**Лекция №1**

**Система информационной безопасности**

План:

Система информационной безопасности

Необходимость системы информационной безопасности

Состояние системы информационной безопасности в России

Понятие "*Система информационной безопасности*" складывается из трех терминов – *система*, *информация* и *безопасность*. Следовательно, для правильного восприятия и понимания того, чем является "*Система информационной безопасности*", необходимо дать определение и пояснение каждому термину.

 *Система* – *это набор устремленных к достижению общих целей и функционирующих как единое целое, взаимосвязанных элементов или частей.*

 В сфере информационной безопасности этими элементами или составными частями будут:

1) специальные организации или подразделения в составе организации (далее просто организации), осуществляющие деятельность в сфере информационной безопасности;
*Примечание 1:* Под понятием "*специальные организации*" будем понимать такие структуры, как *службы безопасности* различных предприятий и фирм. Но проблема безопасности существует и для более крупных организаций, в том числе и для государства.
 2) средства, используемые этими организациями в своей деятельности; мероприятия, проводимые этими организациями в рамках своей деятельности;
методы, применяемые этими организациями при проведении мероприятий.
 В различных сферах деятельности человек пользуется различными определениями понятия информации, в сфере информационной безопасности в России на сегодняшний день используется определение данное в Законе РФ "Об информации, информатизации и защите информации".

*Информация – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления.*

*Безопасность* – *это состояние защищенности* (отсутствие опасности, "без опасности") *от внутренних и внешних угроз жизненно важных интересов:
личности; предприятия; государства.* Здесь мы видим перечень *субъектов защиты*, которыми оперирует понятие безопасность.

*Информационная безопасность – это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств*.

*Цели системы безопасности* *– противодействие внутренним и внешним угрозам жизненно важных интересов субъекта безопасности.*

***Система информационной безопасности*** *– это функционирующая как единое целое совокупность организаций, используемых этими организациями в своей деятельности средств, проводимых ими в рамках своей деятельности мероприятий, и применяемых ими при проведении мероприятий методов, устремленная на ликвидацию внутренних и внешних угроз жизненно важным интересам субъекта безопасности, создание, поддержание и развитие состояния защищенности его информационной среды.*

**Необходимость системы информационной безопасности.**

Информация становится более важным ресурсом, чем материальные или энергетические ресурсы. Ресурсами, как известно, называют элементы экономического потенциала, которыми располагает общество, и которые при необходимости могут быть использованы для достижения конкретных целей хозяйственной деятельности.. Количество информации определяется по разному, это может быть количество машинописных листов, количество занимаемых на носителе или переданных по каналу связи байт, количество пикселей изображения и так далее. Что же касается информации, полученной человеком, ее количество определяется степенью изменения его знаний в результате получения этой информации. Качество же полученной информации определяется полезностью, обретенных в процессе получения знаний. Себестоимость информации определяется количеством, затраченной на ее производство, энергии (умственных усилий), финансовых и материальных затрат на ее документирование, хранение, обеспечение сохранности, обработку и передачу по каналам связи. Цена информации, как и остальных товаров, складывается из себестоимости и величины прибыли от ее реализации. Реализация информации с извлечением прибыли может происходить в результате следующих действий:продажа информации; материализация произведенной или приобретенной (купленной) информации в продукте или технологии; использование информации в процессе принятия решения. Как видно из вышеизложенного, информация обладает свойствами товара, и, следовательно, как и любой товар она может участвовать в товарообороте и являться объектом права, иметь производителя, собственника, владельца и потребителя. С точки зрения потребителя качество используемой информации позволяет получать дополнительный экономический или моральный эффект. С точки зрения обладателя – сохранение в тайне коммерчески важной информации позволяет успешно конкурировать на рынке производства и сбыта товаров и услуг. Это, естественно, требует определенных действий, направленных на защиту конфиденциальной информации. Собственная информация для производителя представляет значительную ценность, так как нередко получение (создание) такой информации – весьма трудоемкий и дорогостоящий процесс. Очевидно, что ценность информации (реальная или потенциальная) определяется в первую очередь приносимыми доходами.

Особое место отводится информационным ресурсам в условиях рыночной экономики. В конкурентной борьбе широко распространены разнообразные действия, направленные на получение конфиденциальной информации самыми различными способами, вплоть до прямого промышленного шпионажа с использованием современных технических средств разведки. На сегодняшний день примерно 47% охраняемых сведений добывается с помощью технических средств промышленного шпионажа. А в 60% случаев утери лишь 20% имеющейся коммерческой информации приводила к банкротству фирм. Вывод напрашивается сам. Защите информации от неправомерного овладения ею, необходимо отводить весьма значительное место. И здесь не обойтись разовыми мерами, будь то эпизодические мероприятия, частичное использование средств защиты или привлечение некоторых специалистов по защите информации. Необходим четко продуманный, качественно спланированный и профессионально проводимый комплекс мер по защите информации. Необходима грамотно и профессионально отлаженная система информационной защиты. И чем раньше это будет воспринято предпринимателем, бизнесменом, руководителем фирмы, тем дешевле ему обойдется создание системы информационной безопасности. С развитием рыночных отношений в России и перехода от индустриального общества к информационному, цены на услуги по качественной защите информации несоизмеримо возрастут. Ибо основным правилом ХХI века будет правило: кто владеет информацией, тот владеет миром.

**Состояние системы информационной безопасности в России**

Анализ зафиксированных фактов и уголовных дел, связанных с информационной безопасностью, свидетельствует о стремительном росте правонарушений. Промышленный шпионаж, неправомерное овладение и присвоение информации, недобросовестная конкуренция и т.п. уже превратились в реальный фон деятельности как государственных, так и коммерческих структур. Положение можно охарактеризовать, как довольно напряженное, что обусловлено: крайне тяжелой экономической обстановкой в стране, расслоением общества на "очень богатых" и "очень бедных", падением уровня социальной защиты населения; отсутствием должной координации деятельности правоохранительных органов, специальных служб, суда, прокуратуры и негосударственных служб безопасности; сложностью учета правонарушений в информационной сфере; отсутствием необходимого опыта выявления и пресечения новых видов преступлений в области информационных технологий; ухудшением криминогенной обстановки в целом. Всем известен, наверное, случай обнаружения в 1998 году подслушивающего устройства в кабинете главного редактора "Комсомольской правды" или скандал с фирмой "Атолл" в феврале 1999 года, которая будто бы прослушивала разговоры даже членов семьи президента; или ликвидация правоохранительными органами стационарного пункта для осуществления прослушивания сотовых и спутниковых телефонов, а также переговоров своих сотрудников в холдинге "Медиа-МОСТ" в мае 2000 года. Поэтому очень актуальной становится проблема обеспечения информационной безопасной деятельности не только государственного служащего (что у нас всегда было на высоте), но и бизнесмена, предпринимателя, юриста, публичного политика, да и просто достаточно известного в обществе человека. Мировой уровень технического состояния противодействия попыткам нарушения информационной безопасности личности, общества и государства в целом достаточно высок. Однако для практической деятельности необходимо наличие финансовых средств на: подготовку и периодическую переподготовку персонала служб информационной безопасности; закупку и эксплуатацию средств защиты; проведение плановых и единовременных мероприятий по созданию, поддержанию и развитию состояния защищенности информационной сферы субъекта безопасности; развитие и совершенствование существующих методов противодействия попыткам нарушения информационной безопасности и поиск новых методов.
При наличии этих основных условий можно противостоять любым попыткам злоумышленных действий, однако в настоящее время главный акцент в деятельности различного рода служб безопасности коммерческих структур в России делается на силовой подход к проблеме безопасности в целом, делая ставку на мускулы охранников, а не на интеллект и техническую оснащенность. КПД такого подхода имеет низкий уровень, который не соответствует сложившейся криминогенной обстановке международной практике. Представляет интерес сравнение объема финансирования служб безопасности стран Западной Европы и России. Первые расходуют от 15 до 25% годовой прибыли. Анализ средств, расходуемых на содержание служб безопасности коммерческими банками России, не во всех случаях составляет 1% годовой прибыли. При таком финансировании своей безопасности коммерческими структурами, ухудшение криминогенной обстановки в России неизбежно. Это выглядит как откровенная провокация криминальных структур на различного рода правонарушения. В свою очередь ухудшение криминогенной обстановки в России приведет российские коммерческие структуры к необходимости тратить столько же средств на свою безопасность, как и их коллеги на Западе, а в ряде случаев в силу специфики российской криминальной среды, и более.

**Вопросы для самопроверки**

1. Раскройте содержание основных принципов Доктрины ИБ РФ.

2. Перечислите основные направления обеспечения ИБ в мировой практике.

3. Сформулируйте основные задачи обеспечения ИБ РФ.

4. Приведите основные функции государственной системы обеспече­ния ИБ РФ.

5. Сформулируйте задачи обеспечения безопасности функционирова­ния информации в КС.

6. Каковы основные отечественные и зарубежные стандарты в облас­ти ИБ?

7. Какая система называется безопасной, а какая – надежной?

8. Что такое политика безопасности?

**Перечень рекомендуемых учебных изданий, Интернет-ресурсов:**

1. Партыка Т.Л.Информационная безопасность : учебн. пособие для СПО / Т.Л. Партыка, И.И. Попов. – М. : ФОРУМ: ИНФРА-М, 2013
2. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян . – М.: ФОРУМ, 2011. – 256 с.
3. Пшенко А.В. Документационное обеспечение управления. ОИЦ "Академия" 2010
4. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин – М.: ФОРУМ ИНФРА-М, 2014. – 416 с.
5. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
6. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения

# ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)

**Лекции № 2-3**

**Защита информационной собственности**

План:

Охрана государственной тайны

Охрана коммерческой тайны

Охрана банковской тайны

Охрана профессиональной тайны

Охрана служебной тайны

Основные объекты служебной тайны

Охрана персональных данных

Охрана интеллектуальной собственности

Основным направлением по защите информационной собствен­ности является охрана государственной, коммерческой, банков­ской, профессиональной и служебной тайн, персональных дан­ных и интеллектуальной собственности.

**Охрана государственной тайны.** *Государственная тайна –* это защищаемые государством сведения в области его военной, внеш­неполитической, экономической, разведывательной, контрразве­дывательной и оперативно-розыскной деятельности, распростра­нение которых может нанести ущерб безопасности Российской Федерации.

Сведения могут считаться государственной тайной (могут быть засекречены), если:

• они соответствуют перечню сведений, составляющих госу­дарственную тайну, входят в перечень сведений, подлежащих засекречиванию, и отвечают законодательству Российской Феде­рации о государственной тайне (принцип законности);

• целесообразность засекречивания конкретных сведений уста­новлена путем экспертной оценки вероятных экономических и иных последствий, возможности нанесения ущерба безопасности Российской Федерации исходя из баланса жизненно важных ин­тересов государства, общества и личности (принцип обоснован­ности);

• ограничения на распространение этих сведений и на доступ к ним установлены с момента их получения (разработки) или за­благовременно (принцип своевременности);

• компетентные органы и их должностные лица приняли в от­ношении конкретных сведений решение об отнесении их к госу­дарственной тайне и засекречивании и установили в отношении них соответствующий режим правовой охраны и защиты (прин­цип обязательной защиты).

**Охрана коммерческой тайны.** *Коммерческая тайна* – это ин­формация, которая имеет действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам, к которой нет свободного доступа на законном основании и к которой принимаются меры по охране конфиденциальности. Она охраняется при содействии государства.

Основными субъектами права на коммерческую тайну являют­ся обладатели коммерческой тайны, их правопреемники.

*Обладатели коммерческой тайны* – физические (независимо от гражданства) и юридические (коммерческие и некоммерче­ские организации) лица, занимающиеся предпринимательской деятельностью и имеющие монопольное право на информацию, составляющую для них коммерческую тайну.

*Правопреемники –* это физические и юридические лица, ко­торым в силу служебного положения, по договору или на ином законном основании (в том числе по наследству) известна ин­формация, составляющая коммерческую тайную другого лица.

К коммерческой тайне не может быть отнесена информация:

• содержащаяся в учредительных документах;

• содержащаяся в документах, дающих право заниматься пред­принимательской деятельностью (регистрационные удостоверения,

 содержащаяся в годовых отчетах, бухгалтерских балансах, материалах государственных статистических наблюдений и другой годовой бухгалтерской отчетности, включая аудиторские заклю­чения, а также в иных формах, связанных с исчислением и упла­той налогов, обязательных платежей;

• содержащая сведения об оплачиваемой деятельности государст­венных служащих, о задолженности работодателей по выплате заработной платы и другим выплатам социального характера, чис­ленности и кадровом составе работающих;

• содержащаяся в годовых отчетах фондов об использовании имущества;

• о реализации государственной программы приватизации и об условиях приватизации конкретных объектов;

• о размерах имущества и вложенных средствах при приватиза­ции;

• подлежащая раскрытию эмитентом ценных бумаг, профессио­нальным участником рынка ценных бумаг и владельцем ценных бумаг в соответствии с законодательством Российской Федера­ции о ценных бумагах;

• связанная с соблюдением экологического и антимонополь­ного законодательства, обеспечением безопасных условий труда, реализацией продукции, причиняющей вред здоровью населения, другими нарушениями законодательства Российской Федерации, законодательства субъектов Российской Федерации, а также со­держащая данные о размерах причиненных при этом убытков;

• о деятельности благотворительных организаций и иных не­коммерческих организаций, не связанной с предпринимательской деятельностью;

• о наличии свободных рабочих мест;

• о хранении, использовании или перемещении материалов и использовании технологий, представляющих опасность для жизни и здоровья граждан или окружающей среды;

• о ликвидации юридического лица и о порядке и сроке подачи заявлений или требований его кредиторами;

• для которой определены ограничения по установлению ре­жима коммерческой тайны в соответствии с федеральными зако­нами и принятыми в целях их реализации подзаконными актами.

**Охрана банковской тайны.** *Банковская тайна –* это сведения о банковских операциях по счетам и сделкам в интересах клиентов, счетах и вкладах своих клиентов и корреспондентов, а также све­дения о клиентах и корреспондентах, разглашение которых мо­жет нарушить право последних на неприкосновенность частной жизни.

К основным объектам банковской тайны относятся следующие:

1) *тайна банковского вклада* – сведения о всех видах вкладок клиента в кредитной организации;

2) *тайна частной жизни клиента или корреспондента* – све­дения, составляющие личную, семейную тайну и охраняемые законом как персональные данные этого клиента или коррес­пондента;

3) *тайна банковского счета* – сведения о счетах клиентов и корреспондентов и действиях с ними в кредитной организации (о расчетном, текущем, бюджетном, депозитном, валютном, кор­респондентском и тому подобных счетах, об открытии, о закры­тии, переводе, переоформлении счетов и т.д.);

4) *тайна операций по банковскому счету* – сведения о приня­тии и зачислении поступающих на счет клиента денежных средств, выполнении его распоряжений по перечислению и выдаче соот­ветствующих сумм со счета, а также о проведении других опера­ций и сделок по банковскому счету, предусмотренных договором банковского счета или законом.

**Охрана профессиональной тайны.** *Профессиональная тайна* – защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам держателя или другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.

Информация профессиональной тайны по критериям охрано-способности права может соответствовать следующим требованиям:

• информация не относится к сведениям, составляющим государственную и коммерческую тайну;

• информация стала известной или была доверена лицу лишь в силу исполнения им своих профессиональных обязанностей;

• информация стала известной или была доверена лицу, не состоящему на государственной или муниципальной службе (в противном случае информация считается служебной тайной);

• по федеральному закону имеется запрет на распространение 1-неренной или ставшей известной информации, которое может нанести ущерб правам и законным интересам доверителя.

В соответствии с этими критериями можно выделить следующие *объекты профессиональной тайны.*

I. ***Врачебная тайна*** – информация, содержащая:

• сведения о факте обращения за медицинской помощью, о состоянии здоровья, диагнозе заболевания и иные сведе­ния, полученные при обследовании и лечении гражданина;

• сведения о проведенных искусственном оплодотворении и имплантации эмбриона, а также о личности донора;

• результаты обследования лица, вступающего в брак;

• сведения о доноре и реципиенте при трансплантации ор­ганов и (или) тканей человека;

* сведения о наличии психического расстройства, фактах обращения за психиатрической помощью и лечении в уч­реждении, оказывающем такую помощь, а также иные све­дения о состоянии психического здоровья гражданина;

• иные сведения в медицинских документах гражданина.

2. ***Нотариальная тайна*** – сведения, доверенные нотариусу в связи с совершением нотариальных действий.

3. ***Адвокатская тайна*** – сведения, сообщенные адвокату граж­данином в связи с оказанием ему юридической помощи.

4. ***Тайна связи*** – тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

5. ***Тайна усыновления*** – сведения об усыновлении ребенка, доверенные на законном основании иным лицам, кроме судей, вынесших решение об усыновлении, и должностных лиц, осущест­вляющих государственную регистрацию этого усыновления.

6. ***Тайна страхования*** – сведения о страхователе, застрахован­ном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц, полученные страховщи­ком в результате своей профессиональной деятельности.

7. ***Тайна исповеди*** – сведения, доверенные гражданином свя­щеннослужителю на исповеди.

**Охрана служебной тайны.** *Служебная тайна –* защищаемая по закону конфиденциальная информация, ставшая известной в го­сударственных органах и органах местного самоуправления толь­ко на законных основаниях и в силу исполнения их представите­лями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограни­чен федеральным законом или в силу служебной необходимости.

Служебная тайна является видом конфиденциальной инфор­мации, и право на служебную тайну выступает самостоятельным объектом права. Для осуществления ее правовой охраны принят Закон РФ «О тайне» от 21.07.93 № 5485-1.

**К основным объектам тайны относятся следующие виды ин­формации**:

• *служебная информация о деятельности федеральных государст­венных органов, доступ к которой ограничен федеральным зако­ном в целях защиты государственных интересов*: военная тайна; тайна следствия (данные предварительного расследования либо следствия); судебная тайна (тайна совещания судей, содержание дискуссий и результатов голосования закрытого совещания Кон­ституционного суда РФ, материалы закрытого судебного заседа­ния, тайна совещания присяжных заседателей или в силу служеб­ной необходимости, порядок выработки и принятия решения, организация внутренней работы и т.д.);

• охраноспособная конфиденциальная информация, ставшая известной в силу исполнения служебных обязанностей должностным лицом государственных органов и органов местного само­управления: коммерческая тайна, банковская тайна, профессио­нальная тайна, а также конфиденциальная информация о част­ной жизни лица.

Информация служебной тайны должна отвечать критериям охраноспособности права:

• являться собственной служебной тайной, т.е. должна быть отнесена федеральным законом к служебной информации о де­ятельности государственных органов, доступ к которой ограни­чен по закону или в силу служебной необходимости;

• являться охраноспособной конфиденциальной информацией служебного характера (чужой тайной) другого лица (коммерче­ская тайна, банковская тайна, тайна частной жизни, профессио­нальная тайна);

• не являться государственной тайной и не входить в перечень сведений, доступ к которым не может быть ограничен;

• быть получена представителем государственного органа и орга­на местного самоуправления только в силу исполнения обязанно­стей по службе в случаях и порядке, установленных федеральным законом.

Информация, не отвечающая этим требованиям, не может счи­таться служебной тайной и не подлежит правовой охране. В действу­ющем законодательстве приводится перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения:

• сведения из актов законодательства, устанавливающих правовой статус государственных органов, организаций, общественных объединений, информация о правах, свободах и обязанностях граждан, порядке их реализации;

• сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах; экологическая, гидрометеорологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, производственных объектов, граждан и населения в целом;

• сведения из описаний структур органов исполнительной власти, их функций, направлений и форм деятельности, информация об их адресе и месте расположения;

• информация о порядке рассмотрения и разрешения заявле­ний физических и юридических лиц;

• сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребности населения;

• информация из документов открытых фондов библиотек и архивов, информационных систем организаций, необходимая для реализации прав, свобод и обязанностей граждан.

**Охрана персональных данных.** В Европе для охраны и защиты права на неприкосновенность частной жизни в условиях автома­тизированной обработки личных данных о гражданах более 25 лет назад был введен особый институт правовой охраны личности – институт защиты персональных данных. Более чем в 20 европей­ских государствах приняты национальные законы о персональ­ных данных, в ряде стран введены независимые уполномочен­ные по защите персональных данных, во всех странах Европей­ского Союза с 1998 г. создана единая унифицированная система защиты персональных данных, в том числе в секторе телекомму­никаций.

Объектом правоотношений здесь выступает право на персо­нальные данные – информация (зафиксированная на любом ма­териальном носителе) о конкретном человеке, которая отождест­влена или может быть отождествлена с ним.

*К персональным данным могут быть отнесены сведения, ис­пользование которые без согласия субъекта персональных данных может нанести вред его чести, достоинству, деловой репутации, доброму имени, иным нематериальным благам и имущественным интересам:*

• биографические и опознавательные данные (в том числе об обстоятельствах рождения, усыновления, развода);

• сведения о семейном положении (в том числе о семейных отношениях);

• сведения об имущественном, финансовом положении (кроме случаев, прямо установленных в законе);

• личные характеристики (в том числе о личных привычках и наклонностях);

• сведения о состоянии здоровья.

Субъектами права здесь выступают:

• лица, к которым относятся соответствующие данные, и их наследники;

• держатели персональных данных – органы государственной власти и органы местного самоуправления, юридические и физи­ческие лица, осуществляющие на законных основаниях сбор, хра­нение, передачу, уточнение, блокирование, обезличивание, унич­тожение персональных данных (баз персональных данных).

Для персональных данных и работы с ними предусмотрены следующие правила:

• персональные данные должны быть получены и обработа­ны законным образом на основании действующего законода­тельства;

• данные включаются в базы персональных данных на осно­вании свободного согласия субъекта, выраженного в письмен­ной форме, за исключением случаев, прямо установленных в законе;

• персональные данные должны накапливаться для точно оп­ределенных и законных целей, не использоваться в противоречии с этими целями и не быть избыточными по отношению к ним. Не допускается объединение баз персональных данных, собран­ных держателями в разных целях, для автоматизированной обра­ботки информации;

• персональные данные, предоставляемые держателем, должны быть точными; в случае необходимости они должны обновляться;

• персональные данные должны храниться не дольше, чем это­го требует цель, и подлежать уничтожению по достижении этой цели;

• персональные данные охраняются в режиме конфиденциаль­ной информации, исключающем их случайное или несанкциони­рованное разрушение или случайную утрату, а также несанкци­онированный доступ к данным, их изменение, блокирование или передачу.

• устанавливается специальный правовой режим использования персональных данных лиц, занимающих высшие государственные должности, и кандидатов на эти должности.

**Охрана интеллектуальной собственности.** К числу основных объектов интеллектуальной собственности относятся:

• произведения науки, литературы и искусства;

• результаты исполнительской деятельности артистов, режис­серов, дирижеров;

• результаты творчества;

• звукозаписи и записи изображения;

• передача радио- и телевизионных сигналов;

• изобретения;

• промышленные образцы;

• профессиональные секреты (ноу-хау);

• полезные модели;

• селекционные достижения;

• фирменные наименования и коммерческие обозначения правообладателя;

• товарные знаки и знаки обслуживания;

• наименования мест происхождения товаров;

• другие результаты интеллектуальной деятельности и средства индивидуализации, на которые в соответствии с законом могут признаваться или закрепляться исключительные права.

**Вопросы для самопроверки**

1. Каковы основные предметные направления защиты информации?
2. Что такое государственная тайна?
3. Что такое коммерческая тайна?
4. Что такое служебная тайна?
5. Что такое профессиональная тайна?
6. Что такое персональные данные?
7. Что такое источники права на доступ к информации?
8. Каковы уровни доступа к информации с точки зрения законода­тельства?
9. Что такое информация ограниченного распространения?
10. Каковы виды доступа к информации?
11. В чем может заключаться ответственность за нарушение законода­тельства в информационной сфере?

**Перечень рекомендуемых учебных изданий, Интернет-ресурсов:**

1. Партыка Т.Л.Информационная безопасность : учебн. пособие для СПО / Т.Л. Партыка, И.И. Попов. – М. : ФОРУМ: ИНФРА-М, 2013
2. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян . – М.: ФОРУМ, 2011. – 256 с.
3. Пшенко А.В. Документационное обеспечение управления. ОИЦ "Академия" 2010
4. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин – М.: ФОРУМ ИНФРА-М, 2014. – 416 с.
5. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
6. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения

# ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)

**Лекции № 4-5**

**Информационная безопасность и ее обеспечение**

Информационная безопасность и информационные войны

Система защиты информации

Информационные ресурсы государства

Защищаемая информациия

Принципы засекречивания информации

Рассекречивание информации

Государственная система правового обеспечения защиты информации в Российской Федерации

**Информационная безопасность и информационные войны**

***Информационная безопасность*** определяется способностью государ­ства, общества, личности:

*обеспечивать с определенной вероятностью достаточные и защи­щенные информационные ресурсы и информационные потоки для поддержания своей жизнедеятельности и жизнеспособности, устой­чивого функционирования и развития;*

*противостоять информационным опасностям и угрозам, негативным информационным воздействиям на индивидуальное и общественное сознание и психику людей, а также на компьютерные сети и другие технические источники информации;*

*вырабатывать личностные и групповые навыки и умения безопасного поведения; поддерживать постоянную готовность к адекватным мерам в инфор­мационном противоборстве, кем бы оно ни было навязано.*

*Информационная война* – *действия, принимаемые для достижения информационного превосходства в интересах национальной военной стратегии, осуществляемые путем влияния на информацию и информа­ционные системы противника при одновременной защите собственной информации своих информационных систем*.

**Система защиты информации**

Основная **цель** защиты любой конфиденциальной информации со­стоит в том, *чтобы предотвратить незаконное овладение ею конкурента­ми или злоумышленниками.*

Зарубежный опыт в области защиты интеллектуальной собственно­сти и отечественный опыт в защите государственных секретов показыва­ет, что эффективной может быть только ***комплексная защита***, сочетаю­щая в себе такие направления защиты, как *правовая,* ***организационная*** *и инженерно-техническая*.

Комплексный характер защиты информации проистекает из ком­плексных действий злоумышленников, стремящихся любыми средствами добыть важную для конкурентной борьбы информацию. Здесь правомер­но утверждение, что *оружие защиты должно быть адекватно оружию на­падения.*

Что касается подходов к реализации защитных мероприятий по обес­печению безопасности информационных систем, то сложилась трехэтапная разработка таких мер.

Первая стадия – *выработка требований* – включает: определение состава средств информационной системы (ИС); анализ уязвимых элементов ИС; оценка угроз (выявление проблем, которые могут возникнуть из-за наличия уязвимых элементов); анализ риска (прогнозирование возможных последствий, которые могут вызвать эти проблемы).

Вторая стадия – *определение способов защиты* – включает ответы на следующие вопросы: какие угрозы должны быть устранены и в какой мере? какие ресурсы системы должны быть защищаемы и в какой степени? с помощью каких средств должна быть реализована защита? какова должна быть полная стоимость реализации защиты и затраты на эксплуатацию с учетом потенциальных угроз?

Третья стадия – *определение функций, процедур и средств безопас­ности, реализуемых в виде некоторых механизмов защиты*.

*Система защиты* информации должна быть представлена как нечто целое. *Целостность системы* будет выражаться в наличии единой цели ее функционирования, информационных связей между элемента­ми системы, иерархичности построения подсистемы управления системой защиты информации. *Система защиты информации должна обеспечивать безопасность информации, средств информации, защиту интересов участников информационных отношений и невозможность несанкционированного доступа злоумышленника к защищаемой информации.* Система защиты информации в целом, применяемые методы и средства защиты должны быть по возможности *прозрачными для закон­ного пользователя*, не создавать ему больших дополнительных не­ удобств, связанных с процедурами доступа к информации.

Система защиты информации должна обеспечивать оценку угроз внешних дестабилизирующих факторов и защиту от них.

**Информационные ресурсы государства**

***Организационное обеспечение ИБ*** представляет собою *сово­купность решений, законов, нормативов, регламентирующих как общую организацию работ по обеспечению ИБ, так и создание и функциониро­вание систем защиты информации на конкретных объектах*.

Основные функции организационно-правовой базы следующие:

 – Разработка основных принципов отнесения сведений, имеющих конфиденциальный характер, к защищаемой информации.

 – Определение системы органов и должностных лиц, ответственных за обеспечение ИБ в стране и порядка регулирования деятельности предприятия и организации в этой области.

 – Создание полного комплекса нормативно-правовых руководящих и методических материалов (документов), регламентирующих вопросы обеспечения ИБ как в стране в целом, так и на конкретном объекте.

– Определение мер ответственности за нарушения правил защиты.

– Определение порядка разрешения спорных и конфликтных ситуаций по вопросам защиты информации.

Созданием зако­нодательной базы в области ИБ каждое государство стремится защитить свои информационные ресурсы. Информационные ресурсы государства *в самом первом приближении* могут быть разделены на три большие группы:

* *информацию открытую* – на распространение и использование кото­рой не имеется никаких ограничений;
* *информацию запатентованную* – охраняется внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности;
* *информацию, «защищаемую» ее собственником, владельцем с по­мощью отработанных механизмов защиты государственной, коммер­ческой или другой охраняемой тайны*; к этому виду относят обычно информацию, не известную другим лицам, которая или не может быть запатентована, или умышленно не патентуется с целью избежания или уменьшения риска завладения ее соперниками, конкурентами.

**Защищаемая информация**

Защищают и охраняют, как правило, не всю или не всякую информа­цию, а наиболее важную, ценную для собственника, ограничение распро­странения которой приносит ему какую-то пользу или прибыль, возмож­ность эффективно решать стоящие перед ним задачи.

Какую информацию относят к защищаемой?

Во-первых, **секретную информацию**. *К секретной информации в на­стоящее время принято относить сведения, содержащие государственную тайну*.

Во-вторых, **конфиденциальную информацию**. *К этому виду защи­щаемой информации относят обычно сведения, содержащие коммерче­скую тайну, а также тайну, касающуюся личной (неслужебной) жизни и деятельности граждан*.

Таким образом, под ***защищаемой информацией*** *понимают сведения, на использование и распространение которых введены ограничения их собственником и характеризуемые понятием «тайна».*

Применительно к органам государственной власти и управления под ***тайной*** *понимается то, что скрывается от других, что известно опреде­ленному кругу людей. Иначе говоря, те сведения, которые не подлежат разглашению, и составляют тайну.*

Основное направление использования этого понятия – *засекречива­ние государством определенных сведений, сокрытие которых от сопер­ников, потенциального противника дает ему возможность успешно ре­шать жизненно важные вопросы в области обороны страны, политиче­ских, научно-технических и иных проблем с меньшими затратами сил и средств.*

К подобному же ввиду тайны относится *засекречивание предприяти­ем, фирмой сведений, которые помогают ему эффективно решать задачи производства и выгодной реализации продукции.*

Сюда же примыкают и *тайны личной жизни граждан, обычно гаран­тируемые государством: тайна переписки, врачебная тайна, тайна денеж­ного вклада в банке и др. Классификацию информации с точки зрения ее владельца можно представить в виде таблицы.* Цветом выде­лена та информация, защита которой обеспечивается государством

|  |  |
| --- | --- |
| *Владелец*  | **Вид информации** |
|  | **Защищаемая** | **Запатентованная** |  |
|  | *Секретная*  | *Конфиден­циальная*  | *Патент*  | *Авторское право*  | *Открытая*  |
| Личность  |  | Личная тайна. Персо­нальные данные  | Патент физиче­ского лица  | Авторское право физическо­го лица  |  |
| Общество  |  | Коммерче­ская тайна  | Патент юридиче­ского лица  | Авторское право юридиче­ского лица  |  |
| Госу­дарство  | Государст­венная тайна  | Служеб­ные сведения  | Государст­венный патент  |  |  |

Защищают и охраняют, как правило, не всю или не всякую информа­цию, а наиболее важную, ценную для собственника, ограничение распро­странения которой приносит ему какую-то пользу или прибыль, возмож­ность эффективно решать стоящие перед ним задачи. При этом различа­ют ***признаки защищаемой информации***:

* засекречивать информацию, т. е. ограничивать к ней доступ, может только ее собственник (владелец) или уполномоченные им на то лица;
* чем важнее для собственника информация, тем тщательнее он ее за­щищает; а для того чтобы все, кто сталкивается с этой защищаемой информацией, знали, что одну информацию необходимо оберегать более тщательно, чем другую, собственник определяет ей различную степень секретности;
* защищаемая информация должна приносить определенную пользу ее собственнику и оправдывать затрачиваемые на ее защиту силы и средства;
* секретная информация обладает определенным генетическим свой­ством: если эта информация является основанием для создания новой информации (документов, изделий и т. п.), то созданная на этой ос­нове информация является, как правило, секретной.

*Отличительным признаком защищаемой информации является то, что засекречивать ее может только ее собственник (владелец) или упол­номоченные им на то лица*.

**Владельцами** (собственниками) **защищаемой информации** могут быть:

* государство и его структуры (органы); в этом случае к ней относятся сведения, являющиеся государственной, служебной тайной, иные ви­ды защищаемой информации, принадлежащей государству или ведомству; в их числе могут быть и сведения, являющиеся коммерче­ской тайной;
* предприятия, товарищества, акционерные общества (в том числе
и совместные) и другие – информация является их собственностью
и составляет коммерческую тайну;
* общественные организации – как правило, партийная тайна, не исключена также государственная и коммерческая тайна;
* граждане государства (их права – тайна переписки, телефонных и телеграфных разговоров, врачебная тайна, персональные данные и др. – гарантируются государством, личные тайны – их личное дело; следует отметить, что государство не несет ответственности за сохран­ность личных тайн).

Понятие «***государственная тайна***» является одним из важнейших в системе защиты государственных секретов в любой стране. От ее пра­вильного определения зависит и политика руководства в области защиты секретов.

Определение этого понятия дано в Законе РФ «О государственной тайне»: «***Государственная тайна*** *– защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведыва­тельной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ*».

Модель определения государственных секретов обычно включает в себя следующие существенные признаки:

– Предметы, явления, события, области деятельности, составляющие государственную тайну.

– Противник (данный или потенциальный), от которого в основном осуществляется защита государственной тайны.

– Указание в законе, перечне, инструкции сведений, составляющих го­сударственную тайну.

– Наносимый ущерб обороне, внешней политике, экономике, научно-техническому прогрессу страны и т. п. в случае разглашения (утеч­ки) сведений, составляющих государственную тайну.

Какие сведения могут быть отнесены к государственной тайне, опреде­лено в Указе Президента РФ от 30.11.1995 г. № 1203. К ним отнесены сведения (указаны лишь разделы): *в областях военной, внешнеполитиче­ской и внешнеэкономической, экономической, научной, разведыватель­ной, контрразведывательной и оперативно-розыскной деятельности.*

*Нельзя* засекречивать информацию как имеющую статус государст­венной тайны:

если ее утечка (разглашение и т. п.) не влечет ущерба национальной безопасности страны; в нарушение действующих законов; если сокрытие информации будет нарушать конституционные и за­конодательные права граждан; для сокрытия деятельности, наносящей ущерб окружающей природ­ной среде, угрожающей жизни и здоровью граждан. Подробнее этот перечень содержится в ст. 7 Закона РФ «О государственной тайне».

Какие же используются критерии для отнесения сведений, во-первых, к государственной тайне, во-вторых, к той или иной степени секретности?

Ответ на этот вопрос дают *Правила отнесения сведений*, составляю­щих государственную тайну, к различным степеням секретности, указан­ные в постановлении Правительства РФ № 870 от 04.09.1995 г.

К сведениям ***особой важности*** следует относить сведения, распро­странение которых может нанести ущерб интересам РФ в одной или не­скольких областях.

К ***совершенно секретным сведениям*** следует относить сведения, рас­пространение которых может нанести ущерб интересам министерства (ведомства) или отраслям экономики РФ в одной или нескольких облас­тях.

К ***секретным сведениям*** следует относить все иные из числа сведе­ний, составляющих государственную тайну. Ущерб может быть нанесен интересам предприятия, учреждения или организации.

Как видно из изложенного, разница между тремя степенями секрет­ности зависит от величины ущерба.

Понятие, виды и размер ущерба разработаны пока еще недостаточно и, видимо, будут отличны для каждого конкретного объекта защиты – со­держания сведений, составляющих государственную тайну, сущности отраженных в ней фактов, событий, явлений действительности. В зави­симости от вида, содержания и размеров ущерба можно выделить *группы некоторых видов ущерба при утечке* (или возможной утечке) *сведений, составляющих государственную тайну.*

1) Политический ущерб может наступить при утечке сведений полити­ческого и внешнеполитического характера, о разведывательной деятель­ности спецслужб государства и др. Политический ущерб может выра­жаться в том, что в результате утечки информации могут произойти серь­езные изменения в международной обстановке не в пользу РФ, утрата страной политических приоритетов в каких-то областях, ухудшение от­ношений с какой-либо страной или группой стран и т. д.

2) Экономический ущерб может наступить при утечке сведений любого содержания: политического, экономического, военного, научно-техничес­кого и т. д. Экономический ущерб может быть выражен, прежде всего, в денежном исчислении. Экономические потери от утечки информации могут быть прямыми и косвенными.

Так, *прямые потери* могут наступить в результате утечки секретной информации о системах вооружения, обороны страны, которые в резуль­тате этого практически потеряли или утратили свою эффективность и требуют крупных затрат на их замену или переналадку.

*Косвенные потери* чаще всего выражаются в виде размера упущен­ной выгоды: срыв переговоров с иностранными фирмами, о выгодных сделках с которыми ранее была договоренность; утрата приоритета в на­учном исследовании, в результате соперник быстрее довел свои исследо­вания до завершения и запатентовал их и т. д.

3) Моральный ущерб, как правило, неимущественного характера насту­пает от утечки информации, вызвавшей или инициировавшей противо­правную государству пропагандистскую кампанию, подрывающую репу­тацию страны, приведшую к выдворению из каких-то государств наших дипломатов, разведчиков, действовавших под дипломатическим прикры­тием, и т. п.

*Проблема засекречивания информации и определения степени сек­ретности сведений, документов, изделий и работ является одной из стержневых во всей деятельности по защите информации*. Она имеет большое государственное значение, определяет методологию и методику защиты информации, объем работ по ее защите и другие обстоятельства, связанные с деятельностью государственных органов, предприятий и ор­ганизаций в этой области. Правила засекречивания информации определяют, в конечном счете, политику государства в области защиты секретов. Этим и объясняется, что перечни сведений, составляющих государствен­ную тайну, утверждаются у нас в стране на самом высоком уровне, в них находит отражение концепция руководства страны в области защиты го­сударственных секретов.

Засекречивать информацию имеют право органы власти, управления и должностные лица, наделенные соответствующими полномочиями. Они осуществляют политику государства в области защиты информации; определяют категории сведений, подлежащих защите и, следова­тельно, засекречиванию, и закрепляют это в законодательных актах;

разрабатывают перечни сведений, подлежащих засекречиванию; определяют степени секретности документов, изделий, работ и сведений и проставляют на носителях защищаемой информации соот­ветствующие грифы секретности.

Таким образом, ***засекречивание информации*** – это совокупность ор­ганизационно-правовых мер, регламентированных законами и другими нормативными актами, по введению ограничений на распространение и использование информации в интересах ее собственника (владельца).

**Принципы засекречивания информации**

***Законность*** засекречивания информации. Заключается в осуществлении его строго в рамках действующих законов и других подзакон­ных нормативных актов. Отступление от этого принципа может нанести серьезный ущерб интересам защиты информации, интересам личности, общества и государства, в частности незаконным сокрытием от общества информации, не требующей засекречивания, или утечки важной информации.

***Обоснованность*** засекречивания информации. Заключается в уста­новлении путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических или иных последствий этого акта, исходя из баланса жизненно важных интересов личности, общества и государства. Неоправданно засекречивать ин­формацию, вероятность раскрытия которой превышает возможность сохранения ее в тайне.

***Своевременность*** засекречивания информации. Заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

***Подчиненность*** ведомственных мероприятий по засекречиванию информации общегосударственным интересам. Это в первую очередь относится к области защиты государственной тайны. Что каса­ется коммерческой тайны, то предприятия наделены нравами засек­речивания информации, кроме оговоренных в законе случаев.

В РФ в соответствии с Законом «О государственной тайне» склады­вается в настоящее время следующая форма засекречивания информации.

 Закон определяет категории сведений, отнесенных к государственной тайне, затем президент РФ на основе предложений правительства РФ ут­верждает два перечня:

1. Перечень должностных лиц органов государст­венной власти и управления, наделенных полномочиями по отнесению сведений к государственной тайне.
2. Перечень сведений, отнесенных к государственной тайне – для осуществления единой государственной политики в области засекречивания информации.

Руководители, наделенные полномочиями по засекречиванию ин­формации, утверждают своими приказами перечни сведений, подлежа­щих засекречиванию, в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью. Они же наделяются полномо­чиями распоряжения этими сведениями, пересмотра степени их секрет­ности и рассекречивания.

Предприятия при определении степени (грифа) секретности докумен­тов, изделий, работ по-прежнему будут руководствоваться перечнями сведений, подлежащих засекречиванию. Таким образом, до исполнителей будут доводиться стратегические установки на применение режимных ограничений в конкретных ситуациях. Рассмотренный порядок засекре­чивания сведений представлен на рисунке.

**Порядок засекречивания информации, составляющей государственную** **тайну** 

Степень секретности и конфиденциальности информации, отобра­женной в документах, изделиях и т. д., не остается постоянной. Она обычно уменьшается и, реже (например, документы представляют исто­рическую и иную ценность), может увеличиваться. Степень секретности и конфиденциальности информации периодически должна пересматри­ваться. При этом она может быть увеличена, снижена до фактической или рассекречена вообще.

**Рассекречивание информации**

*Рассекречивание конфиденциальной и секретной информации*, *работ, документов, изделий –* это деятельность предприятий по снятию (частич­ному или полному) ограничений на доступ к ранее засекреченной ин­формации, на доступ к ее носителям, вызываемая требованиями законов и объективными факторами: изменением международной и внутригосу­дарственной обстановки, появлением более совершенных видов опреде­ленной техники, снятием изделий с производства, передачей (продажей) научно-технических решений оборонного характера в народное хозяйст­во, продажей изделия за границу и т. д., а также взятием государством на себя международных обязательств по открытому обмену сведениями, со­ставляющими в РФ государственную тайну. *Информация должна оста­ваться секретной или конфиденциальной до тех пор, пока этого требуют интересы национальной безопасности или конкурентной и коммерческой деятельности предприятия*.

**Принципиальные аспекты рассекречивания информации могут быть изложены**

**в следующих основных положениях**

1. Информация не подлежит засекречиванию, а засекреченная должна быть рассекречена, если это *сделано* *необоснованно и в нарушение действующих законов*, в целях сокрытия нарушений законности в результате неумелого руководства и должностных ошибок, нару­шения конституционных и других законодательных прав граждан.

1. *Информация рассекречивается не позднее сроков, установленных при ее засекречивании*. Ранее этих сроков подлежит рассекречиванию лишь информация, которая попадает под действие взятых РФ на себя международных обязательств по открытому обмену информацией. *Срок засекречивания информации, отнесенной к государственной тайне, не должен превышать 30 лет.* Правом продления сроков засекречивания информации наделяются руководители центральных органов федеральной исполнительной власти, осуществившие отнесение соответствующих сведений к государственной тайне.
2. Информация не подлежит засекречиванию, а засекреченная должна быть рассекречена, если содержащиеся в ней *новые научные, проектные, технологические и т. п. разработки находятся ниже мирового технологического уровня* или достаточно подробно раскрыты в опубликованной зарубежной или в отечественной литературе.
3. Рассекречиванию (разглашению) не подлежат *сведения, затрагивающие личную (неслужебную) жизнь граждан страны*, если на обратное не имеется согласия самих граждан, а в случае их смерти – их ближайших родственников. Иной порядок такого рассекречивания рассматривается через суд.

**Государственная система правового обеспечения защиты информации**

**в Российской Федерации**

*Второй функцией организационно-правового обеспечения информа­ционной безопасности является определение системы органов и должно­стных лиц, ответственных за обеспечение информационной безопасности в стране*. Основой для создания государственной системы организацион­но-правового обеспечения защиты информации является создаваемая в настоящее время ***государственная система защиты информации***, *под которой понимается совокупность федеральных и иных органов управле­ния и взаимоувязанных правовых, организационных и технических мер, осуществляемых на различных уровнях управления и реализации инфор­мационных отношений и направленных на обеспечение безопасности информационных ресурсов*.

**Под информационной безопасностью РФ понимается состояние за­щищенности ее национальных интересов в информационной сфере, оп­ределяющихся совокупностью сбалансированных интересов личности, общества и государства.**

Напомним содержание интересов личности, общества и государства в информационной сфере.

Интересы личности в информационной сфере заключаются в реали­зации конституционных прав человека и гражданина на доступ к инфор­мации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интел­лектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспе­чении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общест­венного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в соз­дании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод чело­века и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверените­та и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного междуна­родного сотрудничества.

На основе национальных интересов РФ в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Основным органом, координирующим действия государственных структур по вопросам защиты информации, является Межведомственная комиссия по защите государственной тайны, созданная Указом Прези­дента РФ № 1108 от 8.11.1995 г. Она действует в рамках Государствен­ной системы защиты информации от утечки по техническим каналам, по­ложение о которой введено в действие постановлением Правительства РФ от 15.09.1993 г. №912-51. В этом постановлении определены структура, задачи и функции, а также организация работ по защите информации применительно к сведениям, составляющим государственную тайну. Ос­новной задачей Государственной системы защиты информации является проведение единой технической политики, организация и координация работ по защите информации в оборонной, экономической, политиче­ской, научно-технической и других сферах деятельности страны.

Общая организация и координация работ в стране по защите инфор­мации, обрабатываемой техническими средствами, осуществляется Фе­деральная служба по техническому и экспортному контролю (ФСТЭК России).

ФСТЭК России является федеральным органом исполнительной вла­сти, осуществляющим реализацию государственной политики, организа­цию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по сле­дующим вопросам в области обеспечения информационной безопасности:

1) обеспечению безопасности информации в системах информацион­ной и телекоммуникационной инфраструктуры, оказывающих сущест­венное влияние на безопасность государства в информационной сфере противодействию иностранным техническим разведкам на территории РФ;

1. обеспечению защиты (не криптографическими методами) инфор­мации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращению ее утечки по техническим каналам, несанкционированного доступа к ней, специ­альных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории РФ;
2. защите информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств.

**Вопросы для самопроверки**

1. Место организационной защиты информации в системе комплексной защиты информации организации (предприятия, учреждения, ведомства).
2. Подходы к реализации защитных мероприятий по обеспечению безопасности информационных систем.
3. Основные функции организационно – правовой базы. Соотношение организационных и правовых методов защиты информации.
4. Защищаемая информация. Виды тайн. Признаки защищаемой информации
5. Государственная тайна в России. Сведения, относимые к государственной тайне.
6. Степени секретности информации, относимой к государственной тайне. Установление и изменение степени секретности сведений, содержащихся в работах, документах и изделиях. Принципы засекречивания информации.
7. Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности. Основания для рассекречивания конфиденциальных сведений, документов и изделий.
8. Засекречивание информации, определение степени ее секретности. Принципы засекречивания информации.
9. Группы видов ущерба при утечке сведений, составляющих государственную тайну.
10. Порядок засекречивания информации, составляющей государственную тайну.
11. Рассекречивание информации. Аспекты рассекречивания информации.

**Перечень рекомендуемых учебных изданий, Интернет-ресурсов:**

1. Партыка Т.Л.Информационная безопасность : учебн. пособие для СПО / Т.Л. Партыка, И.И. Попов. – М. : ФОРУМ: ИНФРА-М, 2013
2. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян . – М.: ФОРУМ, 2011. – 256 с.
3. Пшенко А.В. Документационное обеспечение управления. ОИЦ "Академия" 2010
4. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин – М.: ФОРУМ ИНФРА-М, 2014. – 416 с.
5. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
6. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения

# ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)

Лекции № 6-7

СОСТАВ И СТРУКТУРА СИСТЕМЫ БЕЗОПАСНОСТИ

Структура системы безопасности

Задачи совета безопасности

Объекты безопасности

Система безопасности

Цели системы безопасности

Задачи системы безопасности

Функции системы безопасности

**Структура системы безопасности**

Организационная структура системы безопасности может быть самой разнообразной и зависит от вида конкретного предприятия (банк, фирма), его масштабов, форм собственности и т.п. Созда­вать ее необходимо осознанно и рационально, максимально ис­пользуя опыт специалистов в сфере безопасности бизнеса.

*Структура, численность и состав СБФ определяются реальными потребностями фирмы и степенью конфиденциальности ее инфор­мации*. В зависимости от масштабов и мощности организации ее безопасность и защита информации могут быть обеспечены по-разному: от абонементного обслуживания силами частных охран­ных и детективных структур до развертывания полномасштабной собственной службы и системы безопасности с, развитой структурой и штатной численностью.

***Опорными точками такой структуры являются***:

1) ответственный руководитель системы;

2) совет по безопасности фирмы;

3) служба безопасности фирмы в составе отделов: охраны, ре­жима, кадров, документов с КТ, инженерно-технических средств безопасности и контрразведывательной и информационно-аналити­ческой деятельности;

4) линейные подразделения фирмы, активно участвующие в обеспечении экономической безопасности (кадровое, финансовое, плановое, юридическое, маркетинга и др.).

Решение о создании системы безопасности принимается руково­дством фирмы в соответствии с ее уставом.

*Ответственный руководитель системы безопасности фирмы* – это либо сам директор, либо один из его заместителей. Он должен хорошо знать, что подлежит защите и охране и обладать определенными познаниями в области безопасности.

*Совет по безопасности фирмы* – это коллегиальный орган при руководителе системы безопасности. Совет выполняет консультативные функции, а его предложения носят рекомендательный характер. Все члены совета назначаются директоромиз числа ведущих специалистов, имеющих опыт работы или заинтересованных в обеспечении безопасности.

**Задачи совета безопасности**

**Основными задачами совета являются**:

- оценка и выработка основных направлений деятельности фирмы по обеспечению экономической безопасности;

- разработка перспективных программ совершенствования системы безопасности;

- разработка предложений о содержании и характере взаимодействия с правоохранительными органами, органами местного управления, с соседними СБФ, а также с партнерами, заказчиками, потребителями продукции в целях соблюдения конфиденциальности, установления и поддержания других мер безопасности;

- рассмотрение совместных планов подразделений фирмы по обеспечению безопасности;

- рассмотрение проектов решений о составе, состоянии и деятельности системы безопасности по отчетным периодам.

*В поле зрения совета практически находится**вся сфера деятельности предприятия в целом, рынок товаров и услуг, место данного предприятия на рынке, конкуренты и преступность*.

**В этом плане совет обеспечивает**:

- анализ производственно-технической, коммерческой и административной деятельности;

- анализ информации о рынке и конкурентах, а также партнерах и клиентах (поставщиках и потребителях), определение сведений, подлежащих сбору и накоплению;

- разработку и периодическую корректировку перечня сведений, составляющих коммерческую тайну;

- анализ правильности выполнения работ по присвоению и снятию грифа конфиденциальности (секретности);

- ежегодную оценку обоснованности включения руководителями структурных подразделений своих сотрудников в списки допущенных к конфиденциальным работам и документам.

Таким образом, совет по экономической безопасности является аналитическим центром при руководстве предприятия, нацеленным на выработку стратегии в этой области деятельности. На основе выявления потенциально уязвимых мест в производственном процессе и определенных для защиты сведений, являющихся коммерческой тайной, а также определения тех участников рыночных отношений, которые способны представить или уже представляющих угрозу благополучию предприятия, *совет вырабатывает рекомендации исполнительному органу системы безопасности – службе безопасности предприятия*.

*Служба безопасности фирмы* – самостоятельное структурное подразделение. Она решает задачи по непосредственному обеспечению защиты жизненно важных интересов фирмы в условиях коммерческого и производственного риска, конкурентной борьбы.

В состав службы безопасности фирмы входят:

- отдел охраны и режима;

- отдел кадров;

- отдел специального документооборота;

- отдел инженерно-технической безопасности;

- отдел информационно-аналитической деятельности.

Примерная структура системы безопасности фирмы приведена на рисунке.

Состав, структура, цели и задачи этих подразделений службы безопасности рассматриваются в следующих разделах.

**Объекты безопасности**

*Обеспечение безопасности фирмы* является неотъемлемой составной частью *коммерческой* деятельности. **Состояние безопасности** представляет собой умение и способность противостоять любым попыткам различных структур нанести ущерб фирме и защиту **ее** интересов от внутренних и внешних угроз.

***Объектами безопасности являются***:

• персонал;

• материальные и финансовые средства;

• сведения, составляющие служебную, производственную и коммерческую тайну, а также иная конфиденциальная информация на бумажной, магнитной, оптической основе, информационные массивы и базы данных, программное обеспечение, информативные физические поля различного характера и информационные ресурсы ограниченного доступа;

• средства и системы информатизации (автоматизированные средства и сети), линии телефонной и факсимильной связи, радиосвязь, технические средства передачи, обработки, размножения и отображения информации, вспомогательные технические

средства и системы;

• технические средства и системы охраны и защиты материальных, финансовых и информационных ресурсов.

Зарубежный и отечественный опыт обеспечения безопасности свидетельствует,что для борьбы со всей совокупностью преступных и противоправных действий необходима стройная и целенаправленная организация противодействия злонамеренным и противоправным замыслам.

**Система безопасности**

Основными элементами системы фирмы являются:

• ответственный руководитель системы;

• совет по безопасности;

• служба безопасности (сотрудник по безопасности) – ответственный исполнитель, уполномоченные по безопасности на выделенных объектах;

• руководители линейных подразделений.

Ответственный руководитель системы собственной безопасности – это директор или один из его помощников или заместителей.

*Совет по безопасности* – коллегиальный орган при ответственном руководителе системы безопасности. Совет выполняет консультативную функцию, а его предложения носят рекомендательный характер. Цели и задачи советаизлагаются в Положении о совете по безопасности.

*Служба безопасности* – самостоятельное функциональное направление деятельности фирмы. Структура, численность и состав СБ определяются реальными потребностями и возможностями фирмы.

*Руководители линейных подразделений* участвуют в обеспечении безопасности и несут прямую ответственностьза реализацию мероприятий по безопасности в своих подразделениях.

**Цели системы безопасности**

***Целями системы безопасности являются***:

• защита прав фирмы, ее структурных подразделений и сотрудников;

• сохранение и эффективное использование финансовых, материальных и информационных ресурсов;

• своевременное выявление и устранение угроз, причин и условий, способствующих нанесению ущерба, нарушению нормального функционирования и развития;

• отнесение информации к категории ограниченного доступа (служебной, коммерческой тайнам, иной конфиденциальной информации), к различным уровням уязвимости;

**•** создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций функционирования;

**•** эффективное пресечение посягательств на ресурсы и угроз персоналу на основе комплексного подхода к безопасности;

• создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, для ослабления негативного влияния последствий нарушения безопасности на достижение стратегических целей.

**Задачи системы безопасности**

Основными задачами системы безопасности являются:

**•** обеспечение безопасности функционирования фирмы и ее предпринимательской деятельности и защита конфиденциальной информации;

• организация работы по правовой, организационной и инженерно-технической защите материальных, финансовых и информационных ресурсов;

• организацияспециального делопроизводства, исключающего несанкционированноеполучениеконфиденциальныхсведений**;**

• выявлениеилокализация возможныхканалов разглашения, утечки и несанкционированного доступа к конфиденциальной информации впроцессе повседневной деятельности и в экстремальных ситуациях;

• обеспечение режима безопасности при проведениивсех видов деятельности,включая встречи, переговоры, совещания, связанные сделовым сотрудничествомна национальном и международномуровне**;**

**•** обеспечениеохраны зданий, помещений, оборудования и технических средств обеспечения производственной деятельности;

• обеспечение безопасности персонала;

• информационно-аналитическая деятельность в интересах оценки ситуаций и выявления неправомерных действий злоумышленников и конкурентов.

*Система безопасности действует на**основе следующих организационно-правовых документов*:

• устава;

• положенияосистеме собственной безопасности;

• руководствапо защите конфиденциальной информации;

• инструкции опорядке работы с иностранными специалистами;

• руководства по инженерно-технической защите помещений и технических средств.

**Функции системы безопасности**

Система безопасности выполняет следующие конкретные функции:

• руководит работами по правовому и организационному регулированию безопасности фирмы и ее структурных подразделений;

• участвует в разработке основополагающих документов с целью закрепления в них требований обеспечения безопасности и защиты информации;

• разрабатывает документы, регламентирующие порядок и организацию мер безопасности;

• разрабатывает и осуществляет меры по сохранности информации и сведений конфиденциального характера;

• осуществляет контакты с правоохранительными органами и обмен с ними информацией в установленном порядке в целях выполнения задач, возложенных на СБ в интересах изучения криминогеннойобстановки**;**

• проводит, привлекая соответствующие подразделения, служебные расследования по фактам нарушения требований безопасности, несоблюдения правил охраны средств и имущества, разглашения служебной и коммерческой тайн;

• организует и обеспечивает пропускной и внутриобъектовый режим, осуществляет контроль его соблюдения;

• осуществляет методическое руководство и контроль за безопасностью на объектах и в самостоятельных подразделениях;

• участвует в определении инженерно-технических средств охраны и разрабатывает предложения по их приобретению и установке;

• обеспечивает физическую охрану имущества и материальных ценностей;

• осуществляет выявление и локализацию возможных каналов утечки информации;

• осуществляет контроль за соблюдением требований по защите коммерческой тайны;

• проводит учет и анализ нарушений режимных требований, проводит аттестацию выделенных помещений и осуществляет контроль проводимых в них закрытых мероприятий и работ;

• организует и контролирует работу администратора безопасности локальной сети;

• проводит разработку и осуществляет меры по защите информации при ее обработке средствами вычислительной техники;

• организует обучение и проверку уровня подготовки специалистов и сотрудников по вопросам безопасности;

• участвует в разработке приказов, распоряжений и других документов по вопросам безопасности.

**Вопросы для самопроверки**

1. Структура и состав системы безопасности фирмы.
2. Совет безопасности фирмы и его задачи.
3. Состояние безопасности, объекты безопасности.
4. Система безопасности фирмы. Правовые основы деятельности системы безопасности. Основные задачи системы безопасности.
5. Общие функции системы безопасности.
6. Управление безопасностью.
7. Кризисная группа, цель ее создания.
8. Режимы функционирования системы безопасности.
9. Организация службы безопасности.
10. Персонал организации.
11. Особенности подбора персонала. Оценка кандидатов на должности, связанные с доступом к конфиденциальной информации. Методы проверки кандидатов на должности. Особенности документирования трудовых отношений с персоналом.

**Перечень рекомендуемых учебных изданий, Интернет-ресурсов:**

1. Партыка Т.Л.Информационная безопасность : учебн. пособие для СПО / Т.Л. Партыка, И.И. Попов. – М. : ФОРУМ: ИНФРА-М, 2013
2. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян . – М.: ФОРУМ, 2011. – 256 с.
3. Пшенко А.В. Документационное обеспечение управления. ОИЦ "Академия" 2010
4. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин – М.: ФОРУМ ИНФРА-М, 2014. – 416 с.
5. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
6. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения

# ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)

Лекция № 8

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ

План

Основные понятия

Кризисная группа

Режимы функционирования системы безопасности

**Основные понятия**

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

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

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

Служба безопасности должна быть всегда готова к возникновению критических (кризис­ных) ситуаций, проявляющихся в результате столкновения интере­сов бизнеса и преступного мира.

***Кризисная ситуация*** – *это проявление фактов угроз со стороны отдельных лиц или групп*. Кризисная ситуация может проявляться и развиваться по-разному: *медленно или спонтанно, мгновенно*.

**Кризисная группа**

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

Кризисная группа может быть создана на постоянной основе с непременным включением в число ее членов;

- руководителя фирмы;

- юриста;

- финансиста;

- руководителя службы безопасности.

Руководство кризисной группой может быть возложено на главу фирмы.

**Кризисная группа решает следующие задачи**:

- оценка обстановки;

- принятие неотложных мер по безопасности;

- управление деятельностью фирмы в экстренных условиях;

- обеспечение оперативного взаимодействия с органами право-

порядка.

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

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

- план действий при угрозе взрыва;

- план действий при захвате заложников или похищении сотрудников фирмы;

- план действий при вымогательстве;

- план действий при нападении на помещения фирмы;

- план действий при нападении на инкассаторов.

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

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

**Режимы функционирования системы безопасности**

Рассмотрим возможные режимы функционирования системы безопасности.

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

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

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

2) разработку, корректировку планов и программ обеспечения безопасности;

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

**Режим повышенной готовности –** *это функционирование системы безопасности при наличии угроз, требующих мер по их пресечению*.

Этому режиму свойственно проведение мер по нейтрализации угроз, уточнение и совершенствование планов отражения с учетом особенностей ситуации, повышение готовности сил поддержки.

При этом режиме возможно начало работы группы оперативного управления безопасностью (кризисной группы).

Группа оперативного управления принимает любые необходимые меры по защите фирмы по ходу обеспечения безопасности.

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

4) уточнение и совершенствование планов отражения угроз;

5) повышение готовности сил поддержки;

6) начало работы группы оперативного управления.

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

В этом случае:

7) совет по безопасности начинает работать ежедневно;

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

9) привлекаются силы поддержки и усиления органов внутренних дел.

**РЕЖИМ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ БЕЗОПАСНОСТИ**

7) Совет по безопасности начинает работать ежедневно;

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

9} Привлекаются силы поддержки и усиления органов внутренних дел

ЧРЕЗВЫЧАЙНОГО ПОЛОЖЕНИЯ

ПОВЫШЕННОЙ

ГОТОВНОСТИ

Функционирование при наличии угроз, отражения и уничтожения злоумышленников

Нормальное

функционирование

4) Уточнение и совершенствование планов отражения угроз;

5) Повышение готовности сил поддержки;

6) Начало работы группы оперативного управления безопасностью

1) Прогнозирование, выявление, оценка, предотвращение и нейтрализация всех видов угроз;

2) Разработка, корректировка планов и программ обеспечения безопасности;

3) Подбор, обучение, мониторинг и совершенствование кадров СБ и в среде сотрудников

Функционирование при наличии угроз, требующих их пресечения

Нормальное

функционирование

ПОВСЕДНЕВНЫЙ

**ОБЪЕКТ**

**ЗАЩИТЫ**

Р

Е

Ж

И

М

Ы

**СИСТЕМА**

**БЕЗОПАС-**

**НОСТИ**

**Вопросы для самопроверки**

1. Управление безопасностью.
2. Кризисная ситуация.
3. Кризисная группа, цель ее создания.
4. Антикризисные планы.
5. Режимы функционирования системы безопасности.
6. Организация службы безопасности. Предприятие учредитель. Ликвидация службы безопасности. Персонал службы безопасности.

**Перечень рекомендуемых учебных изданий, Интернет-ресурсов:**

1. Партыка Т.Л.Информационная безопасность : учебн. пособие для СПО / Т.Л. Партыка, И.И. Попов. – М. : ФОРУМ: ИНФРА-М, 2013
2. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян . – М.: ФОРУМ, 2011. – 256 с.
3. Пшенко А.В. Документационное обеспечение управления. ОИЦ "Академия" 2010
4. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин – М.: ФОРУМ ИНФРА-М, 2014. – 416 с.
5. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
6. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения

# ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)

**Лекции № 9-10**

**ЛИЦЕНЗИРОВАНИЕ ДЕЯТЕЛЬНОСТИ**

План:

Лицензия

Органы, уполномоченные на ведение лицензионной деятельности

Документы необходимые для получения лицензии

Выдача лицензий

Переоформление лицензии

Основание для отказа в выдаче лицензии

Организация и порядок проведения специальных экспертиз предприятий

**Лицензия**

В соответствии с Законом Российской Федерации "О государственной тайне" и в целях установления порядка допуска предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, Правительство Российской Федерации постановляет:

1. Утвердить Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны (прилагается).

2. Установить, что размер платы за рассмотрение заявлений о выдаче лицензий на проведение работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, составляет 10 минимальных размеров оплаты труда. Суммы, полученные от рассмотрения заявления и выдачи лицензии, поступают в федеральный бюджет, за счет средств которого содержится орган, уполномоченный на ведение лицензионной деятельности.

3. Федеральной службе безопасности Российской Федерации, Государственной технической комиссии при Президенте Российской Федерации, Федеральному агентству правительственной связи и информации при Президенте Российской Федерации, Службе внешней разведки Российской Федерации совместно с заинтересованными министерствами и ведомствами Российской Федерации в 3-месячный срок разработать комплекс мер организационного, материально-технического и иного характера, необходимых для осуществления лицензирования деятельности предприятий, организаций и учреждений по проведению работ, связанных с использованием сведений, составляющих государственную тайну.

***Лицензия*** *является официальным документом, который разрешает осуществление на определенных условиях конкретного вида деятельности в течение установленного срока. Лицензия действительна на всей территории Российской Федерации, а также в учреждениях Российской Федерации, находящихся за границей.*

**Органы, уполномоченные на ведение лицензионной деятельности**

Органами, уполномоченными на ведение лицензионной деятельности, являются:

по допуску предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну, – *Федеральная служба безопасности Российской Федерации и ее территориальные органы* (*на территории Российской Федерации), Служба внешней разведки Российской Федерации (за рубежом*);

на право проведения работ, связанных с созданием средств защиты информации, – *Федеральная служба по техническому и экспортному контролю и ее территориальные органы, Служба внешней разведки Российской Федерации, Министерство обороны Российской Федерации, Федеральная служба безопасности Российской Федерации (в пределах их компетенции*);

на право осуществления мероприятий и (или) оказания услуг в области защиты государственной тайны – *Федеральная служба безопасности Российской Федерации и ее территориальные органы, Федеральная служба по техническому и экспортному контролю и ее территориальные органы, Служба внешней разведки Российской Федерации (в пределах их компетенции*).

Лицензирование деятельности предприятий ФСБ, Минобороны РФ, Федеральной пограничной службы РФ, Службы внешней разведки РФ, ФС по техническому и экспортному контролю по допуску к проведению работ, связанных с использованием сведений, составляющих государственную тайну, *осуществляется руководителями министерств и ведомств Российской Федерации, которым подчинены указанные предприятия.*

*На орган, уполномоченный на ведение лицензионной деятельности, возлагается*:

* организация лицензирования деятельности предприятий;
* организация и проведение специальных экспертиз предприятий;
* рассмотрение заявлений предприятий о выдаче лицензий;
* принятие решений о выдаче или об отказе в выдаче лицензий;
* выдача лицензий;
* принятие решений о приостановлении действия лицензии или о ее аннулировании;
* разработка нормативно-методических документов по вопросам лицензирования;
* привлечение в случае необходимости представителей министерств и ведомств Российской Федерации для проведения специальных экспертиз;
* ведение реестра выданных, приостановленных и аннулированных лицензий.

Работа органов, уполномоченных на ведение лицензионной деятельности, координируется Межведомственной комиссией по защите государственной тайны.

**Документы необходимые для получения лицензии**

***Для получения лицензии*** заявитель представляет в соответствующий орган, уполномоченный на ведение лицензионной деятельности:

**а)** заявление о выдаче лицензии с указанием:

наименования и организационно-правовой формы, юридического адреса предприятия, номера его расчетного счета в банке;

вида деятельности, на осуществление которого должна быть выдана лицензия;

срока действия лицензии;

**б)** копии учредительных документов (с предъявлением оригиналов, в случае если копии не заверены нотариусом);

**в)** копию документа, подтверждающего факт внесения записи о юридическом лице в Единый государственный реестр юридических лиц;

**г)** копии документов, подтверждающих право собственности, право полного хозяйственного ведения и (или) договора аренды на имущество, необходимое для ведения заявленного вида деятельности;

**д)** справку о постановке на учет в налоговом органе;

**е)** документ, подтверждающий оплату рассмотрения заявления.

Заявитель несет ответственность за достоверность представляемых им сведений.

Все документы, представленные для получения лицензии, регистрируются органом, уполномоченным на ведение лицензионной деятельности.

**Выдача лицензий**

 ***В лицензии указываются:***

* наименование органа, ее выдавшего;
* наименование и юридический адрес предприятия, ее получившего;
* вид деятельности, на осуществление которого выдана лицензия;
* условия осуществления данного вида деятельности;
* срок действия лицензии;
* ее регистрационный номер и дата выдачи.
* Срок действия лицензии устанавливается в зависимости от специфики вида деятельности, но не может быть менее трех и более пяти лет.
* По просьбе заявителя лицензии могут выдаваться на срок менее трех лет.
* Продление срока действия лицензии производится в порядке, установленном для ее получения.

На каждый вид деятельности выдается отдельная лицензия. В случае если лицензируемый вид деятельности осуществляется на нескольких территориально обособленных объектах, лицензиату одновременно с лицензией выдаются заверенные копии с указанием местоположения каждого объекта. Копии лицензий регистрируются органом, уполномоченным на ведение лицензионной деятельности. Предприятие может иметь лицензии на несколько видов деятельности.

Лицензии оформляются на бланках, имеющих степень защиты, соответствующую степени защиты ценной бумаги на предъявителя.

Бланки лицензий являются документами строгой отчетности, имеют учетную серию и номер. Приобретение, учет и хранение бланков лицензий возлагается на органы, уполномоченные на ведение лицензионной деятельности.

Лицензия выдается после представления заявителем документа, подтверждающего ее оплату, размер которой равен стоимости бланка лицензии.

Лицензия подписывается руководителем (заместителем руководителя) органа, уполномоченного на ведение лицензионной деятельности, и заверяется печатью этого органа. Копия лицензии хранится в органе, уполномоченном на ведение лицензионной деятельности.

Передача лицензии другому юридическому лицу запрещена.

***Орган***, уполномоченный на ведение лицензионной деятельности, ***принимает решение о выдаче*** или об отказе в выдаче лицензии в течение 30 дней со дня получения заявления со всеми необходимыми документами.

*Лицензии выдаются на основании результатов специальных экспертиз предприятий и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну (далее именуются – руководители предприятий), и при выполнении следующих условий*:

соблюдение требований законодательных и иных нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;

* наличие в структуре предприятия подразделения по защите государственной тайны и необходимого числа специально подготовленных сотрудников для работы по защите информации, уровень квалификации которых достаточен для обеспечения защиты государственной тайны;
* наличие на предприятии средств защиты информации, имеющих сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

В случае реорганизации предприятия, получившего лицензию, изменения его местонахождения или наименования, утраты им лицензии оно обязано в 15-дневный срок подать заявление о переоформлении лицензии.

**Переоформление лицензии**

*Переоформление лицензии производится в порядке, установленном для ее получения*.

До переоформления лицензии лицензиат осуществляет деятельность на основании ранее выданной лицензии или временного разрешения, выдаваемого органом, уполномоченным на ведение лицензионной деятельности, в случае утраты лицензии.

***Орган, уполномоченный на ведение лицензионной деятельности, вправе отказать в выдаче лицензии***. Письменное уведомление об отказе в выдаче лицензии с указанием причин отказа направляется заявителю в 3-дневный срок после принятия соответствующего решения.

**Основание для отказа в выдаче лицензии**

*Основанием для отказа в выдаче лицензии является*:

* наличие в документах, представленных заявителем, недостоверной или искаженной информации;
* отрицательное заключение экспертизы, установившей несоответствие необходимым для осуществления заявленного вида деятельности условиям;
* отрицательное заключение по результатам государственной аттестации руководителя предприятия.

*Специальная экспертиза предприятия проводится путем проверки выполнения требований нормативно-методических документов по режиму секретности, противодействию иностранным техническим разведкам и защите информации от утечки по техническим каналам, а также соблюдения других условий, необходимых для получения лицензии*.

Государственными органами, ответственными за организацию и проведение специальных экспертиз предприятий, являются ФСБ РФ, ФС по техническому и экспортному контролю, Служба внешней разведки РФ, Минобороны РФ, другие министерства и ведомства РФ, руководители которых наделены полномочиями по отнесению к государственной тайне сведений в отношении подведомственных им предприятий.

**Организация и порядок проведения специальных экспертиз предприятий**

*Организация и порядок проведения специальных экспертиз предприятий определяются инструкциями,* которые разрабатываются указанными государственными органами и согласовываются с Межведомственной комиссией.

Для проведения специальных экспертиз эти государственные органы могут создавать аттестационные центры, которые получают лицензии в соответствии с требованиями настоящего Положения.

*Специальные экспертизы аттестационных центров проводят* ФСБ РФ, ФС по техническому и экспортному контролю, Служба внешней разведки РФ, Минобороны РФ и их органы на местах (в пределах их компетенции).

Специальные экспертизы проводятся на основе договора между предприятием и органом, проводящим специальную экспертизу. Расходы по проведению специальных экспертиз относятся на счет предприятия.

***Органы, уполномоченные на ведение лицензионной деятельности, приостанавливают действие лицензии или аннулируют ее в случае***:

* предоставления лицензиатом соответствующего заявления;
* обнаружения недостоверных данных в документах, представленных для получения лицензии;
* нарушения лицензиатом условий действия лицензии;
* невыполнения лицензиатом предписаний или распоряжений государственных органов или приостановления этими государственными органами деятельности предприятия в соответствии с законодательством Российской Федерации;
* ликвидации предприятия.

Решение о приостановлении, возобновлении и аннулировании лицензии принимается органом, выдавшим лицензию.

Орган, уполномоченный на ведение лицензионной деятельности, в 3-дневный срок со дня принятия решения о приостановлении действия лицензии или о ее аннулировании в письменной форме уведомляет об этом лицензиата и органы Государственной налоговой службы РФ. Действие лицензии приостанавливается со дня получения лицензиатом указанного уведомления.

После уведомления владельца лицензии о ее аннулировании она подлежит возврату в 10-дневный срок в орган, ее выдавший.

**Вопросы для самопроверки**

1. Порядок лицензирования деятельности предприятий, учреждений по проведению работ, связанных с использованием сведений, составляющих гостайну.
2. Организация и проведение специальных экспертиз предприятий.
3. Порядок рассмотрения заявлений предприятий о выдаче лицензии.
4. Документы необходимые для выдачи лицензий.
5. Основания для отказа выдачи лицензии.
6. Приостановление действия лицензии или ее аннулирование.
7. Организация и порядок проведения специальных экспертиз предприятий

**Перечень рекомендуемых учебных изданий, Интернет-ресурсов:**

1. Партыка Т.Л.Информационная безопасность : учебн. пособие для СПО / Т.Л. Партыка, И.И. Попов. – М. : ФОРУМ: ИНФРА-М, 2013
2. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян . – М.: ФОРУМ, 2011. – 256 с.
3. Пшенко А.В. Документационное обеспечение управления. ОИЦ "Академия" 2010
4. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин – М.: ФОРУМ ИНФРА-М, 2014. – 416 с.
5. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
6. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
7. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)

# Лекция № 11-12

# Организация и создание службы безопасности

План:

Правовой статус службы безопасности

Учредители службы безопасности

Ликвидация службы безопасности

Перечень возможных действий службы безопасности

Примерный вариант Устава службы безопасности

Основные разделы Устава службы безопасности

**Правовой статус службы безопасности**

*Правовой статус службы безопасности предприятия имеет ряд особенностей, которые выделяют его из других форм охранной деятельности.* Знание этих особенностей имеет не только научное, но и практическое значение.

*Прежде всего, обращает на себя внимание 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).

Предприятие-учредитель представляет в органы внутренних дел (по месту своего нахождения) следующие документы:

* заявление о согласовании Устава службы безопасности;
* Устав службы безопасности;
* лицензии на руководителя и персонал службы безопасности;
* сведения о характере и направлениях деятельности службы безопасности, составе и предполагаемой численности персонала, наличии специальных средств, технических и иных средств, а также потребности в них и оружии.

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 охранную деятельность происходит параллельно.

**Учредители службы безопасности**

**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.

**Ликвидация службы безопасности**

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

**Перечень возможных действий службы безопасности**

*Важнейшей особенностью любой службы безопасности является обязательное наличие в ее структуре как детективных, так и охранных подразделений*.

Можно рекомендовать при определении соотношения детективных и охранных подразделений внутри службы безопасности использовать следующие критерии:

* наличие коммерческой тайны;
* состояние, структура и динамика правонарушений на предприятии;
* наличие значительных материальных ценностей, и валюты;
* реальная и потенциальная сумма нанесенного предприятию ущерба;
* имеющиеся факты промышленного шпионажа;
* реальность угроз физической расправы над сотрудниками предприятия со стороны преступных элементов;
* фактические возможности со стороны местных правоохранительных органов в оказании помощи предприятию в пресечении правонарушений;
* взаимоотношения с конкурентами и соблюдение правил функционирования рыночной экономики;
* степень правовой и иной подготовки сотрудников по вопросам обеспечения безопасности предприятия и т.д.

Следует отметить, что **в** **Законе под персоналом службы безопасности понимаются только те лица, которые в установленном порядке получили лицензии детективов и охранников**.

В то же время статус руководителей службы безопасности, выполняющих, прежде всего организационно-управленческие функции, не определен. *Устраняется этот пробел обычно путем разработки должностных инструкций*. Помимо детективов и охранников в службе безопасности работают лица, относящиеся к вспомогательному персоналу (водители, программисты, секретари, машинистки и т.д.). Их статус определяется также должностными инструкциями, а количество – регламентируется существующими нормативами.

*В Законе четко определено, что служба безопасности создается в интересах собственной безопасности учредителя, однако роль службы безопасности в ее обеспечении не определена. Представляется, что служба безопасности предназначена, прежде всего, для организации защиты от всех видов угроз*.

Детализация тех угроз, устранение, пресечение или нейтрализация которых входит в компетенцию службы безопасности, должна найти отражение в ее уставе применительно к основным видам безопасности. **Краткий перечень возможных действий службы безопасности по пресечению, устранению или нейтрализации угроз в рамках основных видов безопасности.**

1. ***Физическая безопасность*** – охрана персонала от насильственных преступлений, предупреждение таких преступлений и т.д.
2. ***Информационная безопасность*** – сохранение коммерческой тайны, борьба с хакерами и т.д.
3. ***Экономическая безопасность*** – охрана имущества предприятия, борьба с экономическим шпионажем и т.д.
4. ***Экологическая безопасность*** – документирование экологических правонарушений, выставление экологических постов и т.д.
5. ***Пожарная безопасность*** – проектирование, монтаж и эксплуатационное обслуживание пожарной сигнализации, выставление постов в местах возможного загорания и пожаров и т.д.
6. ***Техногенная безопасность*** – охрана наиболее опасных участков предприятия от террористов, участие в расследовании техногенных катастроф и т.д.
7. ***Психологическая безопасность*** – информирование персонала предприятия об отсутствии реальных угроз, адекватное реагирование на дезинформационные мероприятия и т.д.
8. ***Научно-техническая безопасность*** – охрана ноу-хау, организация охраны научных лабораторий и т.д.

**Примерный вариант Устава службы безопасности**

Под Уставом понимается правовой акт, определяющий свод правил, регулирующих деятельность организации, её взаимоотношения с другими организациями и гражданами, права и обязанности в определенной сфере её деятельности. Типовой Устав службы безопасности, на основе которого путем их конкретизации создаются индивидуальные Уставы, пока не разработан, хотя их образцы и появились в различных публикациях. *Сложность в разработке устава заключается в том, что в нем должны быть изложены в краткой, но емкой форме, основы жизнедеятельности службы безопасности*.

Рассмотрим ***примерный вариант Устава***.

Прежде всего, в него целесообразно включить следующие разделы:

1. Общие положения
2. Основные задачи
3. Функции
4. Права и обязанности
5. Руководство
6. Взаимоотношения и связи
7. Охранная и детективная деятельность
8. Имущество и средства
9. Контроль, проверка и ревизия деятельности
10. Реорганизация и ликвидация.

**Основные разделы Устава службы безопасности**

**Раздел «Общие положения» содержит**:

* перечень нормативных актов, которыми должны руководствоваться в своей деятельности сотрудники службы безопасности;
* полное наименование и адрес местонахождения предприятия-учредителя;
* название документа, на основании которого создается служба безопасности (протокол, приказ, решение коллегии и т.д.) и дату его учреждения;
* место службы безопасности и его подчиненность в структуре предприятия;
* деятельность службы безопасности, принципы деятельности;
* наличие текущего, расчетного счета;
* порядок финансирования.

*Чрезвычайно большое значение имеет формулирование цели деятельности службы безопасности*, т.к. именно от этого зависит, какие задачи и функции будут поставлены перед ней. Анализ закона, других нормативных актов и литературы позволяет определять цель деятельности службы безопасности как своевременное пресечение (нейтрализацию) противоправных посягательств на экономические интересы и персонал предприятия. Следует при этом учитывать, что цель деятельности службы безопасности определяет руководитель предприятия-учредителя, поэтому возможны и другие его формулировки. Среди принципов деятельности выделим такие как соблюдение законности, эффективность и конфиденциальность, выполнение общепризнанных этических норм, плановость, защита законных интересов учредителя.

**В разделе «Основные задачи»** перечисляются только те задачи, выполнение которых возможно в рамках предоставленной службе безопасности компетенции, и реализация которых приведет к достижению обозначенной цели. {Применительно к приведенной нами выше цели, основные задачи можно сформулировать следующим образом:

* охрана собственности и защита персонала от противоправных посягательств;
* координация действий сотрудников и структур предприятия по вопросам обеспечения безопасности;
* содействие правоохранительным органам и судам по вопросам, затрагивающим интересы предприятия;
* защита от несанкционированного доступа к закрытой информации о персонале и деятельности предприятия;
* сбор, обработка и анализ конфиденциальной информации среди персонала предприятия и в сфере предпринимательства.}

Перечень функций в **третьем разделе «Функции»** составляется с учетом того, что их выполнение позволит реализовать ранее обозначенные основные задачи. Сами ***функции*** можно разделить на группы: ***внешние и внутренние***. **К внешним функциям относятся** те из них, которые названы в Законе **видами предоставляемых услуг**:

* обеспечение порядка в местах проведения предприятием представительских, конфиденциальных и массовых мероприятий;
* консультирование и предоставление рекомендаций руководству и персоналу предприятия по вопросам обеспечения безопасности;
* охрана имущества предприятий;
* защита жизни и здоровья персонала от противоправных посягательств;
* сбор информации для проведения деловых переговоров;
* изучение криминальных аспектов рынка;
* выявление ненадежных деловых партнеров;
* сбор сведений по гражданским делам;
* розыск без вести пропавших сотрудников предприятия;
* выявление некредитоспособных партнеров;
* поиск утраченного имущества предприятия;
* расследование фактов неправомерного использования товарных (фирменных) знаков предприятия;
* сбор информации о лицах, заключавших с предприятием контракты;
* расследование фактов разглашения коммерческой тайны предприятия;
* сбор сведений по уголовным делам;
* установление обстоятельств недобросовестной конкуренции со стороны других предприятий;
* проектирование, монтаж и эксплуатационное обслуживание средств охранно-пожарной сигнализации.

Соотношение между контрразведывательными и разведывательными функциями службы безопасности среди различных предприятий различно, это связано со спецификой их деятельности, финансовыми возможностями и т.д. Что касается разработки внутренних функций, то здесь никаких ограничений не существует.

Можно лишь рекомендовать тот минимум функций, отсутствие которых негативным образом скажется на эффективности деятельности службы безопасности. К ним, в частности, относятся: анализ состояния безопасности предприятия, планирование деятельности по обеспечению этой безопасности, координация деятельности и организация взаимодействия между подразделениями службы безопасности и предприятия, ресурсное (кадровое, финансовое, материально-техническое и т.д.) обеспечение, контроль и проверка деятельности, оценка эффективности деятельности службы безопасности и предприятия по вопросам безопасности. Встречающееся в уставах «дробление» (декомпозиция) этих функций на более мелкие не должно вызывать возражений, хотя более целесообразным следует считать все же их отражение в положениях об отделах (отделениях) охраны и сыска.

**В четвертом разделе «Права и обязанности»** должны быть раздельно ***перечислены права*** и обязанности, присущие службе безопасности в целом. Среди прав следует отметить такие, как:

* внесение предложений руководству и структурным подразделениям предприятия;
* контроль за соблюдением режима безопасности;
* проведение расследований;
* изменение структуры службы безопасности;
* осуществление взаимодействия с правоохранительными и контрольно-надзорными органами;
* распоряжение предоставленными финансовыми средствами по своему усмотрению;
* в некоторых случаях запрета проведения определенных работ;
* самостоятельный набор и увольнение своих сотрудников и т.д.

В дополнение к правам службе безопасности должны быть представлены ***следующие обязанности***:

* выполнение всех функций в рамках действующего законодательства;
* систематическое обучение персонала предприятия и своих сотрудников по вопросам безопасности;
* предоставление установленной отчетности о своей деятельности;
* предотвращение и пресечение правонарушений в рамках своей компетенции и т.д.

При определении прав и обязанностей важно исходить из следующего основополагающего принципа: ***реализация установленных обязанностей возможна лишь при наличии адекватных прав.***

**В разделе «Руководство»** необходимо отразить подчиненность начальника службы безопасности одному из руководителей предприятия, порядок выполнения распоряжений руководителя предприятия-Учредителя, обязанности персонала выполнять указания руководители службы безопасности и процедуру обжалования их неправомерных действий, порядок назначения и освобождения руководителей службы безопасности, перечень основных квалифицированных требований к ним, ответственность и т.д.

В этом же разделе целесообразно определить критерии эффективности деятельности службы безопасности. Представляется, что наиболее ***целесообразно сформулировать их в виде нанесенного*** (по вине их сотрудников) ***или предотвращенного*** (в силу активных действий сотрудников службы безопасности) ***материального ущерба и морального вреда***.

**В разделе «Взаимоотношения и связи»** излагаются процедуры контактов службы безопасности с руководителями и конкретными подразделениями предприятия, правоохранительными, контрольно-надзорными и судебными органами, средствами массовой информации, деловыми партнерами учредителя, депутатским корпусом и т.д.

**Седьмой раздел «Охранная и детективная деятельность»** отражает такие вопросы, как наименования оргструктурных формирований, занимающихся сыскной и охранной деятельностью, методы и средства, применяемые сотрудниками службы безопасности, ограничения в охранной и детективной деятельности, обязательность регулирования деятельности сотрудников службы безопасности внутренними нормативными актами (положения об отделах, должностные инструкции и т.д.), критерии оценки деятельности службы безопасности и т.д.

Перечень необходимых для функционирования службы безопасности мебели, компьютеров, автомашин, средств связи, помещений, спецсредств и оружия, форменного обмундирования и т.д. (без указания потребного их количества) приводится в **разделе «Имущество и средства».** Кроме материально-технических средств в этот перечень ***рекомендуется включить условия и порядок финансирования службы безопасности и её сотрудников, наличие компьютерных программ, специальной литературы и нормативных актов*** и т.д.

Даже если это имущество и средства не могут быть предоставлены в момент создания службы безопасности в полном объеме, их фиксация в Уставе позволит в дальнейшем избежать конфликтов с контрольными органами и создать правовую основу для количественного и качественного улучшения её работы.

Важным представляется **раздел «Контроль, проверка и ревизия деятельности»**, в котором ***определяются субъекты этой деятельности, их правомочия, порядок доступа к документации службы безопасности, место и время хранения контрольных документов, формы и методы устранения выявленных недостатков.***

Наконец, в **десятом разделе «Реорганизация и ликвидация»** фиксируются ***основания и порядок реорганизации и ликвидации службы безопасности, необходимость создания ликвидационной комиссии, сохранения социальных гарантий в отношении увольняемых сотрудников*** и т.д.

Проект Устава службы безопасности подписывается его начальником, утверждается руководителем предприятия-учредителя и представляется на согласование начальнику органа внутренних дел.

**Вопросы для самопроверки**

* 1. Служба безопасности фирмы.
	2. Правовые основы деятельности службы безопасности.
	3. Основные задачи службы безопасности
	4. Общие функции службы безопасности.
	5. Состав службы безопасности.
	6. Основные задачи секторов службы безопасности.
	7. Организация службы безопасности.
	8. Предприятие учредитель.
	9. Ликвидация службы безопасности.
	10. Персонал службы безопасности.
	11. Действия службы безопасности по пресечению, устранению или нейтрализации угроз в рамках основных видов безопасности.
	12. Устав службы безопасности.
	13. Основные разделы устава.

**Перечень рекомендуемых учебных изданий, Интернет-ресурсов:**

1. Партыка Т.Л.Информационная безопасность : учебн. пособие для СПО / Т.Л. Партыка, И.И. Попов. – М. : ФОРУМ: ИНФРА-М, 2013
2. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян . – М.: ФОРУМ, 2011. – 256 с.
3. Пшенко А.В. Документационное обеспечение управления. ОИЦ "Академия" 2010
4. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин – М.: ФОРУМ ИНФРА-М, 2014. – 416 с.
5. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
6. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
7. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)

**Лекция № 13**

**СЛУЖБА БЕЗОПАСНОСТИ**

План:

1. Служба безопасности фирмы. Правовые основы деятельности службы безопасности.

2. Задачи и функции службы безопасности.

3. Принципы и направления взаимодействия СБ с правоохранительными органами.

**1. Служба безопасности фирмы**

Существуют два принципиальных подхода к созданию службы безопасности.

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

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

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

Очень важно, чтобы это был не просто наемный работник, получающий зарплату, а единомышленник, кровно заинтересованный в успехе.

**Правовые основы деятельности службы безопасности**

Правовые основы безопасности фирмы определяют соответствующие положения Конституции Российской Федерации, законы «О безопасности», «О коммерческой деятельности» и другие нормативные акты.

Правовая защита персонала, материальных и экономических интересов от преступных посягательств обеспечивается на основе норм Уголовного и Уголовно-процессуального кодексов, законов Российской Федерации о прокуратуре, о федеральной службе безопасности, о милиции, об оперативно-розыскной деятельности, о частной детективной и охранной деятельности, об оружии и др.

Защиту имущественных и иных материальных интересов и деловой репутации призваны обеспечивать также гражданское, гражданско-процессуальное и арбитражное и арбитражно-процессуальное законодательство.

Обеспечение информационной безопасности регулируется законами Российской Федерации «О государственной тайне», «Об информации, информационных технологиях и о защите информации».

При практическом решении задач обеспечения безопасности коммерческой деятельности необходимо опираться также на следующие правовые нормативные акты:

постановление Правительства РСФСР от 05.12.91 №35 «О перечне сведений, которые не могут составлять коммерческую тайну»;

Существующие правовые условия обеспечения безопасности в основном позволяют государственным и иным правоохранительным и охранным структурам организовывать противодействие противоправным посягательствам на предпринимательскую деятельность в различных ее сферах.

Успешное и эффективное решение задач обеспечения безопасности конкретного предприятия достигается формированием системы внутренних нормативных актов, инструкций, положений, правил, регламентов и функциональных обязанностей сотрудников предприятия и службы безопасности. Требования по правовому обеспечению безопасности предусматриваются во всех структурно-функциональных правовых документах, начиная с Устава коммерческого предприятия и кончая функциональными обязанностями каждого сотрудника.

Что должно быть в организационно-функциональных документах, обеспечивающих правовую базу экономической безопасности и защиты конфиденциальной информации фирмы?

В уставе фирмы в разделе "права и обязанности"

1. Фирма имеет право:

• обеспечивать свою экономическую безопасность, определять состав, объем и порядок защиты конфиденциальной информации;

• требовать от сотрудников обеспечения экономической безопасности и защиты конфиденциальной информации;

• осуществлять контроль за соблюдением мер обеспечения экономической безопасности и защиты конфиденциальной информации.

2. Фирма обязана:

• обеспечить экономическую безопасность и сохранность конфиденциальной информации;

• осуществлять действенный контроль выполнения мер экономической безопасности и защиты конфиденциальной информации.

В разделе "конфиденциальная информация"

Фирма организует защиту своей конфиденциальной информации. Состав и объем сведений конфиденциального характера и порядок их защиты определяются руководителем фирмы.

ВНЕСЕНИЕ ЭТИХ ДОПОЛНЕНИЙ ДАЕТ ПРАВО АДМИНИСТРАЦИИ:

• создавать организационные структуры по защите коммерческой тайны или возлагать эти функции на соответствующих должностных лиц;

• издавать нормативные и распорядительные документы, определяющие порядок выделения сведений, составляющих коммерческую тайну, и механизмы их защиты;

• включать требования по защите коммерческой тайны в договоры по всем видам хозяйственной деятельности (коллективный и совместные со смежниками);

• требовать защиты интересов фирмы перед государственными и судебными органами;

• распоряжаться информацией, являющейся собственностью фирмы, в целях извлечения выгоды и недопущения экономического ущерба коллективу и собственнику средств производства.

В коллективном договоре в разделе "предмет договора"

• Администрация обязуется в целях недопущения нанесения экономического ущерба коллективу обеспечить разработку и осуществление мероприятий по экономической безопасности и защите конфиденциальной информации.

• Трудовой коллектив принимает на себя обязательства по соблюдению установленных на фирме требований по экономической безопасности и защите конфиденциальной информации.

• Администрации учесть требования экономической безопасности и защиты конфиденциальной информации в правилах внутреннего трудового распорядка, в функциональных обязанностях сотрудников и положениях о структурных подразделениях.

В разделе "кадры, обеспечение дисциплины труда"

Администрация обязуется нарушителей требований по экономической безопасности и защите конфиденциальной информации привлекать к ответственности в соответствии с законодательством РФ.

В правилах внутреннего трудового распорядка для рабочих и служащих

В разделе "порядок приема и увольнения рабочих и служащих"

При приеме сотрудника на работу или при переводе его в установленном порядке на другую работу, связанную с конфиденциальной информацией, а также при увольнении администрация обязана:

• проинструктировать сотрудника о правилах экономической безопасности и сохранения конфиденциальной информации;

• оформить письменное обязательство о неразглашении конфиденциальной информации.

Администрация вправе:

• принимать решения об отстранении от работы лиц, нарушающих требования по защите конфиденциальной информации;

• осуществлять контроль за соблюдением мер по защите и неразглашении конфиденциальной информации в пределах предприятия.

В разделе "основные обязанности рабочих и служащих"

Рабочие и служащие обязаны:

• знать и строго соблюдать требования экономической безопасности и защиты конфиденциальной информации;

• дать добровольное письменное обязательство о неразглашении сведений конфиденциального характера;

• бережно относиться к хранению личных и служебных документов и продукции, содержащих сведения конфиденциального характера. В случае их утраты немедленно сообщить об этом администрации.

В разделе "основные обязанности администрации"

Администрация и руководители подразделений обязаны:

• обеспечить строгое соблюдение требований экономической безопасности и защиты конфиденциальной информации;

• последовательно вести организаторскую, экономическую и воспитательную работу, направленную на защиту экономических интересов и конфиденциальной информации;

• включать в положения о подразделениях и должностные инструкции конкретные требования по экономической безопасности и защите конфиденциальной информации;

• неуклонно выполнять требования устава, коллективного договора, трудовых договоров, правил внутреннего трудового распорядка и других хозяйственных и организационных документов в части обеспечения экономической безопасности и защиты конфиденциальной информации.

Администрация, руководители подразделений несут прямую ответственность за организацию и соблюдение мер по экономической безопасности и защите конфиденциальной информации.

В договоре о проведении совместных работ в разделе "условия конфиденциальности"

Стороны обязуются не передавать лицензии лицам и не раскрывать публично сведения о проводимых совместно работах без взаимного согласования. За нарушение данного условия стороны несут финансовую ответственность по возмещению убытков, упущенной выгоды и морального ущерба.

Лица, нарушившие условия конфиденциальности, могут быть привлечены к ответственности в соответствии с действующим законодательством.

**2. Задачи и функции службы безопасности.**

Основные задачи службы безопасности

Основными задачами службы безопасности фирмы являются:

 – обеспечение безопасности производственно-торговой деятельности и защиты информации и сведений, являющихся коммерческой тайной;

- организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите коммерческой тайны;

- организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной;

- предотвращение необоснованного допуска и доступа к сведениям и работам, составляющим коммерческую тайну;

- выявление и локализация возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (аварийных, пожарных и др.) ситуациях;

- обеспечение режима безопасности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания, связанные с деловым сотрудничеством, как на национальном, так и на международном уровне;

- обеспечение охраны зданий, помещений, оборудования, продукции и технических средств обеспечения производственной деятельности;

- обеспечение личной безопасности руководства и ведущих сотрудников и специалистов;

- оценка маркетинговых ситуаций и неправомерных действий злоумышленников и конкурентов.



В своей деятельности служба безопасности руководствуется:

- инструкцией по организации режима и охраны;

- инструкцией по защите коммерческой тайны;

- перечнем сведений, составляющих коммерческую тайну;

- инструкцией по работе с конфиденциальной информацией для руководителей, специалистов и технического персонала;

- инструкцией по организации хранения дел, содержащих конфиденциальную информацию, в архиве;

- инструкцией по инженерно-технической защите информации;

- инструкцией о порядке работы с иностранными представителями и представительствами.

Общие функции службы безопасности:

Служба безопасности фирмы выполняет следующие общие функции:

- организует и обеспечивает пропускной и внутриобъектовый режим в зданиях и помещениях, порядок несения службы охраны, контролирует соблюдение требований режима сотрудниками, смежниками, партнерами и посетителями;

- руководит работами по правовому и организационному регулированию отношений по защите коммерческой тайны;

- участвует в разработке основополагающих документов с целью закрепления в них требований обеспечения безопасности и защиты коммерческой тайны, в частности устава, правил внутреннего трудового распорядка, положений о подразделениях, а также трудовых договоров, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих;

- разрабатывает и осуществляет совместно с другими подразделениями мероприятия по обеспечению работы с документами, содержащими сведения, являющиеся коммерческой тайной, при всех видах работ организует и контролирует выполнение требований инструкции по защите коммерческой тайны;

- изучает все стороны производственной, коммерческой, финансовой и другой деятельности для выявления и закрытия возможных каналов утечки конфиденциальной информации, ведет учет и анализ нарушений режима безопасности, накапливает и анализирует данные о злоумышленных устремлениях конкурентов и других организаций в отношении деятельности фирмы и ее клиентов, партнеров, смежников;

- организует и проводит служебные расследования по фактам разглашения сведений, утрат документов и других нарушений безопасности предприятия;

- разрабатывает, ведет, обновляет и пополняет перечень сведений, составляющих коммерческую тайну и другие нормативные акты, регламентирующие порядок обеспечения безопасности и защиты информации;

- обеспечивает строгое выполнение требований нормативных документов по защите коммерческой тайны;

- осуществляет руководство службами и подразделениями безопасности подведомственных предприятий, организаций, учреждений в части оговоренных в договорах условий по защите коммерческой тайны;

- организует и регулярно проводит учебу сотрудников фирмы и службы безопасности по всем направлениям защиты коммерческой тайны, добиваясь, чтобы к охране коммерческих секретов был глубоко осознанный подход;

- ведет учет сейфов, металлических шкафов, специальных хранилищ и других помещений, в которых разрешено постоянное или временное хранение конфиденциальных документов;

- ведет учет выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации;

- поддерживает контакты с правоохранительными органами и службами безопасности соседних предприятий в интересах изучения криминогенной обстановки в районе (зоне).

**3. Принципы и направления взаимодействия СБ с правоохранительными органами**

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

Организационно-правовой основой такого взаимодействия являются:

конституционные принципы равенства защиты всех форм собственности;

законы Российской Федерации о полиции, об оперативно-розыскной деятельности, о прокуратуре и другие нормативно-правовые акты.

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

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

• обмен информацией:

о фактах (способах) совершения хищений денежных средств с использованием подложных банковских документов, кредитных карточек, подделки иных документов;

о физических лицах, работающих в коммерческих предприятиях, подозреваемых в совершении правонарушений;

• разработка совместных мер противодействия предполагаемым (реальным) фактам общеуголовных проявлений, угрозам убийства, либо нанесения тяжких телесных повреждений, уничтожения имущества, руководителей, сотрудников и членов их семей по технической укрепленности и оборудованию средствами сигнализации объектов; по созданию так называемой «горячей линии» с территориальным органом внутренних дел (милицией);

• участия в формировании централизованного, регионального банка данных о предприятиях различных форм собственности, недобросовестных участниках деловых отношений;

• работа по подбору, расстановке и профессиональной подготовке кадров служб безопасности: осуществление совместной проверки кандидатур на работу в службу безопасности с использованием информационных возможностей органов внутренних дел, сведений о судимости и т. д.;

• проведение совместной разработки и введение правил об ответственности персонала за противоправное использование либо разглашение коммерческой тайны;

• использование помощи полиции в обучении и повышении квалификации кадров службы безопасности.

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

- недостатком сил и средств СБ;

- ограниченностью источников информации о криминальной обстановке и особенностях деятельности организованной преступности;

- сложностью охраны транспортных перевозок материальных ценностей и финансовых средств на значительные расстояния;

- необходимостью получения информации о новых сотрудниках фирмы и СБ;

- необходимостью привлечения органов правопорядка к отражению нападения и оказания содействия в поимке и задержании преступников и злоумышленников.

**Вопросы для самопроверки**

1. Служба безопасности фирмы.
2. Правовые основы деятельности службы безопасности.
3. Основные задачи службы безопасности
4. Общие функции службы безопасности.
5. Состав службы безопасности.
6. Что должно быть в организационно-функциональных документах, обеспечивающих правовую базу экономической безопасности и защиты конфиденциальной информации фирмы?

**Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы:**

1. Партыка Т.Л.Информационная безопасность : учебн. пособие для СПО / Т.Л. Партыка, И.И. Попов. – М. : ФОРУМ: ИНФРА-М, 2013
2. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян . – М.: ФОРУМ, 2011. – 256 с.
3. Пшенко А.В. Документационное обеспечение управления. ОИЦ "Академия" 2010
4. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин – М.: ФОРУМ ИНФРА-М, 2014. – 416 с.
5. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
6. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
7. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)

**Лекция №14**

**СТРУКТУРА И ШТАТЫ СЛУЖБЫ БЕЗОПАСНОСТИ.**

План:

1. Состав Службы безопасности фирмы.

2. Структура и штаты службы безопасности.

3. Руководитель службы безопасности.

**1. Состав Службы безопасности фирмы**

Основными принципами обеспечения безопасности предприятия являются следующие:

1. законность, т.е. меры безопасности предприятия разрабатываются на основе соответствующих законов, норм и правил.

2. самостоятельность и ответственность. Служба безопасности предприятия должна располагать всеми необходимыми для своей деятельности средствами и ресурсами при использовании которых должно соблюдаться строгое соответствие затрат и достигнутых результатов.

3. экономическая целесообразность и прибыльность. Эффективность службы можно оценивать величиной потерь, которые эта служба предотвращает.

4. специализация и профессионализм. Кадровый состав подразделений службы должен формироваться по направлениям комплексного обеспечения безопасности предприятия и служба должна быть укомплектована специалистами, которые могли бы обеспечивать безопасность по всем видам защиты.

5. программно – целевое планирование заключается в следующем: деятельность службы осуществляется на основе комплексных программ и разрабатываемых на ее основе планов работ и отдельных мероприятий.

6. взаимодействие и координация. Меры безопасности осуществляются на основе взаимодействия и координации, усилий всех заинтересованных подразделений и работников предприятия, а также установление необходимых связей с внешними организациями.

Направления деятельности службы необходимо реализовывать на различных участках предприятия:

1. производственный – сохранность материальных ценностей, технологий, информационных ресурсов задействованных непосредственно в производственном процессе, безопасность сырья и т.д.

2. коммерческий – оценка партнеров, поставщиков и потребителей, юридическая защита интересов предприятия, защита движения денежных и материальных ценностей и т.д.

3. информационный участок – определение значимости информации, определение объема необходимой информации, порядок ее поступления, использования, передачи, хранения и защиты ее от всех видов и форм проявления угроз безопасности этой информации.

4. кадровый участок – обеспечение необходимыми работниками и специалистами как всего предприятия, так и службы для того, чтоб предприятие могло нормально функционировать.

**Состав службы безопасности**

Служба безопасности является самостоятельной организационной единицей, подчиняющейся непосредственно руководителю предприятия.

Возглавляет службу безопасности начальник службы в должности заместителя руководителя предприятия по безопасности.

*Организационно служба безопасности состоит из следующих структурных единиц:*

* отдела режима и охраны, в составе сектора режима и сектора охраны;
* специального отдела в составе сектора обработки секретных документов и сектора обработки документов с грифом «Коммерческая тайна";
* инженерно-технической группы;
* группы безопасности внешней деятельности.

**Права, обязанности и ответственность сотрудников службы безопасности.**

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

требовать от всех сотрудников предприятия, партнеров, клиентов строгого и неукоснительного выполнения требований нормативных документов или договорных обязательств по защите коммерческой тайны;

вносить предложения по совершенствованию правовых, организационных и инженерно-технических мероприятий по защите коммерческой тайны.

Сотрудники службы безопасности обязаны:

осуществлять контроль за соблюдением «инструкции по защите коммерческой тайны";

докладывать руководству о фактах нарушения требований нормативных документов по защите коммерческой тайны и других действий, могущих привести к утечке конфиденциальной информации или утрате документов или изделий;

не допускать неправомерного ознакомления с документами и материалами с грифом «Коммерческая тайна» посторонних лиц.

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

**2. Структура и штаты службы безопасности**

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

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

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

Сектор охраны:

- охрана помещений и зданий;

- охрана оборудования и имущества;

- охрана сотрудников и мероприятий;

- охрана перевозок.

Сектор режима:

- обеспечение секретности документов;

- обеспечение режима допуска;

- контроль посетителей и транспорта;

- расследование случаев нарушений режима.

Сектор технической защиты:

- выявление технических каналов утечки информации;

- контроль за попытками несанкционированного доступа к информации с помощью техники;

- оборудование фирмы средствами сигнализации и связи;

- оборудование фирмы противопожарными средствами.

Сектор оперативной работы:

- выявление и изучение фирм и преступных сообществ, являющихся потенциальными конкурентами или врагами фирмы;

- учет и анализ попыток проникновения в секреты фирмы, осуществления каких-либо враждебных акций;

- выявление возможных "слабых" мест в деятельности фирмы;

- разработка и осуществление мер противодействия "наездам".

С целью более широкого охвата и качественного исполнения требований защиты коммерческой тайны решением руководства предприятия и службы безопасности могут создаваться отдельные комиссии, решающие определенные контрольно-ревизионные функции на временной или постоянной основе, такие как:

квартальные или годовые комиссии по проверке наличия, состояния и учета документов (материалов, сведений, ценностей);

комиссия по оценке возможностей публикации периодических документов, объявлений, проспектов, интервью и других выступлений в печати, на радио и телевидении, семинарах, симпозиумах, конференциях и т.п.;

периодические проверочные комиссии для проверки знаний и умений выполнять требования нормативных документов по защите коммерческой тайны, а также по оценке эффективности и надежности защитных мероприятий по обеспечению безопасности предприятия.

**3. Руководитель службы безопасности**

Органами управления безопасностью фирмы являются:

- дирекция фирмы – высший орган управления;

- управление службы безопасности – исполнительный орган.

В состав управления, как правило, входят начальник службы безопасности, заместитель начальника службы безопасности и сек­ретарь-инспектор.

**Начальник службы безопасности**

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

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

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

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

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

На время своего отсутствия начальник СБ передает свои права заместителю.

Начальник службы безопасности отвечает за:

- оказание охранных и сыскных услуг в интересах безопасности своей фирмы-учредителя при строгом и точном соблюдении дейст­вующего законодательства Российской Федерации;

- обеспечение сохранности специальных средств, оружия и бое­припасов, приобретенных фирмой;

- качество профессиональной подготовки лиц из состава служ­бы безопасности.

Он обязан:

- руководствоваться в своей деятельности требованиями Закона Российской Федерации "О частной детективной и охранной дея­тельности в Российской Федерации", другими законами и правовы­ми актами Российской Федерации, нормативами устава фирмы и положения о службе безопасности;

- на себя лично и на вверенную ему службу безопасности полу­чить лицензии на право заниматься охранной деятельностью;

- организовать несение службы подчиненными лицами и кон­тролировать ее качество;

- принять незамедлительные меры по обеспечению сохранности вверенного имущества собственника, организовать отражение про­тивоправных посягательств на него, на здоровье и жизнь граждан и личного состава службы безопасности; обо всех таких посяга­тельствах и их последствиях немедленно докладывать своему не­посредственному руководителю;

- обо всех случаях применения огнестрельного оружия личным составом службы немедленно уведомлять органы внутренних дел по месту применения оружия;

- немедленно уведомлять прокурора о всех случаях смерти или причинения телесных повреждений;

- представлять на подпись руководству фирмы договоры с предприятиями и организациями на услуги инкассации, заключае­мые по распоряжению руководства фирмы;

- своевременно организовывать подготовку, переподготовку и повышение квалификации личного состава службы безопасности, используя для этих целей на договорной основе специализирован­ные базы (центры, полигоны, тиры, стрельбища и т. п.) государст­венных либо негосударственных лицензированных учебных (обра­зовательных) учреждений;

- организовывать в порядке, определяемом Министерством внутренних дел Российской Федерации, прохождение периодиче­ской проверки частных охранников и детективов на их пригодность к действиям, связанным с применением специальных средств и ог­нестрельного оружия;

- осуществлять взаимодействие с кадровыми и финансовыми органами фирмы по вопросам исчисления трудового стажа для ра­ботников службы, стажа для начисления пособий по государствен­ному социальному страхованию, обязательности страхования на случай гибели, получения увечья или иного повреждения здоровья в связи с осуществлением охранных действий;

- контролировать сроки действия лицензий на личный состав и службу безопасности, принимать своевременные меры для их про­дления;

- организовать учет и обеспечить надежную сохранность ору­жия, боеприпасов и специальных средств;

- осуществлять контроль за порядком учета, хранения, ношения и перевозки огнестрельного оружия, боеприпасов к нему и специ­альных средств;

- проводить служебное расследование по каждому случаю не­достачи, порчи, излишков специальных средств, огнестрельного оружия и боеприпасов;

- своевременно выполнять налоговые и иные финансовые обя­зательства службы безопасности и контролировать соблюдение аналогичных обязательств личным составом службы;

- предоставлять уполномоченным лицам органов, осуществ­ляющих контроль за деятельностью частных детективных и охран­ных предприятий и служб безопасности, требуемые документы, письменную и (или) устную информацию, необходимую для выпол­нения контрольных функций.

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

**Вопросы для самопроверки**

1. Основные принципы обеспечения безопасности предприятия.
2. Направления деятельности службы безопасности предприятия.
3. Состав службы безопасности.
4. Структурные единицы службы безопасности.
5. Права, обязанности и ответственность сотрудников службы безопасности
6. Структура и штаты службы безопасности.
7. Органы управления безопасностью фирмы.
8. Начальник службы безопасности
9. Ответственность и обязанности начальника.

**Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы:**

1. Партыка Т.Л.Информационная безопасность : учебн. пособие для СПО / Т.Л. Партыка, И.И. Попов. – М. : ФОРУМ: ИНФРА-М, 2013
2. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян . – М.: ФОРУМ, 2011. – 256 с.
3. Пшенко А.В. Документационное обеспечение управления. ОИЦ "Академия" 2010
4. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин – М.: ФОРУМ ИНФРА-М, 2014. – 416 с.
5. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
6. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
7. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)

**Лекции № 15-16**

**Подразделение режима и охраны службы безопасности**

План:

1.Подразделения режима и охраны

2. Пропускной режим.

3. Охранная деятельность

4. Охрана финансовых средств

5. Обеспечение безопасности персонала.

6. Положение о структурном подразделении

**1. Подразделения режима и охраны**

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

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

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

Основными задачами организации режима и охраны являются:

- предупреждение проникновения в служебные помещения, в охраняемые зоны и на территорию объекта посторонних лиц;

- обеспечение порядка вноса (выноса), ввоза (вывоза) материальных ценностей и входа (выхода) сотрудников и клиентов.

Все помещения фирмы в зависимости от назначения и характера совершаемых в них актов, действий или операций разделяются на несколько зон доступности (безопасности), которые учитывают степень важности различных частей объекта с точки зрения возможного ущерба от криминальных угроз. Зоны безопасности располагаются последовательно, от забора на территории объекта до хранилища ценностей и информации, создавая цепь чередующихся препятствий, которые придется преодолевать злоумышленнику.

Требования внутриобъектового режима

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

2. Внутриобъектовый режим предусматривает следующие основные требования:

- установление четкого распорядка рабочего времени;

- строгое соблюдение сотрудниками правил экономической и информационной безопасности, правил противопожарной и противоаварийной безопасности и техники безопасности;

- установление порядка приема и работы с посетителями сторонних организаций;

- оборудование фирмы техническими средствами обеспечения производственной деятельности (связь, автоматизация, охранная и пожарная сигнализация, замки, ограждения и др.);

- порядок сдачи и приема помещений под охрану;

- порядок ведения телефонных, факсовых и телекоммуникационных обменов информацией с соблюдением режима конфиденциальности и экономии.

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

- принимающий специалист накануне делает заявку канцелярии на следующий день с указанием Ф.И.О. прибывающих, их места работы и времени предполагаемого прибытия;

- в день прибытия приглашенных канцелярия фиксирует их прибытие в журнале учета посетителей и приглашает специалиста фирмы;

- специалист встречает прибывших, получает в канцелярии ключи от комнаты переговоров и сопровождает туда посетителей. Запрещается прием представителей сторонних организаций в других помещениях офиса без специального на то разрешения директора или его заместителя;

- в ходе работы необходимо плотно закрывать окна и шторы;

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

**2. Пропускной режим**

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

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

Пропускной режим предусматривает:

- установление определенного порядка допуска на территорию объекта рабочих и служащих данного объекта и посетителей;

- установление определенного порядка вывоза (выноса), ввоза (вноса) продукции и материальных ценностей;

- устройство ограждения, освещения, оборудование контрольно-проходных и проездных пунктов (постов) и бюро пропусков средствами сигнализации, связи и др. необходимой техникой, обеспечивающей осуществление пропускного режима, а также обеспечение их документацией и инвентарем;

- определение круга должностных лиц, имеющих право выдачи и подписи всех видов пропусков;

- оборудование камер хранения личных вещей и площадок для личного автотранспорта,

Организация пропускного режима

Система регулирования доступа в фирму должна предусматривать:

- объективное определение надежности лиц, допускаемых к работе;

- максимальное ограничение количества лиц, допускаемых на объекты фирмы;

- установление для каждого работника (или посетителей) дифференцированного по времени, месту и виду деятельности права доступа на объект;

- четкое определение порядка выдачи разрешений и оформление документов для входа (въезда) на объект;

- определение объемов контрольно-пропускных функций на каждом пропускном и проездном пункте;

- оборудование контрольно-пропускных пунктов (постов) техническими средствами, обеспечивающими достоверный контроль проходящих, объективную регистрацию прохода и предотвращение несанкционированного (в том числе силового) проникновения посторонних лиц;

- высокую подготовленность и защищенность персонала контрольно-пропускных пунктов.

Пропускные документы

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

- удостоверения;

- пропуска.

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

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

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

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

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

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

Временные пропуска с фотографиями на срок до трех месяцев выдаются лицам, работающим временно, или прикомандированным. Временные пропуска без фотографии на срок до одного месяца действуют при предъявлении паспорта (удостоверения личности).

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

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

Разовые и материальные пропуска

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

Материальные пропуска выдаются лицом, ответственным за сохранность материальных средств.

Учет пропускных документов

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

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

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

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

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

- дело с приказами и распоряжениями по пропускному режиму;

- дело с заявками структурных подразделений на удостоверения, постоянные и временные пропуска;

- дело с инструкциями по пропускному режиму и образцами подписей на материальные пропуска;

- дело с актами на уничтожение пропускных документов;

- дело переписки по пропускному режиму;

- книга учета ежедневного расхода бланков разовых пропусков;

- книга учета выдачи удостоверений, постоянных и временных пропусков.

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

**3. Охранная деятельность**

Основными направлениями охранной деятельности СБ являются:

- защита жизни и здоровья граждан;

- охрана имущества собственников, в том числе при его транспортировке;

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

Каждое из указанных направлений имеет свои особенности при обеспечении безопасности конкретного объекта защиты. Объектами охраны выступают:

- стационарные объекты;

- подвижные объекты;

- персонал;

- денежные средства, ценные бумаги и другие ценности.



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

* возможные .способы преступных посягательств на охраняемый объект;
* степень технической укрепленности охраняемого объекта;
* наличие и качество средств охранно-пожарной сигнализации;
* наличие уязвимых мест в технической укрепленности объекта, которые известны только охране и службе безопасности;
* условия местности, на которой расположен охраняемый объект, а также его конструктивные особенности;
* режим и характер работы охраняемого объекта, его технологические характеристики, имеющиеся на объекте материальные и финансовые ценности
* режим охраны объекта;
* количественные и качественные характеристики сил охраны;
* вооруженность и техническая оснащенность охранников, наличие у них автотранспорта, средств связи, сигнализации и Специальных средств

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

Существует несколько видов охраны, в том числе:

- охрана с помощью технических средств – с подключением на пульт централизованного наблюдения и с установкой автоматической сигнализации;

* охрана путем выставления постов (силами отдела охраны или милиции);
* комбинированная охрана.

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

1) встречу гостей, прибывающих на деловой прием;

2) взаимодействие основной охраны и телохранителей приглашенных лиц;

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

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

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

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

7) наблюдение за лицами:

- приходящими на деловую встречу или прием со свертками, портфелями, кейсами и т. п.;

- приносящими на мероприятие аудио- или видеоаппаратуру;

- быстро покинувшими место встречи;

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

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

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

Элементами технической укрепленности стационарных объектов являются:

- инженерно-технические средства защиты периметра объекта, включающие: запретную зону, средства и системы контроля про­никновения в нее, контрольно-следовые полосы и другие системы;

- освещение объектов охраны;

- контрольно-пропускные пункты;

- средства видеонаблюдения;

- средства связи.

**4. Охрана финансовых средств**

В целях безопасности финансовых средств необходимо обеспечить условия их сохранности на всех этапах обращения: получение (сдача) в банке, транспортирование, временное хранение в кассе -выдача (прием). Каждая из этих ситуаций требует специальных знаний и умений, профессионализма и предусмотрительности.

Обеспечение безопасности финансовых средств в фирме

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

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

- быть изолированными от других служебных помещений;

- иметь капитальные стены, прочные перекрытия пола и потолка;

- иметь сейф (металлический шкаф) для хранения денег и ценностей, в обязательном порядке прочно прикрепленный к строительным конструкциям;

- двери, окна, вентиляционные шахты должны быть оборудованы надежными средствами, исключающими проникновение в помещение.

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

Транспортировка денег и ценностей

Особой опасности финансовые средства подвергаются при их перевозке.

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

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

б) обладать улучшенными ходовыми характеристиками;

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

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

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

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

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

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

- захламленные подъездные пути;

- близко прилегающие к маршруту криминогенные объекты;

- темные коридоры;

- неосвещенные дворы;

- проход инкассатора-сборщика через смежные организации, не имеющие отношения к инкассируемому объекту;

- отсутствие удобной стоянки для автомобиля инкассаторов.

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

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

Инкассацию денежных средств осуществляет, как правило, отдел инкассации.

**5. Обеспечение безопасности персонала**

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

- охраны с использованием охранников-телохранителей;

- собственной безопасности лица, включающей физическую готовность к отражению преступных действий, психологическую готовность к восприятию и реагированию на критические условия;

- использования средств собственной безопасности, разрешенных к использованию в личных целях соответствующими законами.

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

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

"СВИДЕТЕЛЬ БУДЕТ ЗАЩИЩЕН!

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

ОТВЕТ: Конечно же, есть. Не так давно было утверждено Положение "О мерах социальной защиты и материального стимулирования граждан, способствовавших раскрытию преступлений, совершенных организованными преступными группами (№ 791-РП).

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

-личная охрана, охрана жилища и имущества;

- выдача в установленном законодательством порядке оружия, специальных средств индивидуальной защиты;

- временное (от месяца до года) помещение в безопасное место;

- обеспечение конфиденциальности сведений о защищаемых лицах в информационных системах;

- перевод на другую работу (службу), изменение места работы или учебы;

- предоставление другого места жительства;

- замена в установленном порядке документов, изменение внешности.

**6. Положение о подразделении режима и охраны**

Состав и функции подразделений службы безопасности определяются соответствующими Положениями.

Положение о структурном подразделении – документ, предназначенный для нормативно-правовой регламентации деятельности каждого структурного подразделения. Положение определяет статус подразделения, отражает его место в составе службы безопасности, показывает его внутреннюю организацию. На основе Положения составляется штатное расписание подразделения, определяется степень ответственности за выполнение возложенных на него задач.

***Подразделения режима и охраны***

Отдел режима и охраны является самостоятельным структурным подразделением службы безопасности и подчиняется начальнику службы безопасности. В своей деятельности отдел руководствуется требованиями «Инструкции по организации режима и охране».

Задачи

Организация и осуществление мер по обеспечению безопасности деятельности и защите сведений, составляющих государственную и коммерческую тайну.

Разработка и совершенствование системы предотвращения несанкционированного допуска и доступа к сведениям, составляющим коммерческую тайну.

Организация и поддержание пропускного и внутри объектного режима.

Организация охраны арестованных по режиму конфиденциальных помещений.

Организация личной охраны руководителей и ведущих сотрудников.

Организация и установление мер физической и технической защиты зданий и помещений.

Организация, разработка и контроль системы безопасности в повседневных и в особых условиях (стихийные бедствия, поломки, аварии, беспорядки и т.п.).

Структура

В составе отдела режима и охраны имеются следующие структурные единицы:

Сектор режима. Сектор охраны.

Функции

В соответствии с основными задачами отдел режима и охраны выполняет следующие функции:

Организует работу по выполнению решений, приказов и распоряжений руководства предприятия по обеспечению защиты коммерческих секретов и обеспечению безопасности деятельности.

Определяет единство действий и организует защиту, безопасность, сохранность документов и ценностей в обычных и особых условиях.

Разрабатывает, обновляет и дополняет инструкции, положения и иные нормативные материалы по режиму и охране.

Осуществляет руководство работой по установлению степени конфиденциальности сведений, содержащихся в документах. Совместно с основными подразделениями проводит работу по анализу практики применения «Перечня сведений, составляющих коммерческую тайну», по подготовке и внесению в него в установленном порядке необходимых изменений и дополнений, а также организует его переработку и переиздание.

Организует разработку и контроль за эффективностью действующей разрешительной системы допуска сотрудников, компаньонов и клиентов к ознакомлению и работе с документами конфиденциального характера, с целью исключения возможности ознакомления со сведениями, не относящимися к выполняемой ими работе.

Разрабатывает и рассматривает совместно со специальным отделом и подразделениями предложения по совершенствованию делопроизводства с грифом «Коммерческая тайна», предотвращению факторов включения в документы секретного и несекретного характера излишнего объема сведений, являющихся коммерческой тайной, сокращению издаваемых и разрабатываемых документов конфиденциального характера, неоправданной из рассылки.

Организует и обеспечивает систему контролируемого доступа и специального пропускного режима в здания и помещения.

Организует, обеспечивает и контролирует выполнение требований внутри объектного режима.

Определяет систему охраны и участвует в ее организации и обеспечении работы выделенных помещений.

Организует разработку тактических принципов использования средств автоматизации, сигнализации, связи и охраны.

Организует охрану, пропускной, допускной и внутри объектный режим и осуществляет оперативно-методическое руководство работами по защите выделенных помещений и информации, обрабатываемой и передаваемой с использованием технических средств.

Осуществляет руководство и режим защиты коммерческих сведений в работе по отбору, хранению и использованию архивных материалов.

Осуществляет методическое руководство и принимает непосредственное участие в проведении предупредительно-профилактической работы с исполнителями работ и документов конфиденциального характера.

Организует проведение служебных расследований по фактам утраты документов конфиденциального характера, разглашения охраняемых сведений, нарушения охраны и пропускного режима, необоснованного ознакомления сотрудников и командированных лиц со сведениями, составляющими государственную и коммерческую тайну и по другим фактам, которые привели или создавали условия, способствующие утечке конфиденциальной информации.

Обеспечивает личную охрану руководства и сотрудников.

Права начальника отдела

На основе единоличия руководит деятельностью отдела режима и охраны по выполнению возложенных на отдел задач и функций.

Назначает проведение проверок состояния и эффективности работы по обеспечению сохранения коммерческих секретов, режима безопасности, охраны и технического ее обеспечения.

Требует от сотрудников представления объяснений по фактам, которые привели или могли привести к утечке информации, составляющей коммерческую тайну.

Ходатайствует о поощрении сотрудников, активно участвующих в работе по предупреждению утечки охраняемых сведений, выполнении требований режима и охраны.

Вопросы для самопроверки

1. Основные задачами организации режима и охраны
2. Требования внутриобъектового режима
3. Пропускной режим
4. Пропускные документы
5. Разовые и материальные пропуска
6. Учет пропускных документов
7. Основные направления охранной деятельности СлБ
8. Факторы, влияющие на выбор приемов и средств охраны
9. Виды режима охраны объекта по времени
10. Охрана финансовых средств
11. Обеспечение безопасности финансовых средств в фирме
12. Транспортировка денег и ценностей
13. Обеспечение безопасности персонала

**Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы:**

1. Партыка Т.Л.Информационная безопасность : учебн. пособие для СПО / Т.Л. Партыка, И.И. Попов. – М. : ФОРУМ: ИНФРА-М, 2013
2. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян . – М.: ФОРУМ, 2011. – 256 с.
3. Пшенко А.В. Документационное обеспечение управления. ОИЦ "Академия" 2010
4. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин – М.: ФОРУМ ИНФРА-М, 2014. – 416 с.
5. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
6. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
7. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)

**Лекция №17-18**

**Кадровая политика**

План:

1. Кадровая политика безопасности

2. Ведение досье на работников

3. Методы получения, сбора и обработки информации для ведения досье

4. Тестирование кандидатов

5. Проверка персонала во время работы

6. Проведение служебного расследования по фактам имущественных преступлений

**1. Кадровая политика безопасности**

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

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

- профессиональная надежность;

- психологическая надежность;

- моральная надежность.

Анализируя оперативные сводки органов внутренних дел о происшествиях и преступлениях против российского бизнеса и ряда ее представителей, можно сделать определенный вывод о хорошей осведомленности преступников, которые тщательно и до последних мелочей изучали все вопросы, связанные с бизнесом конкретной предпринимательской структуры. В этом кроется их высокая «эффективность» при совершении преступлений. Все преступления тщательно планируются. Одним из главных элементов при подготовке преступления является сбор и обработка информации о фирме и ее руководящем составе. В ход идет все: внедрение агентов (шпионов), наружное наблюдение, хищение документов из офиса, фотографирование и видеозапись, перехват информации на каналах внутренней и внешней связи фирмы, изучение внутреннего распорядка и т.д.

В настоящее время весьма эффективным является использование работников фирмы в качестве источников внутренней информации как быстрый, эффективный способ ее получения. Для этих целей используются как рядовые исполнители, так и работники, определяющие топ-менеджмент, влияющий на стратегию и тактику поведения фирмы.

Еще угроза экономической безопасности фирмы со стороны конкурентов с использованием вашего персонала может проявиться:

1) в переманивании работников – носителей конфиденциальной информации;

2) в выдвижении ложных предложений вашим работникам с целью выведывания информации;

3) в применении подкупа работников фирмы;

4) в том, что под видом работника к вам устраивается доверенное лицо конкурентов – агент (шпион);

5) в получении сведений через болтливых родственников.

От того, насколько верно, грамотно и профессионально будут подходить к отбору кадров, зависит исход вашего дела.

Благонадежность и лояльность персонала – один из ключевых моментов, позволяющих любой фирме выжить и преуспеть в современном деловом мире. Вы должны овладеть эффективными и надежными методами проверки на лояльность фирме своих работников, позволяющими сделать правильный и единственно верный выбор из множества кандидатов на вакантное место.

Сразу необходимо подчеркнуть, что решение этой задачи должно органично вписываться в решение других задач, которые составляют и формируют целостную концепцию безопасности фирмы. Только комплексный подход позволяет добиться высокой степени обеспечения экономической безопасности любой коммерческой структуры.

Справедливости ради надо сказать, что среди них встречаются действительно профессионалы своего дела, но обычно все наоборот. Устроенные по блату, как правило, отличаются наихудшей подготовкой. Они чаще всего способны на различного рода нарушения дисциплины и даже на хищения имущества, так как абсолютно уверены в своей безнаказанности. Ведь если провинившегося работника немедленно уволят, то родственника или знакомого уволить просто будет неудобно, поэтому ему многое прощается. Это бомба замедленного действия, они будут вести себя высокомерно, считая, что им многое прощается, так как общие правила на них не распространяются. Как следствие, на фирме формируется атмосфера недовольства.

Нельзя путать друга и партнера, даже если это один человек. Эта заповедь самая сложная для человеческого понимания: на кого же тогда надеяться в бизнесе, как не на друзей?

Но пока все в жизни основывается на личном интересе – от чисто денежного до карьерного роста, нужно навсегда помнить это правило. Необходимо отметить, что большинство людей в повседневной жизни – честные и приличные люди. Однако при изменении внутреннего и внешнего мира возможны нежелательные поступки со стороны этих же людей. Хотя это не всегда справедливо, однако реалии современного бизнеса не позволяют относиться беспечно к таким важным моментам.

Предающими интересы фирмы, как правило, становятся люди:

- с большим самомнением, считающие, что их недооценили по достоинству;

-ставящие свои личные интересы во главу всех возникающих отношений, в том числе и производственных;

- не прощающие ошибок кому бы то ни было;

-авантюристы, готовые ради удовлетворения собственных амбиций «прокопать проход к центру земли».

С точки зрения экономической безопасности психологический профотбор обязан выявить:

- судимости, преступные связи, наклонности;

-предрасположенность кандидата к совершению противоправных действий при определенных обстоятельствах;

- факты, свидетельствующие о морально-психологической неустойчивости кандидата (состоит на учете у нарколога, невропатолога, перенесены тяжелые заболевания и т.д.). Можно потребовать соответствующие справки от кандидатов либо самим выдать направления в поликлиники для прохождения полной диспансеризации.

Получение негативной информации хотя бы по одной вышеперечисленной позиции автоматически освобождает вас от дальнейшей работы с таким кандидатом.

Вы решили нанять определенные категории работников. Как это сделать? Основные пути подбора персонала:

- объявления в газету;

- объявление конкурса на замещение вакантных должностей или мест;

- подбор персонала через кадровое агентство;

- по знакомству, «блату», за деньги.

Каждый из указанных способов имеет свои недостатки и преимущества. Два первых варианта подбора практически хорошо подходят, но важно дозировать информацию при подаче объявления, иначе косвенно можно раскрыть важную информацию.

Идеальный вариант привлечения работников – через кадровое агентство. Однако эти услуги дороже и информация весьма поверхностна, вам придется многое перепроверять, так как агентство не несет ответственности за своего кандидата.

Устройства на работу по знакомству или «блату» необходимо напрочь избегать.

А для того чтобы избежать негативных последствий от будущих работников при проявлении ими нелояльности к фирме и руководителю, мы ниже рассмотрим специальные способы и приемы, позволяющие свести эту проблему к минимуму.

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

- низкая квалификация;

- моральная неудовлетворенность работой;

- вредные привычки и др.

**2. Ведение досье на работников**

Предварительное собеседование с кандидатом может быть реализовано исходя из ваших возможностей и опыта, носить поверхностный или детальный характер. Поверхностный характер при собеседовании применяется в условиях недостатка времени при открытии своего дела, когда наблюдается активный приток кандидатов, которым задается несколько конкретных вопросов.

При детальном подходе число вопросов к кандидату возрастает, узнают мотивацию перехода, профессиональные возможности и личностные особенности.

Для удобства обработки информации и получения результатов с их последующим хранением составляются анкеты.

В процессе беседы можно поинтересоваться о прежнем месте работы для получения нужной информации.

Предварительно необходимо узнать у кандидата о его готовности подписать необходимые внутренние документы, касающиеся сохранения коммерческой тайны (далее – КТ) и других сведений конфиденциального характера. Если кандидат проявляет нерешительность либо категорически отказывается подписывать предложенные документы, то собеседование немедленно прекращается. Каждый раз при приеме на работу нового работника собеседование следует проводить под лозунгом: «В чужой монастырь со своим уставом не ходят», а также «Изначально не нравятся условия работы – не устраивайся».

Если кандидат начинает сообщать коммерческую информацию по предыдущему месту работы, то собеседование приостанавливается на несколько дней и после наведения справок по прежнему месту работы принимается решение о целесообразности продолжения собеседования.

Принимает решение о ведении досье на работников или кандидатов на вакантное место непосредственно руководитель фирмы. Для чего необходимо принять такое решение.

1. Для аргументированного и обоснованного решения вопроса о приеме работника на работу.

2. Для преемственности при организации нового дела.

3. Для составления подробной и полной характеристики на своего работника.

4. Досье – это своеобразный заградительный барьер против неблаговидных действий ваших работников.

5. Оно позволит в сжатые сроки ответить на ряд вопросов, связанных с персоналом для принятия верного решения:

Досье поможет объяснить поведение человека в той или иной ситуации и осуществить действенную профилактику нарушений.

Однако, перед тем как занести соответствующую информацию в досье, вы обязаны обеспечить ее сохранность.

Ответственность за сохранность досье должна быть строго персонифицирована.

Поэтому при составлении и ведении досье следует проявлять особую бдительность и осторожность в отношении статуса информации об объекте и методов ее сбора.

Общие требования при обработке персональных данных работника и гарантии их защиты установлены главой 14 Трудового кодекса Российской Федерации (далее- ТК РФ), которой необходимо руководствоваться при составлении досье в первую очередь.

Нужно провести четкую грань между досье и компроматом. Компромат используется для поиска исключительно негативной информации с последующим использованием для шантажа и психологического давления. Задачи, возлагаемые на досье – это вся информация по конкретному человеку или фирме, полученная законным путем и не запрещенными средствами исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, безопасности бизнеса, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

***Особенности работы с сотрудниками, допущенными к конфиденциальной информации***

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

Основанием для проведения проверки могут служить:

- информация, полученная от правоохранительных органов, органов государственной налоговой службы, судебных органов, организации и предприятий по прежнему месту работы;

- недостоверность или неполнота сведений, полученных от правоохранительных органов.

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

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

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

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

При установлении в ходе проверки обстоятельств, свидетельствующих, что лицо, в отношении которого она проводилась, сообщило о себе неполные или недостоверные сведения либо представило заведомо ложные сведения, администрация вправе отказать лицу в трудоустройстве.

***Порядок ведения личных дел лиц, допущенных к конфиденциальной информации***

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

К личному делу приобщаются заявление о согласии работать на должности с режимом конфиденциальной информации, добровольное согласие (подписка) о неразглашении сведений, отнесенных. предприятием к конфиденциальной информации, личный листок по учету кадров.

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

**3. Методы получения, сбора и обработки информации для ведения досье**

Полученная вами информация по возможности должна быть объективной, корректной и полной. Словом, исследования биографических и иных данных очень важны. Необходимо изучать всю доступную информацию о проверяемых работниках или кандидатах на вакантное место. Проблема расходов должна вами рассматриваться на фоне тех потерь, которые может нанести нелояльный контингент или умышленно неквалифицированный менеджмент. Данные проверок необходимо периодически обновлять, постоянно общаться с лицами, которые находятся с проверяемыми в доверительных отношениях.

Исследование биографических данных следует провести по возможности на прежних (2-3 последних) местах работы. Запросите необходимую информацию в письменном виде с обязательным указанием цели использования запрашиваемой информации и причины. При этом необходимо иметь в виду, что в соответствии со ст. 88 ТК РФ работодатель не вправе сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом. Кроме этого нужно знать, что все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение (ст. 86 ТК РФ). Получите такое согласие. Если работник (кандидат на вакансию) чист, он такое согласие даст, естественно, при хороших условиях труда и достойной оплате. Этим вы обезопасите себя от недобросовестных работников, агентов (шпионов) и претензий за несанкционированный сбор и обработку информации.

Чтобы обеспечить чистоту эксперимента и получения информации о кандидате требуемого качества, при приеме на работу необходимо предъявить к нему ряд требований, что называется, задать ряд начальных условий, при невыполнении или несоблюдении которых следует категорический отказ. Например, должностные инструкции, стиль поведения в компании, отношения с сослуживцами и клиентами, система поощрения, сохранение КТ, недопустимость контактов с сотрудниками фирм-конкурентов и т.д.

Должностная инструкция работника представляет собой документ, который определяет весь круг вопросов, связанных с его трудовой деятельностью в фирме. Юридически грамотно составленная инструкция позволяет определить обязанности, права и ответственность персонала и защитить его от выполнения несвойственных функций, определить систему взаимоотношений между руководителями и подчиненными.

Должностная инструкция содержит:

* полное название должности;
* порядок подчиненности;
* кому можно отдавать распоряжения;
* какие требования предъявляются к работнику;
* цели и функции для указанной должности;
* ответственность, которая предусмотрена должностью;
* оценку труда работника;
* степень доступа к КТ, а также порядок ограничения физического доступа в помещения фирмы, не связанные с исполнением указанных обязанностей.

**4. Тестирование кандидатов**

Существуют разные виды тестирования:

-открытое психологическое тестирование. Позволяет оценить способности кандидата, его возможности и склонности к определенному виду деятельности. Тестов очень много, выбор теста необходимо доверить профессионалу-психологу;

- проверка на детекторе лжи;

- скрытое психологическое тестирование;

-косвенное тестирование (через проявление психических особенностей). Используется эффект проецирования психики человека на его внешние проявления (мимика, интонация голоса, предпочтения в цвете, почерк и т.д.);

- замаскированное тестирование (под видом анкетирования). Важно на этой стадии знакомства с кандидатом провести комплексное психологическое тестирование. Конспективно:

- личностные опросные листы;

- бланковые методики;

- проективные методики;

- использование полиграфа.

Очень интересный результат можно получить при проверке на «детекторе лжи». При этом обследуемый дает письменную расписку о добровольности обследования.

Следует сказать, что отказ от обследования на полиграфе не должен квалифицироваться как свидетельство лживости объекта или его причастности к расследуемому событию.

Полученная оценка носит всегда вероятностный характер, поэтому она не может служить доказательством.

**5. Проверка персонала во время работы**

Мошенничают практически все, только для одних уровень – мелкое воровство, для других – работа на сторону в интересах другой компании. Повсеместно распространено использование телефонных переговоров и автомобильной техники в своих мелкособственнических и корыстных интересах.

Внутрикорпоративному мошенничеству в наибольшей степени подвержены крупные компании и холдинги, имеющие множество разбросанных по стране филиалов. Поиск эффективных мер противодействия этой «болезни» является для фирмы весьма актуальным вопросом.

Средний уровень потерь в розничной торговле от воровства составляет 1-1,5 процента от оборота. От 70 до 90 процентов этих потерь приходится на долю воровства со стороны собственного персонала. Причем тащат продавцы и грузчики, кладовщики и менеджеры, администраторы и кассиры, охранники и управляющие – вне зависимости от успешности торговой точки и вида товара.

Как показывает мировой опыт, латентность совершаемых преступлений на производстве очень высока. Тем не менее, можно свести наносимый ущерб собственными работниками к минимуму, если поощрять работников, которые оказывают помощь при проведении служебных расследований по фактам имущественных преступлений. Ведь обычно практически весь коллектив достаточно хорошо осведомлен обо всех этих негативных проявлениях, однако эти факты не становятся достоянием руководства

Поэтому первейшая задача – постоянно проводить активную политику пропаганды для убеждения персонала в необходимости оказания помощи в этих вопросах. Такого рода сотрудничество должно поощряться по заранее оговоренной схеме, предусматривающей выплату определенного процента от суммы предотвращенного ущерба, который мог бы быть нанесен фирме. Однако это не исключает проверки персонала, которые могут быть:

1) регулярные (по заранее определенному графику);

2) оперативные (носят спонтанный характер, в случае ЧП, разглашения конфиденциальной информации, подозрения в отношении конкретных работников и т.п.).

Проверки могут быть гласными (соблюдение инструкции по сохранности конфиденциальной информации, учет корреспонденции, проведение ревизии) и негласные (втайне от работника).

Наблюдение позволяет выявить поведение человека на работе и дома во время отдыха, праздников, а также его контакты.

*Признаки совершения преступления VIP-персонами*

А) дезорганизация работы фирмы:

- организационная чехарда в совете директоров;

- заключение сомнительных сделок;

- слишком громоздкая организационная структура;

- постоянное участие в судебных разбирательствах;

- постоянное нахождение на грани банкротства;

- зависимость фирмы от продажи продукции нескольким компаниям;

-нет своего подразделения аудита, внешние аудиторские

фирмы постоянно меняются;

Б) чрезмерное отклонение финансовых показателей от ранее существовавших:

- резкое увеличение доходов при уменьшении различного вида запасов, уменьшение оборота по кассе;

-увеличение запасов при уменьшении кредиторской задолженности;

- увеличение числа продаж при увеличении цены за единицу продукции;

- увеличение оборота при сокращении остатков;

-увеличение запасов при уменьшении затрат на обслуживание складской инфраструктуры;

- из квартала в квартал резкие скачки в балансовой отчетности;

- трудности возвращения дебиторской задолженности;

- резкий рост расходов на фоне снижения доходов.

*Признаки преступления, совершаемого наемными работниками*

А) нарушения первичного бухгалтерского учета:

- задержки при осуществлении платежей;

- предоставление копий платежных документов;

-указание искаженных платежных реквизитов заказчиков и получателей платежей;

- большая дебиторская и кредиторская задолженность;

Б) отклонения от средних значений показателей:

- появление недостачи или излишков;

- резкое увеличение остатков и т.д.

Наиболее уязвимые места в бизнесе, позволяющие нечестным работникам использовать служебное положение в корыстных интересах:

- складские операции;

- получение товаров;

- расходование денег, взятых под отчет, и т.д.

*Признаки совершения преступления с участием сторонних организаций:*

- частые смены юристов, участие в судебных процессах;

- частые смены аудиторских фирм;

- постоянные проверки контролирующих органов;

- обслуживание несколькими банками, постоянная их смена;

- зависимость фирмы от полученных кредитов;

- работа с фирмами сомнительного толка без проверки последних и т.д.

**6.** **Проведение служебного расследования по фактам имущественных преступлений**

Основная часть убытков фирмы образуется за счет вполне определенных действий персонала. Причины могут быть разными, но все они порождаются людьми и их отношением к своим служебным обязанностям. Речь идет об умышленном нанесении ущерба экономической безопасности фирмы ее работниками. Причем это может быть инициативное деяние в целях личного обогащения и (или) мести фирме либо по заданию конкурентов, партнеров по бизнесу или криминала. Особенно опасен первый случай.

Первый круг таких людей это те, кто имеет право подписи финансовых документов и материальных пропусков. Ко второму кругу относятся те, кто знает все о финансах фирмы и контролирует материальные ценности.

Чего от них можно ожидать:

-изготовления ложных финансовых документов (контрактов, договоров и т.д.);

- присвоения наличных денег из кассы;

- расходования наличных денег не по назначению;

- фальсификации сумм, находящихся на банковских счетах;

- фальсификации накладных, записей и подписей в счетах, платежных поручениях, бухгалтерских книгах;

- разного рода хищений;

- завышения установленных цен;

- завышения сверхурочных часов;

- оплаты работ и услуг сторонних организаций, которые не выполнялась и т.д.

Самый доступный способ – проведение служебного расследования, которое проводится по письменному распоряжению (приказу) руководителя, в котором четко указывается, кто его проводит и какова его цель, права членов и председателя комиссии. Необходимо однозначно доказать, что данные потери фирма понесла от действий конкретных людей, иначе будут наказаны невиновные.

К человеку, проводящему служебное расследование, предъявляются следующие основные требования – наличие знаний в области права и экономики, а также опыта в проведении подобных расследований. Лучшие результаты достигаются при комплексном привлечении к расследованию работников бухгалтерии, отдела кадров и других специалистов. Достаточно часто как на Западе, так и в России проводятся финансовые расследования (forensic research). По сравнению с обычным аудитом они обладают определенной спецификой и требуют особой методики.

Основные этапы в проведении служебного расследования:

- поиск виновного (виновных);

- выяснение причин совершения преступления;

-выработка предложений по недопущению данного типа преступлений в будущем.

Предлагается следующий алгоритм служебного расследования.

1. Уяснить суть произошедшего: что произошло, какие наступили последствия, выявить причины произошедшего.

2. Осуществить сбор информации: показания свидетелей, сбор информации, имеющей какое-либо отношение к произошедшему.

3. Осуществить анализ собранного материала.

4. Оформить заключение, в котором определить виновного, причины, приведшие к случившемуся, и меры по недопущению подобного в будущем.

Проведение служебного расследования – процесс трудоемкий. Помните, что дотошный юрист-адвокат приложит все усилия, чтобы доказать несостоятельность служебного расследования и выявить массу процессуальных нарушений. В любом случае без аудиторских проверок и дорогостоящих экспертиз вам не обойтись.

Применение полиграфа в ходе служебных разбирательств по фактам, относящимся к имущественным преступлениям, весьма эффективно. Его использование позволяет выявить злоумышленника или, как минимум, сузить круг подозреваемых лиц, снять необоснованные подозрения с честных работников, а также восстановить нормальный психологический климат в коллективе.

**Вопросы для самопроверки**

1. Кадровая политика безопасности
2. Критерии надежности персонала
3. В чем проявляется угроза экономической безопасности фирмы со стороны конкурентов с использованием вашего персонала?
4. Какие люди, как правило, предают интересы фирмы?
5. Основные пути подбора персонала
6. Ведение досье на работников
7. Особенности работы с сотрудниками, допущенными к конфиденциальной информации
8. Порядок ведения личных дел лиц, допущенных к конфиденциальной информации
9. Методы получения, сбора и обработки информации для ведения досье
10. Тестирование кандидатов
11. Виды тестирования
12. Проверка персонала во время работы
13. Признаки совершения преступления VIP-персонами
14. Признаки преступления, совершаемого наемными работниками
15. Проведение служебного расследования по фактам имущественных преступлений

**Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы:**

1. Аскеров Т.М. Защита информации и информационная безопасность: Учебное пособие/Под общей ред. Курбакова К.И. – М.: Рос. экон. академия, 2001.-387 с.
2. Румынина Л.А. Документационное обеспечение управления 2009 ОИЦ "Академия"
3. Организация и современные методы защиты информации / Под общ. ред. С.И. Диева, А.Г .Шаваева. М.: Концерн "Банковский Деловой Центр", 1998. Организация работы с документами: Учеб. / Под ред. проф. В.А. Кудряева. 2-е изд., перераб. и доп. М.: ИНФРА-М, 2007.
4. Аверченков В.И, Рытов М.Ю. «Служба защиты информации: организация и управление». БГТУ, 2005
5. Яскевич В.И. «Секьюрити. Организационные основы безопасности фирмы». М.: Ось-89, 2008
6. Ярочкин В.И. «Система безопасности фирмы». М.: Ось-89, 2003

**Интернет ресурсы:**

* [www.avosp.ru](http://www.avosp.ru/)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)

**Лекция № 19-20**

**СПЕЦИАЛЬНЫЙ ОТДЕЛ**

План:

1. Положение о подразделении Специальный отдел.

3. Механизмы защиты КТ

4. Правила, обеспечивающие сохранность КТ

**1. Положение о подразделении Специальный отдел**

Специальный отдел является самостоятельным структурным подразделением службы безопасности и подчиняется непосредственно начальнику службы.

В своей деятельности отдел руководствуется требованиями «Инструкции по режиму и охране» в части коммерческих секретов.

Задачи

Организация и руководство делопроизводством секретных документов и документов с грифом «Коммерческая тайна».

Структура

Специальный отдел состоит из следующих структурных единиц:

сектор обработки секретных документов;

сектор обработки документов с грифом «Коммерческая тайна";

машинописное бюро оформления специальных документов;

экспедиция.

Функции

Обработка поступающей и отправляемой корреспонденции, доставка ее по назначению.

Осуществление контроля за сроками исполнения документов.

Организация работы по регистрации, учету и хранению документальных материалов текущего пользования.

Разработка номенклатуры дел, осуществление контроля за правильным формированием дел в подразделениях и подготовкой материалов к своевременной сдаче в архив.

Разработка и внедрение предложений по совершенствованию системы делопроизводства.

Печатание и размножение секретных документов и документов с грифом «Коммерческая тайна».

Участие в подготовке созываемых и проводимых руководством закрытых совещаний и организация их технического обслуживания.

Специальный отдел в части обеспечения обработки секретных документов руководствуется соответствующими документами, в части ведения делопроизводства с грифом «Коммерческая тайна» выполняет требование «Инструкции по защите коммерческой тайны».

Права

Требовать от руководителей подразделений и исполнителей четкого и своевременного выполнения нормативных документов по организации и ведению специального делопроизводства.

Регулярно проверять правильность ведения делопроизводства в подразделениях, указывать руководителям подразделений на выявленные недостатки и требовать их устранения.

Возвращать исполнителям документы, оформленные с нарушением установленных правил делопроизводства.

Указания специального отдела в пределах его функций, предусмотренных Положением, являются обязательными к руководству и исполнению подразделениями предприятия.

Ответственность

Всю полноту ответственности за качество и своевременное выполнение возложенных настоящим Положением задач и функций несет заведующий отделом.

Степень ответственности других сотрудников отдела устанавливается должностными инструкциями.

*Эффективная защита обеспечивается при выполнении следующих условий:*

- единство в решении производственных, коммерческих, финансовых и режимных вопросов;

-координация мер безопасности между заинтересованными подразделениями фирмы;

-разработка режимных мер на основе оценки информации и объектов, подлежащих защите (классификации);

- персональная ответственность на всех исполнительских уровнях за обеспечение сохранности конфиденциальной информации;

-организация специального делопроизводства, введение соответствующей маркировки документов;

- разработка и утверждение списка с перечнем лиц, допущенным к такого рода информации;

-наличие охраны, а также пропускного и внутриобъектового режимов.

В обязательном порядке в обязанности работников включаются требования по соблюдению режима КТ (коллективный договор, трудовой договор, правила внутреннего трудового распорядка и иные локальные нормативные акты работодателя).

Итак, с чего начать? Переход от абстрактной к конкретной защите КТ начинается с выявления и анализа наиболее уязвимых мест фирмы. Необходимо также ответить на следующие вопросы:

- какая информация нуждается в защите. Разрабатывается перечень сведений, составляющих КТ.

- кого она может интересовать;

- какое время необходимо хранить КТ. На основании работы комиссии определяется актуальность дальнейшего хранения отдельных положений КТ.

- какие потребуются материальные и финансовые ресурсы для сохранения КТ.

**2. Механизм защиты коммерческой тайны**

В общем виде последовательность действий по введению режима КТ можно представить следующим алгоритмом:

1. Определяется, по каким критериям будет относиться информация к КТ.

2. Выясняется, какие объекты собственности, в том числе интеллектуальной, должны быть защищены.

3. Выбираются методы защиты (патентование, авторское право, коммерческая тайна).

4. Разрабатывается и утверждается перечень сведений, составляющих КТ.

5. Устанавливаются правила допуска и определяются механизмы доступа к сведениям, составляющим КТ.

6. Определяется перечень должностей и оформляется список лиц, имеющих право работать с конкретными объектами КТ.

7. Разрабатываются правила классификации и маркировки документов, а также порядок снятия грифа «Коммерческая тайна».

8. Устанавливается порядок работы с документами (учет, пере­сылка, хранение, размножение, уничтожение и т.д.).

9. Определяется перечень помещений, где разрешена работа с такими документами. Устанавливается порядок проведения закрытых совещаний, прохода на такие совещания.

10. Планируются мероприятия по контролю за проведением всех видов работ с КТ.

11. Проводится обучение руководителей структурных подразделений правилам защиты сведений, относящихся к КТ, оказывается помощь работникам на стадиях оформления документов для последующего их опубликования в открытой печати, использования на выставках и конференциях, в рекламе.

12. Разрабатываются режимные меры приема представителей сторонних организаций, командированных лиц, представителей власти (приложение 2.4).

13. Устанавливается порядок работы на ПЭВМ и система противодействия техническим средствам промышленного шпионажа

14. Для охраны разрабатываются правила охраны офиса, закрытых помещений, осуществления пропускного и внутриобъектового режимов и устанавливаются необходимые технические средства защиты (ТСО).

15. Проводится обучение и допуск работников к работам, связанным с КТ, принимаются у них зачеты. Проводятся служебные расследования по фактам нарушения режима КТ.

Важно подчеркнуть, что установление на фирме режима КТ существенно повышает надежность защиты КТ, снижает вероятность разглашения и утраты носителей этих сведений.

**3. Правила, обеспечивающие сохранность кт**

1. На документах, содержащих сведения, составляющие КТ, проставляется гриф «Коммерческая тайна» с указанием обладателя этой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства), а в документах и изданиях, кроме того, - номера экземпляров.

2. Срок действия КТ, содержащейся в документе, определяется в каждом конкретном случае исполнителем или лицом, подписавшим документ, в виде конкретной даты, или «до заключения контракта», или «бессрочно».

3. Гриф «Коммерческая тайна» с указанием обладателя этой информации 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 оборотной стороне последнего листа каждого экземпляра документа, содержащего КТ, печатается разметка, в которой указывается: количество отпечатанных экземпляров, номер, фамилия исполнителя и его телефон, дата, срок действия КТ, фамилия машинистки.

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

5. Решение комиссии оформляется актом произвольной формы, который утверждается директором или его заместителем по направлению. В акте перечисляются дела, с которых гриф «КТ» снимается. Один экземпляр акта вместе с делами предается в архив.

6. На обложках гриф «Коммерческая тайна» погашается штампом или записью от руки с указанием даты и номера акта, послужившего основанием для его снятия. Аналогичные отметки вносятся в описи и номенклатуры дел.

7. Допуск работников к сведениям утверждается директором или его заместителем по направлению, а также руководителями структурных подразделений.

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

9. Выписки из документов и изданий, содержащие сведения с грифом «Коммерческая тайна», производятся в тетрадях, имеющих такой же гриф.

10. Дела и издания с грифом «Коммерческая тайна» выдаются исполнителям и принимаются от них под расписку в карточке учета выдаваемых дел и изданий.

11. Документы, содержащие сведения, составляющие КТ, подлежат обязательной регистрации в канцелярии службы безопасности или общего делопроизводства подразделения уполномоченным СБ. В тексте документа и его реквизитах дополнительно могут оговариваться права на информацию, ее порядок использования, сроки ограничения на публикацию и т.д.

12. Вся поступающая корреспонденция с грифом «Коммерческая тайна» или другими грифами принимается и вскрывается работниками канцелярии, которым поручена работа с этими материалами. При этом проверяется количество листов и экземпляров документов и изданий, а также наличие указанных в сопроводительном письме приложений. В случае отсутствия в конвертах документов с грифом «Коммерческая тайна» или приложений к ним составляется акт в двух экземплярах, один из которых отправляется отправителю.

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

14. Отпечатанные и подписанные документы с грифом «Коммерческая тайна» вместе с их черновиками и вариантами передаются для регистрации работнику канцелярии, осуществляющему их учет. Черновики и варианты уничтожаются этим работником с подтверждением факта уничтожения записью на копии исходящего документа.

15. Размножение документов и изданий с грифом «Коммерческая тайна» производится с разрешения СБ и под контролем канцелярии по заказам, подписанным руководителем подразделения и утвержденным заместителем директора по направлению.

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

17. Документы с грифом «Коммерческая тайна» после исполнения группируются в отдельные дела. Порядок их группировки предусматривается перечнем номенклатурных дел несекретного делопроизводства.

18. Снятие копий (рукописных, машинописных, микро- и фотокопий, электрографических и др.), а также производство выписок из документов и изданий с грифом «Коммерческая тайна» работниками производится по разрешению руководителей подразделений.

19. Порядок работы на ЭВМ при обработке информации с грифом «Коммерческая тайна» осуществляется в соответствии с требованиями инструкции о порядке работы на ПЭВМ при обработке несекретной информации.

**4. Обеспечение сохранности документов, дел, изданий**

Не всякий документ является носителем КТ, однако это не означает, что такой документ не представляет никакой ценности. Не бывает важных или не очень важных документов. Самый малозначительный на первый взгляд документ при определенных обстоятельствах может оказаться чрезвычайно важным. Организация контроля за документацией фирмы позволит избежать непредвиденных ситуаций, путаницы и неразберихи.

Систему контроля и учета документов можно представить в следующем виде:

-учет всей документации фирмы с классификацией по сфере применения, дате, содержанию;

-регистрация и учет всех входящих/исходящих документов фирмы с фиксацией в специальном журнале информации о дате получения/отправления документа, откуда поступил или куда отправлен, классификация (письмо, счет, договор и т.п.);

- регистрация документов, с которых делаются копии, с фиксацией в специальном журнале (дата копирования, количество копий, для кого или с какой целью производятся копии и т.п.);

- особый режим уничтожения документов. Перед уничтожением документов необходимо проконтролировать их содержание во избежание случайного уничтожения нужных документов. Для уничтожения документов следует использовать уничтожитель бумаг или подвергать их сжиганию. В обязательном порядке нужно составить акт, подписываемый ответственными лицами и присутствующими при уничтожении.

Для облегчения системы контроля все документы следует разделить на три группы:

1. Документы общего пользования.

2. Документы для служебного пользования.

3. Документы секретного характера.

Каждой категории необходимо присвоить свой гриф. Это можно сделать при помощи штампов, специальных отметок, а можно использовать цветовую гамму (общего пользования - белый цвет, служебного - желтые, секретные - красного).

Приведем требования к осуществлению работ с каждой категорией документов.

*Документы общего пользования.* Предварительный контроль содержания, в дальнейшем свободный оборот (копирование, пересылка и т.п.), уничтожается обычным порядком.

*Документы служебного пользования.* Предварительный контроль содержания с присвоением грифа «Для служебного пользования». Ограничение доступа (только для ограниченного круга работников). Учет и хранение в соответствующем реестре. Копирование ограничено, указывается цель копирования и для кого делается копия. Уничтожение производится с составлением акта.

*Документы секретного характера.* Присвоение грифа «Коммерческая тайна». Ограничение доступа (только для ограниченного круга работников, имеющих соответствующий допуск). Список лиц знакомых с информацией обязателен. При ознакомлении оформляется обязательство о неразглашении документа. Копирование и уничтожение производится под жестким контролем ответственных работников с оформлением соответствующей документации.

*Правила предосторожности при работе с документами:*

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

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

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

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

5. Запрещается изъятие из дел или перемещение документов с грифом «Коммерческая тайна» 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.

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

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

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

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

электронном виде.

**Вопросы для самопроверки**

1. Задачи специального отдела.
2. Структура специального отдела.
3. Функции специального отдела.
4. Права специального отдела.
5. Ответственность специального отдела.
6. При выполнении каких условий обеспечивается эффективная защита?
7. Механизм защиты коммерческой тайны.
8. Последовательность действий по введению режима КТ.
9. Правила, обеспечивающие сохранность КТ
10. Обеспечение сохранности документов, дел, изданий.
11. Система контроля и учета документов.
12. Грифы конфиденциальности.
13. Правила предосторожности при работе с документами

**Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы:**

1. Аскеров Т.М. Защита информации и информационная безопасность: Учебное пособие/Под общей ред. Курбакова К.И. – М.: Рос. экон. академия, 2001.-387 с.
2. Румынина Л.А. Документационное обеспечение управления 2009 ОИЦ "Академия"
3. Организация и современные методы защиты информации / Под общ. ред. С.И. Диева, А.Г .Шаваева. М.: Концерн "Банковский Деловой Центр", 1998. Организация работы с документами: Учеб. / Под ред. проф. В.А. Кудряева. 2-е изд., перераб. и доп. М.: ИНФРА-М, 2007.
4. Аверченков В.И, Рытов М.Ю. «Служба защиты информации: организация и управление». БГТУ, 2005
5. Яскевич В.И. «Секьюрити. Организационные основы безопасности фирмы». М.: Ось-89, 2008
6. Ярочкин В.И. «Система безопасности фирмы». М.: Ось-89, 2003

**Интернет ресурсы:**

* [www.avosp.ru](http://www.avosp.ru/)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)

**Лекция № 21-22**

**ПОДРАЗДЕЛЕНИЕ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ**

**ДЕЯТЕЛЬНОСТИ**

План:

1. Положение о подразделении информационно-аналитической деятельности;

**2. Содержание информационной и аналитической работы**

3. Методы информационно-аналитической работы

**4. Обеспечение безопасности и защиты информации.**

**1. Положение о подразделении информационно-аналитической деятельности**

Сектор обработки документов с грифом «Коммерческая тайна» является структурным подразделением специального отдела службы безопасности и подчиняется непосредственно заведующему отделом. В своей работе сектор руководствуется «Инструкцией по защите коммерческой тайны».

Задачи

Организация и руководство делопроизводством документов с грифом «Коммерческая тайна».

Структура

В составе вектора устанавливаются следующие должности:

* заведующий сектором;
* делопроизводитель;
* машинистка.

Функции

Получение, учет, исполнение и документирование поступающих и разрабатываемых документов, организация оптимального документооборота, обеспечение отправки, размножения и надежного хранения документов, их сохранности и своевременного уничтожения, а также проверка их наличия и контроль своевременного и правильного их исполнения.

Разработка нормативных документов, направленных на обеспечение сохранности коммерческой тайны.

Участие в разработке, пополнении и обновлении «Перечня сведений, составляющих коммерческую тайну».

Участие в процессе обучения персонала работе с документами, содержащими коммерческую тайну.

Права

Требовать от подразделений, руководителей, сотрудников соблюдения требования по ведению делопроизводства с грифом «Коммерческая тайна».

Проверять правильность ведения делопроизводства в подразделениях, указывать руководителям подразделений на выявленные недостатки и требовать их устранения.

Представлять к поощрению сотрудников, четко выполняющих требования по сохранению коммерческой тайны. Принимать меры воздействия к лицам, допускающим нарушения в работе с документами, содержащими сведения, составляющие коммерческую тайну.

Ответственность

Всю полноту ответственности за качество и своевременное выполнение возложенных настоящим Положением на сектор задач и функций несет заведующий сектором.

Степень ответственности других сотрудников сектора устанавливается должностными инструкциями.

**2. Содержание информационной и аналитической работы**

**Информационная работа**

Информация – это сведения о значимых фактах (лицах, действиях, организациях, событиях), которые служат основой для принятия решений о проведении административных, организационных мероприятий, а также для подготовки предложений и рекомендаций. В философском понимании информация обеспечивает уменьшение или снятие неопределенности наших представлений об изучаемых явлениях (процессах) в результате получения сообщения (знака).

Информационная работа – деятельность по обеспечению должностных лиц сведениями, необходимыми для решения возложенных на них задач.

Средства информационной работы – это совокупность документальных, технических и иных устройств, предназначенных для накопления, обработки, систематизации, хранения и выдачи информации.

Формы информационной работы – особенности документирования, накопления, сбережения, интеграции информационных данных в различных звеньях системы управления в целях рационального и эффективного осуществления управленческой деятельности.

Процесс информационной работы – это последовательная совокупность операций (регистрация, передача, накопление, хранение, обработка, выдача информации), позволяющая быстро найти в полном объеме нужные сведения, затребованные конкретными потребителями.

Качество информации – это степень развитости свойств информации, определяющая ее практическую пригодность для исследования. Качество информации зависит от следующих характеристик:

* достоверность;
* относимость;
* своевременность;
* полнота;
* важность.

Отбор информации – это результат просмотра материалов и документов, уточнения, дополнения и формализации информации.

Накопление информации – это результат интеграции, систематизации, уточнения и учета информации в определенных системах.

Хранение информации – это результат централизации, коррекции, обновления и сбережения банков данных.

Обработка информации – это результат преобразования (сортировка, группировка, обогащение, сравнение и т. д.) в формы, удобные для работы.

Выдача информации – это передача информации потребителю в режиме сигнального информирования или в соответствии с программой, указанной в запросе.

Способы отбора и рамки информационного поиска определяются с учетом:

* структуры и содержания изучаемой проблемы с выделением конкретных задач, подлежащих анализу;
* наличия смежных областей и проблем, в которых может находиться нужная информация;
* глубины ретроспективного поиска;
* видов документальных источников, необходимых для исследования.

**Аналитическая работа.**

Аналитическая работа – составная часть творческой деятельности. Она предназначена для оценки информации и подготовки принятия решений. Составляет основное содержание повседневной работы каждого руководителя и работника.

Аналитическая работа, как процесс познания объективной реальности, осуществляется по законам диалектики, формальной логики, с применением общенаучных методов исследования.

Содержание аналитической работы – приведение разрозненных сведений в логически обоснованную систему зависимостей (пространственно-временных, причинно-следственных и иных), позволяющих дать правильную оценку как всей совокупности фактов, так и каждому из них в отдельности.

Цель исследования – общая направленность исследования, ожидаемый конечный результат. Цель исследования указывает на характер задач

исследования и достигается посредством их решения.

Задачи исследования – совокупность целевых установок, в которых формулируются основные требования к анализу и решению исследуемой проблемы.

Объект исследования – область практической деятельности, на которую направлен процесс исследования. Выбор объекта исследования определяет границы применения полученных результатов.

Предмет исследования – существенные свойства объекта исследования, познание которых необходимо для решения проблемы, в пределах которых объект изучается в данном конкретном исследовании.

Тематическое исследование – организационная форма аналитического слежения за состоянием и развитием обстановки, в рамках которой изучаются ее элементы с целью выработки тактических задач для практической деятельности.

Исследования в повседневной деятельности проводятся по мере накопления проблем. Исследуются: актуальность, важность, объективность, перспективность. Предметом исследования становятся события и процессы, развитие которых может повлиять на выбор форм и методов деятельности на определенном участке и в определенное время.

Средства аналитической работы – это законы и методы мыслительной деятельности, а также иные технические средства, на основе и с помощью которых осуществляется обработка фактических данных с более высоким качеством, позволяющим извлечь из нее все, что она может дать.

Формы аналитической работы – организационные особенности осуществления аналитической работы, обусловленные целями, средствами и результатами ее проведения, образующие систему аналитического слежения за состоянием и развитием обстановки.

Процесс аналитической работы – совокупность мыслительных операций, осуществляемых в определенной последовательности с использованием аналитических средств, приводящих к достижению целей и задач исследования.

Технология аналитической работы – получение нового знания (выводной информации), обеспечивающего сложный процесс исследования, имеющий определенную логическую последовательность.

**Основные этапы информационно-аналитической работы.**

Этап 1. Общее знакомство с проблемой. Ознакомление с проблемой в целом, а также со смежными вопросами, изучение которых может оказаться полезным; составление общего плана работы с указанием срока выполнения, исполнителей и основных источников, которые предположительно могут быть использованы.

Чтобы успешно справиться с заданием, очень важно вначале, при общем знакомстве с проблемой и составлении плана, действовать со знанием дела, обдуманно и рассудительно.

Этап 2. Определение используемых терминов и понятий. Необходимо определить и объяснить тот или иной термин или понятие так, чтобы это было ясно нам самим, тем, кто контролирует нашу работу, и тем, кто пользуется нашей информацией. “Определение понятий” является одним из девяти принципов информационной работы.

Этап 3. Сбор фактов.

Этап 4. Истолкование фактов. Так кратко можно назвать процесс изучения и обработки фактов с целью выжать из них все, что они значат. Этот этап включает оценку, классификацию, анализ и уяснение фактов.

Этап 5. Построение гипотезы. Рабочие гипотезы, выдвигаемые на этом этапе, обычно связаны с какими-либо конкретными вопросами, отвечая на которые можно проверить сами гипотезы. Многие считают построение гипотезы важнейшим моментом любого исследования как в области естественных или общественных наук, так и в области информационно-аналитической работы. По мере изучения данного этапа мы открываем все новые полезные стороны рабочей гипотезы.

Этап 6. Выводы. На этом этапе производятся исследования, необходимые для доказательства или опровержения рабочих гипотез, выдвинутых на этапе 5, и формулируются окончательные выводы, являющиеся душой почти любого информационного документа. (“Выводы” – последний из девяти принципов информационной работы.)

Этап 7. Изложение. Составление документа, завершающее работу. Составитель информационного документа должен не только ясно представлять себе то, о чем он пишет, но и уметь выразить свои мысли в ясной форме.

Необходимо указывать степень достоверности каждого утверждения. Доклад о научных кадрах, вероятно, должен содержать таблицы и диаграммы. Правильно сравнить положение, существующее в различных странах, – дело трудное. Однако в рассматриваемом нами примере та часть информации, где сравнивается положение с научными кадрами, может оказаться самой ценной.

**3. Методы информационно-аналитической работы**

Аналогия – один из самых полезных методов информационной работы. Мы часто прибегаем к аналогии в нашей повседневной жизни.

Иногда нам не удается использовать всех возможностей этого метода. Часто, рассуждая по аналогии, мы не замечаем многочисленных скрытых опасностей и совершаем ошибки. Для того чтобы наилучшим образом использовать метод аналогии, так же как и остальные методы информационной работы, надо рассмотреть достоинства и недостатки этого метода.

Рассуждая по аналогии, мы начинаем с явления, о котором хотим получить дополнительные сведения (например, мы хотим узнать, как жарко будет в августе текущего года). В поисках дополнительных сведений мы обращаемся к аналогичному явлению, имевшему место в прошлом, о котором мы кое-что уже знаем (в данном случае мы рассматриваем температуру в августе прошлого года).

**Принципы оценки и анализа информации.**

Полученные разнообразными путями данные станут полезными лишь после того, как все они подвергнутся необходимому анализу и предельно точному истолкованию. Подоплека многих деловых неудач заключается не в игнорировании информации, а в ее ошибочном анализе.

Сведения, как правило, оцениваются по достоверности, значимости, согласованности, полноте, возможности использования.

**А. Достоверность и надежность материалов.**

Любая поступающая извне информация характеризуется определенной степенью достоверности, в частности, зависящей от степени надежности источника и того, откуда он ее получил.

Чтобы высветить такие показатели, каждый регистрируемый факт полезно дополнять специальной буквенно-цифровой отметкой, причем буквами обозначают уровень надежности источника, а цифрами – откуда тот взял сведения.

Уровень надежности источника принято кодировать так:

А – абсолютно надежный и компетентный;

Б – обычно надежный;

В – не слишком надежный;

Г – ненадежный;

Д – неопределенный.

То, как этот источник получил представляемые данные, отмечают следующим образом:

1 – сам видел;

2 – слышал от того, кому можно верить;

3 – слухи.

Никогда не стоит забывать, что не вызывающий сомнений источник (А) иной раз способен передать явную дезинформацию, а совершенно ненадежный тип (Г) – сообщить ценнейшие данные. Памятуя об этом, двухзначковый индекс иногда дополняется римской цифрой, указующей на предполагаемую достоверность факта:

I – подтверждается другими фактами;

II – вероятно, правдив (III к I);

III – возможно, правдив (I к I);

IV – сомнителен (III против I);

V – неправдоподобен;

VI – неопределяем.

Маркировка Ш-Б2, к примеру, означает, что фактура предоставлена довольно надежным информатором (Б) со слов знающего человека (2) и, возможно, – “50 на 50” – правдива (Ш).

При наличии каких-либо сомнений в достоверности дошедших до вас данных их полезно отложить про запас в ожидании других подтверждающих или опровергающих фактов.

**Б. Искажение информации и дезинформация.**

Следует учитывать, что поступающая к вам фактура может быть:

– подсунута источнику как дезинформация;

– искажена им преднамеренно;

– изменена – произвольно или непроизвольно – в ходе ее передачи.

Устные сообщения, циркулирующие по горизонтальным и неформальным каналам, менее подвержены искажениям, а вот информация, поставляемая наверх, чаще приукрашивается (ввиду явного желания угодить, получить вознаграждение, избежать наказания...), чем наоборот.

При намеренной дезинформации применяют как заведомую ложь, так и утонченную полуправду, исподволь подталкивающую воспринимающих к ложным суждениям.

Наиболее распространенными приемами здесь являются:

– прямое сокрытие фактов;

– тенденциозный подбор данных;

– нарушение логических и временных связей между событиями;

– подача правды в таком контексте (с добавлением ложного факта или намека...), чтобы она воспринималась как ложь;

– изложение важнейших данных на ярком фоне отвлекающих внимание сведений;

– смешивание разнородных мнений и фактов;

– сообщение информации такими словами, которые можно истолковывать по-разному;

– неупоминание ключевых деталей факта.

Искажения, возникающие в процессе ретрансляции исходных данных, чаще всего происходят из-за:

– передачи только части сообщения;

– пересказа услышанного своими словами (“испорченный телефон”);

– пропуска фактуры через призму субъективно-личностных отношений.

Для успешной борьбы с вероятной дезинформацией следует:

– различать факты и мнения;

– понимать, способен ли информатор по своему положению иметь доступ к сообщаемым фактам;

– учитывать субъективные (самомнение, фантазийность...) характеристики источника и его предполагаемое отношение к выдаваемому сообщению;

– применять дублирующие каналы информации;

– исключать все лишние промежуточные звенья;

– помнить, что особенно легко воспринимается та дезинформация, которую вы предполагаете или желаете услышать.

**4. Обеспечение безопасности и защиты информации.** **Безопасность информационной работы**

Информация играет особую роль в процессе развития цивилизации. Владение информационными ресурсами и рациональное их использование создают условия оптимального управления обществом. И напротив, искажение информации, блокирование ее получения, использование недостоверных данных ведут к ошибочным решениям.

Особенно актуальна проблема использования экономической информации в сфере управления материальным производством, где рост информационного потока находится в квадратичной зависимости от промышленного потенциала страны. В свою очередь, быстрое развитие процессов автоматизации, использование компьютеров во всех сферах современной жизни, помимо несомненных преимуществ, повлекли появление ряда специфичных проблем. Одна из них – необходимость обеспечения эффективной защиты информации. Исходя из этого создание правовых норм, закрепляющих права и обязанности граждан, коллективов и государства на информацию, а также защита этой информации становятся важнейшим аспектом информационной политики государства. Защита информации, особенно в экономической сфере, – очень специфический и важный вид деятельности. Достаточно сказать, что в мире средняя величина ущерба от одной банковской кражи с применением электронных средств оценивается в 9 тыс. долл. Ежегодные потери от компьютерных преступлений в США и Западной Европе достигают 140 млрд. долл. По мнению американских специалистов, снятие систем защиты информации с компьютерных сетей приведет к разорению 20% средних компаний в течение нескольких часов, 40% средних и 16% крупных компаний потерпят крах через несколько дней, 33% банков лопнут за 2–5 часов, 50% банков – через 2–3 дня.

**Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы:**

1. Аскеров Т.М. Защита информации и информационная безопасность: Учебное пособие/Под общей ред. Курбакова К.И. – М.: Рос. экон. академия, 2001.-387 с.
2. Румынина Л.А. Документационное обеспечение управления 2009 ОИЦ "Академия"
3. Организация и современные методы защиты информации / Под общ. ред. С.И. Диева, А.Г .Шаваева. М.: Концерн "Банковский Деловой Центр", 1998. Организация работы с документами: Учеб. / Под ред. проф. В.А. Кудряева. 2-е изд., перераб. и доп. М.: ИНФРА-М, 2007.
4. Аверченков В.И, Рытов М.Ю. «Служба защиты информации: организация и управление». БГТУ, 2005
5. Яскевич В.И. «Секьюрити. Организационные основы безопасности фирмы». М.: Ось-89, 2008
6. Ярочкин В.И. «Система безопасности фирмы». М.: Ось-89, 2003

**Интернет ресурсы:**

* [www.avosp.ru](http://www.avosp.ru/)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)

**Лекция №23**

**ПОДРАЗДЕЛЕНИЕ РАЗВЕДКИ**

План:

1. Положение о Подразделении разведки
2. Источники шпионажа.

**Положение о Подразделении разведки**

Группа безопасности внешней деятельности является самостоятельным структурным подразделением службы безопасности и подчиняется непосредственно начальнику службы.

Группа организует работу в тесном взаимодействии с основными структурными подразделениями службы безопасности и предприятия.

Задачи

Изучение и выявление предприятий и организаций, потенциально являющихся союзниками и конкурентами.

Добывание, сбор и обработка сведений о деятельности потенциальных и реальных конкурентов для выявления возможных злонамеренных действий по добыванию охраняемых сведений.

Учет и анализ попыток несанкционированного получения коммерческих секретов конкурентами.

Оценка степени реальных конкурентных отношений между сотрудничающими (конкурирующими) организациями.

Анализ возможных каналов утечки конфиденциальной информации.

Структура

Структура и штатное расписание определяется с учетом объемов и особенностей обстановки.

Функции

Изучение торгово-конъюнктурных ситуаций в пространстве деятельности учредителей, партнеров, клиентов и потенциально возможных конкурентов.

Ситуационный анализ текущего состояния финансово-торговой деятельности с точки зрения прогнозирования возможных последствий, могущих привести к неправомерным действиям со стороны конкурирующих организаций и предприятий.

Выявление платежеспособности юридических и физических лиц, их возможности по своевременному выполнению платежных обязательств.

Установление антагонистических конкурентов, выявление их методов ведения конкурентной борьбы и способов достижения своих целей.

Определение возможных направлений и характера злоумышленных действий со стороны специальных служб промышленного шпионажа против предприятия, его партнеров и клиентов.

Права

Требовать от соответствующих служб и подразделений необходимые для анализа сведения о деятельности партнеров и клиентов.

Осуществлять сбор и обработку необходимых сведений для выявления злоумышленных действий со стороны конкурирующих организаций.

Ответственность

Вся полнота ответственности за полноту и своевременность оценки степени опасности действий со стороны конкурентов и злоумышленников по отношению к охраняемым сведениям и безопасности руководства и сотрудников лежит на группе безопасности внешней деятельности.

**2. Источники шпионажа**

*Открытые источники*

Сбор сведений о фирмах и частных лицах ведется самыми различными способами, причем большинство из них не являются таинственными или секретными. Это относится, в первую очередь, к открытым сведениям, то есть информации, почерпнутой из газет, книг, научных и технических изданий, официальных отчетов и рекламных материалов. Подобным образом работает большинство разведок мира. Такая деятельность ведется широко и основательно, при этом нужно не упустить ничего, что доступно и что могло бы оказаться полезным. Понятно, что для анализа требуется группа аналитиков, способных выловить из моря документов "золотую рыбку".

Другими, не менее важными направлениями получения открытого доступа к конфиденциальной информации являются:

* доклады на конференциях, симпозиумах и т.д.;
* вопросы, осторожно задаваемые специалистами конкурента на этих мероприятиях;
* попытки пригласить на работу специалистов и заполнение ими с этой целью специальных вопросников;
* беседы со служащими конкурирующих фирм (без нарушения закона);
* наем на работу служащего конкурирующей фирмы для получения требуемой информации;
* изучение выставочных образцов;
* притворные переговоры с конкурентом якобы для приобретения лицензии или для совместной деятельности.

*Люди*

В ряду источников конфиденциальной информации люди занимают особое место, ибо способны выступать не только обладателями конфиденциальной информации, но и субъектами злонамеренных действий. Люди являются обладателями и распространителями информации в рамках своих функциональных обязанностей. Помимо обладания сведениями, люди способны их анализировать, обобщать, делать выводы, а также при определенных условиях скрывать, воровать, продавать информацию и совершать иные криминальные действия вплоть до вступления в преступные связи со злоумышленниками.

**Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы:**

1. Аскеров Т.М. Защита информации и информационная безопасность: Учебное пособие/Под общей ред. Курбакова К.И. – М.: Рос. экон. академия, 2001.-387 с.
2. Румынина Л.А. Документационное обеспечение управления 2009 ОИЦ "Академия"
3. Организация и современные методы защиты информации / Под общ. ред. С.И. Диева, А.Г .Шаваева. М.: Концерн "Банковский Деловой Центр", 1998. Организация работы с документами: Учеб. / Под ред. проф. В.А. Кудряева. 2-е изд., перераб. и доп. М.: ИНФРА-М, 2007.
4. Аверченков В.И, Рытов М.Ю. «Служба защиты информации: организация и управление». БГТУ, 2005
5. Яскевич В.И. «Секьюрити. Организационные основы безопасности фирмы». М.: Ось-89, 2008
6. Ярочкин В.И. «Система безопасности фирмы». М.: Ось-89, 2003

**Интернет ресурсы:**

* [www.avosp.ru](http://www.avosp.ru/)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)

**Лекции № 24-26**

 **ПОДРАЗДЕЛЕНИЕ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ**

План:

1. Положение о подразделении инженерно-технической защиты.

**2. Технические средства разведки. Перехват разговора.**

**3. Перехват телефонного разговора**

**4. Несанкционированное получение документа на бумажном носителе.**

**5. Несанкционированное получение документа на небумажном носителе.**

**1. Положение о подразделении инженерно-технической защиты.**

Группа инженерно-технической защиты информации является структурным подразделением службы безопасности и подчиняется непосредственно начальнику службы.

В своей деятельности группа руководствуется требованиями «Инструкции по Инженерно-технической защите».

Задачи

Обследование выделенных помещений с целью установления потенциально возможных каналов утечки конфиденциальной информации через технические средства, конструкции зданий и оборудования.

Выявление и оценка степени опасности технических каналов утечки информации.

Разработка мероприятий по ликвидации (локализации) установленных каналов утечки информации организационными, организационно-техническими или техническими мерами, используя для этого физические, аппаратные и программные средства и математические методы защиты.

Организация контроля (в том числе и инструментального) за эффективностью принятых защитных мероприятий. Проведение обобщения и анализа результатов контроля и разработка предложений по повышению надежности и эффективности мер защиты.

Обеспечение приобретения, установки, эксплуатации и контроля состояния технических средств защиты информации.

Структура

Структура и штатный состав группы Инженерно-технической защиты информации разрабатывается и утверждается руководством службы безопасности исходя из конкретных условий и технической оснащенности подразделений предприятия.

Возможно состав группы установить в следующем составе:

руководитель группы — старший инженер;

Инженер (техник) группы по спец измерениям.

Функции

Определение границ охраняемой (контролируемой) территории (зоны) с учетом возможностей технических средств, наблюдения злоумышленников.

Определение технических средств, используемых для передачи, приема и обработки конфиденциальной информации в пределах охраняемой (контролируемой) территории (зоны).

Определение опасных, с точки зрения возможности образования каналов утечки, технических средств.

Локализация возможных каналов утечки информационно-организационными, организационно-техническими или техническими средствами и мероприятиями.

Организация наблюдения за возможным неконтролируемым излучением за счет ПЭМИН (побочных электромагнитных излучений и наводок).

Организация контроля наличия, проноса каких-либо предметов (устройств, средств, механизмов) в контролируемую зону, способных представлять собой технические средства несанкционированного получения конфиденциальной информации.

Права

Группа Инженерно-технической защиты информации имеет право:

проверять наличие технических средств обеспечения производственной деятельности в выделенных помещениях, измерять их параметры на соответствие требованиям безопасности;

устанавливать технические средства защиты каналов утечки информации через технические средства обеспечения производственной деятельности;

запрещать использование технических средств, не обеспечивающих требования безопасности.

Ответственность

Всю полноту ответственности за инженерно-техническую защиту информации несет руководитель группы.

**2.Технические средства разведки**

Звуковыми или акустическими сигналами называются распространяющиеся в упругой среде механические колебания с малыми амплитудами.

#### Подслушивание

Наиболее простым способом перехвата разговора является обыкновенное подслушивание, причем, очень часто, случайное. Достаточно распространенной является ситуация, когда находящиеся в приемной посетители достаточно отчетливо слышат все, что происходит в кабинете; в курилке сотрудники фирмы, не обращая внимания на присутствие посторонних продолжают обсуждать важные проблемы; летом совещания, в том числе на нижних этажах, ведутся при открытых окнах или форточках. В этих ситуациях, как говорится, не хочешь, а услышишь.

Подслушивание с помощью сверления отверстий в стенах известно с незапамятных времен, оно используется достаточно широко и сегодня. Если есть возможность организовать пункт прослушивания в смежных помещениях, то подобный способ будет наиболее дешевым и безопасным. Любителям, однако, не рекомендуется им пользоваться, ибо необходимо правильно подобрать место сверления, глубину и толщину отверстия.

#### Диктофон

В настоящее время очень широко распространены диктофоны самых различных типов. Многие из них оборудованы акустоматом (системой автоматического выключения при паузах в разговоре) и регулятором скорости движения ленты. Как правило, такие диктофоны (SONY, Panasonic и т.д.) используются для регистрации разговоров одним из собеседников. В этом случае их прячут в дипломатах, свертках а то и просто в карманах.

Существуют диктофоны, вмонтированные в различные предметы: дипломаты, настольные часы и так далее. Тактика применения довольно простая, но эффективная. Дипломат "по рассеянности" забывают в кабинете или приемной, а часы дарят людям, в помещения которых есть доступ у доверенных людей (чтобы менять кассеты) - уборщиц, охранников, сторожей.

#### Микрофоны

#### Передача информации по специально проложенным проводам

Простейшей и наиболее надежной операцией является использование специального малогабаритного микрофона (размером 7x5x2 мм) и специально проложенного провода. Она заключается в том, что скрытно размещенный в интересующем помещении микрофон соединяется с пунктом прослушивания, где перехваченные разговоры записываются через усилитель на магнитофон либо прослушиваются. До появления микро электроники описанный способ применялся чрезвычайно широко.

Недостатком проводов является возможность их обнаружения и проверки назначения при визуально-техническом контроле. В более современных системах используются тончайшие (не толще волоса) оптические волокна, которые возможно вплести в ковровое покрытие, и т.д. Разумеется, микрофон в его привычном понимании отсутствует.

Несмотря на видимую простоту, специалисты не очень любят подобные средства, поскольку по проводу можно обнаружить пункт прослушивания, со всеми вытекающими отсюда неприятными последствиями.

***Использование имеющихся коммуникаций***

Гораздо более безопасным является использование выходящих за пределы помещения проводов сигнализации, радиотрансляции и т.д., а также металлоконструкций типа труб системы отопления, канализации, водоснабжения. Микрофон с предусилителем, скрытно установленный в интересующем помещении, подключается к подобным конструкциям, с которых информация снимается в пункте прослушивания. В данном случае требуется более совершенная аппаратура как для передачи, так и для приема акустических сигналов.

#### Использование сети 220 Вольт

Очень популярным средством съема информации являются системы, устанавливаемые в электророзетках, выключателях и т.д., передающие разговоры по проводам 220 В. Этот способ очень удобен для включения и выключения передатчика, который имеет неограниченный источник энергопитания, но в данном случае осложняется вопрос размещения постов прослушивания, так как передаваемые по электропроводам сигналы не проходят через силовые трансформаторы. Диапазон частот используемых сигналов - от 50 кГц до 300 кГц. При меньших значениях будут сильно сказываться сетевые низкочастотные помехи, а при больших значениях резко возрастает затухание в проводах, а также начинает усиливаться электромагнитное излучение, которое сводит на нет все преимущества по скрытности.

#### Передача информации по телефонным линиям

Широкое распространение в последнее десятилетие за рубежом получили системы акустического прослушивания помещений через телефонную линию. Примерный алгоритм работы подобных систем таков. На телефонной линии (внутри телефонного аппарата) устанавливаются специальные датчики (подключаются параллельно). При необходимости прослушать разговор производится звонок с любого телефона, в том числе и по междугородней связи, и выдается в телефонную трубку специальный сигнал. Звонки в этом случае не проходят на телефон и датчик начинает передавать в линию разговоры, происходящие в помещении. Таких датчиков можно установить до четырех, скажем, для контролирования четырех комнат квартиры, при этом инициировать их в любой последовательности.

#### Радиотелефоны

Радиотелефоны или радиозакладки занимают лидирующее место среди используемых средств технического шпионажа. Простейшее устройство содержит три основных узла, определяющих технические возможности и методы их использования, - микрофон, определяющий зону акустической чувствительности, радиопередатчик, определяющий дальность ее действия, источник питания, от которого зависит продолжительность ее непрерывной работы. На дальность и качество оказывают влияние также и характеристики приемников.

Для приема используются самые различные устройства: от бытовых магнитол до высокопрофессиональных, в том числе импортных устройств. Пожалуй, основной характеристикой системы "закладка-приемник" является чувствительность приемника. Чем лучше этот параметр, тем дальше то расстояние, на которое можно использовать эту систему.

#### ИК-передатчики

Для повышения скрытности, в последние годы стали использовать для передачи перехваченной микрофоном информации инфракрасный канал. В качестве передатчиков используются маломощные полупроводниковые лазеры и светодиоды. В качестве примера рассмотрим закладку TRM-1830. Дальность действия ее днем 150 м, ночью - 400 м. Ток потребления - 8 мА, время непрерывной работы - 20 часов. Габариты не превышают 26x22x20 мм. К недостаткам можно отнести необходимость прямой видимости между закладкой и приемником и влияние фоновой засветки. Все это резко ограничивает оперативные возможности подобных средств..

#### Направленные микрофоны

Обычные микрофоны динамического или электретного типа способны регистрировать голос человека с нормальной громкостью на расстоянии до 15 метров, а ночью, в тихую погоду, - 200 м. Для средств разведки этого мало, так как в некоторых случаях требуется дальность действия примерно в десять раз больше.

Существует несколько модификаций направленных микрофонов, воспринимающих и усиливающих звуки, идущие только из одного направления, и ослабляющих все остальные звуки. В простейших из них узкая диаграмма направленности формируется за счет использования длинной трубки. В более сложных конструкциях могут использоваться несколько трубок разной длинны. Высокие параметры имеют также узко направленные микрофоны, в которых диаграмма направленности создается параболическим концентратором звука.

***Виброканал***

При воздействии акустического сигнала (речи) на поверхность твердых тел в них возникают вибрации, регистрируя которые можно прослушать интересующие разговоры. В качестве датчика используется вибродатчик, преобразующий вибросигналы в электрические.

#### Стетоскоп

Все "профи" очень любят стетоскоп, который избавил их от утомительного сверления, Что это такое, можно показать на примере изделия фирмы DTI. Оно состоит из вибродатчика с нанесенной на него мастикой для прикрепления к стене, блока усиления с регулятором громкости и головных телефонов. Размер датчика - 2, 2x0, 8 см, диапазон принимаемых частот - 300...3000 Гц, вес - 126 г, коэффициент усиления - 20000. С помощью подобных средств можно прослушивать через стены толщиной до 1 м. Кроме свойств вибродатчика, на качество шума влияют толщина и материал изготовления стен, уровень шумов и вибраций в обоих помещениях, правильное место выбора расположения датчика и т.д.

#### Лазерные микрофоны

Наиболее перспективным направлением является использование лазерных микрофонов, первые образцы которых были приняты на вооружение американскими спецслужбами еще в 60-е годы. В качестве примера рассмотрим лазерное устройство HPO150 фирмы "Хъюлет Паккард", обеспечивающее эффективное обнаружение, подслушивание и регистрацию разговоров, ведущихся в помещениях. Дальность действия устройства - 1000 м. Оно сконструировано на гелий-неоновом или полупроводниковом лазере с длиной волны 0, 63 мкм (что, кстати, является большим недостатком, так как пятно видно глазом, более современные системы работают в ближнем ИК-диапазоне). Прослушивание и перехват разговоров ведутся, благодаря получению отраженного сигнала от обычного оконного стекла, представляющего собой своеобразную мембрану, которая колеблется со звуковой частотой, создавая фонограмму происходящего разговора.

***Гидроакустические датчики***

Акустические колебания, возбуждая вибрации в трубах водоснабжения и отопления, вызывают гидроакустические сигналы в находящейся в них жидкости. Теоретически, можно перехватить обсуждаемую информацию в пределах здания с помощью гидроакустического датчика, и по имеющимся данным, такие системы испытывались. Однако очевидно, что датчик будет улавливать разговоры во всех помещениях, а, кроме того, слишком высокий уровень шумов, особенно в водопроводе. В результате остается только один путь: установить в батарее отопления передатчик в гидроакустическом диапазоне. Однако в это случае необходимо проникновение на объект (скажем, под видом сантехника, а для достоверности необходимо предварительно отключить воду в здании), что делает систему менее привлекательной. Бояться подобных средств пока не надо, так как пока только спецслужбы "доросли" до их использования.

***Электроакустические преобразования***

При разговоре акустические волны воздействуют на конструктивные элементы электронных приборов. Они, в свою очередь, влияют на электромагнитное поле излучающих элементов или создают микроскопические токи в проводниках. Все эти токи и поля оказываются промодулированы речью и при соответствующей обработке можно извлечь полезную информацию.

Проиллюстрировать сказанное можно на примере телефона со звонком электромеханического типа. Акустические волны воздействуют на маятник звонка, соединенного с якорем электромагнитного реле. Под воздействием речевых сигналов якорь совершает микроколебания, что, в свою очередь, вызывает колебание якорных пластин в электромагнитном поле катушек, следствием чего является появление микротоков, модулированных речью.

Подобные преобразования происходят в большинстве электронных устройств (электрочасах, телевизорах, радиоприемниках и т.д.). Дальности перехвата подобных сигналов, как правило, невелики, но иногда превышают 100 м. Для усиления эффекта иногда применяется так называемое высокочастотное навязывание. В этом случае электронный прибор облучается извне мощным высокочастотным сигналом, и осуществляется прием промодулированного речью отраженного излучения. Надо сказать, что все это прерогатива спецслужб, любителям подобные действия пока не по плечу.

***Визуально***

С древних времен известна способность глухонемых людей понимать речь по шевелению губ. Это достаточно широко используется для дистанционного перехвата разговора. Обычно, в связи с достаточно большим расстоянием до говорящего, применяются бинокли, подзорные трубы и т.д. Известны случаи, когда проводилась киносъемка разговаривающих в саду советского посольства в Мексике дипломатов с целью расшифровать разговор по движению губ. Хочется отметить, что этот способ часто не приносит ожидаемых от него результатов и в промышленном шпионаже практически не используется.

**3. Перехват телефонного разговора**

### Подключение к линии

Для перехвата телефонных разговоров могут быть использованы те же средства, что и для прослушивания обычных разговоров, но аппаратура должна устанавливаться у обоих абонентов. Гораздо более просто осуществить перехват путем подключения к линии. Это можно сделать как с помощью прямого физического контакта с линией, так и с помощью индуктивного датчика, т. е. не требующего врезаться в линию. На практике используются оба способа, в зависимости от типа применяемой аппаратуры.

#### Стационарное прослушивание

Наиболее удобно организовывать стационарное прослушивание телефонных разговоров, что достаточно просто сделать на телефонной станции (коммутаторе).

#### Трубка

Чаще всего используется прослушивание разговоров с помощью существующего параллельного телефона. Есть некоторые типы аппаратов, на которых не надо даже физически поднимать трубку, так как благодаря некоторым особенностям разговор достаточно хорошо слышно (РН-299).

#### Диктофон

Очень часто для записи телефонных разговоров используются диктофоны, скрытно подключенные к линии. Для подключения используются специальные коробочки (трансформаторы). Если диктофон имеет акустомат, то это идеальное устройство для записи.

#### Телефонный радиотранслятор

Телефонные закладки могут подключатся к любой точке телефонной линии и иметь неограниченный срок службы, так как питаются от телефонной сети. Эти изделия чрезвычайно популярны в среде промышленного шпионажа благодаря простоте и дешевизне (от 15 до 200 $).

Большинство телефонных закладок представляют собой специальные радиозакладки. Они автоматически включаются при поднятии телефонной трубки и передают по радиоканалу телефонный разговор на пункт перехвата, где он может быть прослушан и записан. Так как телефонный аппарат имеет свой микрофон и закладкам не нужен источник питания, их размеры могут быть миниатюрными.

**Побочные электромагнитные сигналы и наводки**

Любое электронное изделие при работе излучает так называемые побочные электромагнитные излучения и наводки. Очень распространены телефоны с кнопочным номеронабирателем типа ТА-Т, ТА-12 и т.д. При наборе номера и ведении переговоров благодаря техническим особенностям блока питания вся информация ретранслируется на десятках частот в СВ, КВ и УКВ диапазонах на расстояние до 200 м. В случае применении подобного телефона радиозакладки не нужны. Обычно перехват осуществляется более сложно. С помощью малогабаритного индуктивного датчика можно улавливать побочные электромагнитные колебания автотрансформатора практически любого телефонного аппарата на расстоянии до полуметра. При этом также регистрируются набираемые номера и все разговоры.

**Перехват разговоров по радиотелефону**

В последнее время большой популярностью среди бизнесменов пользуются радиотелефоны и радиостанции различных типов. Основная масса их импортная, но появляются и отечественные образцы. Как ни странно, но некоторые считают, что используя обычный телефон их могут подслушать, а в случае радиотелефона это практически невозможно. Придется развеять эти иллюзии, но сначала необходимо описать принцип работы различных радиотелефонов. Радиотелефон - это комплект из двух радиостанций, одна из которых является базовой, устанавливается стационарно и подключается к телефонной сети, вторая - подвижная. От обычной радиостанции отличается тем что пользователь радиотелефона выходит непосредственно в городскую телефонную сеть. Следовательно, осуществлять прослушивание телефонных разговоров можно обычными способами.

При наличии сотовой связи в регионе можно стать ее абонентом, при этом качество связи (помехозащищенность) будет значительно лучше. Но при этом можно применять те же способы прослушивания.

Дальность действия радиотелефона зависит от диапазона частот, в котором он работает, от выходной мощности и применяемой антенны. В диапазоне УКВ на дальность радиосвязи влияют также рельеф местности и наличие различных построек. Дальность действия "беспроводных" телефонов редко превышает 300 м. Остальные радиотелефоны работают на дальностях от 1 до 100 км.

С точки зрения съема информации радиотелефоны, в том числе сотовые системы, и радиостанции объединяет то, что при работе они используют радиоволны. Нет необходимости устанавливать радиомикрофоны, телефонные закладки, использовать лазерные микрофоны или стетоскопы, достаточно приобрести качественный приемник, установить хорошую антенну и спокойно прослушивать разговоры. При этом дальность радиоперехвата будет не менее дальности работы радиотелефона, а при использовании хорошей аппаратуры - в несколько раз больше. Кроме того, по излучаемым сигналам можно установить местонахождение автомобиля, оборудованного радиотелефоном.

**4. Несанкционированное получение документа на бумажном носителе**

Большинство документов до сих пор исполняется на бумаге. Это и служебная переписка, и памятные записки, и материалы к совещаниям, и различного рода записные книжки. Специалисты утверждают, что получить в свои руки "ежедневник" руководителя - большая удача, так как оттуда можно почерпнуть громадное количество информации. Очень часто важнейшие записи делаются на отдельных листах и перекидных календарях. Кроме того, вся технологическая и бухгалтерская документация напечатана на бумаге. Все это также интересует злоумышленников.

В большинстве организаций документы не учитываются и кипы бумаг кочуют из кабинета в кабинет или складываются где угодно, даже в коридорах. В такой обстановке утрата любого документа не вызовет большой тревоги, и бумаги теряются, отсылаются по ошибочным адресам и просто исчезают бесследно.

Иногда конфиденциальные бумаги выносятся за пределы организации, где их выкрасть гораздо проще.

**Перехват почтовых отправлений**

Читать чужие письма любили всегда и во всех странах. Для этого использовали подручные средства и специальную технику. Сотрудники ЦРУ пользуются горячими пластинками, металлическими чайниками и различной формы инструментами из кости. Однако наиболее эффективный прием заключается в использовании специального приспособления, напоминающего миниатюрный столик размерами с обычный портфель с плоской поверхностью, подогреваемой горячим паром, который обеспечивается обогревательным элементом, заключенным в пенистую резину. Пар образуется от сырой промокательной бумаги, которую кладут на подогретую поверхность столика, и конверты, положенные на эту промокательную бумагу, раскрываются буквально через несколько секунд. Процесс завершается тщательным запечатыванием конвертов с помощью ватных тампонов и чистого прозрачного клея.

Технический прогресс пришел на помощь любителям чтения чужих писем. Теперь не надо приобретать навыки, безнадежно испортив десятки неумело вскрытых конвертов. Достаточно просто приобрести баллончик, содержащий специальные химические вещества, опрыскать его содержимым конверт. На некоторое время конверт станет прозрачным, и можно легко прочитать содержимое. Подобные баллончики продаются и в России. Невысокая цена (порядка 20...170 $) и простота эксплуатации делает их легко доступными.

1. **Несанкционированное получение документа на небумажном носителе**

В настоящее время все большее количество информации оказывается сосредоточенным на небумажных носителях. К ним, в первую очередь, относятся жесткие диски и дискеты персональных компьютеров, перфоленты и перфокарты кое-где сохранившихся у нас ЭВМ 60-70-х годов, микрофильмы и кинопленки, аудио- и видеокассеты, лазерные диски. Особое внимание следует обратить на персональные компьютеры (ПК), по следующим объективным причинам:

* высокие темпы роста парка ПК, находящихся в эксплуатации;
* широкое применение ПК в самых различных сферах человеческой деятельности;
* высокая степень концентрации информации в ПК;
* усложнение вычислительного процесса в ПК.

Будущее - за небумажными носителями. Только одна компания "Травелерс" насчитывает 35000 терминалов и ПК, при этом ежедневно через сеть коаксиальной и волоконно-оптической связи длиной 600000 км передается 3, 7 миллиона сообщений. Чистая экономия за год - 32 товарных вагона бумаги.

#### Хищение носителей информации

Это, пожалуй, самый популярный в России способ. Воруют все: дискеты и видеокассеты, компьютеры и лазерные диски (вместе с проигрывателями). Вся беда заключается в том, что, чаще всего, воруют все это не как носитель информации, а как обычную материальную ценность, которую можно продать. Вот и ломают голову службы безопасности, станет ли украденная дискета с перечнем потребителей козырной картой в большой конкурентной борьбе, или на нее запишут парочку компьютерных игр.

#### Несанкционированное копирование

Нет необходимости ничего воровать, тем более что за кражу могут привлечь и к уголовной ответственности. Гораздо проще все интересное скопировать на свои дискеты и с сознанием честно выполненного долга покинуть офис. Таким приемом пользуются, как правило, завербованные сотрудники, или все те же "знакомые одного знакомого", которые попросили ненадолго воспользоваться компьютером. Очень часто служащие сами не прочь продать информацию "на сторону".

#### Несанкционированное считывание данных

Иногда нет необходимости копирования всего файла, достаточно просто взглянуть на определенную цифру или имя. В этом случае просто выводят нужную информацию на экран, что не занимает времени, и при этом всегда можно сослаться на ошибку в своих действиях.

В связи с тем, что на очень многих ПК для входа в систему необходимо набрать пароль, злоумышленники стремятся его узнать заранее, а если это невозможно, то пользуются методом перебора наиболее вероятных слов (IBM, DOS, имя хозяина, название фирмы и т.д.). Очень часто пароль может быть записан на календаре, в блокноте, а то и прямо на клавиатуре.

#### Несанкционированное использование ПК зарегистрированных пользователей сети

Если персональные компьютеры объединены в сеть, то все описанные выше операции для зарегистрированных пользователей резко упрощаются. "Хакеры" очень часто прибегают к использованию наиболее физически доступного терминала для считывания информации. По-видимому, это направление наиболее перспективное с точки зрения промышленного шпионажа. Если выход в сеть осуществляется через модем, то "внедриться" в память любого абонента можно достаточно просто.

**Несанкционированный перехват небумажного документа в процессе его обработки**

При обработке небумажного документа возникают некоторые дополнительные возможности для несанкционированного съема информации. Самое важное, что при этом в большинстве случаев не требуется проникновение на объект.

#### Изображение на дисплее

При работе с электронным документом очень часто требуется получить его изображение (дисплей у компьютера, телевизор у видеомагнитофона, экран у слайдоскопа и т.д.). Соответственно, для съема информации можно применить оптические и оптоэлектронные средства, описанные выше, что на самом деле и происходит, если представляется такая возможность.

#### Побочные электромагнитные сигналы и наводки

При работе электронной техники образуются побочные электромагнитные излучения и наводки на провода, кабели и прочие токопроводящие коммуникации (трубы, арматуру и т.д.). Наиболее вероятен перехват сведений при приеме излучений от дисплеев, накопителей на магнитных дисках, принтеров и соединительных кабелей.

Проще всего снять информацию с дисплея. Изображение на экране формируется, в основном, так же, как и в телевизионном приемнике. Видеосигнал, необходимый для получения изображения, модулирует ток электронного луча. Таким образом, он является цифровым сигналом, логическая единица которого создает световую точку, а логический ноль препятствует ее появлению. Кроме того, в цепях дисплея присутствуют тактовые синхроимпульсы.

Источниками излучения видеосигнала могут быть элементы обработки сигнала изображения и электронный луч кинескопа. В отличие от других сигналов, существующих в ПК, видеосигнал усиливается до нескольких десятков киловольт для подачи на электронно-лучевую трубку. Следовательно, видеоусилитель является наиболее мощным (и опасным) источником широкополосного излучения. Источником же узкополосного излучения является система синхронизации.

Излучение дисплеев, содержащих гармоники видеосигналов, охватывает диапазон метровых и дециметровых волн. На некоторых частотах (например, 125 и 210 МГц - чуть выше пятого и десятый телевизионные каналы соответственно) имеются резонансы, которые являются причиной усиления излучения относительно соседних частот.

**Перехват документа на небумажном носителе при его передаче**

В настоящее время гигантское количество информации передается по различным каналам связи, причем, как правило, используется телефонная сеть. Получают все большее развитие такие сервисные службы, как электронная почта, телекс, факс, телетекст, видеотекст, передача биржевой информации, банковские операции и т.д. Главным недостатком использования телефонной связи для передачи данных является ее доступность для любого лица, располагающего соответствующей аппаратурой.

Способы, используемые для перехвата передаваемых сообщений, в основном, те же, что и для подслушивания телефонных разговоров. Рассмотрим это на примере факсимильной связи (факса), поскольку многие бизнесмены считают, что это самый безопасный вид связи. На самом деле передаваемые тексты может перехватывать любой человек с помощью устройства, которое стоит несколько сотен долларов. А японская компания "Ниппон телефон энд телеграф" сообщила о том, что располагает доказательствами подключения к ее факсам не только в Японии, но и во всем мире.

Для передачи информации также распространенным является отправка ее по ошибочным адресам. Дело в том, что человек достаточно часто ошибается в наборе номера, и если в случае обычного телефонного разговора он сразу понимает, что говорит не с тем человеком, то при отправке сообщения по компьютерной сети или факсу этого не происходит. Кроме того, отправляя информацию по правильному адресу, часто не проверяют, кто конкретно ее принял, а этим человеком может быть злоумышленник.

**Получение несанкционированной информации о производственном процессе**

В случае, если невозможно получить информацию в концентрированном виде через агентов, болтунов, посредством подслушивания телефонных переговоров и "взлома" компьютерного банка данных, шпиону приходится внедряться в производство. Это громадный по своему разнообразию способов добывания сведений пласт возможностей. По сути дела, в одной небольшой книге невозможно даже вскользь описать их. Для анализа возможностей по добыванию сведений непосредственно с производства требуется изучить его досконально, выяснить реальные каналы утечки информации о важнейших процессах, разработать операцию по их выявлению с привлечением соответствующей аппаратуры. Все это - дело достаточно хлопотное, требующее привлечения помимо оперативных работников-технологов, ученых различных областей, программистов и т.д.

Так, производя разработку химического завода, необходимо производить анализ выбросов в атмосферу (газоанализаторы), сточных вод (специальные химреактивы), перехватывать побочные электромагнитные сигналы и наводки от технологического оборудования, изучать поступающее сырье и отходы производства и т.д. Все это - громадная кропотливая работа, успех которой негарантирован. Кроме того, к промышленному шпионажу можно отнести и анализ готовой продукции с целью выпуска ее модифицированных версий под своей маркой. Наиболее распространено это в области создания программного обеспечения. "Хакеры" вскрывают защиту программ и используют извлекаемую информацию по своему усмотрению. Благо, для этого требуется только компьютер и голова.

В связи со сложностью и разнообразием работ по добыванию информации о производстве продукции, в России этим делом могут заниматься только иностранные спецслужбы, да и те без особого энтузиазма. Только после того, как наша промышленные гиганты и молодые небольшие предприятия закроют зияющие дыры в своей безопасности, начнется стадия "сбора опилок и сточных вод".

**Вопросы для самопроверки**

1. Задачи подразделения инженерно-технической защиты
2. Структура подразделения инженерно-технической защиты
3. Функции подразделения инженерно-технической защиты
4. Права подразделения инженерно-технической защиты
5. Ответственность подразделения инженерно-технической защиты
6. Технические средства разведки
7. Подслушивание
8. Передача информации по специально проложенным проводам
9. Использование имеющихся коммуникаций
10. Использование сети 220 Вольт
11. Передача информации по телефонным линиям
12. Перехват телефонного разговора
13. Подключение к линии
14. Стационарное прослушивание
15. Побочные электромагнитные сигналы и наводки
16. Перехват разговоров по радиотелефону
17. Несанкционированное получение документа на бумажном носителе
18. Перехват почтовых отправлений
19. Несанкционированное получение документа на небумажном носителе
20. Хищение носителей информации
21. Несанкционированное копирование
22. Несанкционированное считывание данных
23. Несанкционированное использование ПК зарегистрированных пользователей сети
24. Несанкционированный перехват небумажного документа в процессе его обработки
25. Побочные электромагнитные сигналы и наводки
26. Перехват документа на небумажном носителе при его передаче
27. Получение несанкционированной информации о производственном процессе

**Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы:**

1. Аскеров Т.М. Защита информации и информационная безопасность: Учебное пособие/Под общей ред. Курбакова К.И. – М.: Рос. экон. академия, 2001.-387 с.
2. Румынина Л.А. Документационное обеспечение управления 2009 ОИЦ "Академия"
3. Организация и современные методы защиты информации / Под общ. ред. С.И. Диева, А.Г .Шаваева. М.: Концерн "Банковский Деловой Центр", 1998. Организация работы с документами: Учеб. / Под ред. проф. В.А. Кудряева. 2-е изд., перераб. и доп. М.: ИНФРА-М, 2007.
4. Аверченков В.И, Рытов М.Ю. «Служба защиты информации: организация и управление». БГТУ, 2005
5. Яскевич В.И. «Секьюрити. Организационные основы безопасности фирмы». М.: Ось-89, 2008
6. Ярочкин В.И. «Система безопасности фирмы». М.: Ось-89, 2003

**Интернет ресурсы:**

* [www.avosp.ru](http://www.avosp.ru/)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)