**Тема 11: "ПРАВОВЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ"**

***11.1 Основные направления обеспечения информационной безопасности***

Высокая степень информатизации современных предприятий, учреждений и организаций обусловливает необходимость всестороннего комплексного подхода к обеспечению защиты информации, как от внутренних, так и от внешних угроз.

С учетом практики, что сложилась на настоящее время, выделяют следующие направления защиты информации:

* правовая защита это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, которые обеспечивают защиту информации на правовой основе;
* организационная защита это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, которая исключает или ослабляет нанесение каких-либо убытков предприятию;
* инженерно-техническая защита это использование разнообразных технических средств, которые препятствуют нанесению убытков предприятию.

Кроме того, меры защиты, ориентированные на обеспечение безопасности информации, могут быть охарактеризованы целым рядом параметров, которые отображают, кроме направлений, ориентацию на объекты защиты, характер угроз, способы действий, их распространение, размах и масштабность.

Так, по характеру угроз защитные мероприятия ориентированы на защиту информации от разглашения, утечки и несанкционированного доступа.

По способу действия их можно разделить на предупреждение, выявление, прекращение и возмещение убытков или других потерь.

По охвату защитные мероприятия могут распространяться на территорию, здание, помещение, аппаратуру или отдельные элементы аппаратуры.

Масштабность мероприятий защиты характеризуется как объектовая, групповая или индивидуальная защита

***11.2 Законодательно-правовая база обеспечения информационной безопасности на предприятии***

Правовая защита информации на межгосударственном и государственном уровне определяется межгосударственными договорами, конвенциями, декларациями и реализуется патентами, авторским правом и лицензиями на их защиту. На государственном уровне правовая защита регулируется государственными и ведомственными актами.

Правовая защита информации на предприятии обеспечивается нормативно законодательными актами, совокупность которых представляет собой систему от Конституции до функциональных обязанностей и контракта конкретного исполнителя, которые, с одной стороны, определяют перечень сведений, подлежащих охране, и с другой стороны ответственность за их разглашение.

Опираясь на государственные правовые акты и учитывая ведомственные интересы на уровне конкретного предприятия (фирмы, организации), разрабатываются собственные нормативно-правовые документы, ориентированные на обеспечение информационной безопасности

***11.3 Нормативные акты предприятия по информационной безопасности***

Основным документом по информационной безопасности современного коммерческого предприятия является документ под названием "Политика информационной безопасности предприятия (компании, организации и т.д.)".

Политика безопасности организации – совокупность руководящих принципов, правил, процедур и практических приёмов в области безопасности, которые регулируют управление, защиту и распределение ценной информации.

"Политика безопасности" включает в себя комплекс превентивных мер по защите информации на предприятии и содержит требования в адрес персонала, менеджеров и технических служб.

Основные направления разработки политики безопасности:

* определение, какие данные и насколько серьезно необходимо защищать,
* определение, кто и какой ущерб может нанести фирме в информационном аспекте,
* вычисление рисков и определение схемы уменьшения их до приемлемой величины.

Целью политики информационной безопасности является обеспечение развития организации в области ИБ в соответствии с целями бизнеса и требованиями, предъявляемыми различными регулирующими органами.

Данный документ регламентирован международными стандартами по информационной безопасности ISO 27001 и ISO 27002

Стандарт ISO 27001 определяет, что политика информационной безопасности должна быть одобрена руководством компании, опубликована и доведена до сведения всех сотрудников и заинтересованных сторонних организаций.

Политика информационной безопасности должна включать следующее:

* Определение понятия информационная безопасность;
* Цели обеспечения информационной безопасности;
* Признание важности обеспечения информационной безопасности;
* Заявление о намерении руководства компании поддерживать цели и принципы обеспечения информационной безопасности, соответствующим целям бизнеса;
* Подход к управлению рисками и выбора контрмер для минимизации рисков информационной безопасности;
* Краткое объяснение принципов информационной безопасности, требования информационной безопасности (выполнение требований регуляторов, обучение в области информационной безопасности, обеспечение непрерывности бизнеса, последствия нарушения положений политики информационной безопасности);
* Определение общих и специфических обязанностей по обеспечению информационной безопасности;
* Ссылки на более детальные политики и процедуры поддерживающие политику информационной безопасности.

Политика информационной безопасности должна пересматриваться через определенные интервалы времени и в случае значительных изменений (изменения структуры компании, стратегических целей бизнеса) для того, чтобы оставаться актуальной и эффективной.

Помимо того, что политика информационной безопасности должна быть утверждена руководством и должна определять принципы информационной безопасности, подход к выбору мер по снижению рисков информационной безопасности, учитывать требования законодательства и закрепленные в контрактах, не противоречить подходу к управлению рисками, принятом в компании, она должна также определять критерии для оценки рисков.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы, и стратегия защиты определена, составляется программа обеспечения информационной безопасности, которая должна реализовать принятую политику безопасности.

***11.4 Формы правовой защиты информации на предприятии***

В зависимости от характера информации, ее доступности для заинтересованных потребителей, а также экономической целесообразности конкретных защитных мероприятий, могут быть избраны следующие формы защиты информации:

* патентование;
* признание сведений коммерческой тайной ("ноу-хау");
* авторское право;
* товарные знаки;
* применения норм обязательного права.

Существует определенная разница между авторским правом и коммерческой тайной.

К *авторскому праву* прибегают при широкой публикации своей информации, в то время как коммерческую тайну держат в секрете. Очевидно, что по сравнению с патентом и авторским правом коммерческая тайна и производственная тайне являются наиболее удобными, надежными и гибкими формами защиты информации.

*Коммерческая тайна* – это сведения, которые не являются государственными секретами и связанны с производством, технологией, управлением, финансами и другой деятельностью, разглашение, утечка и несанкционированный доступ к которой может привести к убыткам их владельцев (упущенная выгода).

К коммерческой тайне не относятся:

- сведения, которые охраняются государством;

- сведения, которые являются общеизвестными на законном основании;

- сведения о негативных сторонах деятельности;

- учредительные документы и сведения о хозяйственной деятельности.

Кроме вышеизложенных форм правовой защиты информации находит широкое распространение официальная передача права на пользование информацией в виде лицензии.

*Лицензия* – это разрешение, выданное государством на проведение некоторых видов хозяйственной деятельности, включая внешнеторговые операции (ввоз и вывоз) и предоставления права использовать защищенные патентами изобретения, технологии, методики. Лицензионные разрешения предоставляются на определенное время и на определенные виды товаров.

Создавая систему информационной безопасности, необходимо четко понимать, что **без правового обеспечения** защиты информации какие-либо претензии к недобросовестному сотруднику, клиенту, конкуренту и должностному лицу будут просто безосновательными.

Если перечень сведений конфиденциального характера не доведен своевременно до каждого сотрудника (естественно, если от допущен к выполнению должностных обязанностей) в письменном виде, то сотрудник, который похитил важную информацию при нарушении установленного порядка работы с нею скорее всего не будет наказан.

***11.5 Другие документы предприятия, в которых отражаются вопросы обеспечения информационной безопасности***

Правовые нормы обеспечения безопасности и защиты информации на конкретном предприятии (фирме, организации) отображаются в совокупности учред*ительных, организационных и функциональных* документов.

Требования обеспечения безопасности и защиты информации отображаются в Уставе предприятия (учредительном договоре) в виде следующих положений:

- предприятие имеет право определять состав, объемы и порядок защиты конфиденциальных сведений, требовать от своих сотрудников обеспечения их сохранения и защиты от внутренних и внешних угроз;

- предприятие обязано обеспечивать сохранность конфиденциальной информации.

Такие требования дают администрации предприятия следующие права:

- создавать организационные структуры по защите конфиденциальной информации ("Служба защиты информации");

- издавать нормативные и предписывающие документы, которые определяют порядок выделения сведений конфиденциального характера и механизмы их защиты;

- включать требования по защите информации в соглашения по всем видам хозяйственной деятельности;

- требовать защиты интересов предприятия со стороны государственных и судебных инстанций;

- распоряжаться информацией, которая является собственностью предприятия, с целью получения выгоды и недопущения экономических убытков коллективу предприятия и его владельцу;

- разрабатывать "Перечень сведений конфиденциальной информации'".

Требования правового обеспечения защиты информации предусматриваются в *коллективном*

Обязанности конкретного сотрудника, рабочего или служащего относительно защиты информации обязательно должны быть оговорены в трудовом договоре (контракте). В соответствии с КЗоТ при заключении трудового договора работник обязывается выполнять определенные требования, которые действуют на данном предприятии. Независимо от формы заключения договора (устного, письменного ли) подпись работника на приказе о приеме на работу подтверждает его согласие с условиями договора.

Требования по защите конфиденциальной информации могут быть оговорены в тексте договора, если договор заключается в письменной форме. Если же договор заключается в устной форме, то действуют требования по защите информации, которые вытекают из нормативно-правовых документов предприятия. При заключении трудового договора и оформлении приказа о приеме на работу нового сотрудника делается отметка об осведомленности его с порядком защиты информации предприятия. Это создает необходимый элемент привлечения данного лица в механизм обеспечения информационной безопасности.

Не следует считать, что после подписания такого соглашения с новым сотрудником тайна будет сохранена. Это только предупреждение сотруднику, что в дело вступает система мероприятий по защите информации, и правовая основа для того, чтобы прекратить его неверные или противоправные действия. Следующая задача – не допустить потери коммерческих секретов.

Вопросы соблюдения конфиденциальности отражаются отдельным пунктом в договорах, соглашениях и других документах, которые заключаются между различными предприятиями.

Правовая регуляция на предприятии необходима для совершенствования механизма предупреждения противоправных действий по отношению к информационным ресурсам, для уточнения и закрепления заданий и правомочия отдельных субъектов в сфере предупредительной деятельности, охраны прав и законных интересов граждан и организации.

Правовые мероприятия обеспечения безопасности и защиты информации являются основой порядка деятельности и поведения сотрудников предприятия и определяют меру их ответственности за нарушение установленных норм.