры списки переносятся на внутреннюю сторону обложки дела и заверяются лицом, ответственным за учет, обработку и хранение конфиденциальных документов (сотрудником предприятия). Списки составляются руководителями подразделений до утверждения номенклатуры дел.

4.2.9. Изменения в утвержденную номенклатуру, связанные с расширением круга лиц, допускаемых к делам, вносятся с письменного разрешения руководителя предприятия на основании докладных записок руководителей структурных подразделений. Изменения в номенклатуру дел заверяются подписью сотрудника или делается в ней ссылка на документ – основание, если разрешение написано на докладной записке.

4.2.10. В случае увольнения допущенных к делу лиц или изменения их должностных обязанностей производиться корректировка списков за подписью сотрудника.

4.2.11. Исполнители, внесенные в номенклатуру текущего года, допускаются к однотипным делам прошлых лет по письменному разрешению руководителя соответствующего структурного подразделения в карточке учета выдачи дела.

4.2.12. Доступ исполнителей к конфиденциальным документам, находящимся на архивном хранении осуществляется по требованиям установленного архивом предприятия образца. Требование подписывает руководитель структурного подразделения, где работает исполнитель и согласовывается с заведующим архива предприятия (для документов с грифом «Конфиденциально» необходимо согласование с руководителем предприятия).

4.2.13. Выдача конфиденциальных документов авторам, а также исполнителям, которые ранее пользовались ими, производиться по требованиям, подписанными руководителем структурного подразделения, где работает исполнитель. Его подпись означает, что тематика работ исполнителя не изменилась. Согласующие подписи не требуются.

4.3. ПОРЯДОК ДОСТУПА НА СОВЕЩАНИЯ ПО ВОПРОСАМ, СОДЕРЖАЩИМ КОНФИДЕНЦИАЛЬНЫЕ СВЕДЕНИЯ

4.3.0. Конфиденциальные совещания с участием представителей других организаций проводятся с разрешения руководителя предприятия. Руководитель предприятия, разрешая проведение совещания, определяет лицо, ответственное за его проведение.

4.3.1. Ответственное лицо должно своевременно представить сотруднику предприятия список участников совещания. Список утверждается руководителем предприятия или его заместителями. В дальнейшем этот список с отметками о присутствующих на совещании, прилагается к материалам совещания.

4.3.2. На совещания или переговоры допускаются сотрудники, которые имеют непосредственное отношение к обсуждаемым вопросам и участие которых вызывается служебной необходимостью. Сотрудник предприятия (или сотрудник, назначенный ответственным за проведение переговоров или совещания), должен предусмотреть такую очередность рассматриваемых вопросов, которая бы исключала участие в их обсуждении сотрудников, не имеющих отношения к этим вопросам.

4.3.3. Сотрудник предприятия или сотрудник, назначенный ответственным за проведение совещания или переговоров, обязан предупредить присутствующих о степени конфиденциальности обсуждаемых вопросов с целью предотвращения возможного их разглашения.

4.3.4. Обсуждение конфиденциальных вопросов может производиться только в помещении, специально выделенном для этих целей. Сотрудник предприятия осуществляет необходимые организационные и технические мероприятия, обеспечивающие сохранение конфиденциальной информации. Ответственность за сохранение конфиденциальной информации несет руководитель, организовавший данное совещание или переговоры.

4.3.5. Обсуждение на предприятии текущих конфиденциальных вопросов без приглашения представителей сторонних организаций, а также с участием представителей других организаций – соисполнителями по выполняемым совместным работам проводятся по решению руководителя предприятия с согласованием сотрудника предприятия. Составление списков участников в таких случаях не обязательно.

5. ПОДГОТОВКА И ИЗДАНИЕ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

5.1. Исполнители готовят документ в соответствии с функциональными обязанностями или полученным заданием.

5.2. Гриф ограничения доступа (степень конфиденциальности) документа «Конфиденциально» присваивается документу его исполнителем на стадии его создания в соответствии с «Перечнем сведений, составляющих конфиденциальную информацию предприятия».

5.3. На черновике документа в верхнем левом углу или другом свободном месте первого листа должны быть проставлены:

- ❑ наименование подразделения и фамилия исполнителя;
- ❑ количество необходимых экземпляров проекта документа;
- ❑ виза-разрешение соответствующего руководителя подразделения на печатание документа.

5.4. Машинописное оформление документов осуществляется с помощью принтера ЭВМ самим исполнителем или лицами, допущенными к работе с конфиденциальными документами, при условии исключения ознакомления с ними посторонних лиц.

5.5. Оформление документов с грифом «Конфиденциально» осуществляется только должностными лицами, ответственными за соблюдение информационной безопасности в структурных подразделениях предприятия.

5.6. При передаче черновика документа работнику, осуществляющим его печатание, исполнитель обязан оформить разовую расписку, которую оставляет у себя взамен сданных черновиков. После возвращения

черновики и отпечатанных проектов документов исполнитель уничтожает расписку в присутствии работника, осуществлявшего печатание.

5.7. Проект документа печатается в строгом соответствии с количеством экземпляров, указанных на черновике и подтвержденном подписью руководителя подразделения.

5.8. Гриф ограничения доступа («Конфиденциально») проставляется в правом верхнем углу первого листа документа. Ниже под грифом указывается номер экземпляра документа.

Например:

Конфиденциально
Экз. единственный

или

Конфиденциально
Экз. № 2

5.9. На обороте последнего листа каждого экземпляра документа оформляется реквизит «отметка о печатании», который включает в себя:

- ❑ количество отпечатанных экземпляров;
- ❑ фамилия исполнителя, наименование структурного подразделения, номер телефона;
- ❑ фамилия лиц отпечатававшего документ;
- ❑ дата печатания документа;

В середине нижнего поля каждого листа документа (кроме первого и последнего) проставляется его учетный номер и гриф ограничения доступа.

5.10. Производство выписок из документов осуществляется по письменному указанию руководителя структурного подразделения. Выписки учитываются за новыми учетными номерами. При этом на обороте последнего листа самого документа и в карточке учета делается запись, с каких номеров листов или пунктов документа, в каком количестве экземпляров сделана выписка, а также за каким учетным номером зарегистрирована.

Например:

«сделана выписка, пункты 1-4, уч. №21. Конфиденциально от 26.02.2002. Иванов»

5.11. После считывания и внесения возможных поправок в проект документа исполнитель должен проставить номера экземпляров, завизировать подшиваемый в дело экземпляр, получить визы соответствующих должностных лиц и подписать документ у руководителя, а при необходимости утвердить документ. Отпечатанные и подписанные документы вместе с их черновиками учитываются.

5.12. Отобранные к уничтожению черновики и варианты, испорченные при печатании листы уничтожаются на шредере. Факт уничтожения подтверждается записью на обороте последнего листа экземпляра документа, подшиваемого в дело: «Черновик и (варианты, испорченные при печатании листы) документа уничтожены», заверяемой подписями сотрудника предприятия и исполнителя с указанием даты.

6. УЧЕТ, ПРОХОЖДЕНИЕ И ОТПРАВЛЕНИЕ ИЗДАНЫХ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

6.0. Отпечатанные и оформленные в установленном порядке конфиденциальные документы подлежат регистрации в карточке учета изданных документов.

6.1. В случае если внутренний документ подлежит исполнению, он выдается исполнителю под расписку в карточке учета изданных документов и заносится в опись документов, находящихся у исполнителя. Со-

трудник предприятия, ответственный за работу с конфиденциальными документами, в контрольном журнале напротив учетного номера документа указывает фамилию исполнителя, расписавшегося в карточке за получение документа. На время нахождения документа у исполнителя карточка ставится в соответствующий раздел справочной картотеки.

6.2. При приеме документов от исполнителей сотрудник предприятия, ответственный за работу с конфиденциальными документами, должен проверить соответствие учетных номеров и количество листов документов записям в карточке учета изданных документов и в описи документов, находящихся у исполнителя; наличие отметки об исполнении документа и направлении его в дело.

6.3. После проверки сотрудник предприятия, ответственный за работу с конфиденциальными документами должен расписаться за принятые документы в карточке учета изданных документов и в описи документов, находящихся у исполнителя, с указанием даты возврата.

Карточку учета на возвращенный исполнителем документ сотрудник перемещает в соответствующий раздел справочной картотеки.

Исполненные документы подшиваются в дело, о чем делается отметка в карточке учета изданных документов.

В контрольном журнале карандашом зачеркивается фамилия исполнителя, возвратившего документ, и проставляются сведения о новом местонахождении документа.

6.4. Оформление отправления и само отправление исходящих документов производится сотрудником предприятия.

6.5. Документ может быть отправлен в стороннюю организацию с сопроводительным письмом. Приложение и сопроводительное письмо являются самостоятельными документами (имеют свой учетный номер, регистрируются в соответствующей форме учета и т.п.)

6.6. В отметке о наличии приложения в основном документе (сопроводительном письме) указывается наименование каждого приложения (если оно не оговорено в тексте документа), учетный номер, гриф ограничения доступа, количество листов и номера экземпляров. Например:

Приложение: вид и краткое содержание документа, уч. № 11 Конфиденциально на 25 л., экз. №1.

Или

Приложение: уч. № 11 Конфиденциально на 10 л., экз. 1, 2.

При большом количестве приложений составляется их опись с указанием необходимых реквизитов включенных в нее документов, а в отметке о приложении на сопроводительном письме указывается:

Приложение: согласно описи №3 на 2 л.

Если у отправителя не остается копии пересылаемого приложения, то в отметке о приложении на сопроводительном письме пишется:

Приложение: уч. № 10 Конфиденциально на 20 л., экз. № 1 только в адрес.

6.7. На документ, предназначенный для направления в пять и более адресов, составляется список рассылки, который утверждается лицом, подписавшим документ или руководителем структурного подразделения, где готовился документ, а на каждом экземпляре указывается только один адрес. Список рассылки подшивается в дело вместе с копией исходящего документа.

6.8. Сотрудник предприятия, ответственный за работу с конфиденциальными документами, из картотеки подбирает карточку учета основного документа (сопроводительного письма) и карточку учета приложения.

Проверяется соответствие следующих данных в основном документе (сопроводительном письме) и карточке на него:

- ❖ учетный номер и гриф ограничения доступа;
- ❖ количества и номера экземпляров документа;
- ❖ количество листов в каждом экземпляре (с просчетом листов и проверкой наличия учетного номера на каждом листе);
- ❖ заголовка;
- ❖ даты документа.

На основном документе проверяется наличие адресата, даты документа, ссылки на учетный номер и дату документа, на который дается ответ (если документ ответный); отметки о направлении копии документа в дело.

Проверяется соответствие следующих данных приложения записям на сопроводительном письме:

- ❖ наименование приложения;
- ❖ учетный номер и гриф ограничения доступа;
- ❖ номера экземпляров;
- ❖ количество листов.

Гриф ограничения доступа сопроводительного письма должен соответствовать грифу приложения.

6.7. На копии документа, остающийся на предприятии проставляется отметка о заверении копий. Ниже реквизита подпись проставляется:

- ❖ слово «Верно»;
- ❖ наименование должности лица, заверившего копию;
- ❖ его личная подпись и ее расшифровка;
- ❖ дата заверения копии.

Верно. Сотрудник Подпись О. И. Иванова 26.02.01.

В соответствии с ГОСТ Р 6.30-2003 допускается на копиях отправляемых документов, остающихся в деле, не указывать дату заверения и должность лица, заверившего копию.

6.8. Документы отправляются ценными письмами и бандеролями. В этом случае следует использовать двойное конвертирование. На внутреннем конверте указывается гриф ограничения доступа, наименование структурного подразделения, должности и фамилии лица, которому адресованы документы, учетные номера документов и номера экземпляров. Порядок оформления внешнего пакета должен соответствовать Почтовым правилам Министерства связи.

6.12. При необходимости пакеты могут доставляться адресату курьерами предприятия, допущенными к работе с подобными документами. Курьер под расписку получает пакет, который доставляет в стороннюю организацию, где сдает пакет под расписку соответствующего работника. Указанная расписка подшивается в дело, которое хранится у сотрудника предприятия, а расписка курьера уничтожается.

6.13. Доставка пакетов через представителей других организаций производится на основании доверенности.

6.23. Для пересылки пакетов могут по договоренности использоваться каналы спецсвязи. В этом случае, оформление пакетов, порядок их приема-передачи осуществляется в соответствии с требованиями соответствующей Инструкции.

7. ПРИЕМ, УЧЕТ И ПРОХОЖДЕНИЕ ПОСТУПИВШИХ ДОКУМЕНТОВ

7.1. Поступающие в адрес предприятия конверты с указанием степени конфиденциальности документов экспедицией не вскрываются и передаются сотруднику предприятия.

7.2. В случае поступления в предприятия документов, содержащих по «Перечню сведений, составляющих конфиденциальную информацию предприятия» сведения, полученному документу присваивается соответствующий гриф.

7.3. Сотрудник предприятия принимает и вскрывает конверты. При этом проверяется и просчитывается количество листов и экземпляров документа, а также наличие указанных в сопроводительном письме приложений. При недостатке листов, экземпляров документа или приложений к нему составляется акт в двух экземплярах, один из которых высылается отправителю.

7.4. Документы, подлежащие учету, обработке и хранению в структурных подразделениях передаются соответствующему работнику под расписку в передаточном журнале.

7.5. Регистрация документов производится по карточкам учета поступивших документов.

7.6. На нижнем поле первого листа зарегистрированного входящего документа проставляется штамп, в котором указывается присвоенный при поступлении номер и гриф ограничения доступа документа, дата регистрации, количество листов основного документа и приложений.

7.8. После регистрации документы, требующие рассмотрения руководством предприятия, помещаются в папки и передаются соответствующему руководителю под расписку в журнале учета документов, переданных на рассмотрение руководителю. Передавать неучтенные документы не разрешается. Документы могут рассматриваться руководителем в присутствии сотрудника предприятия. В этом случае допускается не вносить документы в журнал. Если после доклада все документы или часть остаются у руководителя, они обязательно вносятся в журнал и руководитель расписывается за эти документы. В карточке учета поступивших документов руководитель за получение документов не расписывается.

7.9. После рассмотрения документов руководством предприятия сотрудник проверяет сохранность документов, наличие на каждом документе резолюции и расписывается в журнале учета документов, переданных на рассмотрение руководству, за возвращенные документы. Руководство предприятия может передавать рассмотренные конфиденциальные документы только через сотрудника предприятия.

7.10. В резолюции на документе, которая является важнейшим элементом системы доступа, должны быть указаны:

- исполнитель (или исполнители); срок исполнения; содержание действий;
- личная подпись лица, написавшего резолюцию; дата резолюции.

Например: *Господину Иванову А.И.*

Прошу подготовить отзыв на проект.... К 20. 04. 2003.

Сидоров 05.04.2003.

Лицо или подразделение, указанное в резолюции первым, является ответственным исполнителем.

7.11. В карточке учета поступивших документов резолюция не переносится за исключением экземпляра карточки, используемого для контроля исполнения документов.

7.12. Документы, подлежащие исполнению, сортируются по папкам исполнителей. После ознакомления с документом исполнитель расписывается на документе с указанием даты. Ответственному исполнителю предоставляется право созыва исполнителей, которые по его требованию обязаны предоставить все необходимые материалы и участвовать в исполнении документа. При необходимости повышения оперативности исполнения документов они могут быть размножены в соответствии с установленными требованиями .

7.13. Документ выдается сотрудником предприятия, ответственным за работу с конфиденциальными документами, исполнителю под расписку в карточке учета входящих документов с указанием количества полученных листов, т.к. документ может быть получен исполнителем не полностью. Кроме того, исполнитель вносит полученный документ в опись документов, находящихся у исполнителя.

7.14. Сотрудник предприятия, ответственный за работу с конфиденциальными документами, в контрольном журнале напротив учетного номера, присвоенному документу, указывает фамилию исполнителя, расписавшегося в карточке за получение документа. Если документ выдается по частям нескольким исполнителям, то в контрольном журнале проставляются фамилии всех исполнителей.

7.15. На время нахождения документа у исполнителя карточка учета поступивших документов ставится в соответствующий раздел (по фамилиям исполнителей) справочной картотеки. Если документ выдается по частям нескольким исполнителям, то все подписи за получение документа проставляются на основной карточке, которая ставится в ячейку картотеки по фамилии одного из исполнителей; в ячейки остальных исполнителей ставятся сигнальные карточки, на которых указываются входящий номер и гриф ограничения доступа документа, фамилия исполнителя и количество полученных им листов.

7.16. После окончательного исполнения документов, они принимаются от исполнителей сотрудником предприятия, ответственным за работу с конфиденциальными документами, который проверяет соответствие учетных номеров и количество листов документов записям в карточке учета входящих документов и в описи документов, находящихся у исполнителя, наличие отметки об исполнении документа и направление его в дело. После проверки работник расписывается за принятые документы в карточке учета входящих документов и в описи документов, находящихся у исполнителя, с указанием даты возврата.

7.17. Карточки учета на возвращенные документы перемещаются в соответствующий раздел справочной картотеки

7.18. В контрольном журнале зачеркивается карандашом фамилия исполнителя, возвратившего документ, и проставляются сведения о новом местонахождении документа.

8. УЧЕТ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ ВЫДЕЛЕННОГО ХРАНЕНИЯ

8.1. Учет конфиденциальных документов выделенного хранения осуществляется в карточках учета документов выделенного хранения.

8.2. При приеме конфиденциальных документов сотрудник предприятия должен проверить соответствие учетного номера и грифа ограничения доступа каждого документа записям в учетной карточке и передаточном журнале.

8.3. При регистрации документов выделенного хранения заполняются графы 1 – 9 карточки учета документов выделенного хранения.

В Гр.1 – проставляется номер, присваиваемый документу в порядке нарастания номеров без распределения по годам, а также гриф ограничения доступа. Каждому документу присваивается один номер независимо от количества листов и учетных номеров, в него входящих.

В Гр.2 – проставляется арабскими цифрами дата регистрации с указанием числа, месяца и года.

В Гр.3 – проставляется вид носителя информации и через тире род документа, например: «*калька – подлинник; ватман-оригинал*». Графа заполняется только при регистрации чертежно-графических документов.

В Гр.4 – указывается индекс (обозначение) чертежно-графического документа или вид и заголовок текстового документа.

В Гр.5 – указывается предприятие, откуда поступил документ, или подразделение данного предприятия, разработавшего документ.

В Гр.6 – проставляются учетные номера документов, присвоенные им до перевода на учет документов выделенного хранения.

В Гр.7 – 9 проставляются соответственно количество, номера экземпляров и количество листов в экземпляре. Гр.10 – используется для отметок о включении документа в папку (альбом), о замене подлинника, о квартальных и годовых проверках и т.д.

8.4. Одновременно с заполнением карточки регистрационные данные проставляются на документе:

 На текстовых документах на обложке и титульном листе в левом верхнем углу проставляется присваиваемый учетный номер, в правом верхнем углу обложки – гриф ограничения доступа и номер экземпляра.

 На чертежно-графических документах, изданных этой фирмой, на каждом листе подлинника проставляется присваиваемый учетный номер в местах, отведенных соответствующими стандартами. Если копии подлинника подлежат брошюровке, учетный номер проставляется дополнительно над основной надписью (угловым штампом).

 На чертежно-графических документах, полученных от других предприятий, проставляется присваиваемый учетный номер:

- ❑ на подлинниках – на каждом листе в отведенном для этого месте, проставленные там регистрационные номера зачеркиваются тонкими линиями;
- ❑ на дубликатах – в соответствующей графе каждого листа;
- ❑ на копиях, хранящихся россыпью (полистно) – в левом верхнем углу каждого листа;
- ❑ на документах, скомплектованных в папки или сброшюрованных в альбом – на этикетке или в верхнем левом углу обложки, а также на титульном листе (если он имеется) и заглавном листе описи папки (альбома).

8.5. После взятия документов на учет сотрудник предприятия должен проставить в карточках учета изданных, поступивших документов соответствующие номера документов выделенного хранения и заверить их своей подписью.

8.6. При производственной необходимости, взятые на учет документов выделенного хранения чертежно-графические документы могут комплектоваться в папки (альбомы) с соблюдением требований от ознакомления исполнителя только с необходимой им информацией. В этом случае папке присваивается новый учетный номер и гриф ограничения доступа в соответствии со степенью конфиденциальности.

В Гр. 6 карточке учета документов выделенного хранения перечисляются учетные номера документов, вошедших в папку. В описи документов в папки перечисляются в последовательности их расположения находящиеся в ней документы с указанием учетных номеров, грифа ограничения доступа, наименования, номеров экземпляра, количества листов. Первым листом описи является титульный лист, составленный на папку. Учетный номер каждого включенного в папку документа закрепляется в Гр. 10 карточки учета документов выделенного хранения отметкой «*Вошел в уч.* № _____».

9. УЧЕТ ЖУРНАЛОВ И КАРТОТЕК

9.1. Учетно-справочный аппарат к документам представляет собой совокупность картотек (карточки изготавливаются форматом 148x210 мм. карточка на отдельные виды, группы документов могут иметь цветовые отличия (окраску бумаги, цветовые полосы).) и журналов.

9.2. Справочная картотека состоит из двух частей: картотек на неисполненные документы и картотек на исполненные документы.

Часть картотеки на неисполненные документы делится на группы карточек: поступивших, отправленных и внутренних документов. Внутри этих групп карточки систематизируются по исполнителям.

Часть картотеки на исполненные документы формируется по классификационной схеме номенклатуры дел. Внутри разделов карточки располагаются в хронологической последовательности.

Карточки из первой части картотеки по мере исполнения документов с проставленными в них необходимыми отметками перемещают в соответствующий раздел второй части картотеки.

9.3. При карточном способе учета по каждому виду учета должны вестись контрольные журналы.

9.4. Листы журналов должны быть пронумерованы. На последнем листе журнала делается заверительная надпись о количестве листов журнала, которая подписывается сотрудником предприятия, отвечающим

за учет, обработку и хранение конфиденциальных документов, с указанием даты.

9.5. Все журналы и карточки должны быть учтены в момент заведения в журнале учета журналов и карточек (Приложение 10), который ведет сотрудник предприятия. Каждый журнал и каждая карточка должны иметь самостоятельные учетные номера.

9.6. При учете журналов данные граф 1 – 8 журнала учета журналов и картотек переносятся на обложку журнала, а при учете картотек печатаются на чистом листе (карточке) и наклеиваются на картотеку.

9.7. Количество карточек в картотеке указывается в конце года. Итоговая заверительная надпись с указанием общего количества карточек делается на чистом листе (карточке), помещаемом в конце картотеки. Количество листов журнала указывается при его заведении.

9.8. В журналах, карточках учета запрещается делать подчистки, исправления с помощью корректирующей жидкости. Внесенные исправления оговариваются и заверяются подписью сотрудника, ответственного за работу с конфиденциальными документами, с указанием даты.

9.9. Журнал учета журналов и картотек ведется непрерывно, номера каждого года продолжают номера предыдущих лет.

9.10. Журнал учета журналов и картотек учитывается в номенклатуре дел.

10. ОРГАНИЗАЦИЯ ХРАНЕНИЯ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

10.1. Организация хранения конфиденциальных документов должна исключать возможность несанкционированного доступа к ним. Основным принципом хранения конфиденциальных документов – персональная ответственность сотрудника предприятия, ответственного за работу с конфиденциальными документами, а также исполнителей за их сохранность.

10.2. За каждым исполнителем закрепляется сейф, в котором исполнитель хранит числящиеся за ним документы. Запрещается хранение конфиденциальных документов с какими-либо другими документами.

10.3. Конфиденциальные документы до завершения исполнения хранятся в сейфах исполнителей.

10.4. Сейфы должны иметь надежные индивидуальные запоры и опечатываться. Ко всем сейфам необходимо иметь по два экземпляра ключей. Один из экземпляров ключей находится у исполнителей, который по окончании рабочего дня он сдает руководителю структурного подразделения. Выносить ключ за пределы служебного помещения не разрешается.

10.5. Руководитель структурного подразделения хранит ключи исполнителей в своем сейфе. Ключ от сейфа в опечатанном пенале руководитель в конце рабочего дня сдает сотруднику охраны. Запасные ключи от всех сейфов хранятся у сотрудника предприятия.

10.6. При вскрытии сейфов должно присутствовать то лицо, которое отвечает за хранение документов. При его отсутствии сейф вскрывается комиссией с составлением акта.

10.7. При отсутствии возможности обеспечить каждого исполнителя сейфом, может применяться сейф на нескольких исполнителей. В этом случае каждая полка сейфа должна быть снабжена дверцей с замком, а общий ключ находится у руководителя структурного подразделения.

10.8. Работа с конфиденциальными документами выполняется только в служебных помещениях. При работе с документами исполнитель должен иметь на рабочем столе только те документы, которые необходимы в данное время. Остальные документы необходимо хранить в сейфе, которые должны быть закрыты, ключи от них убраны.

10.9. Запрещается хранить конфиденциальные документы, в том числе и во время работы с ними, в ящиках стола, шкафах и т.п. не предназначенных для хранения подобного рода документов.

10.10. При временном выходе из рабочей комнаты работник должен убрать все документы в сейф и закрыть его. При выходе из комнаты всех исполнителей дверь закрывается на замок.

10.11. Открывать окна во время работы с конфиденциальными документами возможно, если они оборудованы сетками и, если исключается возможность просмотра документов с улицы.

10.12. Каждый исполнитель прежде, чем закончить работу обязан проверить и удостовериться в наличии всех документов, числящихся за ним по описи документов, находящихся у исполнителя. Он должен убрать документы в сейф, опечатать его и сдать ключ под расписку руководителю структурного подразделения.

11. ТЕХНОЛОГИЯ КОНТРОЛЯ ИСПОЛНЕНИЯ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

Контроль исполнения конфиденциальных документов организуется и ведется в соответствии с требованиями ГСДОУ, но с учетом специфики работы с конфиденциальными документами. Ведение контроля исполнения конфиденциальных документов возлагается на сотрудника предприятия, ответственного за работу с конфиденциальными документами.

11.1. Сотрудник предприятия осуществляет следующие функции:

- ❑ формирование картотеки контролируемых документов;
- ❑ напоминание исполнителям о сроке исполнения;
- ❑ получение информации о ходе и результатах исполнения;
- ❑ запись хода и результатов исполнения в карточке контролируемого документа, которая должна содержать дату проверки и конкретные причины задержки исполнения;
- ❑ снятие документов с контроля по указанию руководителя.

11.2. При организации контроля исполнения используются дополнительные экземпляры учетных карточек, заполняемые на контролируемые документы, в процессе их регистрации. Для перенесения резолюции и контрольных отметок нужно использовать графу «Примечание». Из карточек контролируемых документов формируется контрольная картотека. Карточки в ней систематизируются по видам учета, срокам исполнения, по исполнителям.

11. РАЗМНОЖЕНИЕ И УНИЧТОЖЕНИЕ ДОКУМЕНТОВ

11.3. При размножении конфиденциальных документов необходимо обеспечить:

- ❑ предупреждение безучетного размножения документов;
- ❑ исключение необоснованного размножения документов
- ❑ исключение случаев утраты документов при их копировании и размножении;

- ❖ исключение безучетного уничтожения или утраты бракованных экземпляров;

11.4. Множительный аппараты должны находиться в помещении под контролем сотрудника предприятия и блокироваться при его отсутствии.

Размножение конфиденциальных документов производится только по письменному разрешению соответствующих руководителей, которое оформляется на обороте последнего листа документа: («размножить в экз. Подпись. Дата.»)

11.5. Конфиденциальные документы подлежат размножению только в том количестве, которое указано в визе-разрешении руководителя.

Документы с грифом «Конфиденциально» подлежат размножению только в присутствии исполнителя.

11.6. После размножения на обороте последнего листа подлинника исполнителем делается запись «Дополнительно размножено _____ экз. на _____ листах», которую заверяет своей подписью сотрудник предприятия с указанием даты.

11.7. Бракованные листы уничтожаются в установленном порядке (см. раздел «Уничтожение конфиденциальных документов»).

11.8. Дополнительно размноженные экземпляры регистрируются сотрудником предприятия за учетным номером подлинника и отметка в соответствующей учетной форме. Нумерация дополнительно размноженных экземпляров производится от последнего номера ранее учтенных экземпляров.

11.9. В случае обнаружения неучтенных размноженных экземпляров конфиденциального документа исполнитель, за которым числится документ, несет персональную ответственность за нарушение порядка работы с конфиденциальными документами.

11.10. Снятие копий с конфиденциальных документов, полученных от других организаций, осуществляется только по их письменному согласию с указанием количества экземпляров.

11.11. Уничтожение дел с истекшими сроками хранения производится в архиве и определяется требованиями государственных архивных органов.

11.12. В делопроизводстве работа по уничтожению документов включает:

- ❖ уничтожение черновиков, вариантов, бракованных листов бумаги т.п.;
- ❖ уничтожение копий, лишних экземпляров документов; описей документов, находящихся у исполнителя;

11.13. После проведения квартальной проверки сотрудник предприятия и сотрудник, допущенный к работе с конфиденциальными документами, проверяют целостность печатей на металлической урне, вскрывают ее и перекладывают макулатуру в специальную тару (например, мешок) и доставляют к месту уничтожения. Макулатуру уничтожают путем сжигания или переработке в специальных бумагорезательных машинах. После физического уничтожения указанные сотрудники составляют акт о том, что «макулатура из урн №№ _____ за _____ квартал уничтожена путем сжигания (или переработки)», с указанием подписей и даты.

11.14. При уничтожении копий, лишних экземпляров и т.п. необходимо:

11.14.1. Получить разрешение у руководителя структурного подразделения по тематике документов. Разрешение оформляется записью «УНИЧТОЖИТЬ» с проставлением подписи, соответствующего должностного лица и даты в учетной карточке.

11.14.2. Включить каждый отобранный документ отдельной позицией в Акт (Приложение № 11). Данные о документе, вносимые в Акт должны быть идентичны данным, зафиксированным в учетных формах. Несколько экземпляров одного и того же документа включаются в акт за общим номером. В графе «номера экземпляров» указываются через запятую подлежащие уничтожению экземпляры документов. Описи документов, находящихся у исполнителей, включаются в акт каждая за отдельной позицией, с указанием фамилии исполнителя, наименования структурного подразделения и года ведения описи.

11.15. Отобранные к уничтожению документы откладываются в специальную тару. Уничтожение документов производится не позднее, чем через пять дней после утверждения акта, а документов с грифом «Конфиденциально» в тот же день. Неоправданное накопление большого количества документов не допускается. Физическое уничтожение документов проводят сотрудники, участвовавшие в отборе документов и составлении акта.

11.16. После сжигания или переработке документов с применением технических средств, сотрудники, выполнявшие эту работу, обязаны оформить соответствующую запись в акте об уничтожении. После этого в учетных формах делается запись об уничтожении документов, например: «Экз. № 2, № 3 уничтожены. Акт от «___» _____ № _____», заверяемый подписями с указанием даты. Подписями этих же лиц в Акте заверяется соответствующая графа.

Акт подписывается сотрудниками, принимавшими участие в отборе документов, составлении акта, физическом уничтожении документов, и утверждается руководителем.

12. СОСТАВЛЕНИЕ И ОФОРМЛЕНИЕ НОМЕНКЛАТУРЫ ДЕЛ С ГРИФом «КОНФИДЕНЦИАЛЬНО»

12.1. Для дел с грифом «Конфиденциально» разрабатывается самостоятельная номенклатура отдельно от общей номенклатуры дел предприятия.

12.2. Методика составления номенклатуры дел с грифом «Конфиденциально» основывается на требованиях, изложенных в «Основных правилах архивов организаций» (М., 2002), но с учетом специфики работы конфиденциальными документами.

12.3. Номенклатура дел с грифом «Конфиденциально» предприятия разрабатывается сотрудником предприятия на основе письменных предложений (проектов номенклатур дел) структурных подразделений.

12.4. Номенклатура дел с грифом «Конфиденциально» предприятия подписывается сотрудником предприятия, визируется руководителем структурных подразделений, согласовывается с архивом предприятия и утверждается руководителем предприятия.

12.5. Номенклатуры дел издаются с грифом «Конфиденциально» регистрируются в карточке учета изданных документов.

12.6. Номенклатуры дел с грифом «Конфиденциально» предприятия составляется в двух экземплярах. Первый экземпляр хранится у сотрудника, а по окончании года подшивается в специальное дело, второй –

по передаточному журналу передается в качестве рабочего экземпляра в архив предприятия.

12.7. В структурные подразделения передаются соответствующие выписки из номенклатуры дел с грифом «Конфиденциально» предприятия для использования в работе.

12.8. Изменения в утвержденную номенклатуру дел предприятия, связанные с включением новых дел или расширения круга лиц, допускаемых к делам, вносятся в письменного разрешения руководителя предприятия на основании докладных записок руководителей структурных подразделений. Изменения в номенклатуре дел могут либо заверяться подписью лица, давшего разрешение, либо иметь ссылку на документ – основание, если разрешение оформляется по докладной записке.

12.9. В каждом структурном подразделении, в деятельности которого создаются документы, содержащие конфиденциальную информацию, в конце текущего года на следующий разрабатывают номенклатуру дел.

12.10. Подготовленные номенклатуры дел передаются сотруднику предприятия по передаточному журналу, на их основе составляется единая номенклатура дел с грифом «Конфиденциально» предприятия.

12.11. В номенклатуре дел предприятия систематизация дел производится по структурной схеме, т.е. разделами являются наименования структурных подразделений предприятия. Разделы номенклатуры должны иметь нумерацию. Номер раздела соответствует номеру, присвоенному подразделению. Номера разделов проставляются перед их наименованиями.

12.12. Заполнение граф производится следующим образом:

Гр.1 – указывается индекс, присвоенный делу и гриф ограничения доступа, устанавливаемый из степени конфиденциальности сведений, содержащихся в документах. Графа заполняется при составлении номенклатуры.

Гр.2 – вносятся заголовки дел в последовательности, предусмотренной схемой систематизации дел в номенклатуре. Переходящим делам сохраняются одни и те же заголовки до их закрытия. Графа заполняется при составлении номенклатуры.

Гр.3 – перечисляются инициалы и фамилии всех исполнителей, которым предоставляются право, пользования соответствующим делом. В течение года в список лиц могут вноситься изменения. Графа заполняется при составлении номенклатуры.

Гр.4, Гр. 5 – проставляются арабскими цифрами номер каждого тома и даты его заведения. Графы заполняются в день подшивки первого документа тома. Если дело переходящее, то в графе 5 при составлении номенклатуры дел указывается «переходящее с _____ г.» с проставлением года заведения дел.

Гр. 6 – проставляется арабскими цифрами дата закрытия каждого тома. Графа заполняется в день закрытия тома после подшивки последнего документа. Если дело переходит на следующий год, то в графе указывается «переходит на _____ г.».

Гр.7 – проставляется количество листов в томе. Графа проставляется при закрытии тома. Графы 4-7 заполняются по каждому тому отдельной строкой.

Гр.8 – указывается срок хранения дела и номер статьи по перечню, например: «Пост., Ст. 19К.»

Гр.9 – указывается в каком структурном подразделении храниться дело (все его тома) и фамилия лица, ответственного за формирование и хранение дела.

Гр.10 – проставляется архивный шифр, включающий номер фонда, описи и порядковый номер дела (2-1-16) или номер и дата акта об уничтожении. Графа заполняется после передачи в архив, уничтожении.

Гр. 11 – проставляется срок действия установленных ограничений на разглашение сведений конфиденциального характера.

13. ФОРМИРОВАНИЕ И ОФОРМЛЕНИЕ ДЕЛ

13.1. По мере исполнения документы в соответствии с номенклатурой группируются и систематизируются в комплексы путем формирования дел.

13.2. Дела заводятся при помещении в него первого документа. С момента заведения дела начинается его оформление.

13.3. При заведении дела на обложке указываются:

- ❖ гриф ограничения доступа;
- ❖ название организации;
- ❖ названия структурного подразделения;
- ❖ индекс дела;
- ❖ заголовок дела;
- ❖ срок хранения дела.

Если в деле содержится плановая и отчетная документация, то на обложке проставляется год ведения дела. В течение года на обложке может проставляться номер тома. (при заведении второго тома).

13.4. На внутреннюю сторону обложки из номенклатуры дел переносятся инициалы и фамилии лиц, которым предоставлено право пользования делами. Список допущенных к делу заверяется подписью лица, ответственного за формирование и хранение дела, с указанием даты.

13.5. Одновременно заводиться карточка учета выдачи дела, которое помещается в карман, приклеенный к внутренней стороне обложки. По заполнении одной карточки заводиться следующая а заполненная вносится во внутреннюю опись дела. Карточка не нумеруется, листом дела не считается. Карточки, заводимые после закрытия дела, также вносятся во внутреннюю опись дела.

13.6. С целью обеспечения сохранности и поиска документов при заведении дела в него перед документами подшивается необходимое количество листов внутренней описи. Данные о документе вносятся в момент его подшивки.

13.7. Все листы документов подшиваемых в дело нумеруются. Листы внутренней описи нумеруются отдельно. Нумерация листов осуществляется по каждому тому отдельно. При изъятии документов из дел старая нумерация листов сохраняется.

13.8. Формирование дел должно производиться в соответствии с требованиями, изложенными в «Основных правилах работы архивов организаций» (М., 2002).

13.9. Документы с грифом «Конфиденциально» категорически запрещается формировать в дела с документами без грифа ограничения доступа.

13.10. Изъятие документов из дела разрешается соответствующим руководителем. Вместо изъятых документов в дело помещается справка-заместитель (Приложение 13). О документах, изъятых из дела безвозвратно, производится, кроме того, отметка во внутренней описи дела, а по документам текущего года в их учетных формах.

13.11. Формирование дела производится путем подшивки документов в обложки.

13.12. После подшивки документов в его учетной карточки проставляется индекс дела и номера листов.

13.13. Закрытое дело подлежит дальнейшему оформлению.

13.14. На обложке проставляются крайние даты документов в деле, которые должны соответствовать датам подписания (утверждения) самого раннего и самого позднего документа, в не зависимости от расположения этих документов в деле.

13.15. Уточняются с внесением соответствующих изменений на обложку дела и в номенклатуру дел гриф ограничения доступа, заголовки и срок хранения дела.

13.16. При закрытии дела оформляется лист-заверитель и подшивается в конце дела.

13.17. Листы каждого тома дела при закрытии тома проверяются и прошиваются.

Дела с грифом «Конфиденциально», опечатываются, так что бы захватывались оба конца нити прошивки.

14. ПРОВЕРКА НАЛИЧИЕ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

14.1. Основными задачами проверки наличия документов являются:

Проверка наличия всех полученных и подготовленных документов, правильности оформления учетных данных, а также наличия оправдательных документов, на отсутствующие документы (отправленные, уничтоженные и др.), с целью устранения ошибок, нарушений, излишних операций при ведении учета.

14.2. Своевременное выявление фактов возможных недостатков, неучтенных документов и их безучетного движения;

14.3. Осуществление постоянного контроля за наличием и движением документов.

14.4. Проверки наличия проводятся в плановом порядке (квартальные проверки документов с грифом «Конфиденциально» и исполнителей, годовые проверки), и по мере необходимости (при смене руководителей и сотрудников, отвечающих за учет, обработку и хранение конфиденциальных документов).

14.5. Результаты проверок оформляются актом, в котором указывается вид проверки; основание для ее проведения; состав комиссии и сроки проведения; название подразделения, где она проводилась; общее количество, взятых на учет документов за проверяемый период по видам учета; количество документов, не состоящих на учете, и фамилии лиц, у которых они были обнаружены и по какой причине не учтены; количество и учет-

ные номера документов, не предъявленных в ходе проверки, за кем они числятся и причины не предъявления; другие выявленные нарушения с указанием фамилий, должностей и конкретных фактов нарушений; выводы и предложения по результатам проверки и мероприятия по устранению выявленных нарушений. Акт проверки подписывается членами комиссии и утверждается руководством банка.

14.6. Организация всех видов проверок и контроль за их проведением осуществляется сотрудником предприятия. 14.7. Квартальная проверка наличия документов с грифом «Конфиденциально» проводится сотрудником предприятия, а также дополнительно привлекаемым сотрудником, допущенным ко всем документам с грифом «Конфиденциально». Квартальная проверка проводится в первую декаду первого месяца следующего квартала.

14.8. Ежеквартально проверяются все документы с грифом «Конфиденциально» независимо от времени их получения или создания, а также наличие конфиденциальных документов у исполнителей.

14.9. При проведении проверки документов с грифом «Конфиденциально» проводятся следующие операции:

14.10. Проверяются соответствие учетных данных документа и данных на него в учетной карточке;

14.11. Проверяются наличие номеров и дат оправдательных документов за отправление или уничтожение документа или его частей (экземпляров, листов);

14.12. Просчитываются количество экземпляров и листов документа;

14.13. Проверяются соответствие фактического количества экземпляров и листов документа количеству, числящемуся по учету.

14.14. Выявляют позиции по контрольному журналу, по которым документы не были предъявлены к проверке;

14.15. Разыскиваются документы, не предъявленные при проверке, и проводят проверку соответствия их учетных данных данным на них в учетных карточках;

14.16. Производят установленные отметки о произведенной проверке в контрольных журналах. Например, «*Квартальная проверка документов с грифом «Конфиденциально» проведена*». Если в журнале имеются незакрытые позиции, она вписывается в итоговую запись: «*Квартальная проверка документов с грифом «Конфиденциально» проведена, №№ ____ не закрыты. Документы в наличии*». Запись заверяется подписями лиц, проводившими проверку, с проставлением даты.

14.17. Просчитывают поединично дела с грифом «Конфиденциально», учтенные по номенклатуре, сверив их количество с количеством дел по номенклатуре;

14.18. Проверяют наличие отметок в номенклатуре и оправдательных документов на отсутствующие дела. Выборочно следует проверить полностью дела, наиболее часто выдаваемые исполнителям, а также аккуратность оформления и ведения всех дел с грифом «Конфиденциально», числящиеся по номенклатуре. Против каждой проверяемой позиции в но-

менклатуре делается условная отметка карандашом. Результаты квартальной проверки наличия документов с грифом «Конфиденциально» оформляются актом.

14.19. Исполнители, работающие с конфиденциальными документами, на рабочих местах, проверяются не реже одного раза в квартал. При этом проверяется наличие всех числящихся за исполнителем документов, порядок хранения и работы с ними на рабочих местах.

15. Проверка исполнителей производится сотрудником предприятия.

15.1. Проверка проводится в присутствии исполнителя, в случае его отсутствия – в присутствии руководителя структурного подразделения.

15.2. При проверке исполнителей проверяются:

- наличие в сейфе документов, числящихся за исполнителем по всем видам учета, независимо от сроков регистрации документов;
- соответствие данных документа данным в учетной форме (учетный номер, гриф ограничения доступа, заголовок, количество листов и экземпляров, номера экземпляров);
- правильность ведения описи документов, находящихся у исполнителя;
- наличие сейфа и ключей от него;
- соблюдение исполнителем требований к подготовке, изданию и хранению документов.

15.3. При отсутствии у исполнителя, числящегося за ним документа, проверяется наличие оправдательных документов или подписи лица, получившего документ, в описи документов, находящихся у исполнителя, и обоснованность передачи документа без участия сотрудника предприятия. Проверяется наличие документа и условия его хранения у лица, его получившего. При обнаружении у исполнителя документа, не числящегося за ним по учетным формам, принимаются вышеперечисленные меры.

15.4. О результатах проверки наличия документов у исполнителя делается запись в описи документов, находящихся у исполнителя: *«Проверка проведена, документы в наличии»*. Если имеются отдельные нарушения в ведении описи, хранении документов, то они перечисляются после указанной записи, которая заверяется подписью проверяющего и датируется.

15.5. О результатах проверок информируются руководители и при нарушениях принимаются соответствующие меры.

15.6. При необходимости могут проводиться внеплановые проверки наличия документов у исполнителей при уходе в отпуск или при увольнении по изложенной выше методике.

15.7. Годовая проверка наличия документов проводится в январе следующего за проверяемым годом.

15.8. Годовая проверка проводится комиссией, назначаемой приказом генерального директора. Председателем комиссии назначается

один из его заместителей. В комиссию обязательно включается сотрудник предприятия.

15.9. В годовую проверку проверяется наличие всех без исключения документов, содержащих конфиденциальную информацию (гриф «Конфиденциально»).

15.10. При проведении годовой проверки наличия документов проверяется:

15.10.1. Наличие и правильность записей о проведении квартальных проверок наличия документов с грифом «Конфиденциально» в контрольных журналах. Незакрытые в квартальную проверку позиции перепроверяются;

15.10.2. Наличие всех документов с грифом «Конфиденциально», созданных или полученных в течение года (см. методику проведения проверки п.п. 16.7.1. – 16.7.6.);

15.10.3. В контрольных журналах по каждому виду учета делается запись: *«Годовая проверка проведена»* или *«Годовая проверка проведена, №№_____ не закрыты. Документы в наличии»*, которая заверяется подписями проверяющих с проставлением даты.

15.10.4. Правильность закрытия картотек и журналов и отметок об их учете в журнале учета журналов и картотек, о чем делается запись в указанном журнале: *«Годовая проверка проведена. Учетные документы №№_____ не закрыты»*, заверяемая подписями проверяющих с проставлением даты. Учетные карточки пересчитываются и сверяются с записью об их количестве в журнале учета журналов и картотек.

15.10.5. Дела сверяются поединично с номенклатурой дел. При этом проверяется: соответствии индекса дела, количества листов на обложке записям в номенклатуре; грифа на обложке и в номенклатуре содержанию дела (при не соответствии гриф изменяется); правильность оформления перерегистрации переходящих дел в номенклатуру следующего года. В конце номенклатуры дел производится запись *«Годовая проверка проведена, дела №№_____ не закрыты»*, заверяемая подписями проверяющих с проставлением даты.

15.11. Результаты годовой проверки наличия конфиденциальных документов оформляются актом.

15.12. При наличии грубых нарушений и ошибок, выявленных проверкой, издается приказ о наложении дисциплинарных взысканий на соответствующих должностных лиц.

16. ПОДГОТОВКА КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ НА АРХИВНОЕ ХРАНЕНИЕ

16.1. Законченные делопроизводством дела постоянного и временного (свыше 10 лет) хранения с грифом «Конфиденциально» после окончания календарного года, в котором они были заведены, подлежат научно-технической обработки, которая включает в себя: экспертизу ценности документов, окончательное оформление дел и составление описей дел.

16.2. Организационно-методическое руководство и контроль по вопросам организации и проведения экспертизы ценности осуществляют экспертная комиссия (далее ЭК) и архив предприятия.

16.3. При ЭК создается группа экспертов, имеющих доступ к конфиденциальным документам, основной задачей которой является отбор на хранение конфиденциальных документов подразделений, в которых они работают.

16.4. Экспертиза ценности конфиденциальных документов в подразделениях должна производиться сразу после окончания делопроизводственного года. К отбору документов привлекаются их непосредственные исполнители, чтобы достичь более высокого качества их оценки.

16.5. При проведении экспертизы ценности конфиденциальных документов в структурных подразделениях осуществляется определение сроков хранения всех категорий документов. При этом одновременно проверяется качество и полнота действующей номенклатуры дел с грифом «Конфиденциально» предприятия, правильность установления сроков хранения дел, заведенных в соответствии с номенклатурой, соблюдение установленного порядка формирования и оформления дел.

16.6. Отбор документов проводится на основе «Перечня типовых управленческих документов, образующихся в деятельности организации с указанием сроков хранения» (М., 2000) и номенклатуры дел с грифом «Конфиденциально» предприятия путем полистного просмотра дел. При полистном просмотре дел постоянного хранения подлежат изъятию дублетные экземпляры документов, неоформленные копии документов и документы с временными сроками хранения.

16.7. Дела с отметкой «ЭПК» подвергаются также полистному просмотру с целью определения и выделения из их состава документов, подлежащих постоянному хранению.

16.8. Выделенные из их состава документы постоянного хранения присоединяются к однородным делам или оформляются в самостоятельные дела.

16.9. При расшивке дела с отметкой «ЭПК» вместо изъятых листов помещается справка-заместитель, пересоставляется лист-заверитель, во внутренней описи производятся соответствующие отметки (графа 7) и на обложке дела указывается фактическое количество листов. Изъятые листы подшиваются в дело соответствующего содержания, сроки хранения и доступа. Дело расшивается, листы перенумеровываются, составляется новый лист-заверитель, сведения о документах вносятся во внутреннюю опись, на обложке дела указывается новое количество. Затем дело сшивается и печатывается (для дел с грифом «Конфиденциально»).

16.10. Если из изъятых документов формируется новое дело, его оформление производится в соответствии с установленными требованиями (см. раздел «Формирование и оформление дел»). Вновь созданное дело должно быть учтено и его необходимо внести в номенклатуру дел за соответствующий год.

16.11. По результатам экспертизы ценности конфиденциальных документов сотрудник предприятия составляет описи отдельно на дела постоянного, временного (свыше 10 лет) хранения и по личному составу. На дела временного (до 10 лет включительно) хранения опись не составляется. Они учитываются и передаются в архив по номенклатуре дел.

16.12. Описи дел составляются по установленной форме и представляются в архив через год после завершения дел в делопроизводстве. Описи издаются с грифом «Конфиденциально» и регистрируются в карточке учета изданных документов.

16.13. Составление и оформление описи дел структурного подразделения производится в соответствии с требованиями «Основных правил работы архивов организаций» (М., 2002).

16.14. Опись дел структурного подразделения подписывается сотрудником предприятия и утверждается руководителем структурного подразделения.

16.15. Опись дел составляется в двух экземплярах, один из которых передается с делами в архив предприятия, второй – остается в качестве контрольного экземпляра у сотрудника, где подшивается в дело с описями.

16.16. После составления описи нужно внести дополнения в оформление дел. На обложке дела проставляют номера фонда, описи, дела (порядковый номер по описи). Временная шифровка дел производится черным графитным карандашом.

17. ПОРЯДОК ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ В АРХИВ

17.1. Через год после завершения делопроизводства в архив предприятия передаются дела постоянного, временного (свыше 10 лет) хранения и по личному составу. Их передача осуществляется только по описям.

17.2. Дела временного (до 10 лет включительно) хранения передаются в архив предприятия по номенклатуре дел.

17.3. Передача дел в архив осуществляется по графику, который ежегодно составляется архивом, согласовывается с руководителями структурных подразделений и утверждается сотрудником предприятия.

17.4. В период подготовки дел структурными подразделениями к передаче в архив сотрудником архива предварительно проверяется правильность их формирования, оформления и соответствия количества дел, заведенных по номенклатуре дел. Все выявленные при проверке недостатки обязан устранить сотрудник предприятия.

17.5. Прием каждого дел производится работником архива в присутствии сотрудника предприятия. При этом на обоих экземплярах описи против каждого дела, включенного в нее, делается отметка о наличии дела. В конце каждого экземпляра описи указывается количество фактически принятых в архив дел, дата приема-передачи дел, а также подписи сотрудника архива и сотрудника предприятия, который передал дела в архив.

Приложение 1

Карточка-разрешение выдачи документа (дела)

Фамилия, имя, отчество

Наименование должности, структурного подразделения и учреждения

1. Разрешение на выдачу

Лицевая сторона карточки

№№ п.п.	Учетный номер и гриф ограничения доступа документа (дата)	Наименование документа (дата)	Количество листов или №№ листов дела, с которыми ознакомился исполнитель	Подпись лица, разрешившего выдачу, и дата	Согласовано (подпись руководителя)	На какой срок разрешена выдача

2. Выдача

Оборотная сторона карточки

Дата выдачи	Количество листов	Расписка в получении и дата	Дата возврата	Расписка о возврате и дата

Приложение 2

РАСПИСКА

Дана _____ в том, что мною
(Фамилия Имя Отчество)

_____ получены во временное пользование
(Фамилия Имя Отчество)

документы №№ _____

Всего на _____ листов.

" ____ " _____ г. _____
(подпись)

Приложение 3

Карточка учета изданных документов

Лицевая сторона карточки

Учетный номер и гриф ограничения доступа	Дата документа	Вид и краткое содержание	Количество	
			Экземпляров	Листов в экземплярах

Наименование подразделения	Расписка за получение и дата	Расписка за возврат и дата

Оборотная сторона карточки

Куда направлен	Номера экземпляра	Наименование, номер и дата сопроводительного документа	Отметка о возврате

Индекс дела по номенклатуре	Номера листов дела, куда подшит документ	Примечание

Приложение 4

Контрольный журнал

Учетный номер и гриф ограничения доступа	Движение документа	Отметка о годовой проверке
1	2	3

Приложение 5

Карточка учета поступивших документов

Лицевая сторона карточки

Учетный номер и гриф ограни- чения доступа	Дата регистрации	Откуда поступил	Учетный номер и дата посту- пившего документа	Количество листов	
				Основного документа	Приложения
Вид и краткое содержание					
Куме выдан		Количество листов	Расписка за получение и дата	Расписка за возврат и дата	

Оборотная сторона карточки

Куда направлен	Количество листов	Наименование и номер сопроводительного документа	Отметка о возврате
Индекс дела по номенклатуре		Номера листов, куда подшит документ	Примечание

Приложение 6

Карточка учета документов выделенного хранения

Лицевая сторона

Учетный номер и гриф ограничения	Дата регистрации	Вид носителя и род документа	Индекс (вид) и наименование документа	Откуда посту- пил или каким подразделением разработан	С каких уч. № переведен документ
1	2	3	4	5	6
Количество экземпляров	Номера экземпляров	Количество длистов в экземпляре	Дополнитель- ные учетные данные		
7	8	9	10		

Оборотная сторона карточки

Размножение			Отправление			Возврат		Уничтожение		Отметка о передаче на архивное хранение
Кол-во экз.	Номера экз.	Кол-во листов в экз.	Куда отправлен	Номера экз.	Наименование, номер, дата сопроводительного письма	Номера экз.	Номер по учету пост. документов	Номер экз.	Номер и дата акта об уничтожении	
11	12	13	14	15	16	17	18	19	20	21

Приложение 7

Наименование учреждения	Вх. №	
	Дата регистрации	
	Количество листов	

К вх №	
Количество листов	
Год регистрации	

Приложение 8

Журнал учета документов, переданных на рассмотрение руководству

Учетный номер и гриф ограничения доступа	Количество листов	Расписка за получение и дата	Расписка за возврат и дата
1	2	3	4

Приложение 9

Опись документов,
находящихся у исполнителя

№№ п/п	Учетный номер и гриф ограничения доступа	Дата получения	Вид и краткое содержание	Количество		Расписка за получение и дата	
				экземпляров	листов в экземплярах	исполнителя	референта фирмы
1	2	3	4	5	6	7	8

Приложение 10

ЖУРНАЛ
учета журналов и карточек

Учетный номер и гриф ограничения доступа	Наименование журнала, картотеки	Номер тома журнала	Дата		Количество листов, карточек	Сроки хранения и номер статьи по перечню	Ответственный за ведение и сохранность, роспись и дата	Архивный шифр или номер, дата акта об уничтожении
			заведения картотеки, тома журнала	закрытия картотеки, тома, журнала				
1	2	3	4	5	6	7	8	9

Приложение 11

УТВЕРЖДАЮ
Руководитель
структурного подразделения

(подпись) (расшифровка подписи)

АКТ № _____
О выделении к уничтожению
документов, не подлежащих хранению

На основании _____

отобраны к уничтожению как не имеющие научно-исторической ценности и утратившие практическое значение документы.

№№ п/п	Учетный № гриф ограниче- ния доступа	Заголовок документа	Количество экземпляров	Номера экземпляров	Количество листов в экз-ре	Всего листов
1	2	3	4	5	6	7

Всего подлежит уничтожению _____ наименований документов и

(прописью)

экземплярах*

(прописью)

Правильность произведенных записей в акте с данными учета сверил*

Документы перед уничтожением с записями в акте сверил и полностью уничтожил путем _____ *

Отметки в карточках учета об уничтожении документов произвел.*

Наименование должности _____ подпись _____ расшифровка подписи.

" _____ " _____ Г.

* Каждая запись в акте заверяется подписями лиц, принимающих участие в уничтожении документов, с указанием даты.

Приложение 12

УТВЕРЖДАЮ
Наименование должности _____

(подпись) (расшифровка подписи)

Индексы дел и гриф ограниче- ния досту- па	Заголовок дела	Инициалы и фамилии исполните- лей, кото- рым предостав- лено право пользо- ваться делами	Номер тома	Дата		Количество листов в томе, деле	Срок хра- нения но- мер статьи по перечню	Место фор- мирования дела, фам- илия ответ- ственного за форми- рование и сохране- ние	Архивный шифр, но- мер и дата акта об уничтоже- нии, куда направле- но, номер и дата сопро- водитель- ного письма	Срок огра- ничения доступа
				Заведения тома дела	Закрытия тома дела					
1	2	3	4	5	6	7	8	9	10	11

Наименование должности _____ подпись _____ расшифровка подписи

" _____ " _____ Г.

СОГЛАСОВАНО

Заведующий архивом

подпись

расшифровка подписи

Приложение 13

Справка-заместитель

Документ № _____ от _____ на _____ л. из дела изъятф

* _____

Основание: _____

Наименование должности
работника, производившего
изъятие документа

подпись

расшифровка подписи

* указывается новое местонахождение документа: при подшивке в другое дело – индекс, дата, номера томов, листов; при направлении – куда направлен, постоянно или временно, номер и дата сопроводительного документа; при уничтожении – номер и дата акта об уничтожении.

Приложение 14

Карточка учета выдачи дела

Индекс, гриф ограничения доступа, номер тома, заголовок дела

Дата выдачи	Количество листов	Кому выдано	Расписка за получение и дата	Расписка за возврат и дата
1	2	3	4	5

Приложение 15

Внутренняя опись

Дела № _____, том № _____ за 200__ г.

№№ п/п	Дата документа	Учетный номер и гриф ограничения доступа входящего документа	Учетный номер и гриф ограничения доступа изданного документа	Откуда поступил или каким структурным подразделением составлен	Номера листов дела	Отметка о местонахождении изъятых из дела документа
1	2	3	4	5	6	7

Итого _____ документов.
(цифрами и прописью)

Количество листов внутренней описи _____
(цифрами и прописью)

Наименование должности работника,
составившего опись _____
" ____ " _____ г.

Приложение 16

Лист-заверитель дела № _____

В деле подшито и пронумеровано _____ листов.
(цифрами и прописью)

в том числе:

литерные номера _____

пропущенные номера _____

+ листов внутренней описи _____

Наименование должности лица,
составившего заверительную надпись

подпись

расшифровка подписи

" ____ " _____ 200 ____ г.

Приложение 17

Конфиденциально

(наименование организации)

(наименование структурного подразделения)

УТВЕРЖДАЮ
Наименование должности

" ____ " _____ (подпись) (расшифровка подписи)
_____ г.

ОПИСЬ № _____

№№ п/п	Индекс дела (тома), гриф ограничения доступа	Заголовок дела (тома)	Дата дела (тома)	Количество листов в деле (томе)	Срок хране- ния дела (тома)	Срок ограни- чения доступа	Примечание
1	2	3	4	5	6	7	8

В данную опись внесено _____ дел с № _____ по № _____
(цифрами и прописью)

в том числе:

– дела с грифом "Конфиденциально";

– литерные номера;

– пропущенные номера.

Наименование должности
составителя описи

подпись

расшифровка подписи

СОГЛАСОВАНО

Наименование должности
" ____ " _____ 200 ____ г.

подпись

расшифровка подписи

Передал _____ дел и _____
(цифрами и прописью) (цифрами и прописью)

регистрационно-контрольных карточек к документам.

Наименование должности
" ____ " _____ 200 ____ г.

подпись

расшифровка подписи

Принял _____ дел и _____
(цифрами и прописью) (цифрами и прописью)

регистрационно-контрольных карточек к документам.

Наименование должности
работника архива
" ____ " _____ 200 ____ г.

подпись

расшифровка подписи

Типовая инструкция по охране труда и технике безопасности**1. Общие положения.** (Для Украины).

1. Настоящая Инструкция по охране труда работников охраны разработана на основании Закона Украины от 15.05.1996 года N 196/96-ВР “Об охране труда” и предусматривает основные требования по охране труда работников охранных фирм.

2. Работа по охране труда охранных фирм проводится в соответствии с Украины, другими законодательными и иными нормативными правовыми актами Украины, а также настоящей Инструкцией.

3. Руководители службы охраны и начальники охран объектов проводят организационно-технические, санитарно-гигиенические и иные мероприятия, направленные на сохранение жизни и здоровья работников охраны, а также предупреждение производственного травматизма и предотвращение возникновения профессиональных заболеваний работников охраны.

4. В целях обеспечения соблюдения требований охраны труда, осуществления контроля за их выполнением вводятся внештатный специалист по охране труда. Он осуществляет свою деятельность во взаимодействии со специалистами в области охраны труда предприятий, органов исполнительной власти, государственного надзора и контроля за соблюдением требований охраны труда и органами общественного контроля.

5. Руководители службы охраны объектов и внештатный специалист по охране труда, в должностные обязанности которых включены вопросы охраны труда, должны пройти обучение и проверку знаний в специализированных учебных центрах и иметь допуск установленной формы для права проведения инструктажа работников охраны.

6. Установленные на охраняемых объектах правила внутреннего распорядка, инструкции по охране труда и требования внутриобъектового режима являются обязательными для выполнения всем личным составом охраны.

7. На основе настоящей Инструкции с учетом конкретных особенностей рабочего места (поста) и реальных условий труда на каждом объекте охраны разрабатываются особые инструкции по охране труда для работников охраны. Данные инструкции подписываются внештатным специалистом по охране труда охранной фирмы и согласовывается с отделом (инженером) по технике безопасности охраняемого объекта.

Инструкции для работников охраны утверждаются руководителем охранной фирмы. В случае необходимости Инструкции для работников охраны могут прилагаться к договорам на охрану объекта.

8. Инструкции для работников должны находиться в местах, доступных для ознакомления с ними. Изучение инструкций работниками обеспечивается администрацией охранной фирмы и начальниками (старшими) охран объектов. Требования инструкций являются обязательными для работников охраны, их невыполнение рассматривается как нарушение трудовой дисциплины.

9. Контроль за выполнением требований инструкций для работников возлагается на руководителей охранных фирм.

Всякое отклонение от указанных в инструкции требований влечет за собой ответственность в дисциплинарном или административном порядке согласно действующему законодательству Украины

Контроль за выполнением требований инструкций по охране труда также осуществляют соответствующие уполномоченные работники представительных органов власти и служб охраны труда предприятий, организаций и учреждений с которыми заключены договора на охрану.

Каждый случай травматизма, аварии, профессионального отравления должен быть расследован в соответствии с действующим Положением о расследовании и учете несчастных случаев на производстве.

10. Мероприятия по охране труда закрепляются в контрактах, регулирующих социально-трудовые отношения администрации охранных предприятий и работников охраны.

11. Финансирование мероприятий по улучшению условий и охраны труда осуществляется в соответствии с законодательством Украины.

II. Общие требования безопасности.

Порядок проведения инструктажа и обучения личного состава мерам безопасности

13. Работниками охраны могут быть граждане Украины, достигшие возраста 18 лет, годные по состоянию здоровья и деловым качествам к выполнению задач, возложенных на вневедомственную коммерческую охрану.

14. Работники охраны обязаны проходить в установленном порядке предварительные (при приеме на работу) и ежегодные медицинские осмотры, а также периодические проверки на годность к действиям в условиях, связанных с применением физической силы и специальных средств.

15. Инструктаж и обучение личного состава мерам безопасности при выполнении работ связанных с охраной объекта, сопровождении и охране грузов, эксплуатации инженерно – технических средств охраны должны обязательно проводиться на всех объектах охраны.

Общее руководство и ответственность за правильную организацию проведения инструктажа и обучения, как вновь поступающих, так и работающих в лиц мерам безопасности возлагается на руководителя службы и внештатного специалиста по охране труда.

Ответственность за своевременное и качественное проведение инструктажа и обучение личного состава охраны мерам безопасности возлагается на начальников охран объектов.

16. Обучение личного состава охраны мерам безопасности проводится в процессе служебной подготовки, а также методом специальных инструктажей:

- а) вводного инструктажа;
- б) первичного инструктажа и обучения на посту (рабочем месте);
- в) инструктажа перед заступлением на службу, началом работ (ежедневно);
- г) периодического (повторного) инструктажа;
- д) внепланового (внеочередного) инструктажа.

17. Вводный инструктаж проводится внештатным специалистом по охране труда по специальной программе с целью ознакомления вновь поступающих в охрану лиц с общими положениями по безопасности труда и производственной санитарии, с порядком и правилами поведения на территории и в административно – производственных зданиях (помещениях) охраняемого объекта.

18. Первичный инструктаж проводится перед допуском к самостоятельному выполнению служебных задач. Каждый вновь поступающий в охрану должен пройти первичный инструктаж по мерам безопасности при несении службы по охране объекта, сопровождении и охране грузов, эксплуатации инженерно – технических средств охраны, а также хранении и обращении со специальными средствами.

Помимо первичного инструктажа вновь принятые в охрану лица обязаны пройти обучение безопасным приемам службы (работы) непосредственно на постах (рабочих местах) в течение первых пяти-семи дней. Обучение завершается проверкой теоретических знаний и практических навыков экзаменационной комиссией. Результаты проверки оформляются протоколом.

К самостоятельному выполнению задач вновь принятые в охрану лица допускаются после проверочных занятий по мерам безопасности проведенной в системе служебной подготовки и только с разрешения начальника службы.

Первичный инструктаж и обучение безопасным приемам службы (работы) должен проводить начальник охраны объекта в ведении которого находится данный работник с участием внештатного специалиста по охране труда.

О проведении первичного инструктажа и обучении мерам безопасности делается запись в журнале учета инструктажей (см. приложение 1), который храниться у внештатного специалиста по охране труда.

19. Периодический (повторный) инструктаж по мерам безопасности должен проводиться для всего личного состава охраны не реже одного раза в квартал. Его проводит начальник охраны объекта (вахты) в ведении которого находится данный личный состав, под контролем внештатного специалиста по охране труда в форме живой беседы и подкрепляется разбором конкретных требований инструкции по мерам безопасности и примеров из практической службы отдельных лиц охраны. Инструктирующий должен убедиться в четком знании и понимании каждым сотрудником охраны требований инструкции по мерам безопасности и в умении применять безопасные приемы и методы службы (работы).

Периодический (повторный) инструктаж оформляется записью в журнале учета инструктажей.

20. Внеплановый инструктаж личного состава по мерам безопасности проводится при изменении служебных инструкций, табеля постам и эксплуатационной документации, по требованию проверяющих лиц, а также при выполнении разовых работ, не предусмотренных кругом работ по основной профессии (службе) и в случаях нарушения личным составом требований инструкции по мерам безопасности или когда из-за недостаточных знаний отдельными лицами безопасных приемов и методов службы (работы) имели место несчастные случаи.

Внеплановый инструктаж должен проводиться теми же начальниками, в обязанности которых входит проведение первичного и периодического (повторного) инструктажей. Инструктирующий должен убедиться в четком знании личным составом безопасных приемов службы (работы) и инструкции по мерам безопасности.

О проведении внепланового инструктажа делается запись в том же журнале учета, в котором ведутся записи первичного и периодического (повторного) инструктажей.

21. Работники охраны во время несения службы должны соблюдать правила внутреннего распорядка, установленные руководителем охранной фирмы, с учетом особенностей охраняемых объектов.

22. Работники охраны обеспечиваются вещевым имуществом по установленным нормам. Ношение на работе форменного обмундирования обязательно, кроме случаев, специально оговоренных договором на охрану объекта.

Форменная и специальная одежда должны быть исправны и подогнаны по размеру. Головной убор, воротник или капюшон не должны ограничивать обзор и слышимость, обувь должна быть на низком, широком или сплошном, нескользящем каблуке.

23. На территории охраняемых объектов, где имеются строительные подъемные механизмы, траншеи, колодцы подземных коммуникаций, установки высокого напряжения, хранилища взрывчатых и горюче-смазочных материалов, кислот, газа и другие сооружения повышенной опасности, несение службы работниками охраны осуществляется в соответствии с правилами техники безопасности для работников, производящих работы на этих объектах.

24. В случае возникновения пожара работник охраны должен действовать в соответствии с разработанными правилами пожарной безопасности для охраняемого объекта.

25. Каждый работник охраны должен знать правила оказания первой доврачебной помощи гражданам с признаками нарушения дыхания, остановки сердца, при внезапных заболеваниях и различных травмах.

В помещениях охраны должны быть аптечки с медицинскими средствами и медикаментами для оказания первой доврачебной помощи пострадавшим.

В аптечках должна храниться опись вложений с указанием даты получения медикаментов, подлежащих периодическому обновлению, а также инструкция по правилам применения медикаментов и медицинских средств. Перечень основных медикаментов и медицинских средств, для комплектования аптечки первой доврачебной помощи, приведен в настоящей инструкции.

26. О каждом несчастном случае на производстве работник охраны должен немедленно известить руководство подразделения охраны и администрацию охраняемого объекта.

27. Работник охраны в случае обнаружения неисправности оборудования, приспособлений, других опасных производственных факторов, которые могут повлечь за собой несчастный случай на производстве, уведомляет об этом администрацию охраняемого объекта и руководство подразделения охраны или лицо, в должностные обязанности которого включены вопросы организации работы по охране труда, делает об этом запись в книге приема и сдачи охраняемого объекта. По выявленным недостаткам должны быть приняты меры к их устранению в кратчайшие сроки.

III. Требования безопасности перед началом работы

28. Работник охраны перед заступлением на службу по охране объектов ОБЯЗАН:

28.1. Убедиться в наличии и исправности средств связи, сигнальных устройств и предупреждающих знаков, приборов охранно-пожарной и тревожной сигнализации, периметрального и другого освещения, средств пожаротушения и водоснабжения, электронагревательных приборов, печ-

ного отопления, укомплектованности аптечки первой доврачебной помощи, наличии предусмотренной служебной документации на посту.

28.2. Проверить исправность механизированных ворот и стопорных устройств на них, эстакад для досмотра транспорта, смотровых вышек, турникетов.

28.3. Обойти территорию охраняемого объекта по маршруту согласно план – схемы обхода территории, утвержденной руководством подразделения охраны и согласованной с администрацией охраняемого объекта. Убедиться в наличии ограждений с предупредительными надписями и сигнального освещения у мест производства земляных и иных работ (в том числе у ям, котлованов, траншей).

28.4. На объектах, где используются служебные собаки, проверить надежность запоров калиток в ограждениях зон свободного окарауливания, оборудования и приспособлений блокпостов и постов служебным собакам, глухой привязи собак.

28.5. Обо всех выявленных недостатках, препятствующих безопасно- му несению службы, доложить непосредственному начальнику и администрации охраняемого объекта. Сделать записи в книге приема и сдачи объекта под охрану. В случаях невозможности устранения недостатков действовать по указанию ответственных должностных лиц подразделения охраны.

IV. Требования безопасности во время работы

29. Обход территории охраняемого объекта работники охраны должны совершать по разработанному маршруту и только по тротуару или пешеходной дорожке, придерживаясь левой стороны, а где их нет – по левой обочине дороге, соблюдая меры личной безопасности. Маршрут должен проходить по участкам территории, свободным от захламленности, ям, траншей, кюветов, колодцев подземных коммуникаций, резервуаров с водой, вне полотна железнодорожных путей, на безопасном расстоянии от блокпостов и постов глухой привязи служебных собак. Движение по полотну параллельно железнодорожным линиям допускается лишь в исключительных случаях, когда нельзя избрать другого пути.

В вечернее и ночное время суток при обходе территории пользоваться электрическим фонарем. При передвижении ночью по маршруту следует на некотором расстоянии от зданий и сооружений, выдерживать по возможности необходимую дистанцию по отношению к находящимся или оказавшимся вблизи людям и никого поблизости не оставлять сзади себя.

С наступлением темноты приближаться к человеку надо, как правило, со стороны источника света. При приближении человека сзади – следует отойти в сторону, остановиться, пропустить его или изменить направление движения и пойти навстречу приближающемуся лицу, одновременно быть готовым к действиям отражающие возможное внезапное нападение.

Территория объекта по периметру и внутренние объекты охраны с наступлением темноты должны быть освещены с таким расчетом, чтобы имелась возможность производить обозрение труднодоступных для охраны мест и подходов к ним.

Работникам охраны, за которыми не закреплены служебные собаки, не разрешается заходить в зоны свободного окарауливания служебными собаками.

30. Все имеющиеся на тропе наряда лестницы и переходные мостики через канавы, овраги и водные рубежи во избежания скольжения, особен-

но в зимнее время, должны очищаться от снега, льда и периодически посыпаться песком или шлаком. Мостики и лестницы оборудуются перилами.

31. При проходе по территории строительного объекта работники охраны не должны находиться под поднимаемым грузом или лесами, на которых производятся работы.

Запрещается находиться под проводами высокого и низкого напряжения, прикасаться к опорам, на которых они подвешены, а также к любым оборванным проводам этих линий, линий электросети и сигнализации на земле или же на охраняемых сооружениях.

32. При несении службы непосредственно в цехах, мастерских и других производственных помещениях (зданиях) необходимо строго соблюдать установленные на них по условиям и характеру производства меры по технике безопасности, промышленной санитарии и противопожарных правил. Службу нести на установленных местах.

Нарядам охраны обеспечивающих охрану периметра, внутренних территорий предприятия на которых расположены производственные здания (сооружения, помещения, цеха и т.п.) запрещается в них заходить, ходить между машинами и другим производственным оборудованием, если это не связано с выполнением служебных обязанностей.

33. В ненастную погоду и зимнее время года работникам охраны на обходных постах разрешается, через определенные промежутки времени, пользоваться местами обогрева и укрытия, порядок пользования которыми устанавливается руководителями подразделений охраны.

34. На автотранспортных и железнодорожных КПП оборудование мест несения службы охранниками, а также порядок проверки документов и досмотра транспорта должны полностью исключать несчастные случаи. У проездных ворот должен быть определен безопасный порядок досмотра транспортных средств и место нахождения работников охраны при движении транспорта (уголок безопасности). Все КПП должны оборудоваться шлагбаумами (автоматическим, полуавтоматическим, ручным). Допускается дополнительная установка натяжного троса.

Досмотр автомобилей, локомотивов, железнодорожных вагонов и платформ должен проводиться только на досмотровых площадках, оборудованных для этого устройствами.

В качестве устройств для досмотра железнодорожного транспорта используются вышки, ямы, досмотровые колодцы, а для автомобилей – эстакады, мостики, в исключительных случаях досмотр допускается с помощью лестниц с крюками на концах.

Площадки эстакад должны быть не ниже бортов грузовых автомобилей, иметь площадь не менее 1 квадратного метра, со ступеньками и перилами для безопасного подъема и спуска работников охраны.

35. На досмотровых площадках для автотранспорта не допускается большое скопление машин и объезд досматриваемых автомобилей без разрешения наряда охраны.

Перед началом досмотра автомобиль должен быть поставлен на тормоз, а двигатель заглушен. Водитель обязан выйти из кабины и находиться возле машины.

Очередная машина должна быть заторможена и находится не ближе 5 метров от досматриваемой.

В зимнее время досмотровые площадки, лестницы и площадки эстакад (вышек) должны своевременно очищаться от снега, льда и посыпаться песком или шлаком. Проезжая часть автодороги до 5 м в обе стороны от ворот также должны быть посыпаны песком или шлаком.

36. Перед пропуском транспорта с территории объекта, работник охраны обязан остановить его за 1 – 2 м от ворот, открыть проездные ворота, закрепить их специальными крюками или фиксаторами и встать в строго определенное безопасное место на расстоянии 1,5 – 2 м от линии его движения.

37. При управлении механизированными воротами необходимо:

- убедиться в отсутствии людей, транспорта и посторонних предметов в зоне движения створок ворот. Открытие и закрытие производить только нажатием соответствующих кнопок на пульте до отключения привода и остановки створок в крайних положениях;

- при возникновении шума, вибрации створок ворот и механизмов прекратить работу и сообщить о неисправности непосредственному начальнику и администрации охраняемого объекта;

- в случае появления на линии движения ворот людей или транспорта, ворота должны быть немедленно остановлены.

- по окончании работы створки установить в положение “закрыто”.

38. Створки немеханизированных ворот в открытом состоянии должны быть зафиксированы стопорным устройством. Особую осторожность необходимо соблюдать при открытии ворот во время сильных порывов ветра.

39. Контрольно-проездные пункты должны иметь знаки безопасности в соответствии с требованиями Правил дорожного движения Украины, утвержденных постановлением КМ Украины от 10 октября 2001 г. N 1306.

40. Работникам охраны ЗАПРЕЩАЕТСЯ:

- находиться в створе ворот при закрытых и открытых воротах;

- открывать ворота до неполной остановки транспорта;

- производить досмотр автомобиля (локомотива) без водителя (машиниста);

- во время досмотра железнодорожного транспорта подлезать под вагоны, находиться между вагонами или на железнодорожном пути вблизи локомотива или заднего вагона. Залазить на крышу вагона, локомотива либо другим способом приближаться к контактной сети;

- вскрывать для досмотра высоковольтную камеру тепловоза, производить досмотр шахты холодильника при включенном вентиляторе;

- выходить на полотно железной дороги или проезжую часть во время движения локомотива или автомобиля;

- проезжать на подножках автомобиля, локомотива, садиться и выходить на ходу;

- оставлять ворота открытыми после пропуска транспорта.

41. При работе со служебными собаками:

- расстановку служебных собак на блок-постах производят специальные работники, введенные в штат охраны объекта (вожатые служебных собак, охранники-кинологи). О наличии собаки на посту информируется работник охраны, на участке которого она выставлена;

- в пути следования на посты и с постов служебные собаки обязательно должны быть в намордниках. Перед выставлением служебной собаки на блок-пост вожатый (охранник-кинолог) обязан проверить техническую

исправность поста, прочность привязных цепей, исправность карабинов, колец, роликов и, убедившись в исправности оборудования поста, прикрепить цепь к шейнику, снять с собаки намордник и поводок. В случае обнаружения технических неисправностей в оборудовании поста до полного их устранения выставление служебных собак не производится;

- при выполнении работ в зоне свободного карауливания служебными собаками, вожатый (охранник – кинолог) должен надежно закрыть калитку в ограждении зоны на крючок, а при оставлении зоны – на замок;

- объекты, на которых используются служебные собаки, должны иметь по периметру предупреждающие таблички “Объект охраняется со служебными собаками”;

- при приготовлении пищи служебным собакам должны соблюдаться меры предосторожности при работе с огнем, паром, газом, электричеством.

42. При эксплуатации технических средств охраны (ТСО) и электроприборов.

42.1. Эксплуатация ТСО и электроприборов применяемых в подразделениях охраны, должна осуществляться в строгом соответствии с требованиями основных нормативных документов по правилам и мерам безопасности (ПУЭ, ПТЭ и ПТБ), инструкций заводов-изготовителей по монтажу и эксплуатации средств охранной связи, сигнализации и электроприборов, а также местных инструкций.

Соблюдение правил и мер безопасности обязательно во всех случаях. Условия работ, срочность их выполнения и другие причины не могут служить основанием для нарушения правил и мер безопасности.

42.2. К эксплуатации ТСО допускаются лица, имеющие необходимую теоретическую подготовку, твердые знания материальной части, практические навыки в использовании и обслуживании этих средств, прошедшие вводный, первичный инструктажи, обучение безопасному ведению работ, а также проверку знаний по правилам и мерам безопасности.

42.3. Ответственный за электрохозяйство охраняемого объекта обязан обеспечить инструктаж личного состава, эксплуатирующего технические средства охраны и электроприборы в соответствии с действующими на объекте инструкциями.

42.4. Осмотр, периодическая чистка и ремонт приводных механизмов ворот и шлагбаумов, защитных устройств и ограждений, кабельных линий, а также коммутатора охранной связи и сигнализации должны проводиться электротехническим персоналом в сроки, регламентируемые местными инструкциями, с учетом состояния механизмов, электрооборудования и сетей; среды, нагрузки и условий эксплуатации, но не реже:

- осмотра и периодической чистки – одного раза в неделю;

- ремонта – в соответствии с графиком, утвержденным главным инженером предприятия.

42.5. Исправность ТСО и электроприборов, находящиеся в эксплуатации, должна проверяться ежедневно перед заступлением смены охраны на дежурство и после каждого применения их в работе. Пользоваться средствами защиты, срок годности которых истек – запрещается.

Результаты проверок должны быть записаны в постовой ведомости и в журнале учета работы охранной сигнализации.

42.6. Неисправности и повреждения, при которых запрещена эксплуатация сигнализаторов, датчиков охранной сигнализации и электроприборов:

- наличие открытых токонесущих частей;
- нарушение целостности изоляции;
- слабое крепление отдельных частей прибора, сигнализатора, датчика или их деформация.

При обнаружении указанных или каких-либо других неисправностей работа сигнализаторов, датчиков и электроприборов должна быть немедленно прекращена. Возобновление работы возможно только после устранения неисправности.

42.7. При обнаружении неисправности электромеханических и полуавтоматических ворот, шлагбаумов либо их приводных механизмов, – эксплуатацию их прекратить и доложить начальнику смены (вахты) охраны.

42.8. Каждый работник охраны, заметивший неисправность или неправильные действия личного состава, ведущие к нарушению правил и мер безопасности, обязан немедленно доложить своему начальнику и принять меры по устранению нарушения.

42.9. Работникам охраны ЗАПРЕЩАЕТСЯ:

- вести работу на неисправном оборудовании ТСО;
- класть какие-либо предметы или материалы на оборудование и коммуникации и линейную часть охранной сигнализации;
- допускать к эксплуатации ТСО лиц, не прошедших вводного и первичного инструктажей, обучения безопасному ведению работ и проверки знаний по правилам и мерам безопасности.

43. На взрывоопасных объектах (в том числе складах взрывчатых, горючего и смазочных материалов) не допускается курение, разведение огня, пользование керосиновыми лампами и свечами. Работники охраны обязаны следить, чтобы складам и прилегающей к ним территории не угрожала опасность от огня. Они должны знать правила пользования противопожарным инвентарем, средствами связи. На этих постах должны быть установлены таблички с номерами телефонов пожарной охраны, а в инструкциях указан порядок обесточивания объекта.

44. При пользовании печами и электронагревательными приборами, установленными по согласованию с органами госпожнадзора, на контрольно-пропускных пунктах и в местах обогрева работников охраны необходимо соблюдать следующие правила:

- электронагревательные приборы должны быть с закрытой спиралью заводского изготовления и установлены на несгораемые подставки на безопасном расстоянии от стен и других элементов строительных конструкций. В процессе эксплуатации электросети и электроприборов запрещается подвешивать электропроводку на гвоздях и заклеивать ее обоями, применять электропровода с поврежденной изоляцией, некалиброванные (самодельные) предохранители, обертывать электрические лампы бумагой или материей, использовать электропровода и ролики для подвешивания картин, наглядной агитации, одежды и других предметов.

Печное отопление перед началом отопительного сезона должно быть проверено и отремонтировано. У каждой печи на деревянном полу должен быть прибит предпочный металлический лист размером не менее 50 х 70 см. На постах с печным отоплением должна быть инструкция по пользованию печами и плакат “Бойся угарного газа”.

При эксплуатации печного отопления ЗАПРЕЩАЕТСЯ:

- растапливать печи с помощью бензина, керосина, дизельного топлива и других ЛВЖ (легко-воспламеняющихся жидкостей);
- оставлять топящиеся печи без присмотра;
- сушить и складировать на печах дрова, одежду и другие легковоспламеняющиеся предметы и материалы;
- топить углем, коксом печи, не приспособленные для этой цели;
- применять дрова, длина которых превышает размеры топки.

Перед растопкой печи нагоревшую золу, шлак, уголь необходимо удалить в специально отведенное место, исключив возможность загорания.

45. Работникам охраны при несении службы по охране объектов ЗАПРЕЩАЕТСЯ:

- выполнять работы, не предусмотренные Инструкцией по организации охраны объекта и договором на охрану объекта;
- допускать на пост проверяющих лиц в нерабочее время охраняемого объекта без предъявления пароля, предписания на проверку;
- допускать на рабочее место лиц, не имеющих отношения к выполняемой работе;
- оставлять пост, маршрут, за исключением случаев оказания помощи пострадавшим при аварийных ситуациях, предотвращения правонарушений и задержания преступников;
- ходить по железнодорожным путям, пересекать их под стоящими вагонами;
- передавать лицам спецсредства слезоточивого действия посторонним лицам, оставлять их без присмотра, направлять без надобности их действие в сторону людей, в открытые окна жилых помещений и строений, в которых находятся люди;
- пользоваться электронагревательными приборами кустарного изготовления, самостоятельно ремонтировать электроприборы, оставлять их включенными без присмотра;
- прикасаться к оборванным электропроводам, становиться на них;
- курить в не установленных местах, допускать разведение костров, сжигание тары и производственных отходов вблизи охраняемых объектов;
- использовать для досмотра транспорта приставные лестницы без крючьев, другие подсобные предметы, осматривать его с подножек или колес;
- проверять пропуска на право выезда (въезда) во время движения транспорта;
- допускать к управлению воротами с автоматическим приводом посторонних лиц;
- находиться в зоне производства погрузочно-разгрузочных работ.

46. Работнику охраны запрещается заходить в общественные места, если это не предусмотрено должностными обязанностями, или следовать общественным транспортом к месту несения службы, а также выходить за пределы территории охраняемого объекта, кроме случаев, когда это вызвано служебной необходимостью, спать, отклоняться от установленного маршрута движения на пост или с поста.

47. Специальные средства должны использоваться работниками охраны в строгом соответствии с особенностями применения каждого их вида.

48. В случае заболевания во время несения службы работник охраны должен сообщить об этом непосредственному начальнику, который должен принять меры к вызову врача или доставке пострадавшего в лечебное учреждение и его замене.

V. Требования безопасности при чрезвычайных обстоятельствах

49. Работник охраны должен немедленно доложить в пожарную охрану, подразделение охраны, орган внутренних дел, администрацию охраняемого объекта о пожарах и загораниях, стихийных бедствиях и других чрезвычайных обстоятельствах, возникших на объекте и в районе поста, и, соблюдая меры личной безопасности, организовать мероприятия по устранению опасности, оказав необходимую доврачебную помощь пострадавшим, предварительно вызвав “скорую помощь” или медицинского работника охраняемого объекта.

50. При обнаружении граждан с признаками отсутствия дыхания (поток воздуха возле рта и носа не определяется, отсутствуют на глаз видимые дыхательные экскурсии грудной клетки) и остановки сердца (отсутствие пульса на артериях шеи, зрачки расширены и не реагируют на свет, потеря сознания) осуществить вызов врачей из ближайшего медицинского учреждения либо по телефону “03”.

Одновременно с этим в предельно быстрой и четкой последовательности осуществлять следующие мероприятия по оживлению пострадавшего:

- уложить пострадавшего на твердую поверхность и нанести удар ребром ладони, сжатой в кулак по груди с высоты 25 – 30 см резко, с отскоком выше мечевидного отростка. Сразу после удара проверить наличие пульса на сосудах шеи. Если пульса нет, удар по груди можно повторить. Если пульс не появился – начать наружный массаж сердца и искусственную вентиляцию легких;

- под плечи пострадавшего подложить валик или запрокинуть голову назад и начать ИВЛ методом “рот в рот” или “рот в нос”; при вдыхании воздуха “рот в рот” следует нос зажать пальцами, плотно расположив свои губы вокруг губ пострадавшего; при вдыхании “через нос” рот пострадавшего закрывается большим пальцем, нос плотно охватывается губами, но не сжимается, и в легкие вдувается воздух;

- если ИВЛ на этих этапах не удалась, следует выдвинуть вперед нижнюю челюсть пострадавшего либо одной рукой, поместив большой палец в рот, либо двумя руками, захватив подбородок у основания, очистить полости рта и носа от слизи, съемные протезы изо рта удалить;

- после 3 – 5 глубоких раздуваний легких быстро определить наличие пульсации на артериях шеи, если пульсация артерий определяется, следует продолжить раздувание легких с интервалом в 5 секунд (12 дыханий в минуту).

Если у пострадавшего отсутствует пульс, а зрачки расширены, то для поддержания кровообращения необходимо начать наружный массаж сердца в следующем порядке:

- пострадавшего положить на жесткое основание;
- оказывающий помощь, не сгибая рук в локтях, ладонями, положенными одна на другую в области края грудины пострадавшего, производит сильное ритмичное надавливание на грудину в виде энергичного толчка (из расчета 60 – 70 надавливаний в минуту);

- если помощь оказывают двое, то один из них проводит ИВЛ, а второй – наружный массаж сердца. После толчков – пауза, во время которой производится 2 вдоха воздуха;

- если помощь оказывается одним лицом, необходимо попеременно после 5 надавливаний делать 1 – 2 вдоха воздуха.

В момент вдувания воздуха в легкие надавливание на грудину производить нельзя.

При появлении пульса продолжается ИВЛ (до момента восстановления самостоятельного дыхания).

51. Первая помощь при различных травмах и внезапных заболеваниях.

Раны – если рана сильно кровоточит, то сначала надо остановить кровотечение; рану сверху накрыть чистой марлей, перевязать всю рану бинтом (если в распоряжении имеется настойка йода, спирт этиловый – то кожу вокруг раны сначала дважды или трижды протереть марлей или ватой, смоченной этим раствором).

Ушибы – наложить давящую повязку, холод (платок, смоченный холодной водой, снег или лед в целлофановом пакете).

Растяжения и разрывы связок – наложить тугую повязку, холод.

Вывихи – создать конечности максимальный покой. Вправлять вывихи немедицинскому работнику запрещается.

Переломы – при открытых переломах наложить стерильную повязку на рану, наложить шину (например: из доски, фанеры, палок, картона), зафиксировав 2 ближайших сустава. Даже при подозрении на перелом фиксации конечности обязательна.

Ожоги термические – устранить причину, вызвавшую ожог, промыть холодной водой (при ожоге без нарушения целостности ожоговых пузырей), наложить стерильную повязку, при возможности положить снег, лед или иной холод на 15 – 20 минут.

Ожоги химические – обильно промывать холодной водой или молоком, мочой, мыльной водой, слабым раствором пищевой соды вплоть до прибытия врача.

Отморожения – медленное и постепенное согревание (перенос в теплое помещение), наложение повязок, обильное теплое питье (чай, кофе), заставить двигаться.

Электротравмы – соблюдая меры личной безопасности, прекратить действие тока на организм (например: выключить рубильник, вывернуть предохранительные пробки на щите, оттянуть провод сухой деревянной палкой, сухой веревкой или оттащить пострадавшего, используя при этом диэлектрические перчатки или подручные изолирующие средства: сухую веревку, палку, доску, прорезиненный плащ, резиновый коврик), обеспечить полный покой и вызвать врача. В случае отсутствия у пострадавшего

дыхания и пульса необходимо расстегнуть одежду, начать ИВЛ и массаж сердца до восстановления самостоятельного дыхания и сердцебиения. На область ожога наложить сухую повязку.

Обморок – уложить пострадавшего в горизонтальное положение, приподнять ноги, расстегнуть стесняющую одежду, обеспечить доступ свежего воздуха, лицо обрызгать холодной водой, дать понюхать нашатырный спирт или уксус на ватке, натереть этими средствами виски, надавить болевую точку под носом или помассировать ее.

Тепловой (солнечный) удар – перенести пострадавшего в тень, расстегнуть одежду и уложить с приподнятой головой, наложить холодный компресс, напоить холодной водой. Применить холодное обертывание (например, мокрой простыней). При необходимости провести наружный массаж сердца и ИВЛ.

Отравления (пищевые, разными ядами) – удалить вещества, вызвавшие отравление (промывание желудка, обильное питье, вызвать рвоту путем раздражения задней стенки глотки пальцами).

Отравление алкоголем – очистить полость рта от рвотных масс. Удалить остатки алкоголя из желудка (промывание желудка водой до тех пор, пока рвотные массы перестанут пахнуть алкоголем; вызвать рвоту путем раздражения задней стенки глотки пальцами), обильное питье. При нарушении дыхания провести ИВЛ.

Отравление угарным или светильным газом – соблюдая меры личной безопасности и используя средства индивидуальной защиты дыхания (например, смоченный водой носовой платок) прекратить воздействие газа, обеспечить доступ свежего воздуха, холодное обливание головы, вдыхание нашатырного спирта; при потере сознания и нарушении сердечной деятельности провести ИВЛ и наружный массаж сердца.

Укусы (змей, насекомых, бешенных животных) – уложить пострадавшего с приподнятой конечностью, дать обильное питье, срочно доставить в ближайшее лечебное учреждение для принятия специальных мер.

Остановка кровотечений – при венозном кровотечении конечность приподнять, наложить на рану давящую повязку (индивидуальный перевязочный пакет или бинт, вату, марлю).

Остановку артериального кровотечения осуществить (не снимая одежды) либо прижатием пальцем артерии на конечности выше ее повреждения к кости (на шее и голове – ниже раны или в ране), либо наложением кровоостанавливающего жгута (платка, ремня) или давящей повязки выше раны поверх рубашки, брюк. До наложения жгута поврежденную конечность следует держать в приподнятом положении. Под жгут вложить записку о времени его наложения. Время, на которое может быть наложен жгут, не должно превышать 2 часа в летнее время и 1 – 1,5 часа – в зимнее.

Засорение глаз – при засорении глаза его следует немедленно промыть водой или 2%-м раствором борной кислоты. Голову пострадавшего кладут на противоположную засоренному глазу сторону и направляют

струю воды или раствора от наружного угла засоренного глаза к носу, прикрыть глаз стерильной повязкой. Тереть глаз воспрещается.

VI. Требования безопасности по окончании работы

52. Работники охраны по окончании работы должны:

45.1. В установленном порядке осуществить допуск на объект сменяющего работника охраны, ознакомить его со всеми выявленными при несении службы замечаниями и недостатками, могущими повлиять на безопасное несение службы, передать сменяющему работнику охраны рабочее место в чистоте и порядке, доложить непосредственному начальнику.

45.2. При отсутствии надобности погасить огонь в печах, электроприборы отключить.

45.3. Сделать все необходимые записи в соответствующих журналах и книгах.

**Типовой перечень содержимого аптечки
первой доврачебной помощи**

№ п.п.	НАИМЕНОВАНИЕ	Количество
1.	Анальгин 0,5 N 10 Аспирин 0,5 N 10	1 упаковка 1 упаковка
2.	Портативный гипотермический (охлаждающий) пакет-контейнер “Льдинка”	1 штука
3.	Раствор сульфацила натрия	1 флакон
4.	Жгут для остановки артериального кровотечения с дозированной компрессией (сдавливанием) для само- и взаимопомощи	1 штука
5.	Бинт стерильный 10 x 5 Бинт нестерильный 10 x 5 Бинт нестерильный 5 x 5	1 штука 1 штука 1 штука
6.	Атравматическая повязка МАГ с диоксидином или нитратом серебра 8 x 10 см для перевязки грязных ран или Альтекс – Х или салфетка атравматическая антимикробная с фурагином “Колетекс-СФГ” или салфетка атравматическая антимикробная с хлоргексидином “Колетекс-СХГ”	1 штука 1 штука 1 штука 1 штука
7.	Лейкопластырь бактерицидный 2,5 x 7,2 или 2 x 5	8 штук
8.	Салфетки стерильные для остановки капиллярного и венозного кровотечения “Колетекс ГЕМ” с фурагином 6 x 10 (10 x 18) или статин (порошок) 1,0 г	3 штуки 3 упаковки
9.	Раствор йода спиртовой 5% или бриллиантовой зелени 1%	1 флакон
10.	Лейкопластырь 1 x 500 или 2 x 500; 1 x 250 см	1 штука
11.	Бинт эластичный трубчатый медицинский нестерильный N 1, 3, 6	по 1 штуке
12.	Вата	1 упаковка
13.	Нитроглицерин таб. N 40 или капс. N 20 (тринитратлонг)	1 упаковка
15.	Валидол (таблетки или капсулы)	1 упаковка
16.	Устройство для проведения искусственного дыхания “Рот-устройство-рот”	1 штука
17.	Аммиака раствор (нашатырный спирт)	1 флакон
18.	Энтеродез или уголь активированный табл. N 10	2 упаковки 1 упаковка
19.	Корвалол	1 флакон
20.	Ножницы	1 штука

Общая инструкция по пожарной безопасности охраняемого объекта

1. Общие положения. (Для Украины)

1. Обеспечение пожарной безопасности является составной частью производственной или другой деятельности должностных лиц, работников предприятий и предпринимателей. Пожарная безопасность должна обеспечиваться путем проведения организационных, технических и других мероприятий направленных на предупреждение пожаров, обеспечение безопасности людей, снижение возможных имущественных потерь и уменьшение отрицательных экологических последствий в случае их возникновения, создание условий для быстрого вызова пожарных подразделений и успешного тушения пожаров.

2. В соответствии с Законом Украины «О пожарной безопасности», Правилами пожарной безопасности в Украине обеспечение пожарной безопасности предприятий, учреждений и организаций (далее предприятий) возлагается на их руководителей и уполномоченных ими лиц, если иное не предусмотрено соответствующим договором.

3. В соответствии со ст. 5 Закона Украины «О пожарной безопасности» руководители предприятий и уполномоченные ими лица **о б я з а н ы**:

а) разрабатывать комплексные мероприятия по обеспечению пожарной безопасности, внедрять достижения науки и техники, положительный опыт;

б) в соответствии с нормативными актами по пожарной безопасности разрабатывать и утверждать положения, инструкции, прочие нормативные акты, действующие в пределах предприятия и осуществлять постоянный контроль за их соблюдением;

в) обеспечивать соблюдение противопожарных требований стандартов, норм, правил, а также выполнение требований предписаний и постановлений органов государственного пожарного надзора;

г) организовывать обучение работников правилам пожарной безопасности и пропаганду мероприятий по их обеспечению;

д) содержать в исправном состоянии средства пожарной защиты и связи, пожарную технику, оборудование и инвентарь, не допускать их использования не по назначению;

е) в случае необходимости создавать в соответствии с установленным порядком подразделения пожарной охраны и необходимую для их функционирования материально-техническую базу;

ж) представлять по требованию государственной пожарной охраны сведения и документы о состоянии пожарной безопасности объектов и продукции, которая ими производится;

з) осуществлять меры по внедрению автоматических средств выявления и тушения пожаров и использование с этой целью производственной автоматики;

и) своевременно информировать пожарную охрану о неисправностях пожарной техники, систем противопожарной защиты, водоснабжения, а также закрытии дорог и проездов на своей территории;

й) проводить служебные расследования случаев пожаров.

4. В соответствии со ст. 6 Закона Украины «О пожарной безопасности» в обязанности всех граждан входит неукоснительно выполнять установленные правила пожарной безопасности, своевременно сообщать

в пожарную охрану о возникновении пожара и принимать меры по его ликвидации, спасению людей и имущества.

5. Должностные и физические лица, виновные в нарушении Закона Украины «О пожарной безопасности», Правил пожарной безопасности в Украине, несут административную, уголовную или другую ответственность предусмотренную действующим законодательством.

6. На каждом предприятии с учетом его пожарной опасности приказом (инструкцией) должен быть установлен соответствующий противопожарный режим, в соответствии с которым определены:

6.1. возможность (место) курения, применения открытого огня, бытовых нагревательных приборов;

6.2. порядок проведения временных пожароопасных работ (в том числе сварочных);

6.3. правила проезда и стоянки транспортных средств;

6.4. места хранения и допустимое количество сырья, полуфабрикатов и готовой продукции, которые могут находиться в производственных помещениях и на территории (в местах хранения);

6.5. порядок уборки горючей пыли и отходов, хранения промасленной спецодежды и ветоши, очищения воздухопроводов вентиляционных систем от горючих отложений;

6.6. порядок отключения от сети электрооборудования в случае пожара;

6.7. порядок осмотра и запираания помещений после окончания работы;

6.8. порядок прохождения должностными лицами обучения и проверки знаний по вопросам пожарной безопасности, а также проведения с работниками противопожарных инструктажей и занятий по пожарно-техническому минимуму с назначением ответственных за их проведение;

6.9. порядок организации эксплуатации и обслуживания имеющихся в наличии технических средств противопожарной защиты (противопожарного водопровода, насосных станций, установок пожарной сигнализации, автоматического пожаротушения, дымоудаления, огнетушителей и т.п.);

6.10. порядок проведения планово-предупредительных ремонтов и осмотров электроустановок, отопительного, вентиляционного, технологического и прочего инженерного оборудования;

6.11. действия работников предприятия в случае выявления пожара;

6.12. порядок сбора членов добровольной пожарной дружины и ответственных лиц в случае возникновения пожара, вызова ночью, в выходные и праздничные дни.

Все работники предприятия, в том числе и охранный состав должны быть ознакомлены с этими требованиями на инструктажах, а извлечения из них вывешены на видных местах.

7. На каждом промышленном предприятии разрабатывается общеобъектная инструкция о мерах пожарной безопасности и инструкции для всех взрывопожароопасных и пожароопасных помещений: цехов, складов, участков, мастерских, лабораторий и т.п. Эти инструкции должны быть доведены до личного состава охраны обеспечивающие охрану этих объектов.

8. В зданиях и сооружениях, которые имеют два этажа и более, в случае одновременного нахождения на этаже более 25 лиц должны быть разработаны и вывешены на видных местах планы (схемы) эвакуации людей на случай пожара. В случае изменения планировки или функционального назначения зданий (помещений, сооружений), технологии производства, штатного расписания персонала администрация предприятия обязана обеспечить своевременную переработку планов эвакуации и инструкций.

9. На предприятиях должен быть установлен единый порядок (система) оповещения людей о пожаре, с которым необходимо ознакомить всех работающих. В помещениях на видных местах и возле телефонов должны быть вывешены таблички с указанием номеров телефонов для вызова пожарной охраны.

10. С учетом специфики производства администрация предприятия разрабатывает для охранного состава инструкцию, в которой должно быть определено обязанности работников охраны по контролю за соблюдением противопожарного режима, осмотру территории и помещений, порядок действий в случае выявления пожара, срабатывания средств пожарной сигнализации и автоматического пожаротушения, а также указано, кто из должностных лиц администрации должен вызываться в ночное время (выходные и праздничные дни) в случае пожара.

11. Администрацией предприятия охране должны быть предоставлены списки должностных лиц предприятия с указанием их домашнего адреса, служебного и домашнего телефонов. Охранный состав обязан четко знать порядок действий в случае выявления пожара, правила пользования первичными средствами пожаротушения и приемы тушения.

12. Рабочие, служащие, другие работники предприятия обязаны соблюдать установленный противопожарный режим, выполнять все требования правил и других нормативных актов по вопросам пожарной безопасности, действующих на предприятии.

2. Требования к пожарной безопасности объектов. Содержание территории.

12.1. Территория предприятий, участков граничащих с другими зданиями, пожарные разрывы между домами, сооружениями, площадками для хранения материалов, оборудования и т.п. должны постоянно содержаться в чистоте и систематически очищаться от мусора, отходов производства, тары, опавшей листвы, которые необходимо регулярно удалять (вывозить) в специально отведенные места.

На территории предприятия запрещено устраивать свалки горючих отходов. Дороги, проезды и проходы к зданиям, сооружениям, пожарным водоемосточникам, подступы к внешним стационарным пожарным лестницам, пожарному инвентарю, оборудованию и средствам пожаротушения должны быть всегда свободными, содержаться исправными, зимой очищаться от снега. Запрещается произвольно уменьшать нормированную ширину дорог и проездов.

12.2. Ко всем зданиям и сооружениям предприятия должен быть свободный доступ. Противопожарные разрывы между домами, сооружениями, открытыми площадками для хранения материалов, оборудования и т.п. должны соответствовать требованиям строительных норм. Их не разрешается загромождать, использовать для складирования материалов,

оборудования, стоянки транспорта, строительства и установления временных домов и сооружений, в том числе инвентарных бытовых помещений, гаражей и т.п.

12.3. О закрытии участков дорог или проездов для ремонта (или по другим причинам) должна быть уведомлена территориальное подразделение пожарной охраны. На период закрытия дорог в соответствующих местах должны быть установлены указатели направления объезда или устроены переезды через ремонтируемые участки.

12.4. На однополосных проездах должны устраиваться разъездные площадки, а тупиковые проезды должны заканчиваться поворотными площадками, которые обеспечивают возможность разворота пожарных машин. Основные дороги, проезды должны иметь твердое покрытие, а подъездные пути к зданиям, сооружениям и пожарным водоемам в обязательном порядке укрепляются гравием или шлаком для обеспечения возможности подъезда в любое время года. Рельсовые пути, временные траншеи и канавы не должны усложнять движение пожарных автомобилей. Для этого в необходимых местах оборудуются удобные переезды, которые всегда должны быть свободными для проезда пожарных машин. Проходы и переезды через железнодорожные пути должны иметь сплошные настилы на уровне головок рельсов. Стоянка вагонов без локомотивов на переездах запрещена.

Ворота въезда на территорию предприятия, которые открываются при помощи электропривода, должны иметь приспособления (устройства), позволяющие открывать их вручную. На запасных (пожарных) воротах закрытые на замок должны быть установлены таблички с указанием на них места нахождения ключей.

12.5. На участках территории предприятий, где возможны скопления горючих газов или паров, проезд автомашин и другого автотранспорта не разрешается. Об этом должны быть вывешены соответствующие надписи (указатели).

12.6. Территория предприятий и других объектов должны иметь внешнее освещение, которое обеспечивает быстрое нахождение пожарных лестниц, противопожарного оборудования, входов в дома и сооружения. Временные сооружения, киоски, ларьки, бытовые вагончики и т.п. должны размещаться на расстоянии не менее 10 м от других зданий и сооружений.

12.7. На территории предприятия на видных местах должны быть установлены таблички с указанием порядка вызова пожарной охраны, знаки мест размещения первичных средств пожаротушения, схема движения автотранспорта, в которой следует указывать размещение зданий, водоемов, гидрантов, пирсов и градирен. Стоянка транспорта в сквозных проездах зданий, на расстоянии менее 10 м от въездных ворот на территорию объектов, менее 5 м от пожарных гидрантов, заборных устройств водоемочников, пожарного оборудования и инвентаря, на поворотных площадках тупиковых проездов запрещается. В указанных местах должны устанавливаться соответствующие запрещающие знаки.

12.8. Разводить костер, сжигать отходы, тару, выбрасывать неза тушенный уголь и пепел на расстоянии менее 15 м от зданий и сооружений, а также в пределах установленных строительными нормами противопожарных разрывов не разрешается.

12.9. Запрещается курение:

- на территории и в помещениях объектов по добыче, переработке и хранению ЛВЖ, ГЖ и горючих газов, производству всех видов взрывчатых веществ;

- в зданиях с наличием взрывоопасных помещений (участков), торговых предприятий, складов и баз;

- на хлебных злаковых массивах и зерноприемочных пунктах.

На территории объектов, где курение разрешается, администрация обязана определить и оборудовать специальные места для этого, обозначить их знаком или надписью, установить урну или пепельницу из негорючего материала.

13. Содержание зданий, помещений и сооружений.

13.1. Все здания, помещения и сооружения должны своевременно очищаться от горючего мусора, отходов производства и постоянно содержаться в чистоте. Сроки очистки устанавливаются технологическими регламентами или инструкциями. В случае перепланировки помещений, изменения их функционального назначения, применение нового технологического оборудования необходимо соблюдать противопожарные требования действующих нормативных документов строительного и технологического проектирования.

13.2. Противопожарные системы, установки, оборудование помещений, зданий и сооружений (противодымная защита, пожарная автоматика, противопожарное водоснабжение, противопожарные двери, клапаны, прочие защитные устройства в противопожарных стенах и перекрытиях и т.п.) должны постоянно содержаться в исправном состоянии. Не допускается устанавливать любые устройства, которые препятствуют нормальному функционированию противопожарных и противодымных дверей, а также загромождать запасные выходы.

Взрывоопасные помещения в многоэтажных зданиях должны размещаться возле внешних стен верхних этажей.

13.3. В подвальных и цокольных этажах не допускается:

- размещение взрывоопасных производств, хранение и применение ЛЖВ, ГЖ, взрывчатых веществ, баллонов с газами, целлулоида, карбида кальция и других веществ и материалов, имеющих повышенную взрывопожарную опасность (за исключением случаев, обусловленных действующими нормативными документами);

- устройство складов горючих материалов, мастерских, где используются горючие материалы, а также других хозяйственных помещений, если вход в них не изолирован от общих эвакуационных лестничных клеток;

13.4. Не разрешается использовать чердаки, технические этажи и помещения (в т.ч. венткамеры, электрощитовые) под производственные участки, для хранения продукции, устройств, мебели и других предметов. Двери чердаков, технических этажей, венткамер, электрощитовых, подвалов должны содержаться запертыми. На дверях следует указывать место хранения ключей. Окна чердаков, технических этажей, подвалов должны быть застекленными. Пряжки оконных проемов подвальных и цокольных этажей нужно регулярно очищать от горючих отходов производства, сухой листвы, травы и т.п. Не допускается закрывать их наглухо, а также загромождать или закладывать оконные проемы;

Стационарные внешние пожарные лестницы, лестницы на перепадах высот и ограды на крышах (покрытия) зданий и сооружений должны содержаться постоянно исправными, быть окрашенными;

13.5. В случае необходимости установления на окна помещений, где находятся люди, решеток, последние должны раскрываться, раздвигаться или сниматься. Во время нахождения в этих помещениях людей решетки должны быть открыты (сняты). Устанавливать глухие (несъемные) решетки разрешается в кассах, складах, кладовых, комнатах для хранения оружия и боеприпасов и в других случаях, предусмотренных нормами и правилами, утвержденными в установленном порядке.

13.6. В зданиях, помещениях, сооружениях запрещается:

- убирать помещения и стирать одежду с применением бензина, керосина и других ЛВЖ и ГЖ, а также отогревать замерзшие трубы паяльными лампами и прочими средствами с применением открытого огня;

- разбрасывать и оставлять неубранными промасленные обтирочные материалы. Их необходимо убирать в металлические ящики, плотно закрывать крышками и после окончания работы удалять из помещения в специально отведенные за пределами зданий места, обеспеченные негорючими сборниками с плотно закрывающимися крышками.

13.7. Спецодежда работающих с лаками, красками и прочими ЛВЖ и ГЖ должна своевременно подлежать стирке и ремонту, храниться в развешенном виде в металлических шкафах, установленных в специально отведенных для этой цели помещениях. Администрация предприятия должна устанавливать четкий порядок замены промасленной одежды на чистую.

13.8. При организации и проведении мероприятий с массовым нахождением людей следует соблюдать следующие требования:

- при количестве людей свыше 50 лиц использовать помещения, обеспеченные не менее чем двумя эвакуационными выходами, соответствующие требованиям строительных норм, не имеющими на окна глухих решеток и расположенными не выше второго этажа в зданиях с горючими перекрытиями;

- лица, которым поручено проведение таких мероприятий, перед их началом обязаны тщательно осмотреть помещения и убедиться в полной готовности последних в противопожарном отношении, в т.ч. обеспеченности необходимым количеством первичных средств пожаротушения, исправности средств связи, пожарной автоматики и сигнализации;

- должно быть организовано дежурство членов добровольной пожарной дружины или охраны;

- не разрешается заполнение помещений людьми свыше установленной нормы, уменьшение ширины проходов между рядами, установку в проходах дополнительных кресел, стульев и т.п., полное отключение света, использование для эффектов открытого огня, а также курение.

13.9. Предприятия, учреждения, организации и прочие объекты должны быть обеспечены адресными указателями (название улицы, номер дома), установленными на фасадах зданий или других видных местах и освещенными в темное время суток.

15. Содержание эвакуационных путей и выходов.

13.10. Эвакуационные пути выходы должны содержаться свободными, ничем не загромождаться и в случае возникновения пожара обеспечивать безопасность во время эвакуации всех людей, которые находятся в помещении зданий и сооружений. Количество и размеры эвакуационных выходов из зданий и помещений, их конструктивные и планировочные решения, условия освещенности, обеспечения незадымленности, протяжен-

ность путей эвакуации, их облицовка (отделка) должны соответствовать противопожарным требованиям строительных норм.

13.11. В случае размещения технологического, экспозиционного и другого оборудования в помещениях должны быть обеспечены эвакуационные проходы к лестничным клеткам и другим путям эвакуации в соответствии со строительными нормами.

13.12. В помещении, которое имеет один эвакуационный выход, разрешается одновременно размещать (разрешается нахождение) не более 50 человек.

13.13. Двери на путях эвакуации должны открываться по направлению выхода из зданий (помещений). Допускается устройство дверей с открытием во внутрь помещения в случае одновременного нахождения в нем не более 15 человек, а также в санузлах, с балконов, лоджий, площадок внешних эвакуационных лестниц (за исключением дверей, ведущих в воздушную зону незадымляемой лестничной клетки). При наличии людей в помещении двери эвакуационных выходов могут закрываться лишь на внутренние запоры, которые легко открываются.

13.14. Ковры, ковровые дорожки и другие покрытия пола в помещениях с массовым нахождением людей должны надежно крепиться к полу и быть малоопасными относительно токсичности продуктов горения, а также иметь умеренную дымосоздающую способность. Лестничные марши и площадки должны иметь исправные ограждения с перилами, которые не должны уменьшать установленную строительными нормами ширину лестничных маршей и площадок.

13.15. В лестничных клетках (за исключением незадымляемых) разрешается устанавливать приборы отопления на высоте 2,2м от поверхности ступенек и лестничных площадок, этажные электрощиты и пожарные краны при условии, что это оборудование не уменьшает нормативной ширины прохода по лестничным маршам и площадкам. В незадымляемых лестничных клетках допускается устанавливать лишь приборы отопления.

13.16. Лестничные клетки, внутренние открытые и внешние лестницы, коридоры, проходы и прочие пути эвакуации должны быть обеспечены эвакуационным освещением в соответствии с требованиями строительных норм и правилами устройства электроустановок. Светильники эвакуационного освещения должны включаться с наступлением сумерек в случае нахождения в здании людей. Пути эвакуации, которые не имеют естественного освещения, должны постоянно освещаться электрическим светом (в случае наличия людей).

13.17. Не допускается:

- устраивать на путях эвакуации пороги, выступы, турникеты, раздвижные, подъемные, вращающиеся двери и прочие устройства, которые препятствуют свободной эвакуации людей;
- загромождать пути эвакуации мебелью, оборудованием, различными материалами и готовой продукцией, даже если они не уменьшают нормативной ширины;
- забивать, заваривать, запирать на навесные замки, болтовые соединения и прочие запоры, которые тяжело открываются изнутри, внешние эвакуационные двери зданий;
- применять на путях эвакуации горючие материалы для облицовки стен и потолков, а также лестниц и лестничных площадок;

- располагать в тамбурах выходов гардеробы, вешалки для одежды, сушилки; приспособлять их для торговли, а также для хранения, в том числе временного, любого инвентаря и материала;

- загромождать мебелью, оборудованием и другими предметами двери, люки на балконах и лоджиях, переходы в смежные секции и выходы на внешние эвакуационные лестницы;

- снимать установленные эвакуационные лестницы;

- устраивать на лестничных клетках помещения любого назначения, в т.ч. киоски, ларьки; прокладывать промышленные газопроводы, трубопроводы с ЛВЖ и ГЖ, воздухопроводы;

- устанавливать телекамеры в проходах таким образом, чтобы они препятствовали эвакуации людей;

- застеклять и закладывать жалюзи и отверстия воздушных зон в незадымляемых лестничных клетках;

- снимать предусмотренные проектом двери вестибюлей, холлов, тамбуров и лестничных клеток;

- заменять армированное стекло на обычное в дверях и фрамугах вопреки предусмотренному проекту; развешивать на стенах лестничных клеток, маршах стенды, панно и др.

- уменьшать нормативную площадь фрамуг во внешних стенах лестничных клеток или закладывать их.

14. Требование к оснащению объектов первичными средствами пожаротушения.

14.1. Пожароопасные объекты должны быть оснащены первичными средствами пожаротушения, к которым относятся: огнетушители, пожарный инвентарь (покрывала из негорючего теплоизоляционного холста, грубошерстной ткани или войлока, ящики с песком, бочки с водой, пожарные ведра, совковые лопаты) и пожарный инструмент (багры, ломы, топоры и т.п.).

14.2. Для определения видов и количества первичных средств пожаротушения необходимо учитывать физико-химические и пожароопасные свойства горючих веществ, их взаимодействие с огнетушащими веществами, а также размеры площадей производственных помещений, открытых площадок и установок. Необходимое количество первичных средств пожаротушения определяют отдельно для каждого этажа здания, помещения. Если в одном помещении находятся несколько разных по пожарной опасности производств, не отделенных одно от другого противопожарными стенами, все эти помещения обеспечивают огнетушителями, пожарным инвентарем и прочими видами средств пожаротушения по нормам самого опасного производства.

Покрывала должны иметь размер не менее 1 м х 1 м и предназначены для тушения небольших очагов пожаров в случае воспламенения веществ, горения которых не может происходить без доступа воздуха. В местах применения и хранения ЛВЖ и ГЖ размеры покрывал могут быть увеличены до величин 2 м х 2 м.

Бочки с водой устанавливаются в производственных, складских и других помещениях, сооружениях в случае отсутствия внутреннего противопожарного водопровода и при наличии горючих материалов, а также на территории пожароопасных объектов. Их количество в помещениях определяется из расчета установки одной бочки на 250-300 м² защищаемой

площади. Бочки должны иметь вместимость не менее $0,2\text{ м}^3$, и быть укомплектованы пожарным ведром вместимостью не менее $0,008\text{ м}^3$.

Пожарные щиты (стенды) устанавливаются на территории объекта из расчета один щит (стенд) на площадь 5000 м^2 . В комплект средств пожаротушения, которые размещаются на нем, должны входить: огнетушители – 3 шт., ящик с песком – 1 шт., покрывало из негорючего теплоизоляционного материала или войлока размером $2\text{ м} \times 2\text{ м}$ – 1 шт., крюки – 3 шт., багры – 2 шт., ломы – 2 шт., топоры – 2 шт., пожарное ведро – 2 шт. Ящик с песком должен иметь вместимость $3,0\text{ м}^3$ и быть укомплектован совковой лопатой. Конструкция ящика должна обеспечивать удобство доставания песка и исключать попадания осадков.

Все первичные средства пожаротушения (за исключением покрывала) и пожарные щиты должны быть выкрашены в красный цвет.

14.3. Склады леса, тары и волокнистых материалов должны быть обеспечены увеличенным количеством пожарных щитов с набором первичных средств пожаротушения, исходя из местных условий. Здания и сооружения, должны быть обеспечены первичными средствами пожаротушения из расчета:

- на 200 м^2 площади пола – один огнетушитель, бочка с водой, ящик с песком;
- на каждые 20 м длины лесов – один огнетушитель, а на каждые 100 м длины лесов – бочка с водой;
- на 200 м^2 площади покрытия с горючим утеплителем или горючими кровлями – один огнетушитель, бочка с водой и ящик с песком;
- в месте установки теплогенераторов, calorиферов – два огнетушителя и ящик с песком на каждый агрегат.

14.4. Выбор типа огнетушителя определяется в зависимости от их огнетушащей способности, класса пожара горючих веществ и материалов в защищаемом помещении или на объекте. Пожары делятся на 5 классов:

- **класс А** – пожары твердых веществ, преимущественно органического происхождения, горение которых сопровождается тлением (древесина, текстиль, бумага);
- **класс В** – пожары горючих жидкостей или твердых плавящихся веществ;
- **класс С** – пожары газов;
- **класс Д** – пожары металлов и их сплавов;
- **класс Е** – пожары, связанные с горением электроустановок.

С учетом указанных классов пожаров огнетушители бывают следующих видов: пенные и водные огнетушители вместимостью 10 л. , порошковые огнетушители вместимостью $2, 5, 10\text{ л.}$; хладоновые огнетушители вместимостью $2, 3\text{ л.}$ и углекислотные вместимостью $2, 3, 5, 8\text{ л.}$

14.5. В местах сосредоточения ценной аппаратуры или оборудования оснащение средствами пожаротушения должно быть увеличено. Когда от пожара защищаются помещения с ЭВМ, телефонных станций, архивов и т.п. следует учитывать специфику огнетушащих веществ в огнетушителях, которые приводят во время тушения к порче оборудования. Эти помещения следует оснащать углекислотными огнетушителями с учетом предельно допустимой концентрации огнетушащего вещества.

14.6. Расстояние от возможного очага пожара до места размещения огнетушителя не должно превышать 20 м для общественных зданий и

сооружений; 30м для помещений категорий А,В,С и 40м для помещений категорий Д,Е.

14.7. Работники, которые выполняют временные огневые работы, должны иметь наряд-допуск на их выполнение по форме утвержденной Правилами пожарной безопасности в Украине. Наряд-допуск выдается руководителем структурного подразделения и согласовывается со специалистом по пожарной безопасности предприятия либо со службой охраны труда.

15. Организация профилактических мероприятий по пожарной безопасности обеспечивается точным выполнением всеми должностными лицами предприятий вышеизложенных Правил и проведением с работниками предприятия, охраной противопожарных инструктажей. Противопожарные инструктажи делятся на: вступительный, первичный, повторный, внеплановый и целевой. Давайте вместе рассмотрим эти противопожарные инструктажи:

15.1. **Вступительный противопожарный инструктаж** проводит специалист по пожарной безопасности предприятия со всем охранным составом, которые впервые заступили на охрану объекта. В ходе инструктажа они должны быть ознакомлены с:

- наличием опасных в производственном отношении производств (участков, работ) и их общей характеристикой;
- действующими на объекте правилами, инструкциями, приказами, положениями по вопросам пожарной безопасности, общими требованиями относительно соблюдения противопожарного режима;
- порядком курения, применение открытого огня, проведения огневых и других пожароопасных работ;
- возможными причинами пожаров и мерами предосторожности относительно их;
- ответственностью за нарушение правил пожарной безопасности;
- местом нахождения объектной пожарной охраны, а в случае ее отсутствия – ближайшей пожарной части;
- существующим на предприятии порядком (системой) оповещения людей о пожаре;
- действиями в случае возникновения пожара (порядком вызова пожарной помощи, эвакуации людей, материальных ценностей и т.п.);
- правилами использования первичных средств пожаротушения

15.2. **Первичный и повторный противопожарный инструктаж** проводится на постах, во время проведения которого необходимо охранников ознакомить с:

- краткой характеристикой пожарной опасности объектов находящихся в пределах границ поста, возможными причинами возникновения пожаров и мерами предосторожности, а также действиями относительно их;
- правилами (инструкциями) пожарной безопасности установленными для персонала цехов, участков, складов или иных сооружений, указав места курения, если оно не запрещается;
- средствами связи и местом нахождения ближайшего телефона;
- правилами содержания путей эвакуации людей и имущества;
- местами размещения и назначением существующих установок пожарной сигнализации и автоматического пожаротушения;
- местом нахождения первичных средств пожаротушения и правилами их использования;

– действиями в случае возникновения пожара: порядком вызова пожарной охраны, оповещения людей и должностных лиц предприятия, проведения эвакуации и т.п.

15.3. Инструктаж личного состава охраны производится под роспись в журнале регистрации инструктажей по вопросам пожарной безопасности. Инструктажи проводятся лицами, которые прошли обучение и проверку знаний по вопросам пожарной безопасности. Первичный и повторный инструктаж проводится с охранником до начала его производственной деятельности на посту (рабочем месте). Повторный инструктаж проводится не менее одного раза в год по перечню вопросов, с которыми необходимо ознакомить охранный состав во время проведения вступительного и первичного противопожарных инструктажей.

15.4. **Внеплановый противопожарный инструктаж** проводится:

- в случаях введения в действие новых или доработанных нормативных актов по вопросам пожарной безопасности;
- в случае изменения технологического процесса, применения нового или замены либо модернизации существующего пожароопасного оснащения;
- по требованию государственных инспекторов по пожарному надзору, если выявлено неудовлетворительное знание охранным составом правил пожарной безопасности, неумении действовать в случае пожара и пользоваться первичными средствами пожаротушения. Внеплановый инструктаж проводится как индивидуально, так и в группе.

15.5. **Целевой противопожарный инструктаж** проводится с охранником непосредственно перед заступлением на пост, при ликвидации аварии или стихийного бедствия.

3. Действия личного состава охраны при пожаре.

16. В случае выявления пожара (обнаружения признаков горения: задымление, запах гари, повышенная температура и т.п.) **охранник обязан:**

16.1. **Немедленно** сообщить об этом по телефону начальнику смены (пожарную охрану). При этом назвать: объект (наименования цеха, участка, склада и т.п.) и место возникновения пожара (возгорания); время обнаружения и признаки (задымленность, блики пламени и т.п.); предполагаемая площадь горения и возможность собственными силами локализовать пожар; наличие людей в очаге возгорания и характеристика находящихся в нем материальных ценностей.

В случае если охранник сообщает в пожарную охрану, то он обязан назвать адрес объекта, указать количество этажей здания, место возникновения пожара, примерную площадь горения и обстановку на пожаре, наличие людей, а также сообщить свою фамилию.

16.2. Принять (по возможности) меры по эвакуации людей, тушению (локализации) пожара и сохранению материальных ценностей. Уметь применять первичные средства пожаротушения.

16.3. По прибытию пожарной охраны оказывать им содействие в тушении пожара, спасении людей и материальных ценностей. Точно выполнять все указания старшего пожарной охраны.

17. При поступлении сообщения от охранника поста **начальник смены (вахты) охраны обязан:**

17.1. **Немедленно** сообщить об этом по телефону в пожарную охрану. При этом назвать: адрес объекта, указать количество этажей здания, место возникновения пожара, примерную площадь горения и обстановку на пожаре, наличие людей, а также сообщить свою фамилию. Если на предприятии предусмотрен диспетчер, то сообщить ему о случившемся. В дальнейшем выполнять все его указания.

17.2. **Вызвать** ответственных лиц объекта, на котором произошло возгорание, и сообщить руководству предприятия.

17.3. Принять (по возможности) меры по эвакуации людей, тушению (локализации) пожара и сохранению материальных ценностей при этом не ослаблять внимание за охраной объекта.

17.4. При наличии в очаге горения людей **безотлагательно** вызвать медицинскую скорую помощь и организовать оказание доврачебной помощи пострадавшим.

При необходимости отключить электроэнергию (за исключением систем противопожарной защиты), перекрыть газовые, водяные, паровые коммуникации, остановить работу систем вентиляции в аварийном и смежном с ним помещениях. Проверить включение автоматических систем тушения пожара, если таковые имеются на объекте;

17.5. Прекратить все работы в очаге, кроме работ связанных с мероприятиями по ликвидации пожара;

17.6. Удалить за пределы опасной зоны всех работников, не участвующих в ликвидации пожара;

17.7. Осуществлять общее руководство по ликвидации пожара до прибытия подразделений пожарной охраны;

17.8. Обеспечить встречу и сопровождение пожарных машин к месту тушения пожара, а карет скорой помощи к месту нахождения пострадавших. Показать начальнику пожарного караула кратчайший путь к местам пожарных водоемов. В дальнейшем оказывать содействие пожарной охране в локализации пожара (очага возгорания), точно выполнять все указания начальника пожарного караула.

18. Наряду охраны **запрещается**:

18.1. Нарушать на объекте установленные Правила пожарной безопасности;

18.2. Нарушать меры личной безопасности при локализации пожара собственными силами: тушить не обесточенные электроустановки, агрегаты, помещения от которых может произойти поражение личного состава электрическим током.

18.3. Входить в помещения складов, хранилищ, где находятся предметы повышенной опасности, которые могут привести к внезапным взрывам.

18.4. Самостоятельно, без материально-ответственного лица (уполномоченного представителя предприятия) вскрывать находящиеся под охраной склады, хранилища и другие помещения в которых произошло возгорание.

4. Общие правила поведения охранника на месте пожара.

19. Оказавшись на месте возникновения пожара до прибытия пожарных обесточить объект, если площадь горения незначительная, то накрыть ее одеялом, пальто, курткой. Если горит электропроводка, отключить электропитание на щите (вывернуть пробки). Постараться сбить

огонь с горящих предметов. Сбросить на пол и затоптать горящие занавески, шторы и другие предметы.

20. Организовать присутствующих граждан для доставки воды, тушения огня песком, землей и другими подручными средствами, используя при этом имеющиеся первичные средства тушения пожара (багры, лопаты, кошму, огнетушители и т.д.)

21. Вызвать пожарных, а при необходимости иные службы.

22. Организовать эвакуацию граждан из опасных зон задымления, обвала, возможного взрыва и т.п. В первую очередь следует вывести людей с верхних этажей, так как дым всегда устремляется вверх, и огонь может перекрыть пути вывода людей. Пресекать любые факты паники, вести себя организованно и уверенно.

23. На месте пожара закрывайте рот и нос мокрой тканью (платком, шарфом, тряпкой). Оказавшись в задымленной зоне или проходя через нее, нагнитесь пониже, при сильном дыме передвигайтесь ползком.

24. Оказавшись в изолированном помещении верхних этажей, отрезанном от путей эвакуации огнем и дымом, заделайте щели влажными тряпками, одеждой, дышите нижними слоями воздуха. Попытайтесь из подручных средств сделать канат. Окно лучше не открывать, лишь когда убедитесь, что изготовленный канат достает до нижних этажей или прибыла помощь и вас могут спасти, тогда можно открыть окно. Если есть балкон, стойте на балконе и давайте о себе знать.

25. Открывая дверь, убедитесь, что она не нагрелась. Всегда есть опасность, что из-за открытой двери вырвутся клубы дыма и огня. Поэтому открывайте двери медленно, сидя на корточках или стоя у стены рядом с дверью, лицом в противоположную сторону, чтобы избежать ожогов.

26. Попытайтесь проникнуть в помещение по пожарной лестнице, через балкон, по веревке или связанным гардинам, простыням, предметам одежды.

27. Прыгать из окон второго этажа можно, лишь убедившись, что внизу нет опасных предметов и камней. Перед прыжком надо сомкнуть зубы, и приземляться на обе ступни при полусогнутых коленях, но не на пятки и не на носки. Если есть под рукой подушки, матрасы или иные предметы, смягчающие удар о землю, бросьте их на место вашего приземления.

Прыжки с более высоких этажей опасны для жизни.

28. Используйте одежду, чтобы, привязав ее к раме окна, снизить высоту прыжка либо перебраться на более низкий этаж.

29. При возможности проверьте, есть ли дети в других помещениях. Они обычно прячутся в шкафах или иных укромных местах.

30. Не входите в опасную зону при плохой видимости (=10 м).

31. Опасайтесь оборванных проводов, в том числе и после ликвидации пожара. Оказавшись возле такого провода, проходите осторожно, а чтобы избежать поражения электрическим током, применяйте способ движения «нога к ноге», делая шаги не длиннее полступни. Это необходимо для предупреждения так называемого «шагового замыкания».

32. По прибытии пожарных действуйте по их командам.

33. Используйте внутренние пожарные краны, огнетушители, направляя струю на горящую поверхность, начиная сверху. Горючие жидкости водой не тушите – это лишь увеличит очаг огня. **Помнить** – тушить

пожар с использованием гидрантов, пенных и водных огнетушителей можно только при обесточенном объекте горения.

34. Покидая зону огня, оставляйте пожарные краны открытыми.

35. Выходя из опасной зоны, идите на встречу ветру (сквозняку). В зоне сильных промышленных пожаров не приближайтесь к огню, так как возникает движение воздуха в сторону увеличения очага пожара, образуя эффект затягивания предметов в огонь.

5. Заключительные положения.

Наши авторы предлагают на каждом предприятии, с учетом его пожарной опасности, приказом (инструкцией) разработать положение, и установлены соответствующие противопожарные нормы, в соответствии с действующим Законодательством Вашей страны.

Инструкции, регламенты, договоры, справочные материалы.

1.) Служба безопасности и охраны (21)

“Должностная инструкция Инженера по охране труда”

“Должностная инструкция Начальника отдела охраны труда”

“Примерная должностная инструкция инженера сектора охраны”

“Инструкция: Действия службы безопасности и персонала фирмы при угрозе взрыва”

“Заявка на охрану груза”

“Инструкция для группы сопровождения и охраны грузов”

“Инструкция по организации несения службы суточным нарядом.”

“Инструкция по организации охраны предприятия (фирмы или организации)”

“Должностная инструкция начальника службы инкассации банка”

“Инструкция (вариант) – Правила, порядок и процедуры инкассационных мероприятий”

“Должностная инструкция инкассатора”

“Положение об отделе кадров”

“Требования к хранению оружия (МВД)”

“Порядок приема-выдачи служебного оружия и патронов к нему”

“Карточка заместитель на оружие”

“Рекомендации по разработке охранно-пропускного режима на предприятии”

“Положение о совете безопасности фирмы”

“Должностная инструкция юриста по безопасности”

“Инструкция по безопасности для няни (гувернантки)”

“Инструкция для охранника общежития”

“Должностная инструкция охранника объекта”

2.) Режим и защита информации (25)

Инструкция по защите конфиденциальной информации с образцами документов файл в архиве (ZIP)

Список сведений составляющих коммерческую тайну предприятия

“Примерный образец Положения о разведывательном отделе СБ”

“Примерный образец Положения о контрразведывательном отделе СБ”

“Договорное обязательство о неразглашении коммерческой тайны”

“Обязанности лиц, допущенных к сведениям, составляющим коммерческую тайну”

“Памятка работнику о сохранении коммерческой тайны предприятия”, (Вариант 1)

“Памятка работнику (служащему) о сохранении коммерческой тайны предприятия”, (Вариант 2)

“Обязательства работника о сохранении коммерческой тайны.”

“ПОДПИСКА О СОХРАНЕНИИ КОММЕРЧЕСКОЙ ТАЙНЫ.”

“Предупреждение о необходимости сохранения коммерческой тайны при увольнении с предприятия.”

“Порядок ведения делопроизводства документов, содержащих коммерческую тайну ”

“Порядок работы с документами с грифом ”Коммерческая тайна””

“Примерная должностная инструкция делопроизводителя сектора обработки документов с грифом ”Коммерческая тайна””

“Должностная инструкция машинистки сектора обработки документов с грифом ”коммерческая тайна”

“Примерная должностная инструкция инспектора по режиму”

“Должностная инструкция инспектора сектора режима по работе с персоналом, допущенным к материалам с грифом ”ком. тайна”

“Примерное положение о специальном отделе”

“Примерное положение о секторе обработки документов с грифом ”коммерческая тайна””

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

“Система допуска сотрудников и других лиц к сведениям, составляющим коммерческую тайну”

“Приложение к заявлению об увольнении”

“Акт о выделении к уничтожению документов и дел”

“Аттестат соответствия требованиям безопасности информации”

“Особые условия в договоре (о коммерческой тайне)”

3.) Пожарная безопасность (10)

“Перечень документации по пожарной безопасности”

“Инструкция о мерах пожарной безопасности”

“Классификация пожарных и взрывоопасных зон”

“Эвакуационные и аварийные выходы”

“Категорирование помещений по взрывопожарной и пожарной опасности”

“Пожарная характеристика материалов, зданий и конструкций”

“Паспорт пожарной безопасности предприятия (примерный)”

“План эвакуации при пожаре людей и материальных ценностей”

“Требования к оформлению плана эвакуации людей при пожаре”

“План эвакуации людей при пожаре” графический образец

4.) Договоры (9)

“Договор о конфиденциальности и защите информации”

“Соглашение о коммерческой тайне и изобретениях”

“Договор о защите коммерческой информации (о конфиденциальности)”

“Дополнения рекомендуемые для внесения в договоры и регламентирующие документы”

“Договор на оказание охранных услуг”

“Договор на сопровождение и охрану имущества перевозимого автомобильным транспортом”

“Договор о централизованной охране квартир и других помещений с личным имуществом граждан подразделениями вневедомственной охраны при органах внутренних дел.”

“Примерный договор об охране объектов подразделениями вневедомственной охраны при УВД”

“Договор об охране производственных (хозяйственных) объектов”

5.) Дополнение (По необходимости)

“О Т Ч Е Т частных охранно-сыскных структур о результатах участия в охране общественного порядка и борьбе с преступностью”

Словарь специальных терминов

Амбивалетность – сосуществования двух противоположных оценок, мотивов, эмоций.

Агент – тайный сотрудник разведки или организации, которые занимается добыванием, изучением и обобщением сведений экономического, научно-технического, политического, военного характера о неприятеле или конкуренте.

Анализ безопасности – расчет опасностей, связанных с осуществлением предвиденной деятельности юридического или физического лица.

Анализ опасности – выявление нежелательных событий, которые тянут за собой реализацию опасностей, анализ механизмов возникновения подобных событий и оценка масштаба, и вероятности любого события, способного сделать впечатляющее влияние.

Аппаратные средства защиты – устройства, системы и сооружение, предназначенные для защиты информации от несанкционированного доступа, копирование, кражи или модификации.

Аппаратура информационного снятия – это информационно-специальные, технические средства, предназначенные для получения информации шляхом приема акустических, электромагнитных, световых, тепловых или других сигналов (излучений), что несут оперативно значимые данные.

Аппаратура технической разведки – совокупность технических устройств выявления, приема, регистрации, измерения и анализа, предназначенных для получения данных об объекте.

Аффективный страх – сильнейший страх, вызываемый чрезвычайно опасными, сложными обстоятельствами, который парализует на некоторое время способность человека к произвольным действиям.

Алтаем – состояние, в котором внимание и органы чувств обращены во внешний мир.

Ассоциированность – пребывание “внутри” происходящего, взгляд от первого лица, полное ощущение собственными органами чувств. Понятие указывает на субъективность переживания в противоположность объективной точке зрения.

Аудиальные изменение – это изменение собственного поведения с сохранением рапорта, в результате чего собеседник начинает следовать за вами, неосознанно “подстраивается”.

База данных – совокупность организованных, взаимосвязанных, сохраненных в памяти ЭВМ данных, что относятся к определенному объему или направлению деятельности.

Банда:

1). Разновидность преступного сообщества (объединение), что характеризуется следующими признаками: наличие цели и соглашений об общей преступной деятельности, распределении конкретных обязанностей на из соглашения об общей преступной деятельности, вооруженности.

2). Организованная, вооруженная преступная группа, созданная с целью нападения на предприятия, учреждения или на отдельных граждан.

Бандитизм – один из опаснейших преступлений, которые посягают на основы общественной безопасности и общественного порядка. Заклю-

чается в организации вооруженной группы (банды) с целью нападения на граждан или организации, (руководство ею), участие в вооруженной группе (банде) и в оказываемые ею нападениях.

Банк данных – организационно-техническая система, которая включает в себя несколько баз данных и способы управления ими.

Банковские преступления – незаконные махинации и злоупотребления неопытностью широких слоев населения. К этой категории преступлений относятся: практика использования должностными лицами внутренней конфиденциальной информации в личных интересах, вывод незаконных спекулятивных соглашений или побуждение к ним, эмиссия необеспеченных ценных бумаг, предоставление ошибочной или недостоверной информации и осуществление других действий, которые создают предпосылки для следующих преступлений.

Безопасность информационной сети – меры, которые предохраняют информационную сеть от несанкционированного доступа, случайного или намеренного вмешательства в нормальные действия или попыток разрушения ее компонентов.

Безопасность организации – состояние ее динамической стабильности, в которой она может осуществлять свои функции в полном объеме. Стабильность характеризуется динамической равновесомой, балансом между влиянием дестабилизирующих факторов и способностью системы противостоять им в пределах, за которые наступает ее разрушение

Борьба с преступностью – совокупность мэр экономического, политического, правового, психологического, организационного, технического характера, направленных на ликвидацию, или ослабление факторов, которые оказывают содействие осуществлению преступлений, на предупреждение, прекращение, регистрацию, раскрытие и поиск преступников, расследование преступлений, на осуществление уголовного правосудия, исправление лиц, которые сделали преступление, и контроль за их обращением после отбытия наказания, а также на возмещение отрицательных последствий преступлений.

Бюрократические действия – служащих государственного и хозяйственного аппарата, который систематически требует взятки за выполнение должностных обязанностей по обслуживанию клиентуры других хозяйствующих субъектов.

Виктимность – это свойство одного человека, (или определенной социальной группы), что выражается в склонности быть жертвой преступления.

Вирус компьютерный – небольшая, довольно сложная, тщательно составленная и опасная программа, которая может самостоятельно размножаться, переносить себя на диски, прикрепляться к чужим программам и передаваться по информационным сетям.

Внедрение специальных технических средств -незаконная, негласная установка специальных технических средств на объектах охраны. Вырабатывается в ходе промышленного шпионажа и недобросовестной конкуренции.

“Вор в законе”: 1). Звания, которые присваивает на специальной воровской сходке лицу, которое владеет в среде профессиональных преступников авторитетом, основанным на значительном преступном опыте, выявленных способностях организовывать преступные группы или руко-

водить ими, соблюдении традиций и правил данной среды или на внесении больших сумм в денежный фонд преступного сообщества.

2). Лицо, которое имеет соответствующее звание и выполняет функции: принятие в составе “сообщаковой братвы” (группы “воров в законе” или авторитетов преступной среды) или самостоятельно – решений по определению основных направлений и форм преступной деятельности, форм, источников и объемов пополнения денежных фондов преступного сообщества; взаимодействия с организаторами и руководителями других преступных групп; “правосудие” относительно членов преступного сообщества и некоторые другие.

Выведывание – один из способов получения информации не гласно, что заключается в том, что сотрудник или агент спецслужбы или правоохранительного органа, разговаривая с осведомленным человеком, незаметно для последнего побуждает его рассказать о таких фактах, событиях и сведениях, которые интересуют инициаторов задачи.

Требование – требование передачи чужого имущества или правая на имущество или осуществление других действий имущественного характера под угрозой применения насилия или уничтожение или повреждение чужого имущества, а равняется под угрозой распространения сведений, которые позорят потерпевшего или его близких, или других сведений, которые могут причинить важная жаль правам или законным интересам пострадавшего или его близких.

Газовое оружие – оружие, предназначенное для временного поражения живой цели с помощью применения слезоточивых или раздражающих веществ.

Грабеж – открытое похищение чужого имущества, сделанное с применением насилия, не опасного для жизни или здоровья, или с угрозой применения такого насилия.

Диверсия – осуществление взрыва, поджога или других действий, направленных на разрушение или повреждение предприятий, сооружений, путей и средств сообщения, средств связи, объектов жизнеобеспечения населения с целью подрыва экономической безопасности и обороноспособности.

Добывание информации – действия по сбору, анализу, распространению или хранению информации, не предназначенной для пересказа гласности без согласия тех лиц, организаций и стран, которым данная информация принадлежит.

“Жучок” – радиомикрофон, установленный в помещении, технических средствах, бытовой технике разного назначения с целью перехвата разговора.

Захват заложника – увлечение, или удержание лица как заложник, сделанные с целью понуждения государства, организации или гражданина сделать какое-нибудь действие или удержаться от осуществления какого-нибудь действия как условия освобождения заложника.

Защита информации: 1). Система административных мер и приемов, направленных на классификацию, контролирование и защита от несанкционированного разглашения грифованной информации соответственно законодательству.

2.) Совокупность мероприятий, которые обеспечивают предупреждение несанкционированного доступа к конфиденциальной информации,

охраняемым сведениям промышленного, экономического, торгового, финансового и технического характера.

3.) Охрана любой информации, корреспонденции, идей, которые напечатаны, написанные, высказанные устно отдельным лицом, организацией или правительством.

Зона чрезвычайной ситуация - территория, на которой сложилась чрезвычайная ситуация.

Источник информации – лицо, предмет или вид деятельности, с помощью которых добывается информация.

Источник конфиденциальной информации – носитель информации, с помощью которого частные детективы и охранники получают неофициальные сведения в ходе розыскной или охранительной деятельности. Источником конфиденциальной информации могут быть: физическое и юридическое лица, документы, публикации в средствах массовой информации, объекты визуального наблюдения и др.

Информационная система – из совокупность специалистов, информационных ресурсов, технологий, которая осуществляет информационные процессы.

Информационные процессы – процессы сбора, обработки, накопление, хранение, актуализации, распространение информации.

Информационные ресурсы – документы и массивы документов (библиотеки, архивы, фонды, базы данных, базы сведений), другие формы организации информации из всех направлений жизнедеятельности общества.

Информация – это сведения, знание, сообщение, которые содержат элементы новизны для их получателя и употребятся в процессе принятия решения.

Канал проникновения – физический путь от злоумышленника до источника конфиденциальной информации, с помощью которого возможный несанкционированный доступ к охраняемым сведениям.

Качество информации – степень практической пригодности информации, используемой в процессе управления, обусловленная совокупностью таких свойств, как полнота, плотность, полезность, достоверность, ценность информации.

Клептомания – страсть к кражам.

Конкуренция – соперничество, соревнование между выступающими на рынке предпринимателями, которые имеют целью обеспечить лучшие возможности сбыта своей продукции, удовлетворяя разнообразные нужды покупателей

Консалтинг – это деятельность по консультированию производителей, продавцов и покупателей по широкому кругу экономических и других вопросов, связанных с хозяйством и характером

Конфликтная ситуация – острая форма проявления противоречий. Выражается в столкновении противоположных интересов людей при общей деятельности через расхождение мотивов, целей и способов их решения. Частота и сложность конфликтной ситуации во многом зависит от эффективности материального стимулирования, уровня организации работы, воспитательной работы, социально-психологического климата в трудовом коллективе, авторитету руководителей и стиля руководства.

Концепция защиты информации – система взглядов, требований и условий организации защиты охраняемых сведений от разглашения, источника и несанкционированного доступа к ним через разные каналы.

Концепция национальной безопасности – система научно обоснованных и официально принятых взглядов на пути, средства и механизмы защиты от внешних и внутренних угроз жизненно важным интересам государства, территориальной целостности и политической стабильности, возможности стойкого социально-экономического развития.

Коррупция: 1). Использование лицами, уполномоченными на выполнение государственных функций, своего статуса и связанных с ним возможностей для противоправного получения материальных и других благ и преимуществ, а равняется предоставление им таких благ и преимуществ физическими и юридическими лицами.

2). Сращивание преступного мира с государственно-властными и исполнительными структурами государства.

Кража – тайное разворовывание чужого имущества.

Криминогенная обстановка – совокупность факторов, которые оказывают содействие сохранению или роста преступности (отдельных ее родов и видов) на определенной территории.

Крэкер – разновидность хэкеров, что занимается воровством чужой информации.

Патентная преступность – сумма уголовно преступных действий, которые не становятся известными государственным правоохранительным органам на протяжении определенного периода времени на определенной территории и поэтому не отраженные в официальной уголовной статистике.

Легализация – (отмывание) средства или другого имущества, приобретенного незаконным путем, осуществление финансовых операций и других соглашений со средством или другим имуществом, приобретенным сознательно незаконным путем, а равняется использование указанных средств или другого имущества для осуществления предпринимательской или другой экономической деятельности.

Лжебанкротство – сознательно ошибочное объявление юридическим лицом о неспособности платить по своим долговым обязательствам, которая преследует, цель сокрытия похищенных, растраченных сумм.

Лжепредприятие – создание коммерческих организаций без намерения осуществлять предпринимательскую или банковскую деятельность, которая имеет целью получения кредитов, освобождение от налогов, извлечение другой имущественной выгоды или прикрытие запрещенной деятельности, которое причинило большой убыток гражданам, организациям или государству.

Лицензиат – физическое или юридическое лицо, которое имеет лицензию на осуществление конкретного вида деятельности.

Лицензия – (разрешение) документ, который предоставляет право владельцу на осуществление определенного вида деятельности на протяжении установленного в нем срока при обязательном соблюдении лицензионных требований.

Маргинальные явления – это отрицательные социальные явления, (преступных правонарушений,) в частности, пьянство, наркомания, токсикомания, проституция.

Могущество государства – срок, который включает в себя десять основных показателей развития государства: человеческий потенциал; территория и природные ресурсы; военная сила; морально-политическое единство; национальное богатство; уровень Научно-технического развития; частица участия в международном разделении труда, культурное наследство и достигнут уровень культуры, уровень демократии и личной воли, качество жизни населения.

Намерение – цель, намеченный результат действия. Неправильные или бесцельные на вид поступки могут опираться на благие, хотя и неосознаваемые намерения.

Нейролингвистическое программирование – изучение принципов совершенствования, модель того, как люди структурируют свои переживания.

Нейрологические уровни – различные логические уровни переживания: окружающая среда, поведение, способности, убеждения, личность и духовность.

Неконгруэнтность – внутренний конфликт, отсутствие полной уверенности в утверждении или намеченном результате. Проявляется в расхождении слов человека и его поступков, общего склада характера.

Неопределенные глаголы – глаголы с опущенными наречиями, включающие возможность понять, как именно протекает действие, то есть процесс остается неопределенным.

Неопределенные существительные – существительные, лишенные указания на то, кого или что они обозначают.

Негативизм – сопротивление внешним влияниям.

Нейротизм – психологическая нестабильность личности.

Номинализация – лингвистическое понятие, означающее отглагольные существительные и процесс их образования.

Мониторинг – процесс отслеживания состояния системы или явления.

Нравственно-психологический климат – состояние коллектива, в котором выражаются особенности взаимодействия и расположения духа работников, степень их удовлетворения содержанием и условиями работы, стилем управления и других факторов. Нравственно-психологический климат характеризуется уровнем слаженности и управляемости, освоением нововведений, товарищеской взаимопомощью, отсутствием или наличием конфликтных ситуаций.

Мошенничество – разворовывание чужого имущества или приобретение права на чужое имущество посредством обмана или злоупотребление доверием.

Незаконная банковская деятельность – осуществление банковской деятельности (банковских операций) без регистрации или без специального разрешения (лицензии) в случаях, когда такое разрешение (лицензия) обязательно, или с нарушением условий лицензирования, если это действие нанесло большой ущерб гражданам, организациям или государству или соединено с извлечением дохода в большом размере.

Незаконное получение кредита – получение индивидуальным предпринимателем или руководителем организации кредита или льготных условий кредитования путем предоставления банка или другому кредитору сознательно неправдивых сведения о хозяйственном положении или фи-

нансовом состоянии индивидуального предпринимателя или организации, если это действие нанесло большой ущерб.

Незаконное предпринимательство – осуществление предпринимательской деятельности без регистрации или без специального разрешения (лицензии) в случаях, когда такое решение не принималось.

Носители коммерческой тайны – люди, а также электронные поля и материальные объекты, в которых информация находит свое отражение: документы, записи, отчеты, протоколы, черчение, материалы, образцы, модели, приборы, вещества и т.д.

“Ноу-хау”: 1.) Совокупность разных знаний научного, технического, производственного, финансового, коммерческого или другого характера, опыта, практически применяемых в деятельности предприятия или в профессиональной деятельности, которые еще не стали общим достоянием.

2.) Технические знания, опыт, секреты производства, необходимые для решения какого-нибудь задачи.

3.) Полностью или частично конфиденциальные знания, которые включают сведения технического, экономического, административного, финансового характера, использование которых обеспечивает преимущество лицу, их что получили.

Общественная безопасность – это составленный элемент национальной безопасности, которая включает в себя: систему защиты общества, человека от преступности, коррупции, теневой экономики, любых форм антисоциального обращения; скоординированную деятельность разных социальных объектов по предотвращению возможных отрицательных социальных следствий перехода страны к рыночной экономике (рост безработицы, увеличение разрыва в равные жизни разных социальных пластов общества, ухудшение положения неимущих групп населения); комплекс мэр по предотвращению социальной напряженности в обществе в связи с межнациональными, территориальными, политическими, экономическими, конфессиональными и другими конфликтами.

Организация защиты коммерческой тайны – регистрация права на коммерческую тайну в уставе предприятия; определение перечня должностных лиц, уполномоченных классифицировать информацию как коммерческую тайну; разработка внутренних правил засекречивания, обеспечение сохранности коммерческой тайны и рассекречивание удерживающих ее сведений; введение соответствующего маркирования документов и других носителей информации и отладка секретного делопроизводства; установление и поддержка режима секретности, осуществление контроля за соблюдением режима секретности.

Организованная преступность: 1.) Совокупность зарегистрированных на протяжении определенного периода на определенной территории преступлений, сделанных организованными группами.

2.) Совокупность организованных преступных групп и их участников, зарегистрированных на протяжении определенного периода на определенной территории.

3.) Создание организованных групп, преступных организаций, преступных сообществ и их преступная деятельность.

Охрана – комплекс организационных и технических мероприятий по ограничению доступа и защиты территории, помещений, информации, средств и предметов производства, произведенной продукции.

Охрана объекта – осуществляемые администрацией предприятия, фирмы, банка и/или уполномоченным на то частным охранительным предприятием мероприятия, направленные на предупреждение несанкционированного доступа (проникновение) на охраняемый объект посторонних лиц, а также причинение возможного материального ущерба.

Охранительные мероприятия – совокупность действий по обеспечению безопасности охраняемых объектов и граждан.

Охраняемые объекты – дома, строения, сооружение, транспортные средства, другое имущество, а также территории, которые подлежат защите от противоправных действий.

Первоочередные информационные нужды – это нужды утверждены компетентным лицом или органом перечень наиболее важных проблем, которые представляют особенно большой интерес для лиц, которые принимают решение в конкретной области деятельности.

Платежеспособность – способность и возможность физического или юридического лица своевременно и в полном размере оплатить свои долги. Платежеспособность является необходимым условием для признания данного лица кредитоспособным, т.е. заслуживает доверия для получения кредита.

Подделка документов – изготовление полностью фиктивного документа (письмо, авизо, вексель) или незаконное изменение настоящего документа; исправление, замена или уничтожения части текста, внесение дополнительных данных, воспроизведение подписи за другое лицо и прочее.

Пожарная безопасность объекта – комплекс мероприятий, направленных на приведение объекта в состояние, при котором исключается возможность пожара, а в случае возникновения – обеспечение предотвращения влияния на людей опасных факторов пожара, обеспечение защиты материальных ценностей и их сохранности.

Положение о службе безопасности – нормативно-правовой документ, который определяет состав, структуру и функциональные обязанности подразделов и сотрудников службы безопасности.

Превышение полномочий – действие, сделанная руководителем или служащим частной охранительной службы вопреки задачам своей деятельности с применением насилия или с угрозой его применения.

Преступное сообщество – (преступная организация), что имеет стойкие противоправные связи с лицами, уполномоченными на выполнение государственных или общественных или других публично значимых функций, для использования государственных, общественных структур, кредитно-финансовых учреждений, а также средств массовой информации с целью получения преступных доходов.

Промышленная тайна – секреты производственной деятельности предприятия, методы и способы управления финансами, маркетингом, производством, финансами, выявление которых конкурирующими фирмами может нанести важный ущерб предприятию или разорить его.

Профессиональная этика – кодекс обращения, которое обеспечивает моральный характер тех взаимоотношений между людьми, которые вытекают из их профессиональной деятельности.

Предикаты – “слова-ощущения”, указывающие на использование той или иной системы представления.

Предпочитаемая система – система представления, которой человек обычно пользуется – чаще всего при отслеживании или организации собственных переживаний.

Представление – идея, принцип кодирования и хранения сенсорной информации разумом.

Пресуппозиции – идеи или утверждения, которые приходится принимать как данность, чтобы общение стало осмысленным.

Принципы правильной формулировки – способ обдумывания и выражения результата, который делает намеченную цель достижимой, поддающейся проверке и мотивированной, а также конгруэнтной с прочими результатами; основа устойчивого успеха и взаимовыгодных достижений.

Присоединение – установка и сохранение рапорта с собеседником в течение некоторого времени посредством присоединения к его модели мира. Присоединиться можно не только к поведению, но и к убеждениям, ценностям.

Присоединение к будущему – мысленная репетиция, “проверка” намеченного результата, которая проводится для того, чтобы укрепить желаемое поведение или состояние.

Пунктуационная неоднозначность – неоднозначность, вызванная слиянием двух предложений в одно.

“Радиозакладка” – миниатюрное электронное устройство, которое состоит из микрофона, радиопередатчика что обеспечивает передачу переговоров, которые подслушивают, на значительное расстояние с помощью электромагнитных волн. “Радиозакладки комифлируют” под бытовые и технические приборы, составленные элементы мебели, оборудования офисов и служебных кабинетов.

Руководитель организованной преступной группы – участник организованной преступной группы, которая владеет правом: отдавать указания, обязанности для выполнения другими участниками группы; устанавливать функции последних внутри группы; определять объект (объекты) преступления (преступлений), время и способы его (их) осуществление; распределять доходы от преступной деятельности; принимать в группу и исключать из группы ее участников; принимать меры по обеспечению безопасности группы от уголовного преследования.

Рэкет – требование государственного или личного имущества путем угроз и насилия.

Рэкетир – преступник, который занимается рэкетом, вымогатель, шантажист, гангстер.

Развивающее обучение – вид обучения, при котором процесс получения знаний, навыков и умений целенаправленно ориентирован на достижение главной цели – развитие интеллектуальных возможностей человека.

Развитие – процесс становления личности под влиянием внешних и внутренних, управляемых и неуправляемых социальных и природных факторов.

Рейтинг – комплексный показатель, который учитывает достижения студентов по всем видам занятий и самостоятельной работы по дисциплинам университета (академии) в течении семестра, учебного года и всего периода обучения.

Решение проблем – выявление и формирование проблем, анализ соответствующей информации, поиск альтернатив и планирование мер в отношении решения проблем.

Репродуктивные методы обучения – предусматривают активное восприятие и запоминание учебного материала, который сообщается учителем и другими источниками информации.

Разговорный постулат – “гипнотическая” форма языка, когда вопрос истолковывается как приказ.

Система защиты информации – организованная совокупность мероприятий, методов, органов и средств, создаваемых с целью защиты информации.

Сфера влияния организованной преступной групп – хозяйствующий субъект (группа хозяйствующих субъектов), территориальное образование (район, населенный пункт, регион, группа регионов), область экономики или государственная функция, управление и развитие которых объективно зависит или целеустремленно осуществляется с учетом интересов преступной группы.

Теневая экономика – неконтролируемое обществом производство, распределение, обмен и потребление товарно-материальных ценностей, т.е. скрываемые от органов государственного управления, общественности социально-экономические отношения между отдельными гражданами, социальными группами по использованию существующих форм собственности в корыстных личных или групповых интересах.

Терроризм – осуществление взрыва, поджога или других действий, которые создают опасность гибели людей, причинение значительного имущественного убытка или наступление других общественно опасных следствий, если эти действия сделанные с целью нарушения общественной безопасности, пугание населения или предоставление влияния на принятие решений органами власти, а также угроза осуществления указанных действий в тех же целях.

Техническая защита информации – совокупность мероприятий и технических средств (механических, оптических, электрических и других), что обеспечивают защиту информации.

Технические средства контроля доступа – средства систем контроля доступа на охраняемые территории, у помещение, хранилища и другие пространства и емкости.

Технические средства охраны – аппаратные технические средства, которые обеспечивают контроль доступа, сохранность и противопожарную безопасность территории, помещений, хранилищ и других охраняемых объектов.

Технологический терроризм – применение или угроза применения террористами ядерного, химического, бактериологического оружия и других радиоактивных веществ, а также попытка увлечения или вывод из порядка разного рода промышленных и других объектов (энергетики, химии, связи и т.д.), что имеют важное значение для экономики и/или представляет повышенную опасность для жизни людей и окружающей среды.

Управление безопасностью – система регулярных защитных мероприятий, направленных на обеспечение безопасности соответственно изменению условий внутренней и внешней среды.

Уровень преступности – число сделанных на протяжении определенного периода на определенной территории преступлений (лиц, их что сделали) рассчитывая на 100 тыс. (иногда на 10 тыс.) человек, которые достигли возраста наступления уголовной ответственности.

Утечка информации – неконтролируемый выход конфиденциальной информации за границы организации или круга лиц, которой эта информация доверена.

Уязвимость – свойство системы, которая может привести к нарушению ее защиты при наличии угрозы.

Физическая безопасность – система внешних и внутренних отношений предприятия, которое обеспечивает физическую безопасность работников предприятия, его клиентов, фондов, материальных и интеллектуальных (информационных) ценностей от намеренного или неумышленного их уничтожения, повреждение их качественных характеристик или разворовывание.

Фрэк – телефонный хулиган, который с помощью разных устройств и способов подключается к телефонным сетям, обеспечивая бесконтактное соединение незаконного абонента через линии связи.

Фемининность – комплекс физиологических, психических и др. признаков, определяющих принадлежность к женскому полу.

Фильтры восприятия – уникальные идеи, переживания, убеждения и языковые средства, придающие определенную форму модели мира человека.

Фонологическая неоднозначность – Наличие омонимов, то есть слов, которые звучат похоже, но имеют разный смысл (“спица” и “спит-ся”).

Фундаментализация – усиление взаимосвязи теоретической практической подготовки молодого человека к современной жизнедеятельности.

Фиксация — различают два направления: 1) упорное следование однажды принятой установке, привычке, способу действия; (один из примеров Ф. – это сексуальная Ф. на определенном партнере) или способе сексуального удовлетворения, делающая невозможной иную форму половой жизни;

2) (на травме) — «застревание» больного на каком-либо травмирующем переживании из его прошлого, выражающееся в навязчивом появлении одних и тех же симптомов, невозможности самому освободиться от них и т. п.

Фобия — непреодолимый навязчивый страх перед каким-либо предметом или явлением. Фрейдом выделяются две группы:

1) «житейские страхи» (страх смерти, инфекции, высоты и т. п.);

2) специальные Ф. (боязнь открытых пространств, определенных животных и т. п.). Причиной фобии, как и любого другого симптоматического расстройства – является бессознательный конфликт душевных стремлений.

Фрустрация – психическое состояние, (подавленное настроение) при возникновении непреодолимых препятствий

Хэкер – компьютерный хулиган, который незаконно подключается к чужим сетям .

Цензура - обратное представление тех сил, которые стремятся не допустить в сознание бессознательные мысли и желания.

Ценность информации – свойство информации, обусловленное ее пригодностью к практическому использованию на основе учета таких параметров, как полезность, полнота, достоверность, новизна.

Частная детективная деятельность – предоставление на договорной основе детективных услуг на территории Украины, России юридическими и (или) физическими лицами, зарегистрированными в установленном порядке и имеющие соответствующие лицензии, выданные органами внутренних дел, с целью защиты законных прав и интересов своих клиентов.

Частная охранительная деятельность – предоставление на договорной основе охранительных услуг на территории Украины, России юридическими лицами, зарегистрированными в установленном порядке и имеющие соответствующие лицензии, выданные органами внутренних дел, с целью защиты законных прав и интересов своих клиентов.

Частная детективная организация – организация, учреждаемая в форме хозяйственного общества или общества для предоставления детективных услуг.

Частный охранник – гражданин Украины, России или другой страны, который получил в установленном Законом порядке лицензию на частную охранительную деятельность и работающий в частной охранительной организации или службе безопасности юридического лица.

Частная охранительная организация – организация, учреждаемая в форме хозяйственного общества или общества для предоставления охранительных услуг.

Экспектации – ожидание от человека определенного поведения, общепринятых норм стереотипов.

Экстравертированность, (противоположность – интровертированность) характеристика типов людей, с ориентацией на мир внешних событий или переживаний.

Эмпатия – способность отзываться на переживания другого лица, сочувствие.

Экономическое рассмотрение душевных процессов – рассмотрение психических процессов с точки зрения их энергетического обеспечения.

Я – подструктура душевной жизни, выступающая посредником между *сверх Я* и *Оно*, индивидом и реальностью. Несет на себе функцию восприятия внешнего мира и приспособления к нему, стремится учесть и согласовать между собой требования реальности.

Я-идеал – в работах Фрейда часто употребляется как синоним **сверх Я**. Однако ряд комментаторов творчества З. Фрейда считают, что следует различать **сверх – Я** как результат изначальных ране-детских идентификаций с родителями. **Я-идеал** представляет моральные общественные нормы. В течение жизни могут неоднократно изменяться.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

- 1 Закон Украины «О лицензировании определенных видов хозяйственной деятельности».
- 2 «Про государственную программу борьбы с преступностью» утвержденную Постановлением Верховной Рады Украины 25 июня 1993 года.
- 3 Постановления Кабинета Министров «Про усовершенствование охраны государственной и других форм собственности».
- 4 Постановление № 99 от 15 апреля 1991 года «Про порядок выдачи субъектам предпринимательской деятельности специальных разрешений (лицензий) на осуществление отдельных видов деятельности и размер платы за государственную регистрацию объектов предпринимательства».
- 5 Приказ МВД № 112 от 28 февраля 1994 года «О внесении изменений и дополнений в приказ МВД Украины № 534 от 30 августа 1993 года «О выполнении постановления Кабинета Министров Украины № 615 от 10 августа 1993 года «О мероприятиях по усовершенствованию охраны объектов государственной и других форм собственности».
- 6 Приказ МВД Украины № 812 от 22 декабря 1993 года «Об утверждении состава комиссии по вопросам рассмотрения материалов и выдачи лицензий субъектам предпринимательской деятельности, которые предоставляют услуги по охране государственной, коллективной и частной собственности, монтажу, ремонту и профилактическому обслуживанию средств охранной сигнализации».
- 7 «Инструкция о порядке выдачи субъектам предпринимательской деятельности лицензий на предоставление услуг по охране коллективной и частной собственности, а также охране граждан, монтажу, ремонту и профилактическому обслуживанию средств охранной сигнализации».
- 8 «Инструкция об условиях и правилах осуществления предпринимательской деятельности по предоставлению услуг по охране коллективной и частной собственности, а также охране граждан, монтажу, ремонту и профилактическому обслуживанию средств охранной сигнализации и контролю за их соблюдением».
- 9 Закон Украины «О предпринимательстве»
- 10 Закон Украины «О лицензировании определенных видов хозяйственной деятельности» ,
- 11 Совместным приказ Министерства охраны здоровья Украины и Государственного комитета Украины по надзору за охраной труда от 23.09.1994 г. «Про утверждение Перечня работ, где есть потребность в профессиональном подборе»
- 12 Приказ Государственного комитета Украины по надзору за охраной труда от 30.11.93 №123 «Про перечень работ с повышенной опасностью».
- 13 «Словаря русского языка» Академии наук СССР

- 14 Закон Украины «О милиции»
- 15 Проект Закона Украины «Про частную детективную деятельность»
- 16 Закон Украины «О национальном Банке Украины» (№679-ХН от 20.05.1999 г.)
- 17 Закон Украины «О банках и банковской деятельности» (№2121-111 от 07.12.2000 г.);
- 18 Постановление НБУ №134 от 28.03.2001 г. «Об утверждении Инструкции о требованиях к организации охраны учреждений банков Украины».
- 19 Приказ МВД Украины: №112 от 28.02.1994 г. «О внесении изменений и дополнений в Приказ МВД Украины от 30 августа 1993 года №534 «О выполнении постановления Кабинета Министров Украины от 10 августа 1993 г. №615 «О мерах по усовершенствованию охраны объектов государственной и других форм собственности».
- 20 Приказ МВД Украины: №812 от 22 декабря 1993 г. «Об утверждении состава комиссии по вопросам рассмотрения материалов и выдачи лицензий субъектам предпринимательской деятельности, которые предоставляют услуги по охране государственной, коллективной и частой собственности, монтажу, ремонту и профилактическому обслуживанию средств охранной сигнализации».
- 21 Приказ МВД Украины №1030 от 25.11.2002 г. «Об утверждении Инструкции об организации охраны учреждений банков ГСО при МВД Украины».
- 22 Уголовный кодекс Украины.
- 23 Кодекс об административных правонарушениях.
- 24 Постановление Кабинета Министров Украины №706 от 07.09.93 г. «Положение о порядке продажи, приобретения, регистрации, учета и применения специальных средств самообороны, заряженных веществами слезоточивого и раздражающего действия».
- 25 Приказ МВД № 60 от «5.01.1995 г. «Про утверждение Инструкции про порядок постоянного хранения и ношения табельного огнестрельного оружия, боеприпасов и специальных средств работниками милиции».
- 26 Журавлев СЮ. Частная охрана. Серия: Тайны воинских искусств, книга 10. Москва 1994 г.
- 27 Ревенко А.Н. Волик А.А. √1Р -персонал, Серия: Библиотека телохранителя, Киев. 2003 г.
- 28 Ревенко А.Н. Волик А.А. Организовать охрану, Серия: Библиотека телохранителя, Киев. 2004 г.
- 29 Учебное пособие для подготовки сотрудников личной охраны. Базовый курс. Москва. 1996 г.
- 30 Нейл С. Ливингстоун. «Полное руководство по обеспечению безопасности должностных лиц и представителей деловых кругов», (США).
- 31 Джеймс Шортт «Телохранитель» (Великобритания).
- 32 Михайлюк АА.Быструхин Г.С., Ковтун И.А., Федько И.П. Человек вооруженный. – Киев. 1997 г.

- 33 Гримак Л.Н. Резервы человеческой психики: Введение в психологию активности. - М. 1987. - 286с.
- 34 Гримак Л.П. Гипноз и преступность. -М.: Республика, 1997. - 304с.
- 35 Гитин В., Хигир Б. Анатомия криминала. Убийство. Изнасилование. Харьков. 1996. - 416с.
- 36 Духов В.Е. Экономическая разведка и безопасность бизнеса. - К.: “Студцентр”, 1997. - 175с.
- 37 Делікатний С.К. Професійно-психологічна підготовка працівників органів внутрішніх справ. Інформаційний бюлетень №3. РНМЦ МВС - К.: 1995.-52-55С.
- 38 Делікатний С.К. Психолого-педагогічні питання вирішення конфліктів у колективах працівників УВС. Конфлікти в суспільстві, діагностика, профілактика. 1995.-156-157с.
- 39 Елисеєв О.П. Конструктивная типология и психодиагностика личности. Практ. психол. - Псков, 1994.-280с.
- 40 Еникеев М.И. Основы общей и юридической психологии. - М. 1996.
- 41 Еникеев М.И., Черных Э.А. Психология следователя. Практикум по юрид. психологии. - М., 1988. - 157с.
- 42 Журавлев С.Ю. Частная охрана: организационно-правовые и тактико-специальные аспекты деятельности. М., 1994. - 267с.
- 43 Зарайский Д.А. Управление чужим поведением. Технология личного психологического влияния. - Дубна: Издательский центр “Феникс”, 1997.-272С.
- 44 Замковой В.И., Ильчиков М.З. Терроризм - глобальная проблема современности. М. : Институт международного права и экономики, 1996.-80с.
- 45 Зенькович Н. Вожди на мушке: теракты и инсценировки. Минск: “Польмя”, 1996- 318с.
- 46 Ибрагимов М.М., Куличенко В.В., Стадии Б.Г. Профессиональная этика и этическая культура сотрудников органов внутренних дел.: Учебное пособие. -К.: НИ и РИО Киевской высшей школы МВД СССР, 1990.-304С.
- 47 Шмуратов А.Т. Конфлікт і згода: Основи когнітивної теорії конфліктів. К.: Наукова думка, 1996. - 190с.
- 48 Каретников М.К., Лобашов А.К. Технические средства, применяемые сотрудниками личной охраны. Учебное пособие, М.: Мир безопасности.-1997.-79с.
- 49 Коновалова В.Е. Правовая психология: Учебное пособие. Харьков: Основа, 1990.-198с.
- 50 Карнеги Д. Как завоевать друзей и оказывать влияние на людей, (ред. Зинченко В.П.): Мн.: Беларусь. 1990.-670с.
- 51 Козлов Н.И. Лучшие психологические игры и упражнения. Екатеринбург: АРД ЛТД, 1997.-144С.
- 52 Кейрин Фримин Дьюш и Джордж Дьюш. К-9 - собака для охраны и защиты собственности и бизнеса. - Пер. с англ. А.В. Савинова.- “Библиотека Американского клуба собаководства”. - М.: 1997.-236с.
- 53 Комиссаров В.С. Терроризм, бандитизм, захват заложников и другие тяжкие преступления против безопасности общества. По новому УК РФ. - М.: Изд-во Кросна-Лекс. - 1997.-160с.

- 54 Костин Ю. Безопасность личности : Похищение людей. Как себя вести, если ваш ближайший друг попал в беду. - М.: Олма - Пресс, 1997.-62с.
- 55 Караяни А. Как противостоять опасности. //Телохранитель. 1995. №4. С. 44-47
- 56 Коренко С. Защити свое дело. // Телохранитель №4, 1995. Стр. 14-17.
- 57 Коновалова В.Е. Правовая психология. Учебное пособие. - Харьков, 1990.
- 58 Костицкий М.В. Введение в юридическую психологию: методологические и теоретические проблемы. - К.: Выща шк., 1990. -259с.
- 59 Константинов А., Дикселиус М. Бандитская Россия. - СПб: Олма-Пресс, 1997.- 592с
- 60 Кривич М., Ольгин О. Товарищ убийца. - М.: Текст, 1992.-352с
- 61 Криминалистическое обеспечение деятельности криминальной милиции и органов предварительного расследования. / Под ред. проф. Т.В. Аверьяновой и проф. Р.С. Белкина. - М.; 1997. - 400с.
- 62 Кузьмин И. Психотехнологии и эффективный менеджмент. - М.: Психол. школа бизнеса. 1994. - 192с.
- 63 Кучинский А.В. Преступники и преступления с древности до наших дней. Антология наемного убийства: Энциклопедия.: Сталкер, 1997. - 432с.
- 64 Леонов Н.С. Информационно-аналитическая работа в зарубежных учреждениях. М.: МГИМО.-1996.-96с.
- 65 Линдер И.Б., Нечипоренко О.М., Титков С.А. По ту сторону зеркала /на правах рукописи. - М.: Международная контртеррористическая тренинговая Ассоциация, издательская фирма "Кумир". - 1997.-511с.
- 66 Лихолоб В.Г., Филонов В.П., Коваленко О.И. Михайлов А.Е. Криминология: Учебник для учебных заведений МВД Украины. Под ред. В.Г. Лихолоба и В.П. Филонова, - Киев - Донецк, 1997.-398с.
- 67 Леонгард К. Акцентуированные личности. / Под ред. докт. мед. наук В.М. Блейхера. - К.: В\ школа. 1981.
- 68 Лучшие психологические тесты для профориентации: описание и руководство к использованию / под ред. А.Ф. Кудряшова. Петрозаводск: "Петроком". - 1992. -318с.
- 69 Ларичев В.Д. Как уберечься от мошенничества в сфере бизнеса. М., 1996.
- 70 Леви В. Искусство быть собой. - М., 1991.
- 71 Мельников В.М., Ямпольский Л.Т. Введение в экспериментальную психологию личности. - Учебное пособие для слушателей ИПК, преподавателей педагогических дисциплин. - М.: Просвещение, 1985. - 319с, ил.
- 72 Методы диагностики и развития психологического потенциала, руководителей органов внутренних дел. / Учебно-методическое пособие. - М., 1996.-130С.
- 73 Модестов Н.С. Маньяки... Слепая смерть: Хроника серийных убийств. -М.: Изд-во Надежда-1, 1997. - 288с.
- 74 Москвина Л. Энциклопедия психологических тестов. - Саратов, изд-во Научная книга, 1996. - 336с.

- 75 Малеев В.А. Психофизиологическая саморегуляция. - Ростов-на-Дону, 1980.-89с.
- 76 Максимовский Э. Империя страха. - М., 1992.
- 77 Москвина Л. Энциклопедия психологических тестов. - М., 1996.
- 78 Медведев В.С. Проблеми професійної деформації співробітників органів внутрішніх справ (теоретичні та прикладні аспекти). - К.: МВС України НАВСУ, 1997.- 191с.
- 79 Модестов Н.С. Москва бандитская. - М.: Центорполиграф, 1996. - 395с.
- 80 Модестов Н.С. Москва бандитская - 2. - М.: Центорполиграф, 1997.-392с.
- 81 Новиков В.С. Профессиональная обученность сотрудников милиции к действиям в условиях, связанных с применением газового оружия самообороны в целях нейтрализации физических лиц, и ее организация: лекция. - М.: Академия МВД России, 1996. - 30с.
- 82 Новиков В.С. О применении оружия гражданами России. Научно-практический комментарий к ст. 24 Закона “Об оружии”: лекция. - М.: Изд-во Академии МВД России. 1997. - 46с.
- 83 Общая психодиагностика. Учебное пособие /Под. ред. Бодалева А.А., Стопина В.В. - М.: МГУ, 1987. - 304с.
- 84 Организационно-правовые основы частной охранной деятельности: практические советы деловым людям. /Под общ. ред. А.А. Фастикова. - М., 1993.-112с.
- 85 Основы психологического изучения личности работника. 2 ч. / Под общ. ред. Щекина Г.В. - К. 1991.- 96с, 92с
- 86 Основы педагогического мастерства: Учеб. пособие для пед. спец. высш. учебн. заведений / И.А. Зюзин, И.Ф. Кривонос, Н.Н. Тарасевич и др.; Под ред. И.А. Зюзина. - М.: Просвещение, 1989.-302с
- 87 Плиско В.И. Формирование у сотрудников устойчивого психомоторного состояния к внешним проявлениям опасности. - К.: РИО МВД Украины, 1991.-128с
- 88 Попов П.Г. Использование элементов актерской психотехники в деятельности сотрудников органов внутренних дел. - М.: А.П.О., 1992. - 41с
- 89 Психология. Словарь /Под общ. ред. А.В. Петровского, М.Г. Ярошевского. - М.: Политиздат, 1990. - 494с
- 90 Психология и педагогика в правоохранительной деятельности органов внутренних дел. Учебное пособие / под ред. ИД. Мариновской. - М.: МЮСТ МВД России, изд-во “Щит-М”, 1997. - 176с
- 91 Психологические особенности поведения работников милиции в конфликтных ситуациях: Научно-практическое пособие / Под ред. Г.Г. Романовича. -М. 1988. -66с
- 92 Профессионально-психологическая подготовка милиционеров охраны (методические рекомендации) / под общ. ред. А.М. Столяренко. - М.: Учебно-методический центр, 1990. - 234с
- 93 Рабочая книга практического психолога: технология эффективной профессиональной деятельности (пособие для специали-

- стов, работающих-с персоналом). - М.: Издательский дом "Красная площадь", 1966.
- 94 Разаков Ф.И. Век террора. - М.: ЗАО Изд-во ЭКСМО, 1997. - 432с.
- 95 Разаков Ф.И. Бандиты времен социализма (хроника российской преступности 1917-1991 г.г.). - М.: 1996.-528с.
- 96 Разаков Ф.И. Бандиты времен капитализма (хроника российской преступности 1992-1995 г.г.). - М.:1996. - 608с.
- 97 Рогов Е.И. Настольная книга практического психолога в образовании: Учебное пособие. - М.: 1996.-529с.
- 98 Симмонс Дж.Л., Мак-Колл Дж. 76 способов защитить вашего ребенка от преступников. Питер Пресс, 1995.
- 99 Словарь практического психолога /сост. С.Ю. Головин. - Минск: Харвест, 1997. -800с.
- 100 Собчик Л.Н. Стандартизированный многофакторный метод исследования личности: Методическое руководство. Вып. 1,2,3., М., 1990.
- 101 Столяренко А.М. Психологическая подготовка. Методические рекомендации. М., 199. - 70с.
- 102 Чуфаровский Ю.В. Юридическая психология. -М., 1997.
- 103 Судебная психиатрия: Учебник / Под ред. Г.В. Морозова. - М.: Юридик. лит.; 1997.-256с.
- 104 Судоплатов П.А. Спецоперации. Лубянка и Кремль. 1930-1950 г. М.: ОЛМА-ПРЕСС, 1997.-688с; ил..-32.
- 105 Сухарев В.А. Психология интеллекта. -Донецк: Сталкер, 1997. -416с.
- 106 Украинцев В. Угрозы не так страшны, если их знать в лицо. // Телохранитель. 1995. Стартовый номер.
- 107 Управление конфликтными ситуациями: рекомендации для руководителей. К., 1993. -25с.
- 108 Федоткин ОН., Бураев Ю.И. Сборник материалов по основам организации охранной деятельности: М. 1996.
- 109 Фрейд З. Введение в психоанализ. Лекции. М.: Наука.-1989.-455с.
- 110 Херсонский Б. Г. Психология и профилактика семейных конфликтов. Киев.: Здоровье, 1991. - 127с.
- 111 Хоменко О. Язык блатных: Энциклопедический синонимический словарь, т.1, т.2, К.: "Форт-М"; 1997. - 52 7.
- 112 Цвилюк Г. Школа безопасности, или Как вести себя в экстремальных ситуациях. М.: 1997. - 192с
- 113 Чуфаровский Ю.В. Юридическая психология. - М., 1997.
- 114 Шейнов В.П. Как управлять другими. Как управлять собой: (Искусство менеджера). -Мн.: Амолфея, 1996.
- 115 Шейнов В.П. Психология и этика делового контакта. - Мн.: Амолфея, 1996.-384С.
- 116 Школа выживания, обеспечение безопасности жизнедеятельности: Учебное пособие. Р-Д: "Феникс", 1996.
- 117 Щекин Г.В. Практическая психология менеджмента. Кн. I . Как делать карьеру. - К.: МЗУУП, 1993. - 152с.
- 118 Экономический порядок и криминальная конкуренция: Научно-учебное пособие. – Ч. 1996. - 260с.

- 119 Экспертиза объекта. Сост. С.А. Гурасов. - М.: "Мир Безопасности", 1997. - 164с.
- 120 Юридична психологія. (Альбом схем з коментарями): Навч. посібник. - К.: 1997. - 56с.
- 121 Кадино Э. Электронные системы охраны. М.-"ДМК". - 2001 - 256 с.
- 122 Свирский Ю.К. Рынок периметровых средств охранной сигнализации на пороге третьего тысячелетия. - Системы безопасности средств связи. -2000 - N9 38 с.
- 123 Давыдов Ю.Л., Кузьмичев В.В. Средства и системы для защиты периметров объектов. Системы безопасности средств связи. 1999. № 2
- 124 Введенский Б.С. Системы охраны периметров на выставке.//Спец. техника 2000. № 4, № 5; 2001, № 3, 4
- 125 Петровский Н.П., Пинчук Г.Н. Периметровые технические средства обнаружения нарушителей; особенности выбора. Системы безопасности средств связи. 2000 - № 1
- 126 Отчет по ЗАО. НПЦ. "Барьер-3". Исследование способов преодоления типовых физических барьеров с использованием специальных и слесарных инструментов, взрывчатых веществ и гранатометов. М. 2001.
- 127 Карпов В.Е., Закревский П.Ф. Менеджмент безопасности, (2 т., теория и практика). Кировоград. 2007- 750 с.
- 128 Карпов В.Е. Наука совершенствования. Кировоград. 2008 - 450 с.
- 129 Закревский П.Ф. Электронные книги:
- 130 Карпов В.Е. Аффiliation и власть. Кировоград. 2006 – 240 с.
- 131 Карпов В.Е. Воспитание самосознания. Кировоград. 2007 – 420 с.
- 132 С.К.Деликатный. Основы профессиональной и психологической подготовки сотрудников личной охраны. 1998. 136. В.Кабачный. Индустрия безопасности. К. 2003.
- 133 В.П.Мак-Мак. Служба безопасности предприятия. К. 2004.
- 134 А.И.Белоусов. Как защитить себя и свой бизнес. Кир-д. 2002. – 104 с.
- 135 Э.И. Низенко. Обеспечение безопасности предпринимательской деятельности. К. 2003. – 125 с.
- 136 Р.Н.Макаров. Человек в измерении XX века. Многотомное издание. 1-8 т. М. 2000-2008.

Для заметок

Для заметок

Для заметок

Для заметок

Научно-популярное издание

Карпов В.Е. Закревский П.Ф.

СЛУЖБА БЕЗОПАСНОСТИ

Учебно-практическое пособие в 2 томах

1 том:

**“Служба безопасности —
залог успеха предпринимательства”**

Рецензент: **Н.А.Свирень**, академик, кандидат технических наук,
профессор.

Здано в набор: 10.03.2008 г. Подп. к печати 14.04.2007 г.

Формат 60х84 1/16. Бумага офсетная. Печать офсетная.

Гарнитура Times New Roman CYR. Авт. лист. 19,7. Усл. печ. лист. 17,9

Тираж 1000