Информационная безопасность

Задачи информационного менеджмента

Когда проблема возникает

- Значимость ИБ становится тем более высокой, чем выше степень автоматизации БП предприятия и чем больше "интеллектуальная составляющая" в его продукте,
- Чем больше успешность предприятия зависит от наличия и сохранения технологий, ноу-хау, коммерческих баз данных, маркетинговой информации, результатов научных исследований и т.п., обеспечения ее конфиденциальности и доступности для владельцев и пользователей.

Когда проблема возникает

Обеспечение информационной безопасности зачастую, имеет большое значение не только для стратегического развития предприятия и создания основного продукта, но и для отдельных (вспомогательных) направлений деятельности и бизнес-процессов, таких как коммерческие переговоры и условия контрактов, ценовая политика и т.п.

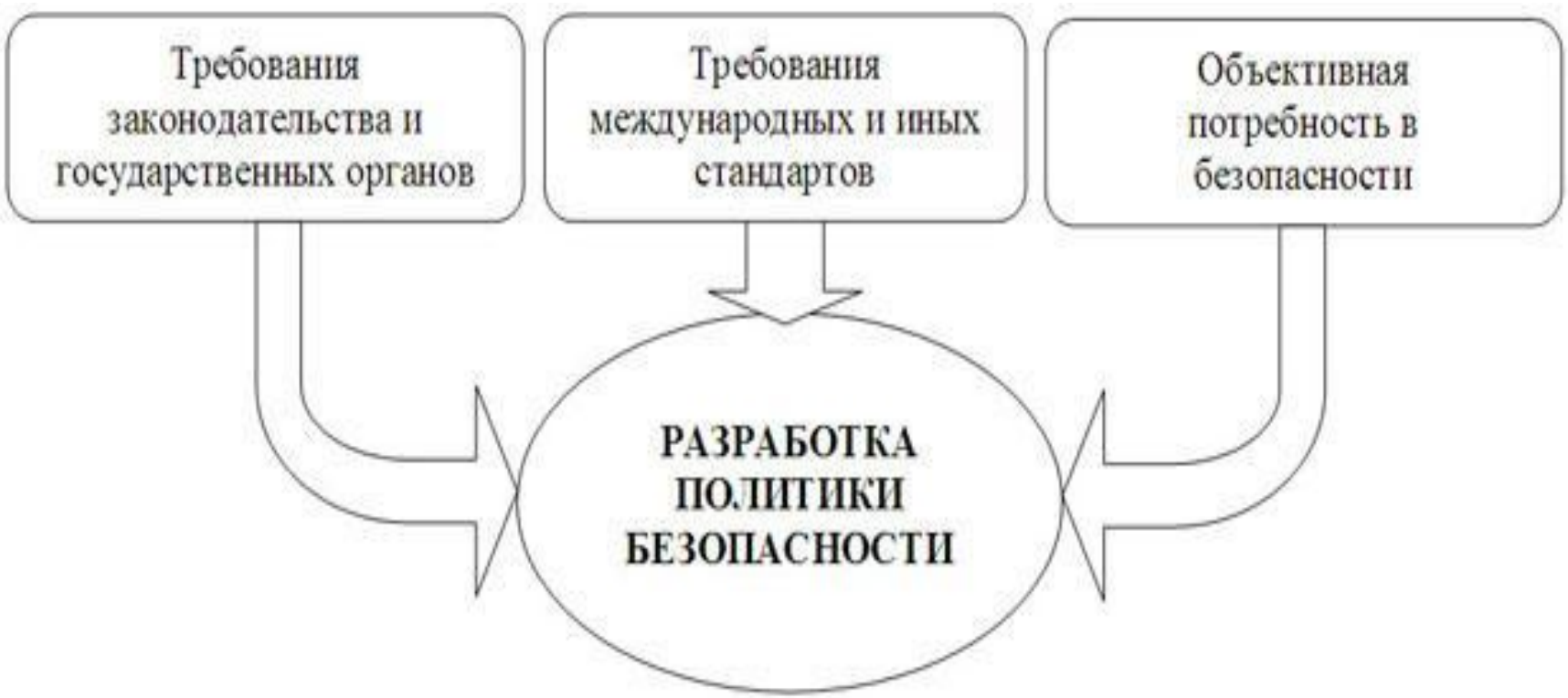
Когда проблема возникает

Значимость обеспечения ИБ в некоторых случаях может определяться наличием в общей системе информационных потоков предприятия сведений, составляющих не только коммерческую, но и государственную тайну, а также другие виды конфиденциальной информации (сведения, составляющие банковскую тайну, врачебную тайну, интеллектуальную собственность

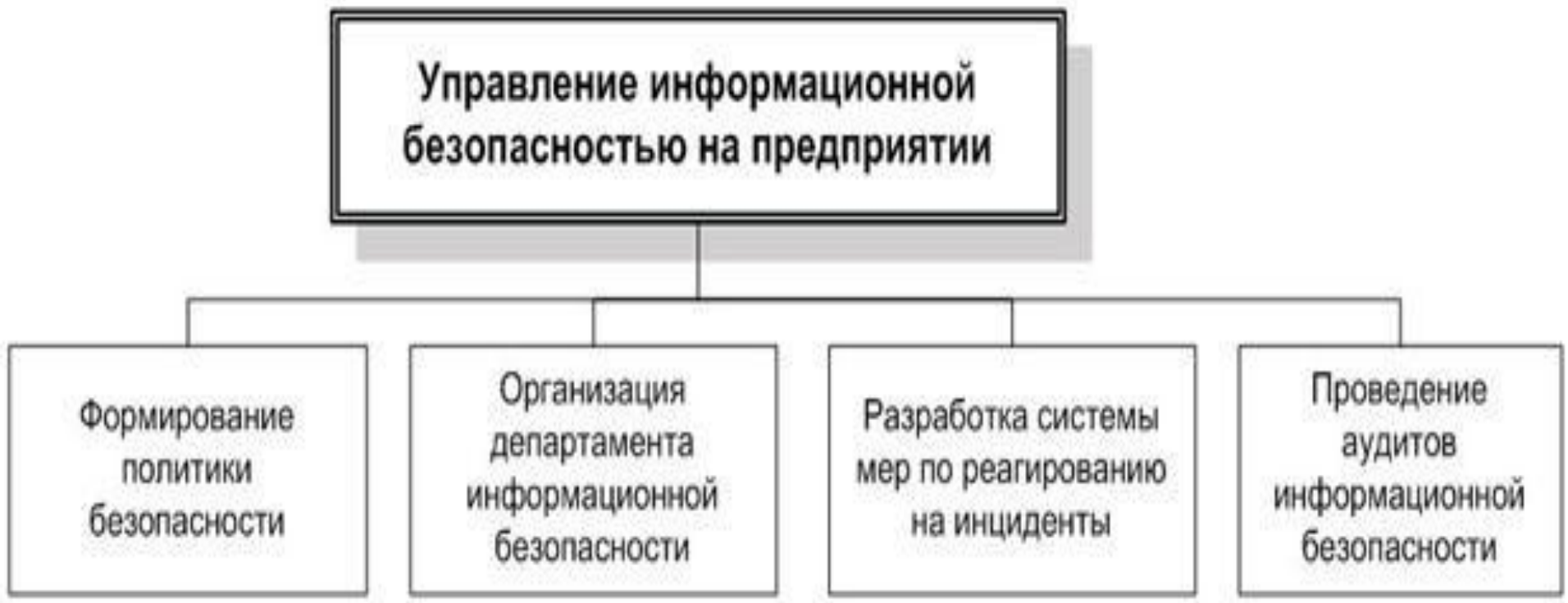
Виды угроз ИБ

- Внешние:
  - неправомерные действия гос. органов (в том числе и зарубежных),
  - деятельность преступников,
  - незаконные действия конкурентов,
  - недобросовестные действия партнеров,
  - отставание правовой базы от фактического развития технологий и общественных отношений,
  - сбои и нарушения в работе глобальных информационных и систем и ИС контрагентов и др.;
- Внутренние:
  - ошибки и халатность персонала предприятия,
  - намеренно допускаемые нарушения,
  - сбои и нарушения в работе собственных ИС и др.

Предпосылки разработки политики безопасности предприятия



Структура деятельности в сфере ИБ на предприятии



Жизненный цикл политики информационной безопасности

- Проведение предварительного исследования состояния информационной безопасности.
- Собственно разработку политики безопасности.
- Внедрение разработанных политик безопасности.
- Анализ соблюдения требований политики безопасности и формулирование требований по ее дальнейшему совершенствованию.

Классификация информационных ресурсов

- Критически важная (абсолютно секретная) информация, требующая особых гарантий безопасности.
- Важная информация (составляющая коммерческую тайну) – используемая только внутри предприятия, нарушение конфиденциальности которой может нанести серьезный ущерб самому предприятию или его партнерам.
- Значимая (конфиденциальная) информация – предназначена для использования ограниченным кругом сотрудников и руководителей предприятия.

Классификация информационных ресурсов

- Персональная информация – данные о сотрудниках, не подлежащие разглашению.
- Информация для внутреннего использования – нарушение конфиденциальности которой не может нанести вреда.
- Прочая информация – открытая информация, конфиденциальность которой не имеет особого значения для деятельности предприятия.

Политики ИБ среднего уровня

- Политики, относящиеся к определенным сферам деятельности предприятия и соответствующим информационным потокам (финансам, коммерческой деятельности).
- Политики, относящиеся к определенным аспектам использования ИТ, организации информационных потоков и организации работы персонала на всем предприятии – вне зависимости от той сферы, где используются эти технологии или занят персонал.

Политики первого типа могут содержать:

- Спец. требования к резервному копированию;
- Спец. требования к идентификации и аутентифика-ции пользователей;
- Спец. требования к копировально-множительной технике, используемой для работы с конфиденци-альной информацией;
- Спец. требования к помещениям, в которых проводятся совещания по секретной тематике и обрабатывается соответствующая информация (толщина и материал стен, расположение помещений в зданиях, защищенность окон, надежность дверей, а также охранной и пожарной сигнализации, обследования на предмет выявления подслушивающих устройств и т.п.)

К политикам второго типа относятся:

- политика опубликования открытых материалов, в том числе организации веб-сайта и внутреннего портала (в части предотвращения возможных утечек и искажений информации);
- политика использования сети Интернет;
- политики использования отдельных ИКТ, в том числе ноутбуков и КПК, удаленного доступа к корпоративным ИС, личных компьютеров сотрудников в служебных целях;
- классификации информационных систем, информационных ресурсов и объектов информации с точки зрения их значимости и усилий, которые необходимо предпринимать для их защиты;

Продолжение

- политика приобретения, установки, модификации и обновления ПО, а также аутсорсинга;
- политика закупки аппаратных средств ИС, систем ИБ;
- политика использования собственного ПО, самостоятельно разрабатываемого предприятием;
- правила использования паролей и других средств персональной идентификации;
- политика использования ЭЦП и публичных ключей;
- политика обеспечения внутреннего режима и физической защищенности информационных активов;
- политика доступа к внутренним информационным ресурсам сторонних пользователей (организаций);
- порядок привлечения к ответственности за нарушение определенных правил информационной безопасности.