Молдавская Экономическая Академия

ЭКОНОМИЧЕСКАЯ ЭФФЕКТИВНОСТЬ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Автор: Чеботарь П. П.

Научный руководитель: доктор хабилитат, профессор Охрименко С.А.

Кишинев 2004

Актуальность темы

- Информация становится основополагающим ресурсом человечества
- С ростом объемов обрабатываемых данных увеличивается число различных информационных злоупотреблений
- В большинстве случаев информация имеет огромно экономическое и социальное значение, но организация-владелец ограничена в ресурсах, выделяемых на защиту

Цели и задачи работы:

Целью работы ставилось:

- Проанализировать подходы к информационной безопасности и предложить методологию построения экономически оптимальной СИБ

Задачами было:

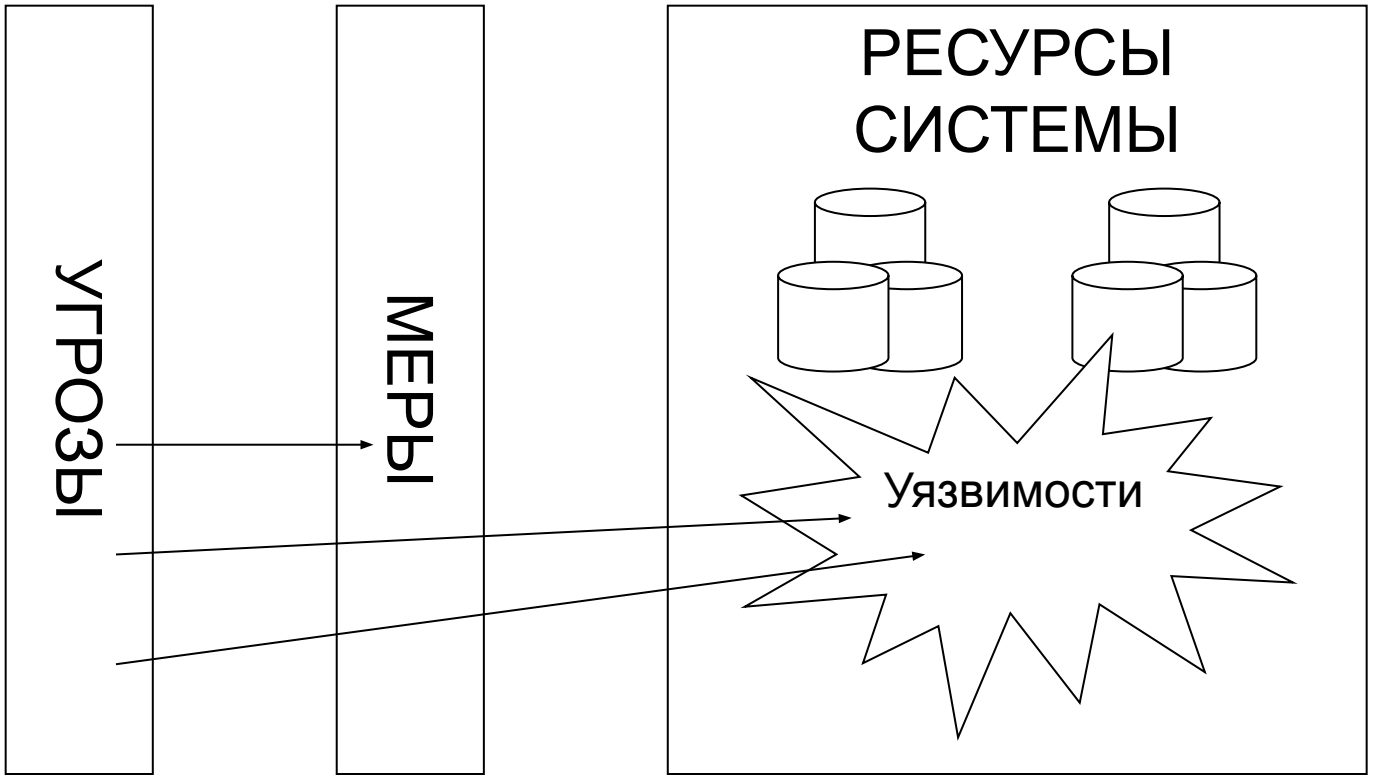
- Рассмотреть категорию «Информационная Безопасность»
- Проанализировать методологии построения систем информационной безопасности
- Рассмотреть и расширить классификации угроз информационной безопасности
- Проанализировать известные меры противодействия угрозам
- Проанализировать подходы к оценке эффективности систем информационной безопасности
- Провести оценку параметров экономически оптимальных систем информационной безопасности

Категория «Информационная безопасность»

<table>
<tr><td colspan="4">Информационная безопасность –
невозможность нанесения вреда свойствам объекта безопасности, обуславливаемым информацией и информационной инфраструктурой (защищенность от угроз)</td></tr>
<tr><td rowspan="2">Объект информационной безопасности - свойства объекта безопасности, обуславливаемые информацией и информационной инфраструктурой</td><td rowspan="2">Угрозы объекту информационной безопасности</td><td colspan="2">Обеспечение информационной безопасности</td></tr>
<tr><td>Деятельность по обеспечению информационной безопасности (по недопущению вреда объекту информационной безопасности)</td><td>Средства осуществления деятельности по обеспечению информационной безопасности</td><td>Субъекты обеспечения информационной безопасности</td></tr>
</table>

Динамическое равновесие систем информационной безопасности

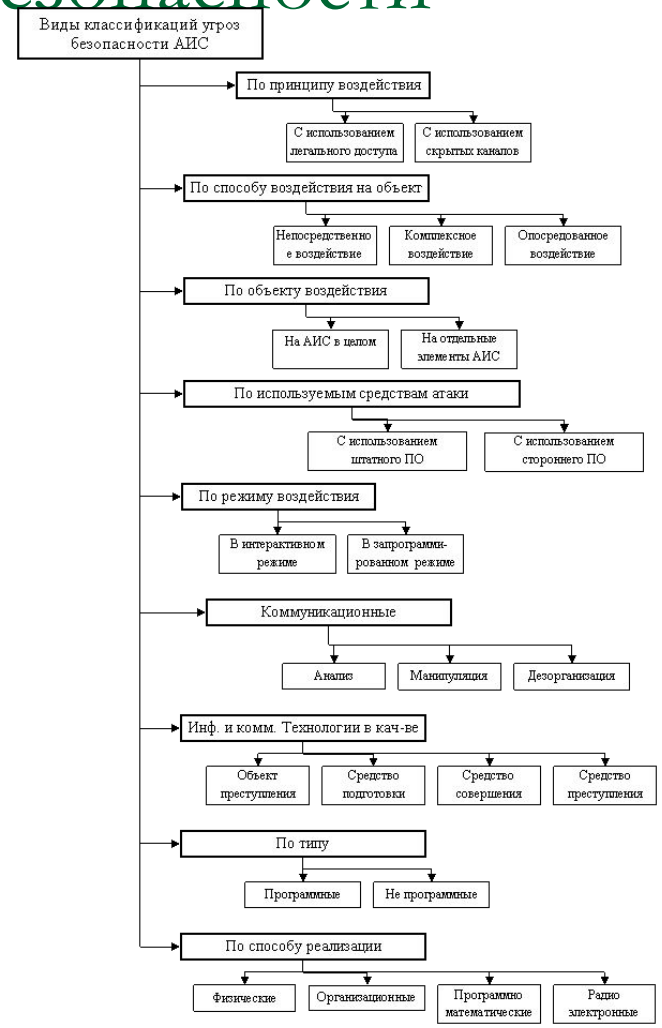
Соотношение угроз, мер и уязвимостей

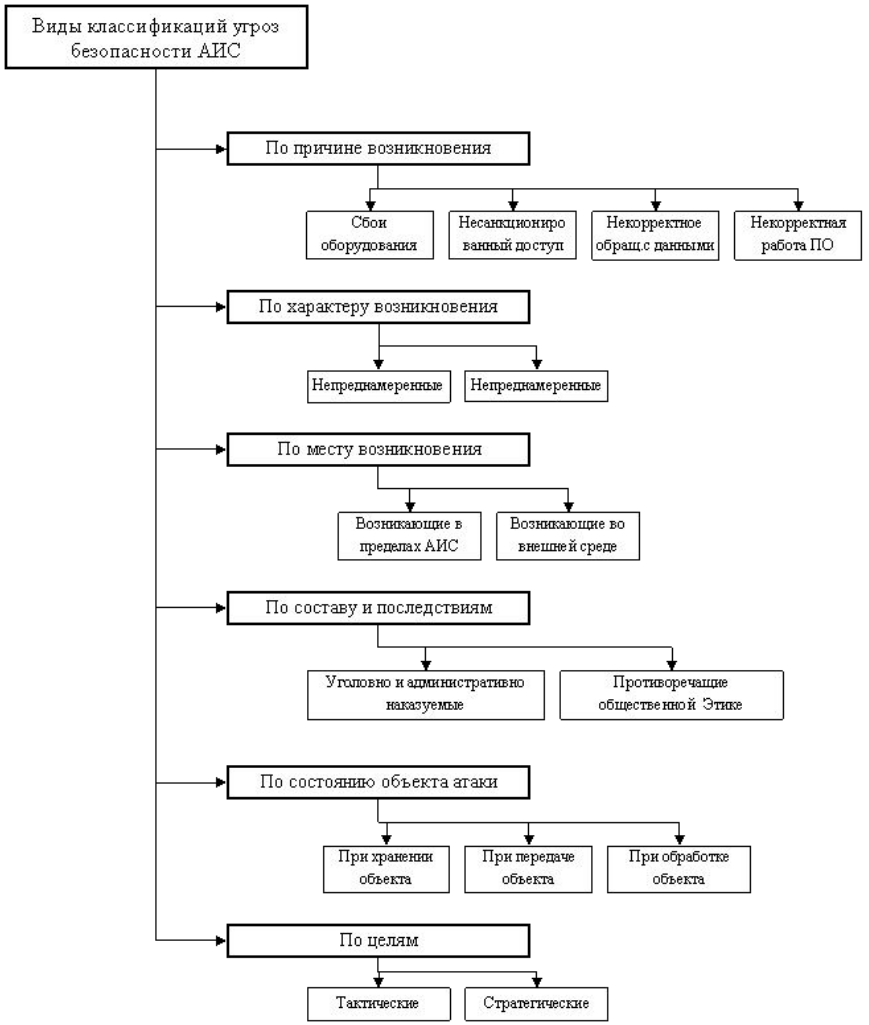


Подходы к созданию систем информационной безопасности

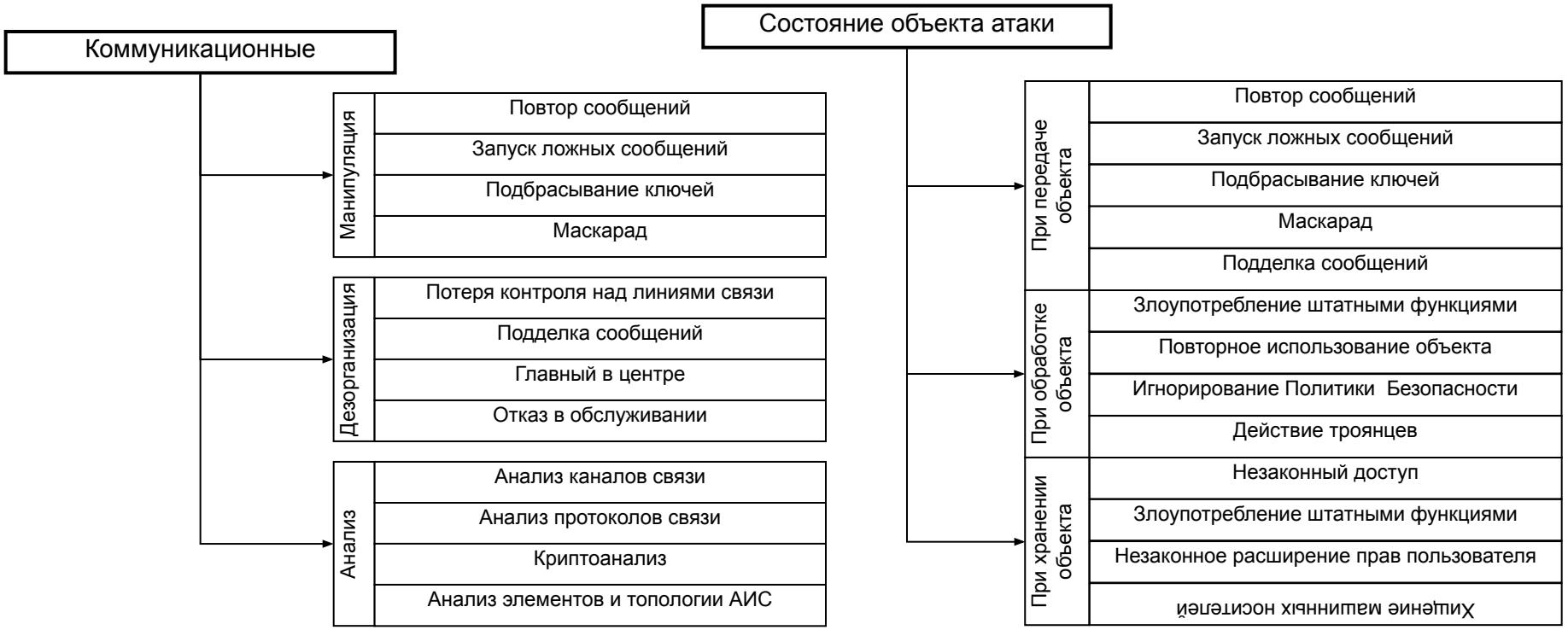
- **«Фрагментарный»** подход ориентируется на противодействие строго определенным угрозам при определенных условиях
- **«Комплексный»** подход ориентируется на создание защищенной среды обработки информации в АИС, объединяющей разнородные меры противодействия угрозам

Классификации угроз информационной безопасности





Предложенные классификации угроз



Меры противодействия угрозам

- Правовые (законодательные),
- Морально-этические,
- Организационные (административные),
- Физические и технические (аппаратурные и программные)

Рассматриваемые методы оценки

- Соответствия АИС техническому заданию
- Анализа функциональной надежности системы
- Количественный метод оценки
  - Метод относительных количественных оценок
  - Метод относительных абсолютных оценок

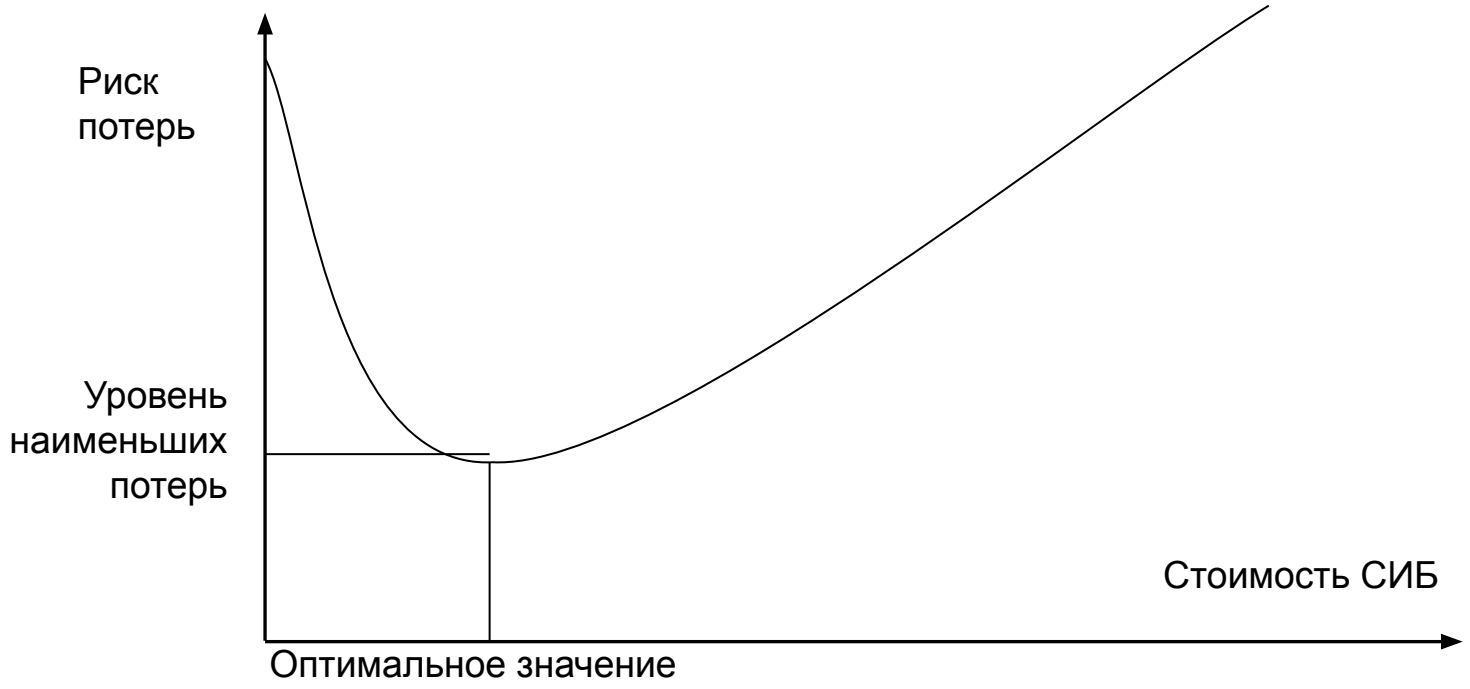
Метод абсолютных количественных показателей

- Технические. В эту группу входят показатели:
  - Количество распознаваемых угроз
  - Качество противостояния угрозам
  - Уменьшение производительности АИС в целом
- Организационные:
  - Количество дополнительно привлеченного персонала для обслуживания СИБ.
  - Затраты на обучение персонала новым методам работы
- Экономические:
  - Стоимость создания, внедрения, эксплуатации и поддержки СИБ АИС.
  - Затраты на специфические материалы
  - Затраты на восстановление нормальной работы после реализации угрозы.
  - Коэффициент уменьшения потенциальных потерь
- Эффективность СИБ

Оценка параметров экономически оптимальных СИБ базируется на анализе:

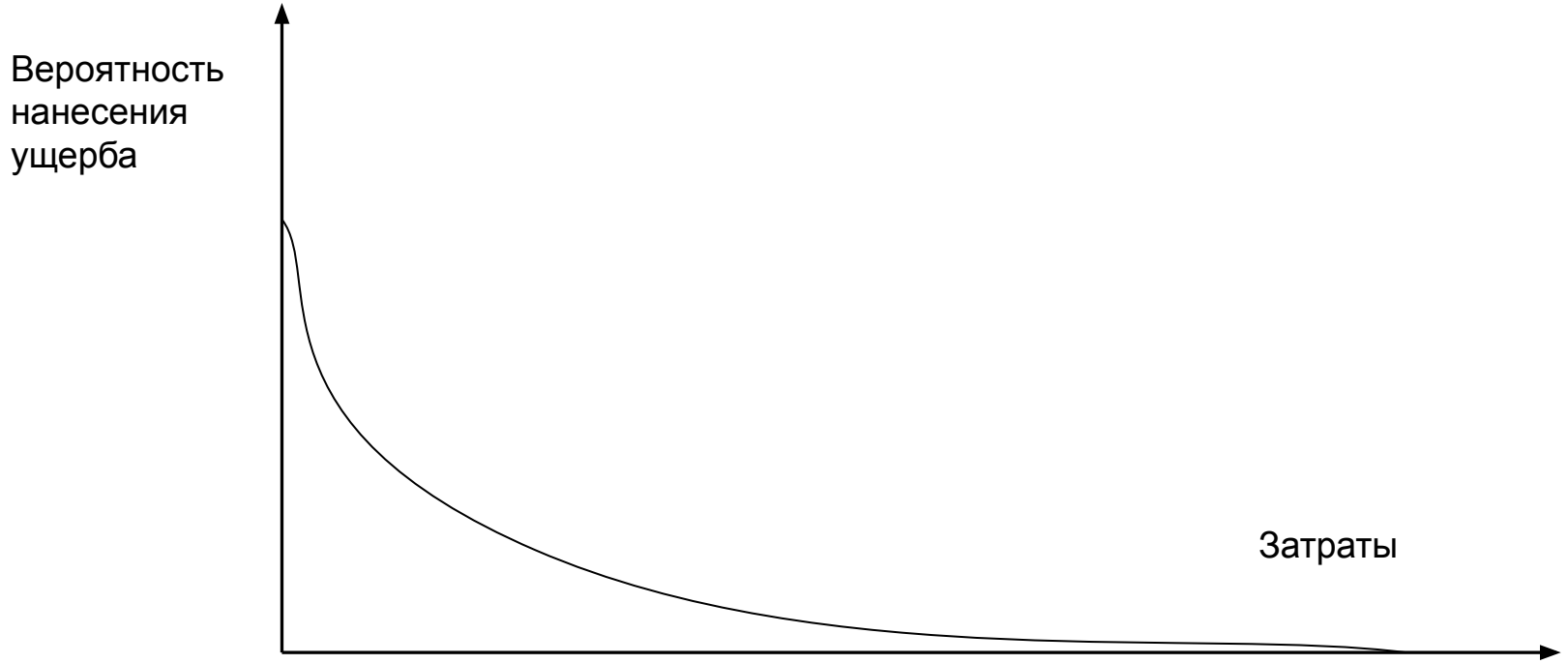
- Риск преодоления СИБ
- Стоимость СИБ (S)
- Вероятность нанесения ущерба собственнику (P)
- Размер возникающего ущерба (U)

Зависимость уровня риска от стоимости СИБ



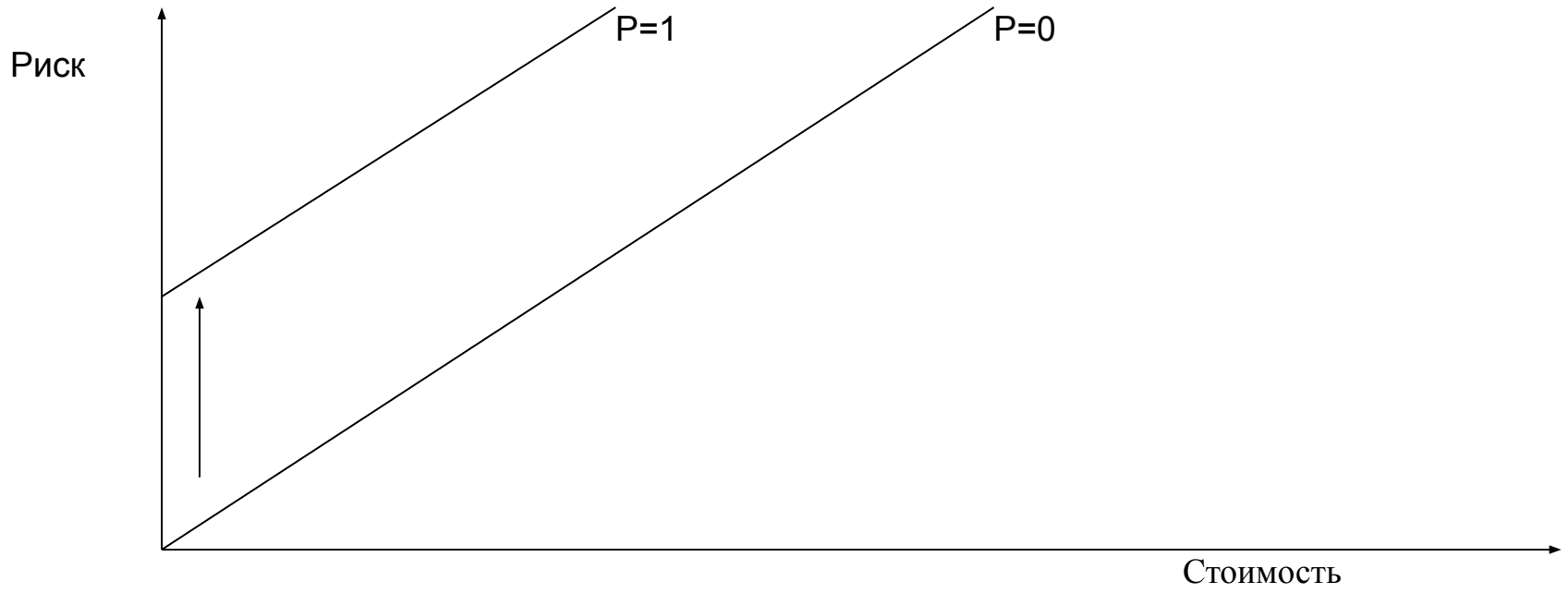
Применение даже недорогих способов и средств защиты информации резко снижает суммарные потери собственника

Вероятность несанкционированных действий в оптимальной СИБ в зависимости от размера возможного ущерба



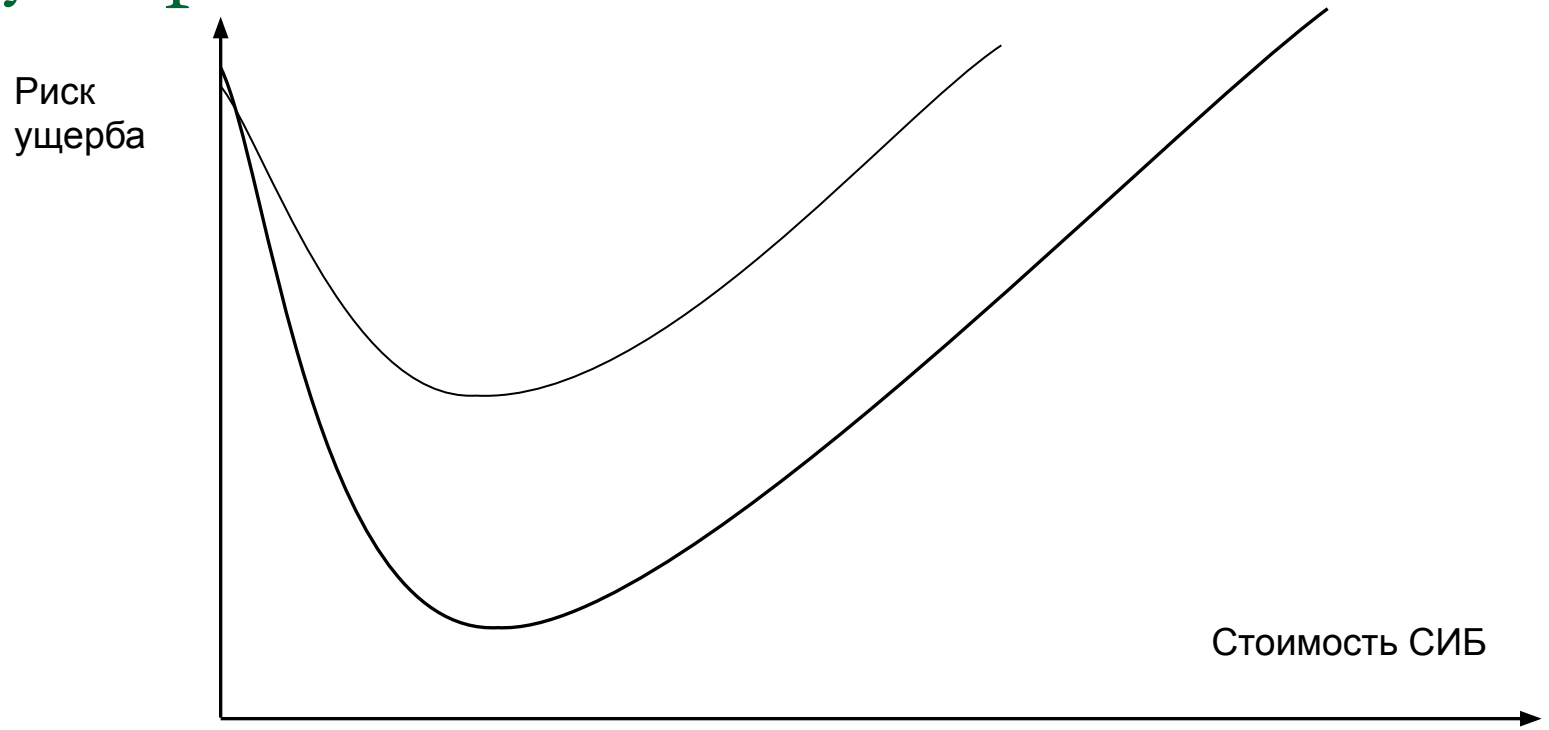
Более высокий уровень безопасности достигается за счет увеличения стоимости СИБ

Вероятности нанесения ущерба не зависит от стоимости системы защиты



Если же изначально характеристики безопасности СИБ неудовлетворительны, то единственно разумным решением является отказ от нее.

Зависимость вероятности нанесения ущерба от стоимости СИБ



Элементы защиты содержат не выявленные ошибки, а СИБ «совершенствуется» путем наращивания из таких элементов

Выводы

- Реализация надежной системы информационной безопасности возможна только при тщательном учете всех аспектов, включая:
  - Комплексное понимание процесса обеспечения информационной безопасности
  - Определение круга угроз СИБ
  - Определения набора возможных мер противодействия угрозам
  - Количественную оценку безопасности и размера ожидаемых потерь.
- Оценка экономически оптимальных параметров и концепция общей стоимости владения системой должны являться основой формирования конкретного технического облика СИБ