Для обеспечения защиты интеллектуальной собственности на предприятиях вводится определенный порядок работы с информацией и доступа к ней, включающий в себя комплекс административных, правовых, организационных, инженерно-технических, финансовых, социально-психологических и иных мер, основывающихся на правовых нормах республики или на организационно-распорядительных положениях руководителя предприятия (фирмы).
Эффективная защита коммерческой тайны возможна при обязательном выполнении ряда условий:

- единство в решении производственных, коммерческих, финансовых и режимных вопросов;
- координация мер безопасности между всеми заинтересованными подразделениями предприятия;
- научная оценка информации и объектов, подлежащих классификации (защите). Разработка режимных мер до начала проведения режимных работ;
- персональная ответственность (в том числе и материальная) руководителей всех уровней, исполнителей, участвующих в закрытых работах, за обеспечение сохранности тайны и поддержание на должном уровне режима охраны проводимых работ.

Включение основных обязанностей рабочих, специалистов и администрации по соблюдению конкретных требований режима в коллективный договор, контракт, трудовое соглашение, правила трудового распорядка.

- Организация специального делопроизводства, порядка хранения, перевозки носителей коммерческой тайны. Введение соответствующей маркировки документов и других носителей закрытых сведений;
- Формирование списка лиц, уполномоченных руководителем предприятия (фирмы) классифицировать информацию и объекты, содержащие сведения, составляющие КТ;
- Оптимальное ограничение числа лиц, допускаемых к КТ;
- Наличие единого порядка доступа и оформления пропусков;
- Выполнение требований по обеспечению сохранения КТ при проектировании и размещении специальных помещений; в процессе НИОКР, испытаний и производства изделий, сбыта, рекламы, подписания контрактов, при проведении особо важных совещаний, в ходе использования технических средств обработки, хранения и передачи информации и т.п.;
- Организация взаимодействия с государственными органами власти, имеющими полномочия по контролю определенных видов деятельности предприятий и фирм;
- Наличие охраны, пропускного и внутри объектового режимов;
- Плановость разработки и осуществления мер по защите КТ, систематический контроль за эффективностью принимаемых мер;
- Создание системы обучения исполнителей правилам обеспечения сохранности КТ.

При организации защиты коммерческой тайны, имущественных и финансовых ценностей директор (президент) предприятия (фирмы) руководствуется прежде всего экономической целесообразностью. Здесь обязательно надо учитывать два момента: 1) затраты на обеспечение экономической безопасности должны быть, как правило, меньшими в сравнении с возможным экономическим ущербом и 2) планируемые меры безопасности содействуют, как правило, повышению экономической эффективности предпринимательства.
Центральное место в организации обеспечения экономической безопасности предприятия (фирмы) занимает выбор структуры службы, позволяющей эффективно решать эти вопросы.

На предприятиях с незначительным объемом сведений, составляющих КТ, а также товарных и денежных средств, управление обеспечением режима безопасности может осуществить сам руководитель предприятия (фирмы) или по совместительству назначенный его приказом сотрудник, имеющий соответствующий опыт работы. Служба безопасности (СБ) предприятия (фирмы), как правило, подчиняется непосредственно руководителю предприятия и создается его приказом.
Она является структурной единицей предприятия, непосредственно участвующей в производственно-коммерческой деятельности. Деятельность СБ осуществляется во взаимодействии со структурными подразделениями предприятия.
Структура и штаты СБ в зависимости от объема работ и особенностей производственно-коммерческой деятельности определяются руководителем предприятия и, по мнению авторов, должны комплектоваться инженерно-техническими работниками специалистами основного профиля работы данного предприятия (фирмы), а также специалистами, имеющими практический опыт защиты информации или работы с различными группами людей. Назначение на должность начальника (зама) СБ предприятия (фирмы), а также его освобождение производится только руководителем предприятия.
Вышеназванные и другие требования вносят в Положение о службе безопасности, которое разрабатывается по указанию директора.
Наиболее оптимальная структура СБ может быть определенная при анализе всех функций обеспечения экономической безопасности и выделении из всего комплекса тех, которые наиболее адекватно соответствуют производственно-коммерческой деятельности предприятия (фирмы).
Для выполнения этого этапа работ приведем наиболее полный комплект функций, выполняемых с привлечением специалистов предприятия службами экономической безопасности.

Функции по защите коммерческой тайны.

1. Выработка критериев выделения ценной информации, подлежащей защите.
2. Определение объектов интеллектуальной собственности, подлежащих охране.
3. Выбор методов защиты (патентование, авторское право, коммерческая тайна).
4. Разработка для последующего утверждения Перечня (дополнений к перечню) сведений, составляющих КТ.
5. Установление правил допуска и разработка разрешительной системы доступа к сведениям, составляющим КТ.
6. Оформление списков лиц (перечней должностей), имеющих право работать с конкретными составляющими коммерческой тайны.
7. Определение списка должностей (лиц), уполномоченных классифицировать информацию.
8. Установление правил и процедур классификации, маркировки документов и других носителей информации, а также вывод их из сферы ограниченного доступа (рассекречивание).
9. Разработка и ввод в действие единого порядка обращения с носителями информации (технологии создания, учет, правила работы, хранение, пересылка, транспортировка, размножение, уничтожение).
10. Составление плана размещения и учет помещений, в которых после соответствующей аттестации разрешено постоянное или временное хранение носителей КТ, работа с ними, а также проведение закрытых совещаний. Установление единого порядка прохода в эти помещения.
11. При непосредственном участии руководителей структурных подразделений и специалистов, имеющих доступ к КТ, планирование, осуществление и контроль за реализацией мероприятий при проведении всех видов работ, в которых используется закрытая информация, классифицированные носители.
12. Оказание методической помощи руководителям подразделений предприятия в разработке и осуществлении мероприятий по защите сведений, в процессе научной, конструкторской, производственной и иной деятельности (какие технологические меры безопасности необходимо ис-

пользовать; какие изменения в технологию надо внести; какие требования целесообразно включить в условия контракта; какую информацию надо защищать даже при выходе товара на рынок и т.п.).

13. Разработка и осуществление совместно со специалистами мер по недопущению разглашения КТ на стадиях:
    - оформления материалов, предназначенных для опубликования в открытой печати, для использования на конференциях, выставках, в рекламной деятельности (аналогичные меры осуществляются в отношении образцов изделий, содержащих КТ);
    - оформления документов (образцов) для передачи заказчику (соисполнителю).
14. Организация с участием исполнителей и специалистов предприятия защитных мероприятий при испытаниях, хранении, транспортировке, уничтожении продукции, содержащей КТ.
15. Разработка порядка и контроль за проведением закрытых совещаний.
16. Определение режимных мер приема представителей других фирм, командированных лиц, представителей контрольных органов власти.
17. Участие совместно со специалистами предприятия в разработке мер по обеспечению безопасности в процессе использования технических средств передачи информации - ЭВМ (ПЭВМ), а также системы противодействия техническим средствам промышленного шпионажа.
18. Организация охраны предприятия, спецпомещений, хранилищ, введение пропускного и внутриобъектового режимов (разграничение доступа в помещения).
19. Формирование предложений на установку технических средств охраны (ТСО), организация работ по их монтажу, эксплуатации ремонту.
20. Участие в подборке и расстановке сотрудников, допускаемых к КТ, выработке мер по снижению текучести кадров.
21. Разработка положений, инструкций, правил, методик и т.п. по обеспечению режима работы для исполнителей закрытых работ, специалистов СБ (несовершенство разработанных норм - одно из главных обстоятельств утечки).
22. Организация и участие в обучении лиц, допущенных к КТ (составление программы обучения, прием зачетов по знанию соответствующих требований режима).
23. С учетом конкретной обстановки совместно с руководителями подразделений в процессе организационной и профилактической работы формирование на плановой основе у сотрудников сознательного отношения к обеспечению защиты информации.
24. Разработка мер по предупреждению несанкционированного уничтожения носителей информации, в том числе в автоматизированных системах хранения, обработки и передачи информации.
25. Контроль исполнения режимных требований: проведение аналитических исследований по оценке надежности принимаемых мер защиты КТ и выработка предложений по повышению эффективности охраны.
26. Проведение служебных расследований по фактам нарушения режима обращения с КТ.

Функции по обеспечению защиты имущественной собственности предприятия (с учетом его особенностей и уязвимости).

1. Определение системы охраны предприятия, дислокации постов, средств ТСО, противопожарной автоматики, связи.
2. Выделение помещений (участков), где хранятся товарно-материальные ценности (деньги), и осуществление через руководителей соответствующих подразделений мер по повышению надежности их физической защиты.
3. Определение участков, уязвимых во взрывопожарном отношении, выход их строя которых может нанести серьезный ущерб предприятию и выработка мер по нейтрализации угроз.
4. Определение технологического оборудования, выход их строя которого может привести к большим экономическим потерям, и разработка мер по нейтрализации угроз.

5. Определение уязвимых мест в технологии производственного цикла, несанкционированное изменение в которых может привести к утрате качества выпускаемой продукции и нанести материальный ущерб, и принятие соответствующих мер.
6. Разработка, ввод в действие и поддержание на охраняемой территории внутри пропускного и объектового режима (порядок, время пропуска рабочих, посетителей на территорию предприятия, в том числе и в праздничные дни; порядок ввоза (ввоза) или выноса (вноса) материальных ценностей, готовой продукции, материалов и т.п.; местоположение и количество контрольных проходов и проездов; помещения и подразделения, доступ куда ограничен; система пропусков и документации).
7. Разработка документов, регламентирующих административно-правовую основу деятельности по охране имущественных ценностей предприятия (положение об охране; инструкция о порядке обеспечения сохранности материальных и документальных ценностей предприятия; инструкция о пропускном и внутриобъектовом режиме).
8. Доведение требований (соответствующих корректив) по вопросам охраны, пропускного и внутриобъектового режимов до сотрудников предприятия.
9. Контроль исполнения и анализ состояния надежности хранения материальных ценностей, охраны, пропускного и внутриобъектового режимов.
10. Проведение служебных расследований по фактам нарушения порядка работы с имущественными ценностями.
11. Организация взаимодействия с федеральными органами безопасности и органами внутренних дел по обеспечению экономической безопасности предприятия (с учетом компетенции этих органов).

Функции по обеспечению безопасности персонала предприятия.

1. Разработка мер обеспечения физической защиты персонала; организация охраны (личной охраны, охраны средств передвижения), пропускного и внутриобъектового режимов; установления соответствующего порядка приема посетителей, работы секретарей-референтов и т.п.
2. Обеспечение персонала средствами технической защиты от несанкционированного проникновения в помещения (кабинеты), в автомашины, на автостоянку, в квартиру для фиксации попыток преступных действий (установка магнитофонов, кинокамер), для скрытой связи руководителя с охраной предприятия.
3. Определение перечня информации, не подлежащей разглашению (не входящей в КТ) посторонним лицам.
4. Сбор СБ информации о признаках, характерных для конкретных видов угроз персоналу (сотрудникам).
5. Обеспечение контроля за проведением ремонтных, профилактических работ, осуществляемых сторонними организациями на предприятии (при необходимости проводятся специальные обследования после завершения работ этих помещений, автомашин, устройств, приборов).
6. Подготовка персонала к действиям в экстремальных ситуациях (выработка навыков оценки информации, соответствующих норм поведения и принятия решений).
7. Обучение персонала и членов их семей выявлению признаков, указывающих на подготовку направленных против них действий.
8. Правовое обучение персонала: правовые возможности защиты от преступника (нормы необходимой обороны, крайней необходимости).
9. Установление и поддержание практических форм взаимодействия СБ с правоохранительными органами по обеспечению безопасности персонала (при получении данных о готовящихся, имевших место противоправных действиях в отношении персонала, затрагивающих вопросы обеспечения экономической безопасности предприятия и т.п.).

Информационное обеспечение деятельности предприятия.

1. Юридически грамотное и экономически безопасное информационное обслуживание деятельности предприятия на рынке рабочей силы, взаимодействия с общественностью и печатью.
2. Обеспечение надежности кооперативных связей, исключающее как одностороннюю зависимость, так и деловые контакты с недобросовестными деловыми партнерами и посредниками.
3. Участие в подготовке и проведении специальных информационных акций, повышающих репутацию фирмы в глазах партнеров, общественности, органов власти (в том числе и в отношении СБ в формировании у окружения убеждения в силе и эффективности ее деятельности по защите).
4. Совместно с другими подразделениями предприятия получение аналитическим путем информации о конкурентах, касающейся возможной подготовки и проведения ими мероприятий, классифицируемых как недобросовестная конкуренция, и выработка мер по их нейтрализации.
5. Планирование организационных мер сбора, оценки информации в интересах обеспечения стабильной и эффективной деятельности предприятия (перечень вопросов, по которым необходим сбор информации, кто, как и когда ее собирает).
6. Разработка мер по накоплению, хранению, использованию, ускоренному доведению до исполнителей ценной информации, в том числе классифицированных документов и сведений.
7. Информационное обеспечение деятельности СБ по получению данных о готовящихся посягательствах на интересы предприятия.
8. Получение и обобщение открытых публикаций по вопросам обеспечения экономической безопасности предприятий и выработка на их основе предложений.

Выбрав из приведенного перечня функции, выполнение которых обеспечивало бы надежную защиту предприятия (фирмы), руководитель определяет структуру и количественный состав СБ.
При оптимальной структуре СБ ее работники должны перекрывать все возложенные на данное подразделение функции. Одновременно исключается дублирование действии не загруженность работников.
Директор предприятия (фирмы) может предоставлять СБ следующие права:

- вносить предложения о запрещении работ с документами, оставляющими КТ, а также об изменении порядка хранения или перевозки товаров других ценностей при выявлении нарушений, которые могли бы повлечь нанесение экономического ущерба;
- контролировать с привлечением специалистов предприятия состояние и надежность защиты закрытых работ и имущества, денежных средств;
- выходить с ходатайством об отстранении конкретных исполнителей предприятия (фирмы) от ведения закрытых работ, переговоров с другими фирмами, перевозки, хранения, охраны имущественной собственности;
- согласовать мероприятия, разрабатываемые подразделениями предприятия в целях обеспечения экономической безопасности;
- давать в рамках своей компетенции руководителям подразделений и исполнителям обязательные для исполнения рекомендации; проводить по вопросам обеспечения экономической безопасности предприятия обучение и инструктаж сотрудников;
- по приказу директора предприятия (фирмы) принимать участие или проводить самостоятельно расследование фактов разглашения КТ, утраты документов и изделий, хищений товаров, других ценностей, а также грубых нарушений установленного режима экономической безопасности предприятия.

Решения и организационно-распорядительные документы по вопросам отношения СБ с другими подразделениями предприятия при необходимости оформляются приказами директора. О наличии такого подразделения и его полномочиях должны знать все сотрудники предприятия. Это объясняет-

ся прежде всего тем, что даже не работающий с КТ сотрудник предприятия может стать создателем ценнейшей информации, требующей немедленной защиты.
Служба безопасности предприятия (фирмы) подчиняется непосредственно руководителю предприятия и создается в соответствии с его приказом. Служба безопасности является структурной единицей предприятия, непосредственно участвующей в производственно-коммерческой деятельности. Работа этого отдела проводится во взаимодействии со структурными подразделениями предприятия.
Структура и штат СБ в зависимости от объема работ и особенностей производственно-коммерческой деятельности определяются руководителем предприятия и, как правило, должны комплектоваться инженерно-техническими работниками - специалистами основного профиля работы данного предприятия (фирмы), а также специалистами, имеющими практический опыт защиты информации или работы с различными группами людей. Назначение на должность начальника (зама) СБ предприятия (фирмы), а также его освобождение производится только руководителем предприятия. Вышеназванные и другие требования вносят в Положение о службе безопасности, которое разрабатывается по указанию директора.
При выполнении возложенных на СБ задач ее сотрудники используют в своей работе различные формы и методы: издание организационно-распорядительной и методической документации, проведение в подразделениях предприятия комплексных и целевых проверок, заслушивание сообщений руководителей соответствующего уровня о состоянии режима в подразделении, различные формы и методы профилактической работы и т.д.

Руководитель службы безопасности регулярно, в установленные сроки отчитывается в своей работе перед директором предприятия.
Приступая к разработке системы мер по обеспечению защиты экономической безопасности предприятия, его руководитель (или начальник СБ) должен получить ответы на следующие вопросы:

- что конкретно необходимо защищать (охранять), от кого и когда?
- кто организует и обеспечивает защиту (охрану)?
- как оценивать эффективность и достаточность защиты (охраны)?

Для иллюстрации рассмотрим этапы организации системы защиты коммерческой тайны.

1. Определяется предмет защиты. Разрабатывается Перечень сведений, составляющих КТ, в котором выделяется наиболее ценная информация, нуждающаяся в особой охране, учитываются требования по защите других предприятий (фирм), участвующих в совместных работах.
2. Устанавливаются периоды существования конкретных сведений в качестве КТ.
3. Выделяются категории носителей ценной информации: персонал, документы, изделия и материалы; технические средства хранения, обработки и передачи информации; физические излучения. Для обеспечения восприятия разрабатываемой системы защиты можно составить схему, в которой указываются конкретные сотрудники, осведомленные о коммерческой тайне, названия (категории) классифицированных документов и изделий и т.п.
4. Перечисляются стадии (этапы) работ, время материализации КТ в носителях информации применительно к пространственным зонам (местам работы с ними внутри и за пределами предприятия). Например, отчеты НИОКР на рабочих местах исполнителей; журнал результатов испытаний изделия на испытательном стенде; договор, подписываемый за рубежом; выступления участников отчетных совещаний в конкретных кабинетах; размножение классифицированных документов на множительном участке; образцы изделий, демонстрирующиеся на выставках и т.п.

5. Составляется схема работ с конкретными сведениями, материализованными в носителях, в пределах предприятия (фирмы) и вне его и предполагаемого их перемещения.
   Рассматриваются возможные для предприятия несанкционированные перемещения, которые могут быть использованы конкурентами для овладения коммерческой тайной.
6. Разрабатываются (или корректируются) в процессе анализа разрешительные подсистемы допуска и доступа к конкретным сведениям, составляющим КТ.
7. определяется, кто реализует мероприятия и кто несет ответственность за защиту конкретной информации, процессов работ с классифицированными данными.
   Намечаются меры по координации, назначаются конкретные исполнители.
8. Планируются действия по активизации и стимулированию лиц, задействованных в защите.
9. Проверяется надежность принятых к реализации мер обеспечения защиты.

Анализ состояния эффективности экономической безопасности включает в себя:

- изучение и оценку фактического состояния;
- выявление недостатков и нарушений режима, которые могут привести к утрате физических носителей тайны (ценного имущества) или разглашению КТ;
- установление причин и условий выявленных недостатков и нарушений;
- выработку положений, направленных на устранение недостатков и предотвращение нарушений.

Объектами анализа и контроля в зависимости от поставленных задач могут быть:

- соблюдение норм, правил хранения и охраны в помещениях, спец хранилищах, на рабочих местах;
- ведение учета и обеспечение личной ответственности за выполнение данной функции;
- соблюдение порядка хранения, учета и уничтожения;
- соблюдение требований порядка обращения;
- меры по предотвращению несанкционированного выноса носителей КТ за территорию предприятия;
- соблюдение режима и охраны при транспортировке, рассылке, доставке;
- организация доступа приглашенных, командированных, приглашенных лиц к информации предприятия;
- организация проведения совещаний, выставок, переговоров и т.п.;
- уровень знаний требований режима лиц, допущенных к закрытым работам и документам;
- степень обеспеченности службы безопасности надежными хранилищами, запирающими устройствами, средствами опечатывания;
- уровень обеспеченности сотрудников соответствующими рабочими местами для работы с носителями секретов;
- состояние пропускного и внутреннего режима в зданиях, помещениях, в целом на предприятии;
- механизм распределения носителей КТ по уровням исполнения и управления;
- обоснованность доступа к различным видам носителей конкретных групп сотрудников;
- порядок обращения с носителями на рабочих местах;

- порядок пользования средствами получения, обработки, хранения, отображения, передачи информации;
- порядок обмена сведениями внутри предприятия и с внешними партнерами;
- своевременность и правильность классификации и раскрытия сведений;
- организация и проведение выставок, конференций, симпозиумов и т.д.;
- качество разработки организационно-методических документов, выполнение планов работ и специальных мероприятий по защите информации;
- уровень и полнота выполнения требований руководства предприятия;
- состояние профилактической работы с сотрудниками;
- уровень организационно-методического обеспечения взаимодействия между подразделениями;
- время поиска и доведения информации до исполнителей.

Анализ включает в себя моделирование различных каналов утечки информации, возможных приемов и способов несанкционированного получения закрытой информации.

Иностранные фирмы к числу наиболее вероятных каналов утечки классифицированной информации относят:

- совместную с другими фирмами деятельность, участие в переговорах;
- фиктивные запросы со стороны о возможности работать в фирме на различных должностях;
- экскурсии и посещения фирмы;
- общения торговых представителей фирмы о характеристиках изделия;
- чрезмерную рекламу;
- поставки смежников;
- консультации специалистов со стороны, которые в результате этого получают доступ к установкам и документам фирмы;
- публикации в печати и выступления;
- совещания, конференции, симпозиумы и т.п.;
- разговоры в нерабочих помещениях;
- обиженных сотрудников фирм.

Службе безопасности при организации защиты коммерческой тайны необходимо учитывать следующие возможные методы и способы сбора информации:

- опрос сотрудников изучаемой фирмы при личной встрече;
- навязывание дискуссий по интересующим проблемам;
- рассылка в адреса предприятий и отдельных сотрудников вопросников и анкет;
- ведение частной переписки научных центров и ученых со специалистами.

Для сбора сведений в ряде случае представители конкурентов могут использовать переговоры по определению перспектив сотрудничества, созданию совместных предприятий.
Наличие такой формы сотрудничества, как выполнение совместных программ, предусматривающих непосредственное участие представителей других организаций в работе с документами, посещение рабочих мест, расширяет возможности для снятия копий с документов, сбора различных образцов материалов, проб и т.д. При этом с учетом практики развитых стран экономические соперники могут прибегнуть в том числе и к противоправным действиям, промышленному шпионажу.
Наиболее вероятно использование следующих способов добывания информации:

- визуальное наблюдение;
- подслушивание;
- техническое наблюдение;
- прямой опрос, выведывание;
- ознакомление с материалами, документами, изделиями и т.д.;
- сбор открытых документов и других источников информации;
- хищение документов и других источников информации;
- изучение множества источников информации, содержащих по частям необходимые сведения.

Аналитические исследования, моделирование вероятных угроз позволяют наметить при необходимости дополнительные меры защиты. При этом следует оценить вероятность их выполнения, наличие методического материала, материального обеспечения, готовность СБ и персонала их выполнить. При планировании учитываются имевшие место на предприятии недостатки в обеспечении сохранности КТ.

Планируемые мероприятия должны:

- способствовать достижению определенных задач, соответствовать общему замыслу;
- являться оптимальными.

Не должны:

- противоречить законам, требованиям руководителя фирмы (интересам кооперирующихся фирм);
- дублировать другие действия.

Организация системы защиты вписывается в обстановку на фирме. В связи с этим крайне важен учет принципиальных проходящих в ней и предполагаемых изменений.
Таким образом, система организации защиты КТ включает в себя комплекс заранее разработанных на определенный срок мер, охватывающих совокупность всех видов деятельности, направленных на совершенствование обеспечения сохранности информации с учетом изменений внешних и внутренних условий и предписывающих конкретным лицам или подразделений определенный порядок действий.