Лекция: Концепция построения системы безопасности предприятия

Определение и основные понятия системы безопасности

- Под **системой безопасности** предприятия понимается организованная совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз.

- **Опасности** – это возможные или реальные явления, события и процессы, способные нанести моральный или материальный ущерб предприятию и предпринимательской деятельности.
- Опасность способна приобретать различные формы. Она может быть в виде намерений, планирования действий и их реализация с целью унич тожения, ограбления, изменения, ослабления и т. д.

- **Угроза** – потенциально возможное или реальное действие злоумышленников, способных нанести моральный, материальный или физический ущерб персоналу. Различают внутренние и внешние угрозы, которые могут быть направлены на персонал, материальные, финансовые и информационные ресурсы.

Рис. 1. Виды угроз безопасности предприятия

Целями системы безопасности являются:

- защита прав предприятия, его структурных подразделений и сотрудников;
- сохранение и эффективное использование финансовых, материальных и информационных ресурсов;
- повышение имиджа и роста прибылей за счет обеспечения качества услуг и безопасности клиентов.

В качестве основных задач системы безопасности рассматриваются:

- своевременное выявление и устранение угроз персоналу и ресурсам; причин и условий, способствующих нанесению финансового, материального и морального ущерба интересам предприятия, нарушению его нормального функционирования и развития;
- создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций в функционировании предприятия;

- пресечение посягательств на ресурсы и угроз персоналу на основе комплексного подхода к безопасности;
- создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, для ослабления негативного влияния последствий нарушения безопасности на достижение стратегических целей.

Для достижения указанных целей и задач используются различные **средства обеспечения безопасности** предприятия, среди которых можно выделить следующие:

- *Технические средства.* К ним относятся охранно-пожарные системы, видео-радиоаппаратура, средства обнаружения взрывных устройств, бронежилеты, заграждения и т.д.
- *Организационные средства.* Создание специализированных оргструктурных формирований, обеспечивающих безопасность предприятия.

- *Информационные средства.* Это печатная и видеопродукция по вопросам сохранения конфиденциальной информации. Важнейшая информация для принятия решений по вопросам безопасности сохраняется в компьютерах.
- *Финансовые средства.* Совершенно очевидно, что без достаточных финансовых средств невозможно функционирование системы безопасности, вопрос лишь в том, чтобы использовать их целенаправленно и с высокой отдачей.

- *Правовые средства.* Использование изданных вышестоящими органами власти законов и подзаконных актов и разработка собственных, так называемых локальных правовых актов по вопросам обеспечения безопасности.
- *Кадровые средства.* Достаточность кадров, занимающихся вопросами обеспечения безопасности. Своевременное повышения их профессионального мастерства.
- *Интеллектуальные средства.* Привлечение к работе высококлассных специалистов, научных работников (иногда целесообразно привлекать их со стороны) позволяет внедрять новые системы безопасности.

При построении модели информационной безопасности предприятия учитывают целый ряд компонентов (источников, объектов, действий). Таких как:

- объекты угроз;
- угрозы;
- источники угроз;
- цели угроз со стороны злоумышленников;
- источники информации;
- способы доступа;
- направления, способы и средства защиты информации.

Неправомерное овладение конфиденциальной информацией возможно путем

- разглашения источниками сведений,

- утечки информации через технические средства

- несанкционированного доступа к охраняемым сведениям.

1. Разглашение – это умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним .

- 2. **Утечка** – это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.
- **3. Несанкционированный доступ** – это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам.

Каждая угроза влечет за собой определенный ущерб – моральный или материальный, а защита и противодействие угрозе призвана снизить его величину, в идеале – полностью, реально – значительно или хотя бы частично. Но и это удается далеко не всегда.

С учетом этого угрозы могут быть классифицированы по следующим признакам:

- *по величине принесенного ущерба:*
  - предельный, после которого фирма может стать банкротом;
  - значительный, но не приводящий к банкротству;
  - незначительный, который фирма за какое-то время может компенсировать и др.;
- *по характеру нанесенного ущерба:*

  - материальный;
  - моральный;

- *по причинам появления:*
  - стихийные бедствия;
  - преднамеренные действия;
- *по вероятности возникновения:*
  - весьма вероятная угроза ;
  - вероятная угроза ;
  - маловероятная угроза;
- *по характеру воздействиям:*
  - активные;
  - пассивные;
- *по отношению к объекту:*

- внутренние;
- внешние.

Анализ условий, способствующих неправомерному овладению конфиденциальной информацией :

- разглашение (излишняя болтливость сотрудников) – 32%;
- несанкционированный доступ путем подкупа и склонения к сотрудничеству со стороны конкурентов и преступных группировок – 24%;
- отсутствие в фирме надлежащего контроля и жестких условий обеспечения информационной безопасности – 14%;

- традиционный обмен производственным опытом – 12%;
- бесконтрольное использование информационных систем – 10%
- наличие предпосылок возникновения среди сотрудников конфликтных ситуаций, связанных с отсутствием высокой трудовой дисциплины, психологической несовместимостью, случайным подбором кадров, слабой работой кадров по сплочению коллектива – 8%.

Концептуальные модели компонентов системы безопасности предприятия

Концепция выражает систему взглядов на проблему безопасности предприятия на различных этапах и уровнях производственной деятельности, а также основные принципы, направления и этапы реализации мер безопасности.

Мировой опыт показывает, что:

- *обеспечение безопасности не может быть одноразовым актом*. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных форм, методов, способов и путей создания, совершенствования и развития системы безопасности, непрерывном управлении ею, контроле, выявлении ее узких мест и потенциальных угроз фирме;

- *безопасность может быть обеспечена лишь при комплексном использовании всего арсенала средств защиты* и противодействия во всех структурных элементах производственной системы и на всех этапах технологического цикла. Наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый целостный механизм – СИСТЕМУ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ (СБП);
- *никакая СБП не может обеспечить требуемый уровень безопасности без надлежащей подготовки персонала и пользователей* и соблюдения ими всех

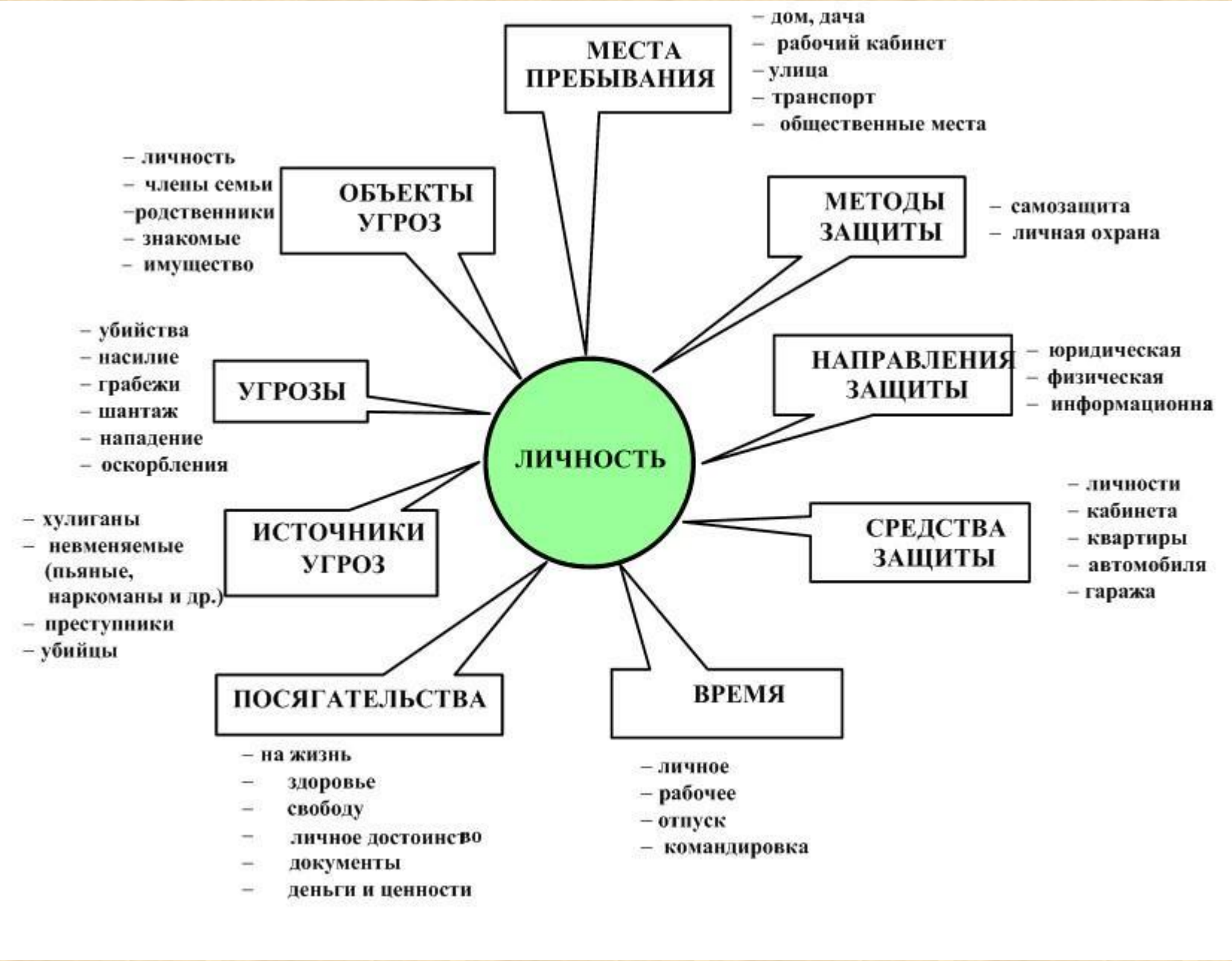

Рис. 2. Концептуальная модель безопасности личности

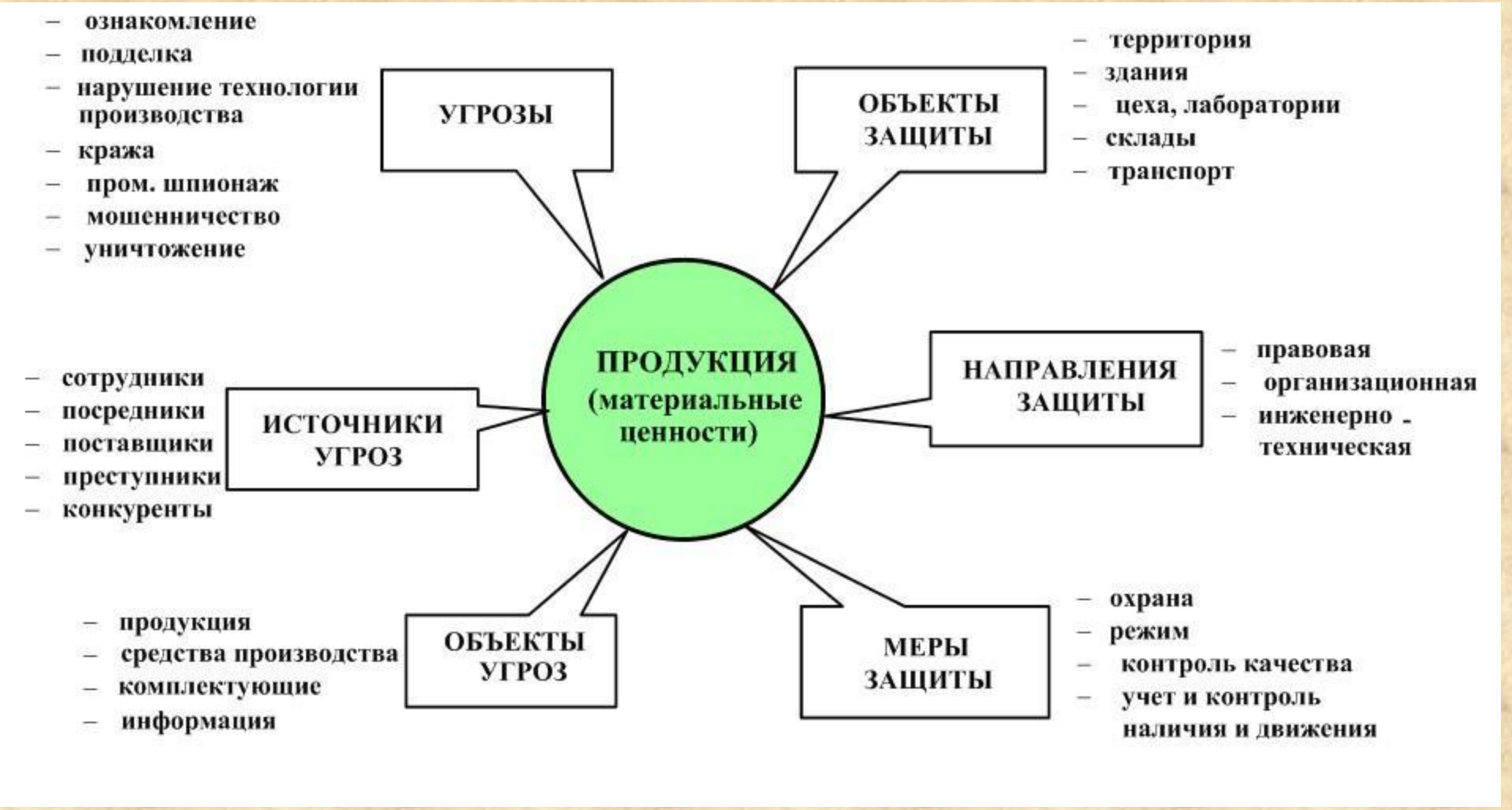

Рис. 3. Концептуальная модель безопасности продукции

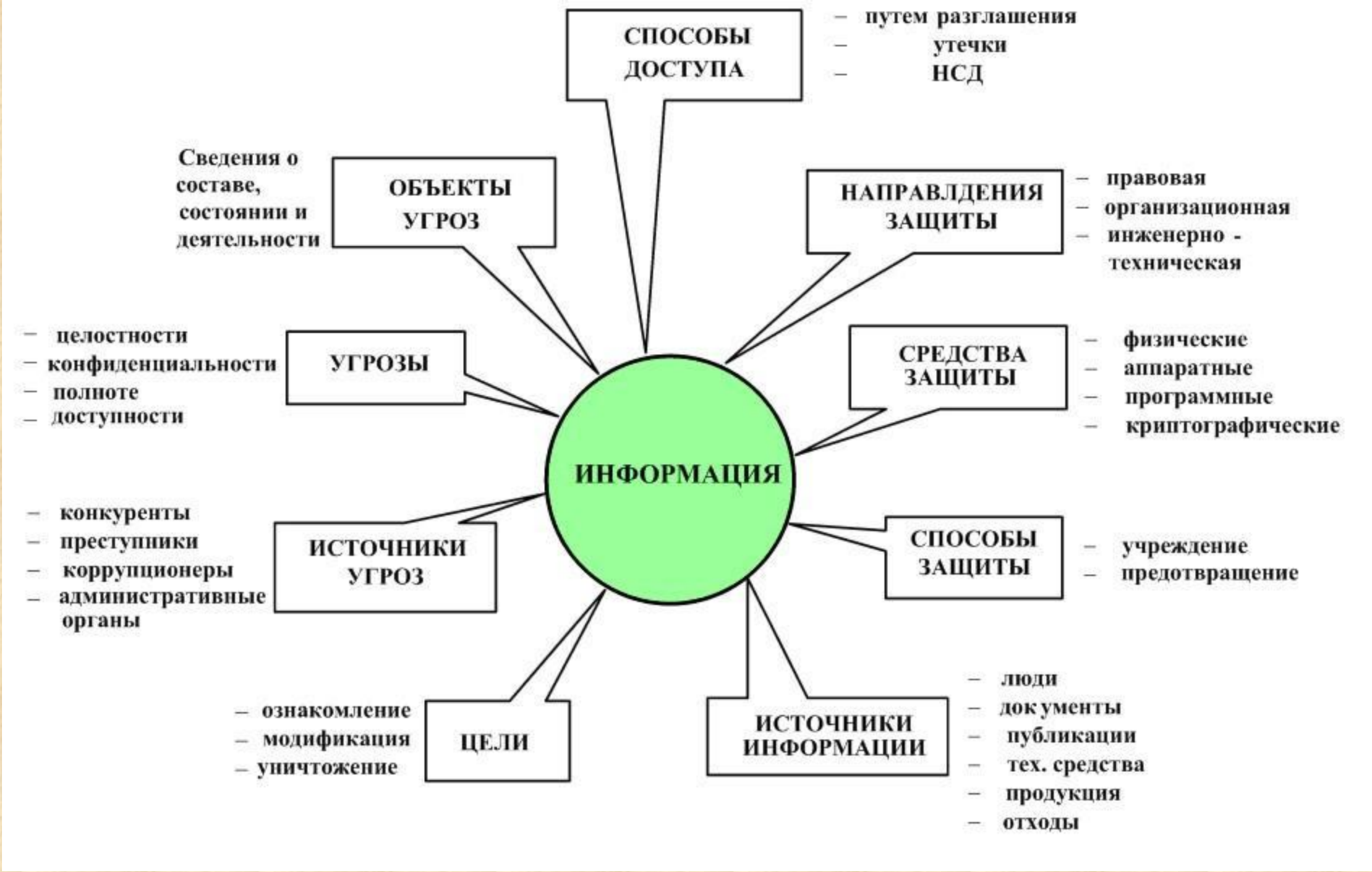

Рис. 4. Концептуальная модель безопасности информации

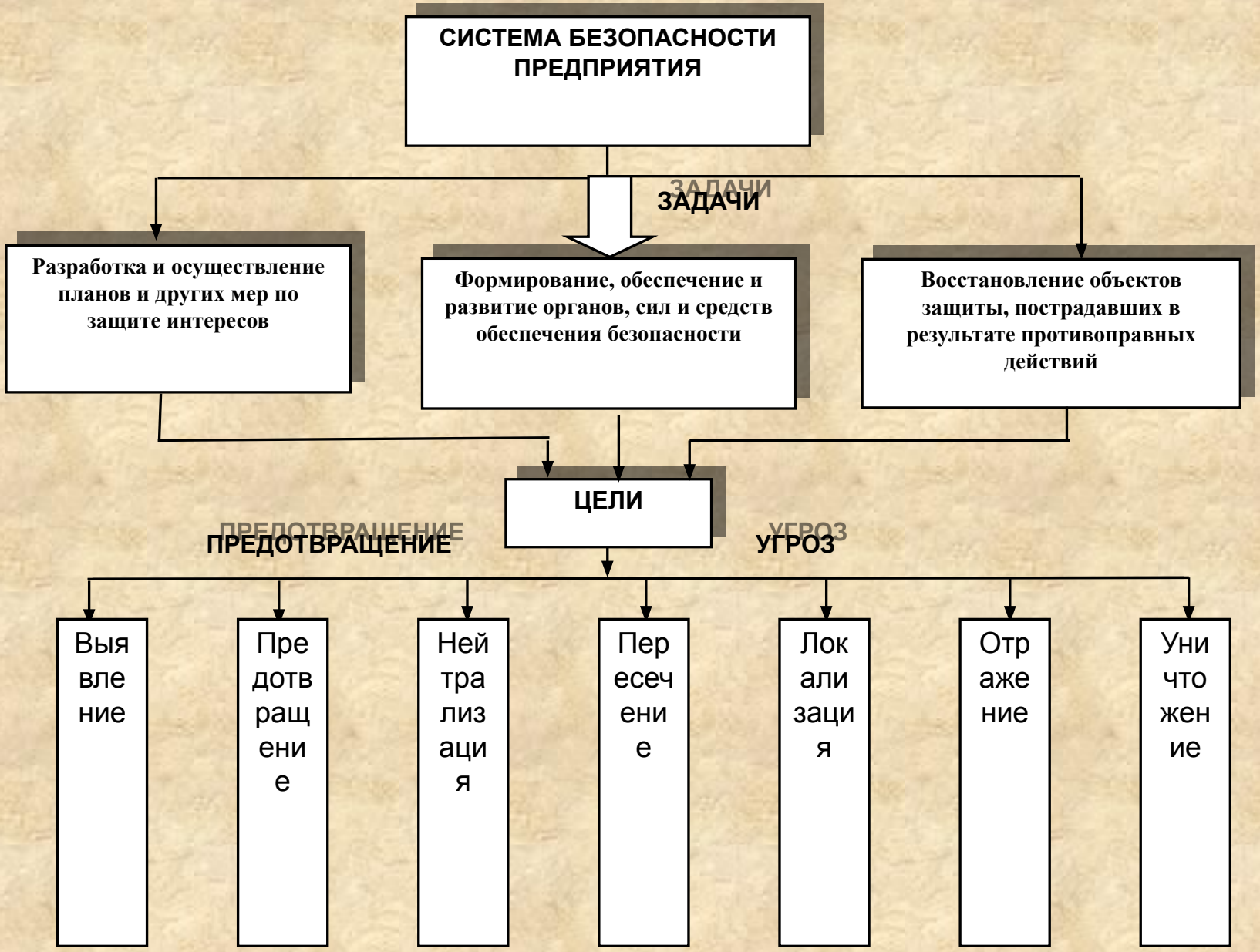

Рис. 5. Цели и задачи системы безопасности

Принципы построения системы безопасности предприятия

1. Комплексность. предусматривает обеспечение безопасности персонала, материальных, финансовых и информационных ресурсов от возможных угроз всеми доступными законными средствами, методами и мероприятиями.

2. Своевременность. Этот принцип ориентирован на упреждающий характер мер обеспечения безопасности на ранних стадиях разработки системы безопасности и прогнозирования обстановки, угроз безопасности, а также разработку эффективных мер предупреждения посягательств на законные интересы.

3. Непрерывность. Считается, что злоумышленники только и ищут возможность, как бы обойти защитные меры, прибегая для этого к легальным и нелегальным методам.

4. Активность. Защищать интересы предприятия необходимо с достаточной степенью настойчивости, широко используя маневр силами и средствами обеспечения безопасности и нестандартные меры защиты.

5. Законность. Предполагает разработку системы безопасности на основе федерального законодательства в области предпринимательской деятельности, информатизации и защиты информации, частной охранной деятельности, а также других нормативных актов по безопасности с применением всех дозволенных методов обнаружения и пресечения правонарушений.

6. Обоснованность. Предлагаемые меры и средства защиты должны реализовываться на современном уровне развития науки и техники, быть обоснованными с точки зрения заданного уровня безопасности и соответствовать установленным требованиям и нормам.

7. Экономическая целесообразность и сопоставимость. Этот принцип ориентирован на определение возможного ущерба и затрат на обеспечение безопасности (критерий "эффективность – стоимость").

- *8. Специализация.* Предполагается привлечение к разработке и внедрению мер и средств защиты специализированных организаций по обеспечению безопасности, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области.
- *9. Взаимодействие и координация.* Предполагает осуществление мер обеспечения безопасности на основе четкого взаимодействия всех заинтересованных подразделений и служб, сторонних специализированных организаций в этой области, координацию

- *10. Совершенствование*. Предусматривает совершенствование мер и средств защиты на основе собственного опыта, появления новых технических средств с учетом изменений в методах и средствах разведки и промышленного шпионажа, нормативно-технических требований, накопленного отечественного и зарубежного опыта.
- *11. Централизация управления.* Предполагает самостоятельное функционирование системы безопасности по единым организационным, функциональным и методологическим принципам с централизованным управлением деятельностью системы безопасности.