Обеспечение экономической безопасности предприятия

Кротов К. А. ЭБ 41-16

Логика и последовательность разработки раздела «Экономическая и финансовая безопасность»

1. Теоретические аспекты экономической и финансовой безопасности фирмы.

- Содержание понятия «экономической и финансовой безопасности фирмы
- Цель экономической и финансовой безопасности фирмы
- Задачи экономической и финансовой безопасности фирмы
- Направления экономической и финансовой безопасности фирмы

2. Необходимо выявить актуальные направления обеспечения экономической и финансовой безопасности для исследуемого объекта (фирмы, предприятия, территории).

- Информационная безопасность:
  - угрозы информационной безопасности, существующие на предприятии.
  - методы снижения вероятности реализации угроз, применяемые на предприятии.
- Финансовая безопасность:
  - угрозы информационной безопасности, существующие на предприятии.
  - методы снижения вероятности реализации угроз, применяемые на предприятии.
- …

3. Необходимо провести анализ влияния прогнозной стратегии (модели) и прогнозных ключевых показателей на финансовую безопасность исследуемого объекта (фирмы, предприятия, территории).

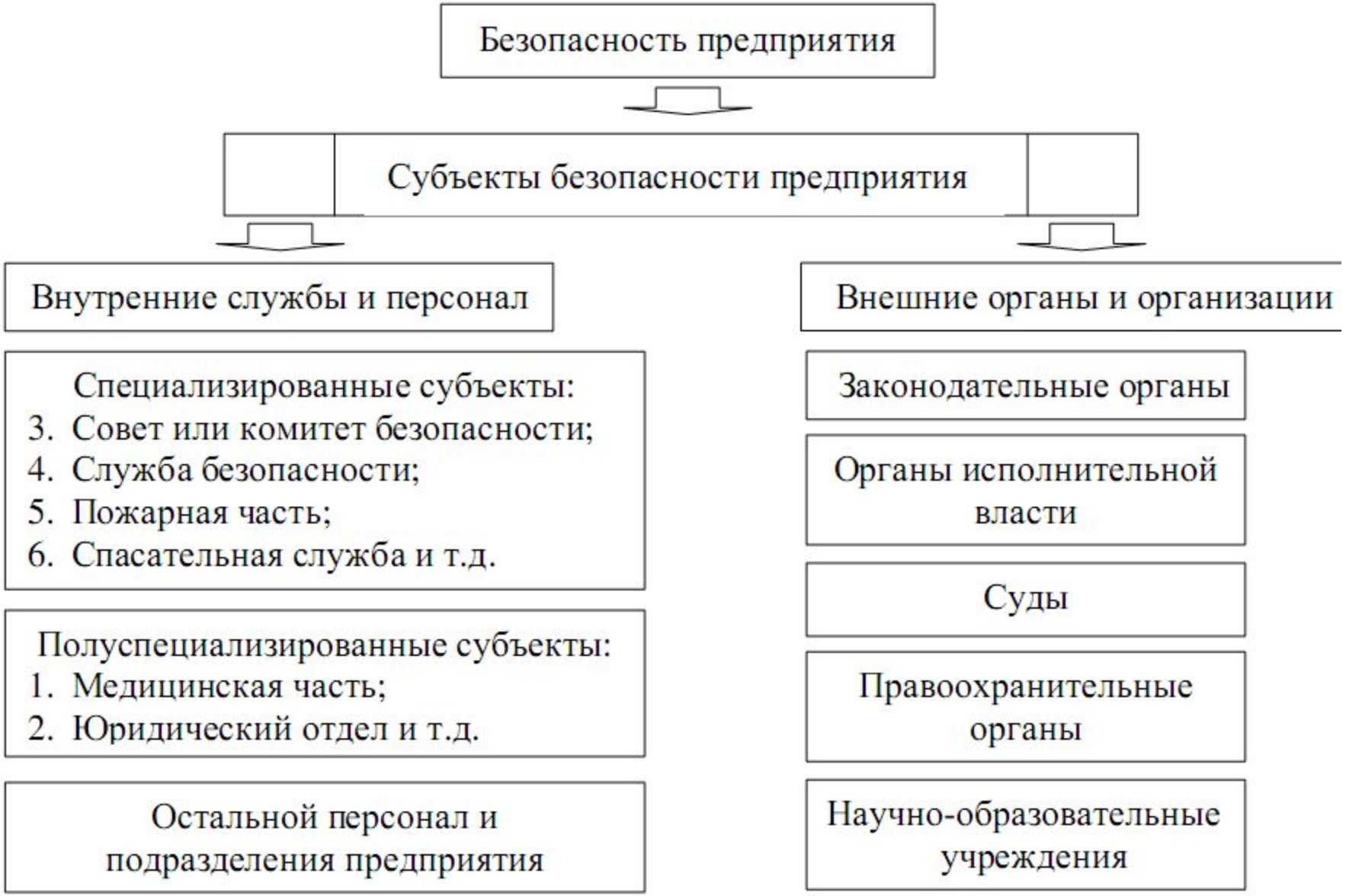
Сущность экономической безопасности предприятия

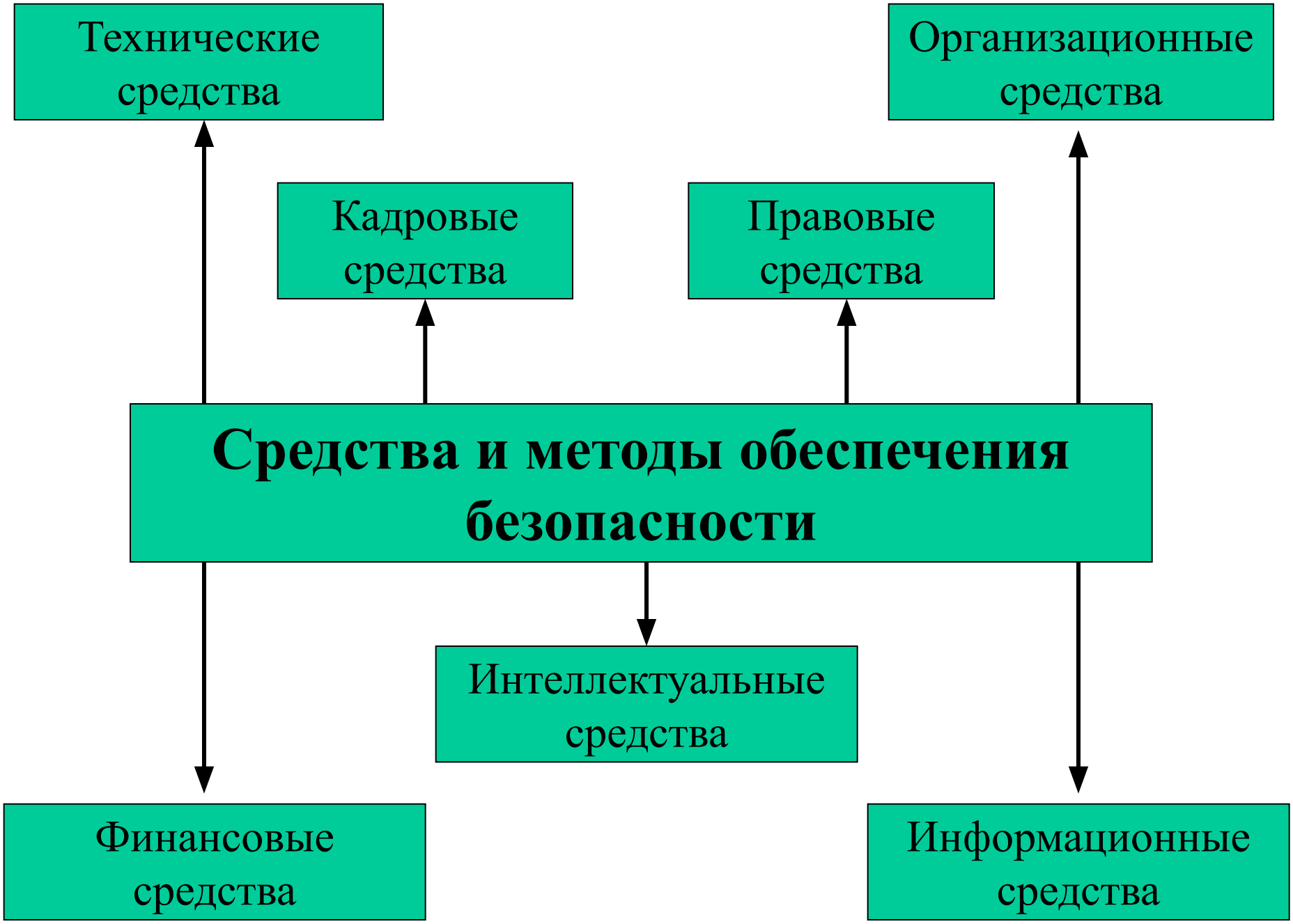
Экономическая безопасность - это состояние предприятия в системе его связей с точки зрения способности к устойчивости и развитию в условиях внутренних и внешних угроз, действий непредсказуемых и трудно прогнозируемых факторов.

Угроза безопасности предприятия - это потенциально или реально возможное событие, действие, процесс или явление, которое способно нарушить его устойчивость и развитие или привести к остановке его деятельности.

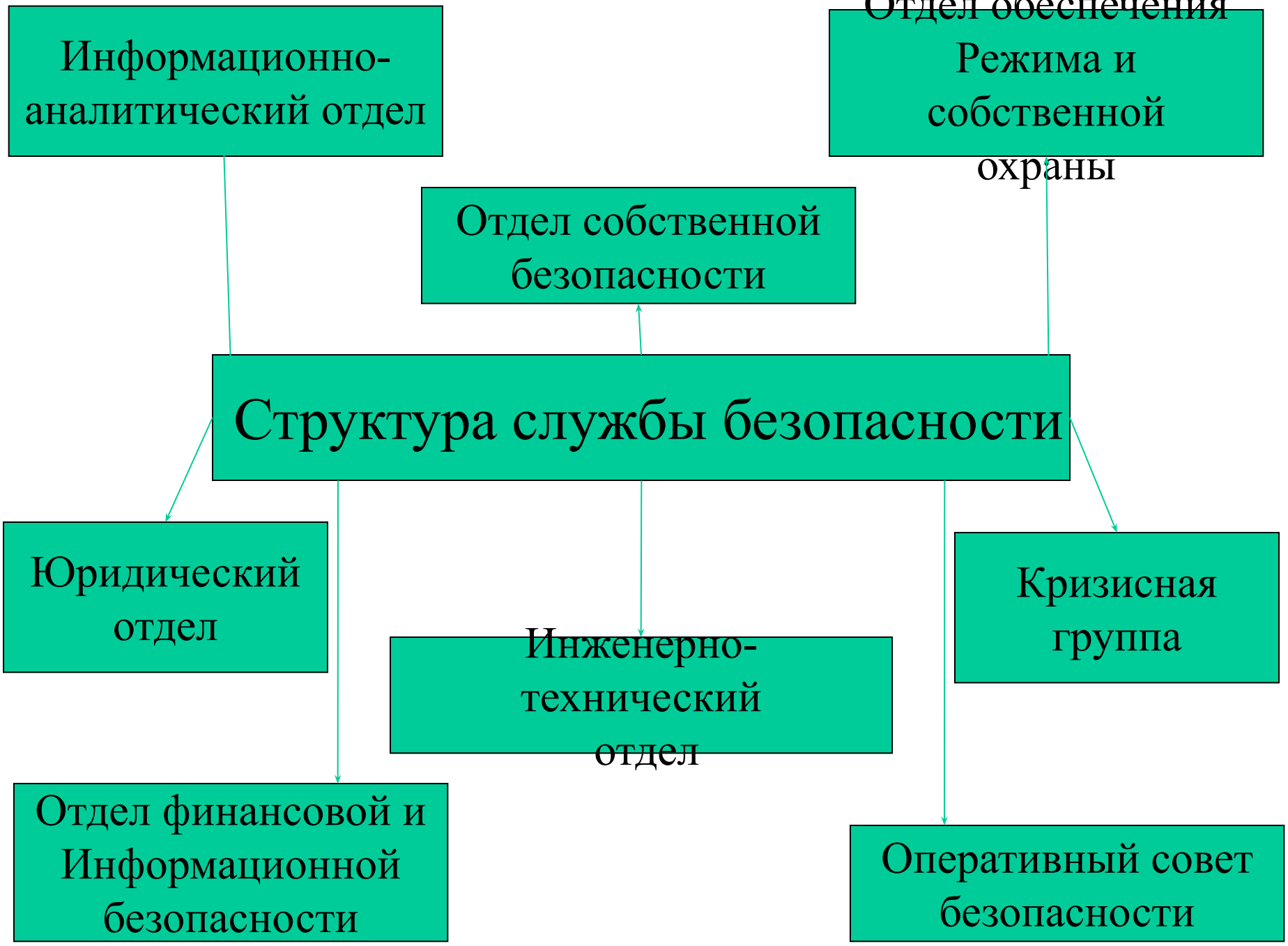
Целью обеспечения безопасности предприятия является комплексное воздействие на потенциальные и реальные угрозы, позволяющее ему успешно функционировать в нестабильных условиях внешней и внутренней среды.

Рисунок 1.1 – Разделение функций безопасности по отношению к угрозам


Безопасность предприятия
Субъекты безопасности предприятия
Внутренние службы и персонал
Внешние органы и организации
Специализированные субъекты:
3. Совет или комитет безопасности;
4. Служба безопасности;
5. Пожарная часть;
6. Спасательная служба и т.д.
Полуспециализированные субъекты:
1. Медицинская часть;
2. Юридический отдел и т.д.
Остальной персонал и подразделения предприятия
Законодательные органы
Органы исполнительной власти
Суды
Правоохранительные органы
Научно-образовательные учреждения


Технические средства
Организационные средства
Кадровые средства
Правовые средства
Средства и методы обеспечения безопасности
Интеллектуальные средства
Финансовые средства
Информационные средства


Физическая
Информационная
Экономическая
Экологическая
Безопасность предприятия
Психологическая
Пожарная
Техногенная
Научно-техническая


Информационно-аналитический отдел
Отдел обеспечения Режима и собственной охраны
Отдел собственной безопасности
Структура службы безопасности
Юридический отдел
Инженерно-технический отдел
Кризисная группа
Отдел финансовой и Информационной безопасности
Оперативный совет безопасности

Экономическая безопасность в информационной сфере

Вся совокупность информации представляет различную ценность для самого предпринимателя и, соответственно, ее разглашение может привести (либо не привести) к угрозам экономической безопасности различной степени тяжести.

Информацию необходимо разделить на три группы:

1. информация для открытого пользования любым потребителем в любой форме;

2. информация ограниченного доступа - только для органов, имеющих соответствующие законодательно установленные права;

3. информация только для сотрудников фирмы.

Классификация информации по важности

Жизненно важная	-незаменимая информация, наличие которой необходимо для нормального функционирования объекта защиты (предприятия).
Важная	-информация, которая может быть заменена или восстановлена, но процесс восстановления очень труден и связан с большими затратами.
Полезная	-информация, которая полезна и которую трудно восстановить, однако предприятие может эффективно функционировать и без нее.
Несущественная	-информация, которая больше не нужна предприятию.

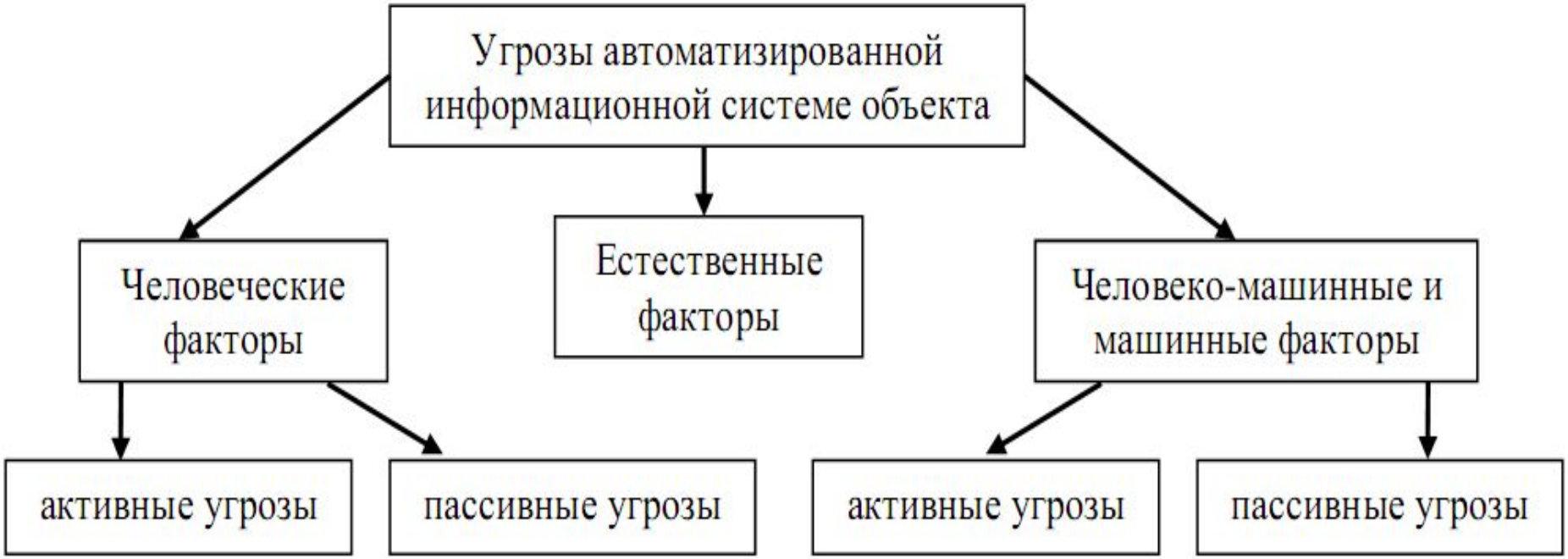


Рисунок 3.1 - Угрозы автоматизированной информационной системе объекта

Детализация способов воздействия угроз на объекты информационной безопасности

Информационные способы	✗ нарушение адресности и своевременности информационного обмена, противозаконный сбор и использование информации; ✗ несанкционированный доступ к информационным ресурсам; ✗ манипулирование информацией (дезинформация, сокрытие или искажение информации); ✗ незаконное копирование данных в информационных системах; ✗ нарушение технологии обработки информации.
Программно-математические способы	✗ внедрение компьютерных вирусов; ✗ установку программных и аппаратных закладных устройств; ✗ уничтожение или модификацию данных в автоматизированных информационных системах.
Физические способы	✗ уничтожение или разрушение средств обработки информации и связи; ✗ уничтожение, разрушение или хищение машинных иди других оригинальных носителей информации; ✗ хищение программных или аппаратных ключей и средств криптографической защиты информации; ✗ воздействие на персонал; ✗ поставка «зараженных» компонентов автоматизированных информационных систем.

Детализация способов воздействия угроз на объекты информационной безопасности

Радиоэлектронные способы	✗ перехват информации в технических каналах ее возможной утечки; ✗ внедрение электронных устройств перехвата информации в технические средства и помещения; ✗ перехват, дешифровка и навязывание ложной информации в сетях передачи данных и линиях связи; ✗ радиоэлектронное подавление линий связи и систем управления.
Организационно-правовые способы	✗ невыполнение требований законодательства и задержки в принятии необходимых нормативно-правовых положений в информационной сфере; ✗ неправомерное ограничение доступа к документам, содержащим важную для граждан и организаций информацию.

Конфиденциальная информация - это документированная (то есть зафиксированная на материальном носителе и с реквизитами, позволяющими ее идентифицировать) информация, доступ к которой ограничивается в соответствии с законодательством РФ.

Коммерческая тайна это информация которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель принимает меры к охране ее конфиденциальности.

Составляющие коммерческой тайны по функционально-целевому признаку

Деловая информация	- сведения о контрагентах; - сведения о конкурентах; - сведения о потребителях; - сведения о деловых переговорах; - коммерческая переписка; - сведения о заключенных и планируемых контрактах.
Научно-техническая информация	- содержание и планы научно-исследовательских работ; - содержание “ноу-хау”, рационализаторских предложений; планы внедрения новых технологий и видов продукции.
Производственная информация	- технология; - планы выпуска продукции; - объем незавершенного производства и запасов; - планы инвестиционной деятельности.
Организационно-управленческая информация	- сведения о структуре управления фирмой не содержащиеся в уставе; - оригинальные методы организации управления; - система организации труда.

Составляющие коммерческой тайны по функционально-целевому признаку

Маркетинговая информация	- рыночная стратегия; - планы рекламной деятельности; - планы обеспечения конкурентных преимуществ по сравнению с продукцией других фирм; - методы работы на рынках; - планы сбыта продукции; - анализ конкурентоспособности выпускаемой продукции.
Финансовая информация	- планирование прибыли, себестоимости; - ценообразование – методы расчета, структура цен, скидки; - возможные источники финансирования; - финансовые прогнозы.
Информация о персонале фирмы	- личные дела сотрудников; - планы увеличения (сокращения) персонала; - содержание тестов для проверки вновь принимаемых на работу.
Программное обеспечение	- программы; - пароли, коды доступа к конфиденциальной информации, расположенной на электронных носителях.

При работе с документами, содержащими коммерческую тайну, следует соблюдать определенные правила, которые сводятся к нижеследующим:

1. строгий контроль (лично или через службу безопасности) за допуском персонала к секретным документам;

2. назначение ответственных лиц за контролем секретного делопроизводства и наделение их соответствующими полномочиями;

3. разработка инструкции (памятки) по работе с секретными документами, ознакомление с ней сотрудников фирмы;

4. контроль за принятием служащими письменных обязательств о сохранении коммерческой тайны фирмы;

5. введение системы материального и морального поощрения сотрудников, имеющих доступ к секретной информации;

6. внедрение в повседневную практику современных технологий защиты коммерческой тайны фирмы;

7. личный контроль со стороны руководителя фирмы за службами внутренней безопасности и секретного делопроизводства.

Компьютерная безопасность

К наиболее типичным целям совершения компьютерных преступлений специалисты относят следующие:

- подделка отчетов и платежных ведомостей;
- приписка сверхурочных часов работы;
- фальсификация платежных документов;
- хищение из денежных фондов;
- добывание запасных частей и редких материалов;
- кража машинного времени;
- вторичное получение уже произведенных выплат;
- фиктивное продвижение по службе;
- получение фальшивых документов;
- внесение изменений в программы и машинную информацию;
- перечисление денег на фиктивные счета;
- совершение покупок с фиктивной оплатой и др.

Направления организационного обеспечения компьютерной безопасности

Слияния и поглощения. Методы защиты

Само понятие **«враждебное поглощение»** пришло в Россию из США. На английском языке данный термин звучит как:

HOS-TILE TAKE-OVER

Дословный перевод на русский язык:
скупка группой лиц или лицом контрольного пакета акций передприятия без согласия его руководителей

Основные этапы сделки по слиянию или поглащению:

1. Разработка стратегии слияний и поглощений;
2. Анализ потенциального объекта слияния или поглощения;
3. Переговорный процесс и заключение соглашения;
4. Оценка и стабилизация положения;
5. Интеграция;
6. Постинтеграция.

Таблица 5.1 – Сопоставление стратегического плана фирмы с возможностью слияния или поглощения

Типовое содержание стратегического плана	Вопрос слияния или поглощения
Миссия (главная цель существования организации)	Насколько предлагаемое слияние или поглощение отвечает миссии организации?
Цели (финансовые, размер бизнеса, эффективность операций)	Каким образом предлагаемое слияние или поглощение будет способствовать осуществлению целей организации?
Макроэкономические тенденции и предпосылки развития рынка	Насколько макроэкономические тенденции (включая государственное регулирование), возможности рынка будут адекватны для проведения слияния или поглощения?
Оценка конкурентоспособности организации	Насколько слияние или поглощение повысит конкурентоспособность организации? Как укрепятся сильные стороны, удастся ли решить проблемные аспекты?
Оценка возможностей развития	Каким образом слияние или поглощение будет способствовать оптимальному использованию возможностей развития? Удастся ли нивелировать угрозы?
Стратегии по основным сегментам рынка	Какое воздействие слияния или поглощения на позицию компании во всех сегментах рынка окажет слияние или поглощение?
Стратегические задачи по основным видам деятельности	Будут ли достигнуты необходимые результаты по основным видам деятельности?
Планы мероприятий по реализации основных стратегических задач	Насколько слияние или поглощение будет способствовать реализации планов мероприятий?
Ожидаемые финансовые результаты	Насколько слияние или поглощение будет способствовать достижению установленных показателей?

Рисунок 5.1 – Категории слияний и поглощений

Таблица 5.2 - Краткое описание видов защиты от "недружественного поглощения"

Тип защиты	Описание
"Противоакульи поправки к уставу"	
Разделенный совет	Совет делится на три равные группы. Каждый год избирается только одна группа. Поэтому захватчик не может получить контроль над мишенью сразу же после получения большинства голосов.
Супербольшинство	Высокий процент акций, необходимый для одобрения слияния, обычно 80%.
Справедливая цена	Ограничивает слияния акционерам, владеющим более чем определенной долей акций в обращении, если не платится справедливая цена (определяемая формулой или процедурой оценки).
Прочие	
"Ядовитая пилюля"	Для существующих акционеров выпускаются права, которые в случае покупки значительной доли акций захватчиком могут быть использованы для приобретения обыкновенных акций компании по низкой цене, обычно до половины рыночной цены. В случае слияния права могут быть использованы для приобретения акций покупающей компании.
Рекапитализация высшего класса	Распространение обыкновенных акций нового класса с более высокими правами голоса. Позволяет менеджерам компании-мишени получить большинство голосов без владения большей долей акций.
Защита после предложения	
Защита Пэкмена	Контр нападение на акции захватчика.
Тяжба	Возбуждается судебное разбирательство против захватчика за нарушение антитрестовского закона или закона о ценных бумагах.
Реструктуризация активов	Покупка активов, которые не понравятся захватчику или которые создадут антитрестовские проблемы.
Реструктуризация обязательств (пассивов)	Выпуск акций для дружественной третьей стороны или увеличение числа акционеров. Выкуп акций с премией у существующих акционеров.

Спасибо за внимание!