**Тема 12: "ОРГАНИЗАЦИОННЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ"**

***12.1 Общие положения организационной защиты***

**Организационная защита** – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативной основе, что исключает или существенно осложняет неправомерное овладение конфиденциальной информацией и проявления внутренних и внешних угроз.

Организационная защита обеспечивает:

- организацию режима, охраны, работу с кадрами, с документами;

- использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз деятельности предприятия (организации).

Организационные мероприятия играют существенную роль в создании надежного механизма защиты информации, поскольку возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловливаются не техническими аспектами, а злоумышленными действиями и небрежностью пользователей или персонала. Именно люди являются главной угрозой, поэтому "человеческий фактор" заслуживает особого внимания.

Угрозы информационной безопасности, связанные с людьми, практически невозможно предотвратить с помощью технических мероприятий.

Для этого необходима совокупность организационно-правовых и организационно-технических мероприятий, которые исключали бы (или сводили к минимуму) возможность возникновения опасности утечки конфиденциальной информации.

К основным организационным мероприятиям обычно относят следующие:

**1. Организация режима и охраны**.

Цель:

- исключение возможности тайного проникновения на территорию и в помещение посторонних лиц;

- обеспечение удобства прохода и перемещения сотрудников и посетителей;

- создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа;

- контроль и соблюдение временного режима труда и пребывания на территории персонала предприятия;

- организация и поддержка надежного пропускного режима и контроля сотрудников и посетителей; организация работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерой ответственности за нарушение правил защиты информации.

**2.** **Организация работы с документами и документируемой информацией**, включая организацию разработки и использование документов и носителей конфиденциальной информации, их учет, использование, возврат, хранение и уничтожение.

**3.** **Организация использования технических средств** сбора, обработки и хранения конфиденциальной информации.

**4.** **Организация работы по анализу внутренних и внешних угроз** конфиденциальной информации и разработка мероприятий по обеспечению ее защиты.

**5. Организация работы по проведению систематического** контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

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

***12.2 Особенности организационной защиты компьютерных информационных систем и сетей***

Организация защиты компьютерных информационных систем и сетей определяет порядок и схему функционирования их основных подсистем, использования устройств и ресурсов, взаимоотношения пользователей между собой в соответствии с нормативно-правовыми требованиями и правилами.

Защита информации на основе организационных мероприятий играет значительную роль в обеспечении надежности и эффективности, поскольку несанкционированный доступ и утечка информации чаще всего обусловлены злоумышленными действиями, небрежностью пользователей или персонала. Эти факторы практически невозможно исключить или локализовать с помощью аппаратных и программных средств, криптографии и физических средств защиты, поэтому совокупность организационных, организационно правовых и организационно-технических мероприятий, которые применяются вместе с техническими методами, имеют целью исключить, уменьшить или полностью устранить потери при действии разнообразных деструктивных факторов.

Организационные средства защиты компьютерных информационных систем и сетей чаще всего применяются в **следующих случаях**:

- при проектировании, строительстве и оборудовании помещений, узлов сети и других объектов информационной системы, исключающих влияние стихийных бедствий, возможность недозволенного проникновения в помещения и др.;

- при подборе и подготовке персонала в этом случае предусматривается проверка лиц, которые принимаются на работу, создание условий, при которых персонал был бы заинтересован в сохранности информации, обучение правилам работы с закрытой информацией, ознакомление с мерой ответственности за нарушение правил защиты и т.д.;

- при хранении и использовании документов и других носителей (маркировка, регистрация, определение правил выдачи и возвращения, ведение документации и др.);

- при соблюдении надежного пропускного режима к техническим средствам, к ЭВМ и информационным системам при сменной работе (выделение ответственных за защиту информации в сменах, контроль за работой персонала, ведение (возможно и автоматизированное) журналов работы, уничтожение в установленном порядке закрытых производственных документов);

- при внесении изменений в программное обеспечение (строгое санкционирование, рассмотрение и утверждение проектов изменений, проверка их на удовлетворение требований защиты, документальное оформление изменений и т.п.);

- при подготовке и контроле работы пользователей.

Обязательными документами являются Положения о службе защиты информации в ИС и План защиты информации в ИС.

Положение о службе защиты информации в ИС определяет задачи, функции, штатную структуру службы защиты информации, обязанности, права и ответственность работников службы, взаимодействие с другими подразделениями организации.

План защиты информации в ИС определяет: задачи защиты, классификацию информации, описание технологии обработки секретной информации, а так же календарный план работ по защите информации в ИС.

План защиты определяет перечень организационных мероприятий по защите информации в ИС.

**Организационные мероприятия по защите информации в ИС.**

Для обеспечения режима секретности во время обработки в ИС информации, что составляет государственную тайну, и надлежащего функционирования комплексной системы защиты информации создается служба защиты информации. Состав и функции службы защиты информации определяются в соответствии с документом "Положения о службе защиты информации".

Полномочия пользователей устанавливаются руководителем предприятия и согласовываются с РСО. Учет пользователей информационных систем осуществляется с помощью учетных карточек, на основании которых администратор безопасности вводит, изменяет или удаляет информацию о пользователе ИС. Учетные карточки заполняются и хранятся в РСО.

Учетная карточка обычного пользователя содержит такие данные:

- имя пользователя для регистрации в ОС;

- фамилию и инициалы, подразделение и должность пользователя;

- уровень допуска пользователя; перечень ролей пользователя.

Выполнение работ в ИС позволяется работникам, которые имеют оформленный в установленном порядке допуск к государственной тайне.

РСО предприятия обеспечивает выполнение требований нормативных документов относительно обеспечения режима секретности во время работы с информацией, что составляет государственную тайну, а именно:

- контроль за процессом печати информации и копированием на съемные носители;

- учет печатных документов; учет съемных носителей (дискет, накопителей USB Flash и др.);

- учет технических средств, что прошли спецобследования;

- ведение учетных карточек пользователей.

Основные функции относительно обеспечения защиты информации в ИС возлагаются на администратора безопасности. К его основным функциям относятся такие:

- ведение учетных карточек пользователей;

- ведение базы данных защиты;

- установление параметров работы системы;

- изменение, в случае необходимости, владельца документов;

- отслеживание потенциально опасных событий;

- архивация данных защиты.

Системный администратор должен выполнять такие функции:

- сопровождение программного обеспечения ИС;

- обеспечение антивирусной защиты;

- сопровождение аппаратного обеспечения (вместе с ответственным за безопасность информации).

Ответственный за безопасность информации должен выполнять такие функции:

- организация печати и учета носителей, что содержат ИзОД;

- наблюдение за работой системы;

- настройка аппаратного обеспечения.

За организацию работ с документами отвечает администратор документов. К его функциям относятся такие:

- создание баз документов;

- управление доступом к документам.

Все действия, которые прямо или опосредствовано могут повлиять на защищенность информации (изменения разрешений на доступ к файлам и папкам, очистки журналов ОС, изменения настроек BIOS и тому подобное), системный администратор выполняет с разрешения администратора безопасности, что фиксируется в Журнале.

Контроль за соблюдением персоналом и пользователями ИС положений политики безопасности возлагается на РСО и службу защиты информации.

Ответственность за обеспечение режима секретности в ИС, своевременная разработка и внедрение необходимых мер возлагается на руководителя организации и руководителей ее структурных подразделений

***12.3 Служба безопасности предприятия***

Одним из важнейших организационных мероприятий является создание специальных штатных служб защиты информации в закрытых информационных системах в виде администратора безопасности сети и администратора безопасности распределенных баз и банков данных, которые содержат сведения конфиденциального характера.

Вполне очевидно, что организационные мероприятия должны четко планироваться, направляться и осуществляться определенной организационной структурой, определенным специально созданным для этих целей структурным подразделением, укомплектованным соответствующими специалистами по безопасности деятельности и защиты информации.

Чаще всего таким структурным подразделением является служба безопасности предприятия (фирмы, организации), на которую возлагаются следующие функции:

- организация и обеспечение охраны персонала, материальных и финансовых ценностей и защиты конфиденциальной информации;

- обеспечение пропускного и внутриобъектового режима на территории, в зданиях и помещениях, контроль соблюдения требований режима сотрудниками, смежниками, партнерами и посетителями;

- руководство работами по правовой и организационной регуляции отношений по защите информации;

- участие в разработке основополагающих документов с целью закрепления в них требований обеспечения безопасности и защиты информации, а также положений о подразделениях, трудовых договорах, соглашениях, подрядах, должностных инструкциях и обязанностях руководства, специалистах, рабочих и служащих;

- разработка и осуществление вместе с другими подразделениями мероприятий по обеспечению работы с документами, которые содержат конфиденциальные сведения; при всех видах работ организация и контроль выполнения требований "Инструкции по защите конфиденциальной информации";

- изучение всех сторон производственной, коммерческой, финансовой и другой деятельности для выявления и следующего противодействия каким-нибудь попыткам нанесения ущерба, ведение учета и анализ нарушений режима безопасности, накопление и анализ данных о злоумышленных стремлениях конкурентной и других организаций, о деятельности предприятия и его клиентов, партнеров, смежников;

- разработка, ведение, обновление и пополнение "Перечня сведений, что носят конфиденциальный характер" и других нормативных актов, которые регламентируют порядок обеспечения и защиты информации;

- обеспечение строгого выполнения требований нормативных актов по защите производственных секретов предприятия;

- осуществление руководства службами и подразделениями безопасности подведомственных предприятий, организаций, заведений и другими структурами в части оговоренных в договорах условий по защите информации;

- организация и регулярное проведение учета сотрудников предприятия и службы безопасности по всем направлениям защиты информации и обеспечения безопасности производственной деятельности;

- ведения учета и строгого контроля выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации и каналами проникновения к источникам информации, которые находятся под охраной;

- обеспечение проведения всех необходимых мероприятий по пресечению попыток нанесения морального и материального ущерба со стороны внутренних и внешних угроз;

- поддержка контактов с правоохранительными органами и службами безопасности соседних предприятий для изучения криминогенной обстановки в районе, (зоне) и предоставление взаимной помощи в кризисных ситуациях.

Служба безопасности является самостоятельной организационной единицей предприятия, которая подчиняется непосредственно руководителю предприятия. Возглавляет службу безопасности начальник службы безопасности в должности заместителя руководителя предприятия по безопасности.

Организационно служба безопасности может состоять из следующих структурных единиц:

- подразделения режима и охраны;

- специального подразделения по обработке документов конфиденциального характера (Служба защиты информации);

- инженерно-технических подразделений;

- информационно-аналитических подразделений.

В таком составе служба безопасности способна обеспечить защиту конфиденциальной информации от каких-либо угроз.

На службу безопасности возлагаются следующие задачи:

- определение круга лиц, которые в соответствии с положением, которое они занимают на предприятии, прямо или косвенно имеют доступ к сведениям конфиденциального характера;

- определение участков сосредоточения конфиденциальных сведений;

- определение круга посторонних предприятий, связанных с данным предприятием кооперативными связями, на которых в силу производственных отношений возможен выход из-под контроля сведений конфиденциального характера;

- выявление круга лиц, не допущенных к конфиденциальной информации, но которые проявляют повышенный интерес к таким сведениям;

- выявление круга предприятий, в том числе иностранных, что заинтересованы в доступе к сведениям, которые охраняются, с целью нанесения экономического ущерба данному предприятию, устранения экономического конкурента или его компрометации;

- разработка системы защиты документов, которые содержат сведения экономического характера;

- определение на предприятии участков, уязвимых в аварийном отношении, выход из строя которых может нанести материальный ущерб предприятию и сорвать поставки готовой продукции или комплектующих предприятиям, связанных с ним кооперацией;

- определение на предприятии технологического оборудования, выход (или выведение) которого из строя может привести к большим экономическим потерям;

- определение уязвимых мест в технологии производственного цикла, несанкционированное изменение в котором может привести к потере качества продукции и нанести материальный или моральный ущерб предприятию (потеря конкурентоспособности);

- определение на предприятии мест, несанкционированное посещение которых может привести к изъятию (хищению) готовой продукции или полуфабрикатов, заготовок и т.п. и организация их физической защиты;

- определение и обоснование мероприятий правовой, организационной и инженерно-физической защиты предприятия, персонала, продукции и информации;

- разработка необходимых мер, направленных на совершенствование системы экономической, социальной и информационной безопасности;

- внедрение в деятельность предприятия новейших достижений науки и техники, передового опыта в области обеспечения экономической и информационной безопасности;

- организация обучения сотрудников службы безопасности в соответствии с их функциональными обязанностями;

- изучение, анализ и оценка состояния обеспечения экономической и информационной безопасности предприятия и разработка предложений и рекомендаций для его усовершенствования;

- разработка технико-экономических обоснований, направленных на приобретение технических средств, получения консультации у специалистов, разработку необходимой документации с целью усовершенствования системы мероприятий по обеспечению экономической и информационной безопасности.

Организационные мероприятия являются решающим звеном формирования и реализации комплексной защиты информации и создания системы безопасности предприятия.