НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ЦЕНТР ПРЕДПРИНИМАТЕЛЬСКИХ РИСКОВ»

СИСТЕМА ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

(КОНСПЕКТ)

Санкт-Петербург
2008

Содержание:

1. Конфиденциальная информация как объект защиты. Структура, цели и задачи системы защиты конфиденциальной информации на предприятии.

С появлением и развитием информационно-управляющих технологий автоматизированных средств коммуникации, усложнением процедур обмена сообщениями и их обработки в комплексах специального и общего назначения все актуальнее становятся вопросы безопасности информации (information security), т. е. предотвращения несанкционированного распространения (утечки, хищения), утраты, уничтожения, искажения, подделки или несанкционированного копирования, блокирования информации.

По оценкам Счетной палаты правительства США, федеральные министерства и ведомства ежегодно тратят свыше $38 млрд на создание, использование и развитие информационных систем и сетей. В то же время ежегодный ущерб от хищений и мошенничества, совершенных с помощью информационных технологий только через Интернет, достигает $5 млрд. Однако экономические потери - не главный источник угрозы. Проведенные Пентагоном учения по имитации проникновения в информационные системы военного назначения показали, что 88 % случаев атаки увенчались успехом и лишь 4 % попыток несанкционированного доступа (НСД) были обнаружены.

С каждым годом вопросы комплексной безопасности предприятия и защиты информации приобретают большую актуальность. С насыщением рынка и усилением конкуренции все возрастающую ценность получает коммерческая информация о клиентах, поставщиках и результатах переговоров. Старые классические методы защиты не выдерживают "напора" современных технологий воздействия.

Защита каждого объекта, а также подход к ее планированию и реализации уникальны. Для организации эффективной комплексной защиты должны быть решены следующие основные вопросы:

• выявление ресурсов, подлежащих защите;

• оценка возможного ущерба от утечки конфиденциальных сведений и классификация информации по степени важности;

• выявление всех видов носителей информации, подлежащей защите;

• определение и оценка потенциальных условий уязвимости информации, подлежащей защите;

• создание комплекса мер безопасности информации.

При решении проблемы защиты информации учитывается степень достижения требуемых значений интегральных и частных показателей эффективности защиты, а также возможные стратегии потенциального злоумышленника.

Планирование защиты объекта условно разделяется на этапы:

1. Анализ ресурсов, подлежащих защите; оценка их важности.

2. Прогноз потенциальных угроз и определение способов их нейтрализации при требуемой степени риска, которому они подвергаются.

3. Обоснование и выбор стратегии безопасности на базе принятых принципов защиты информации.

4. Реализация концепции безопасности - меры по выполнению требований защиты информации на объекте.

5. Поддержание уровня защиты информации.

Рассмотрим основы информационной безопасности, а также понятие национальная безопасность; роль и место информационной безопасности в системе национальной безопасности

Информация - совокупность сведений (сообщений)"об окружающем нас мире (события, лица, явления, процессы, факторы и их взаимосвязи), представленных в виде, пригодном для передачи одними людьми и восприятия другими, и используемых в целях получения знаний и принятия решения.

"Критичная" (конфиденциальная, защищаемая) информация - информация с соответствующими грифами секретности, информация для служебного пользования; информация, являющаяся собственностью учреждения.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (ГОСТ Р 50922-96, дата введения 01.07.97). Собственником информации может

быть государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Информационная угроза - фактор или совокупность факторов, создающих опасность нарушения свойств информации.

Защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных воздействий на защищаемую информацию.

Информационные ресурсы - информация по всем направлениям жизнедеятельности общества, организованная в форме документов и массивов документов (архивы, фонды), программ для ЭВМ, баз данных, баз знаний и др.

База данных - совокупность организованных, взаимосвязанных данных на машиночитаемых и других физических носителях.

Информационно-телекоммуникационная система (ИТКС) - совокупность взаимосвязанных каналами дальнего приема и передачи *информации* программно-аппаратных и технических средств, объединенных в единое целое из территориально разнесенных элементов с целью обеспечения технологического цикла обработки информации (поиск, сбор, хранение, переработка, редактирование) и выдачи потребителю в заданной форме результатов такой обработки. ИТКС включает компьютерные сети, программное обеспечение и систему связи.

Информационная безопасность (information security) - состояние информации, информационных ресурсов и ИТКС, при котором с требуемой надежностью обеспечивается защищенность от угроз системы формирования, распространения и использования информационных ресурсов. В общем случае под ИБ предлагается понимать состояние защищенности национальных интересов страны (жизненно важные интересы личности, общества и государства на сбалансированной основе) в информационной сфере от внутренних и внешних угроз.

Технические каналы утечки информации - физическая среда распространения "опасных" сигналов (ОСГ), несущих конфиденциальную информацию, выходящая за пределы охраняемой территории.

Защита информации от утечки - деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.

Защита информации от несанкционированного воздействия - деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к ней, а также к утрате, уничтожению или сбою функционирования носителя информации.

Национальная безопасность обеспечивается путем предотвращения или парирования внутренних и внешних угроз в различных сферах жизни общества - политической, экономической, оборонной, экологической, информационной и др. В каждой из этих сфер государство, выражающее интересы всего общества, обязано принимать меры, предотвращающие угрозы безопасности.

Организацию информационной безопасности следует рассматривать в двух аспектах - как обеспечение информационной безопасности личности, общества и государства и как соблюдение информационной безопасности составляющих собственно системы национальной безопасности.

Выбор и реализация способов организации ИБ основываются на переработке информации, отражающей возникшую в той или иной сфере ситуацию угрозы и возможности государства по ее устранению. Достоверность, полнота, своевременность и защищенность являются важнейшими показателями, характеризующими правильность и эффективность принимаемых решений по обеспечению безопасности. Это позволяет рассматривать информационную безопасность как неотъемлемую часть системы национальной безопасности в целом и каждой из ее составляющих.