Лекция 25 ноября

О подходах к изучению сложных систем

Другой взгляд на этапы СА

12 этапов системного анализа можно сгруппировать, исходя из концепции принятия решений:

- анализ исходной ситуации;

- анализ возможностей выбора;

- выбор решения;

- оценка последствий решения и его корректировка.

Различные ситуации при принятии решений

- Для ЛПР можно различать такие модели в зависимости от степени определенности исходных позиций или последствий:

---- принятие решений в условиях определённости

---- принятие решений в условиях частичной определённости (условия риска!!)

---- принятие решений в условиях неопределённости

---- выбор решения в условиях активного противника

«матрица последствий»

В клетке ij записана «выгода»
Так называемая матрица последствий

Номер решения	ситуация	1	2	3
1		20	10	45
2		10	30	20
3		40	20	30

Критерий Вальда

- Т.н. максиминный критерий ММ (выбираем лучшую стратегию из худших) !!

- о возможности появления внешних состояний ничего не известно;

- приходится считаться с появлением различных внешних состояний ;

- решение реализуется лишь один раз;

- необходимо исключить какой бы то ни было риск, т.е. ни при каких условиях F^j не допускается получать результат, меньший, чем ***по ММ***.

Номер решения	ситуация	1	2	3
1		20	10	45
2		10	30	20
3		40	20	30

Сразу смотрим ММ критерий. Минимумы по столбцам : -
10, 10, 20, - максимальный минимум = 20, значит вариант **по критерию Вальда - №2**

Критерий азартного игрока

это диаметральная противоположность принципу максимина

Критерий азартного игрока допустим в случаях очень низкого риска, а также когда выигрыш намного превышает возможные потери

(кто не рискует…)

Критерий минимаксного риска Сэвиджа

-это наименьшее значение риска,

то есть гарантированное значение

минимальных потерь

Критерий минимаксного риска Сэвиджа

- *Каждый элемент матрицы решений вычитается из наибольшего результата соответствующего столбца.*
- *Разности образуют матрицу остатков (рисков).*
- *Эта матрица пополняется столбцом наибольших разностей .*
- *Выбираются те варианты , в строках которых стоит наименьшее для этого столбца значение*

По критерию Сэвиджа – вариант №3:

Номер решения	ситуация	1		2		3		Макс. риски	
1		20	20	10	20	45	0	20	
2		10	30	30	0	20	25	30	
3		40	0	20	10	30	15	*1*	мин
								5	макс
Макс. столбцов		40		30		45			

Пример – проверка на вирусы.

Решения (поступки) – это про проверку:

- П1 – провести полную проверку с остановкой процесса
- П2 – провести частичную проверку
- П3 – не проводить проверку

Внешнее состояние - заражённость:

В1 – вирусов нет

В2 – вирусы есть, но основные файлы не заражены

В3 – сильное заражение

Техника вычислений

Составляем матрицу из возможных решений и внешних состояний,

В клетках – вероятные убытки в условных единицах (проверка ПЗВ1=0, а ПЗВ3=max убыток.)

	В1	**В2**	**В3**
П1	**-20,0**	**-22,0**	**-25,0**
П2	**-14,0**	**-23,0**	**-31,0**
П3	**0,0**	**-24,0**	**-40,0**

По **ММ** : (максимальные убытки по строкам (-25 -31 -40),
Наилучший из них - -25, значит решение по критерию ММ=П1.

По **Байесу-Лапласу**: средние по строкам (-22,33 -22,67 -21,33)
Наилучший вариант (с меньшими потерями) = П3.
По критерию **Азартного Игрока** - П3.

- По Сэвиджу – П2!! (*покажем это*)

Алгоритм действий по критерию Сэвиджа

1. Записываем матрицу рисков (каждое значение заменяется на отклонение его от наилучшего внешнего состояния в столбце

2. Рядом запишем столбец максимальных рисков решений:

20	0	0	20
14	1	6	**14**
0	2	15	15

3. Минимальный риск 14= П2. Это принятое нами решение по критерию Сэвиджа

Критерий Гурвица

От выбора C зависит приближения критерия к ММ или к АИ

C*min+(1-C)*max

Критерий Ходжа - Лемана

Так же, как и критерий Гурвица, но

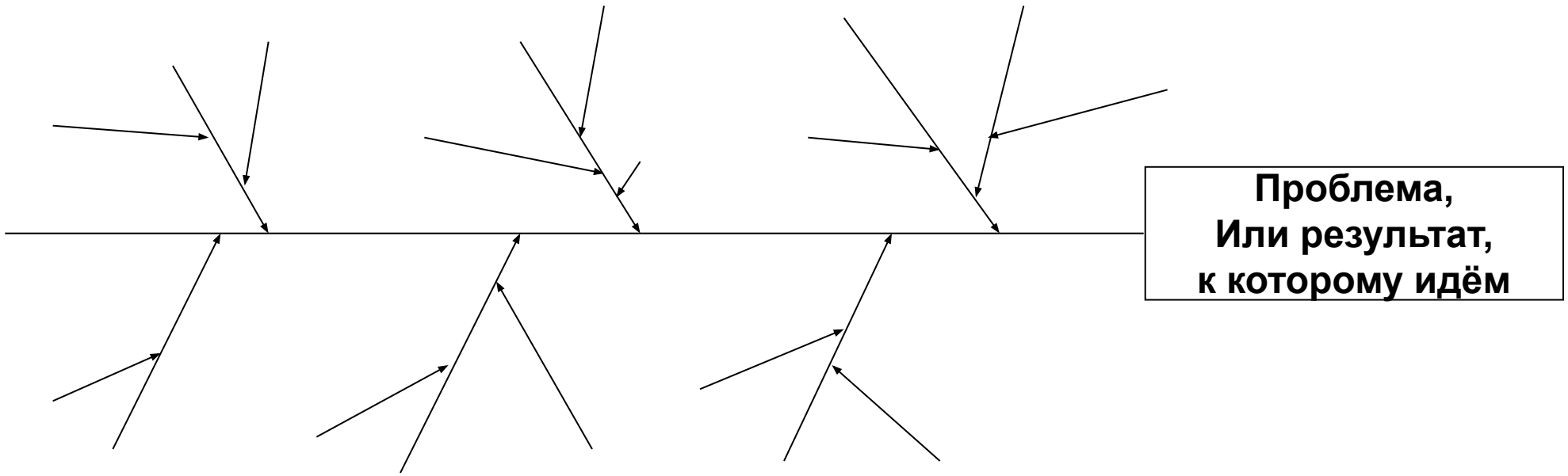
среднее между ММ и Байесом-Лапласом

Ещё несколько критериев :

- - Гермейера
- Б-Л – ММ
- Критерий произведений
- Производные (усложнённые) критерии

Диаграмма Исикавы

«рыбный скелет» или «дерево проблем»

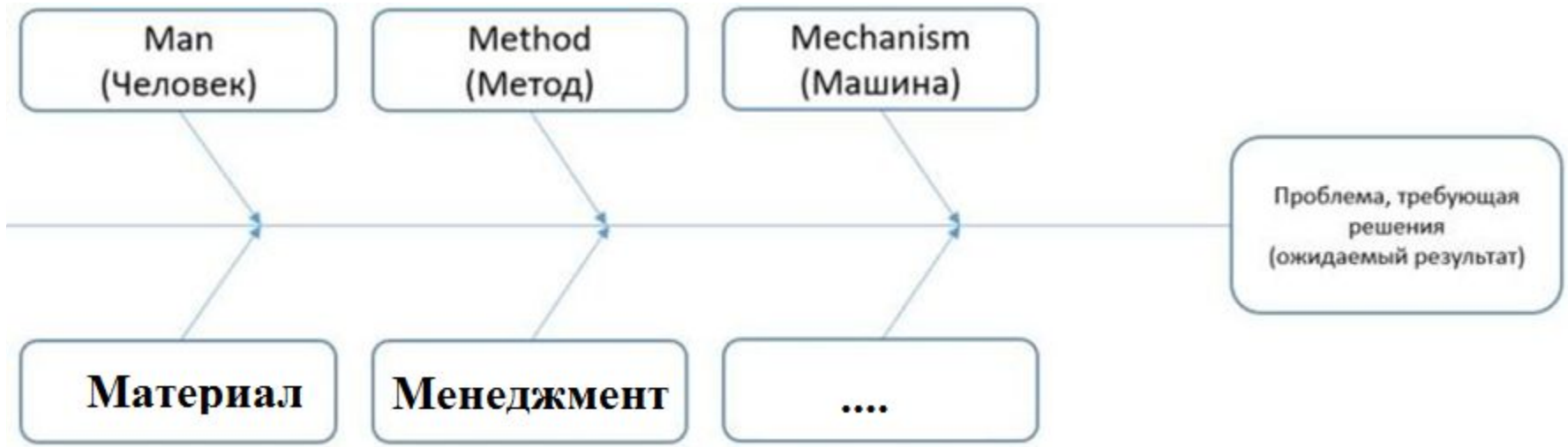


1. При построении диаграммы необходимо нарисовать основную кость
и в правой части кости в «голове рыбы»
сформулировать проблему, требующую решения

2. На втором этапе к основной кости пририсовываются влияющие факторы в зависимости от решаемой проблемы.
Классически для производства их шесть:

- **Man (Человек)**
- **Method (Метод)**
- **Mechanism (Механизм, машина)**
- **Material (Материал)**
- **Management (Менеджмент, управление процессом)**
- **Media (Условия, среда)**

Из-за этого данную диаграмму часто называют 6M по первым буквам шести факторов, но иногда используют 5M (нет Media) и 4M (нет Management).


Man
(Человек)
Method
(Метод)
Mechanism
(Машина)
Проблема, требующая
решения
(ожидаемый результат)
Материал
Менеджмент
....

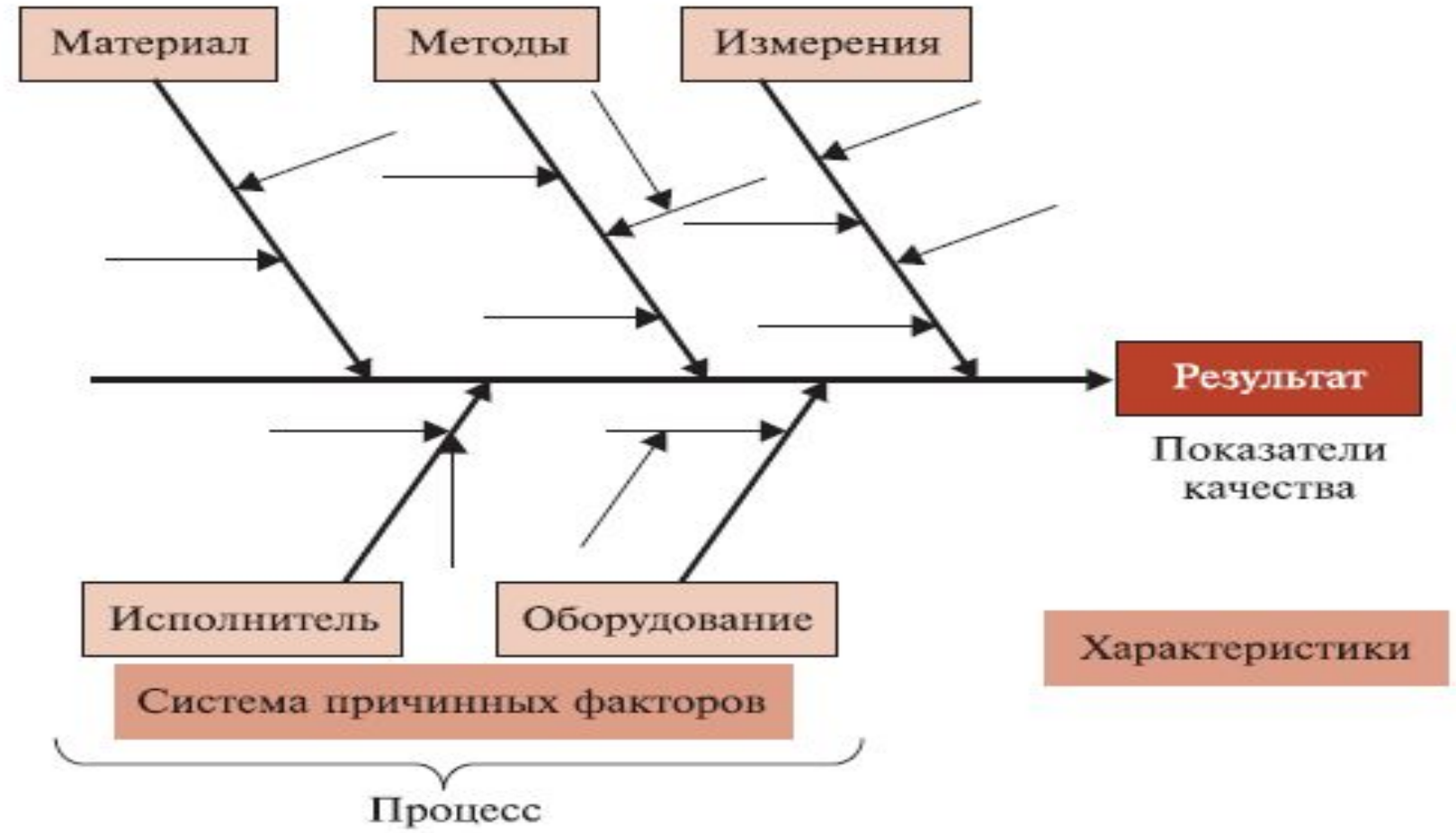
Для сферы услуг использую диаграмму 4S, состоящую из следующих четырёх факторов:

- **Surroundings (Окружение)**
- **Suppliers (Поставщики)**
- **Systems (Системы [используемые])**
- **Standard, documentation, skills (стандарты, документация, навыки)**

В Маркетинговой индустрии используют диаграмму 8P, состоящую из следующих 8 факторов:

- **Product/Service (Продукт/услуга)**
- **Price (Цена)**
- **Place (Место)**
- **Promotion (Продвижение, поддержка [продукта])**
- **People (Люди, персонал)**
- **Process (Процесс)**
- **Physical Evidence (визуальное, вещественное доказательство)**
- **Packaging (Упаковка)**

Причинно-следственная диаграмма ("рыбий скелет")

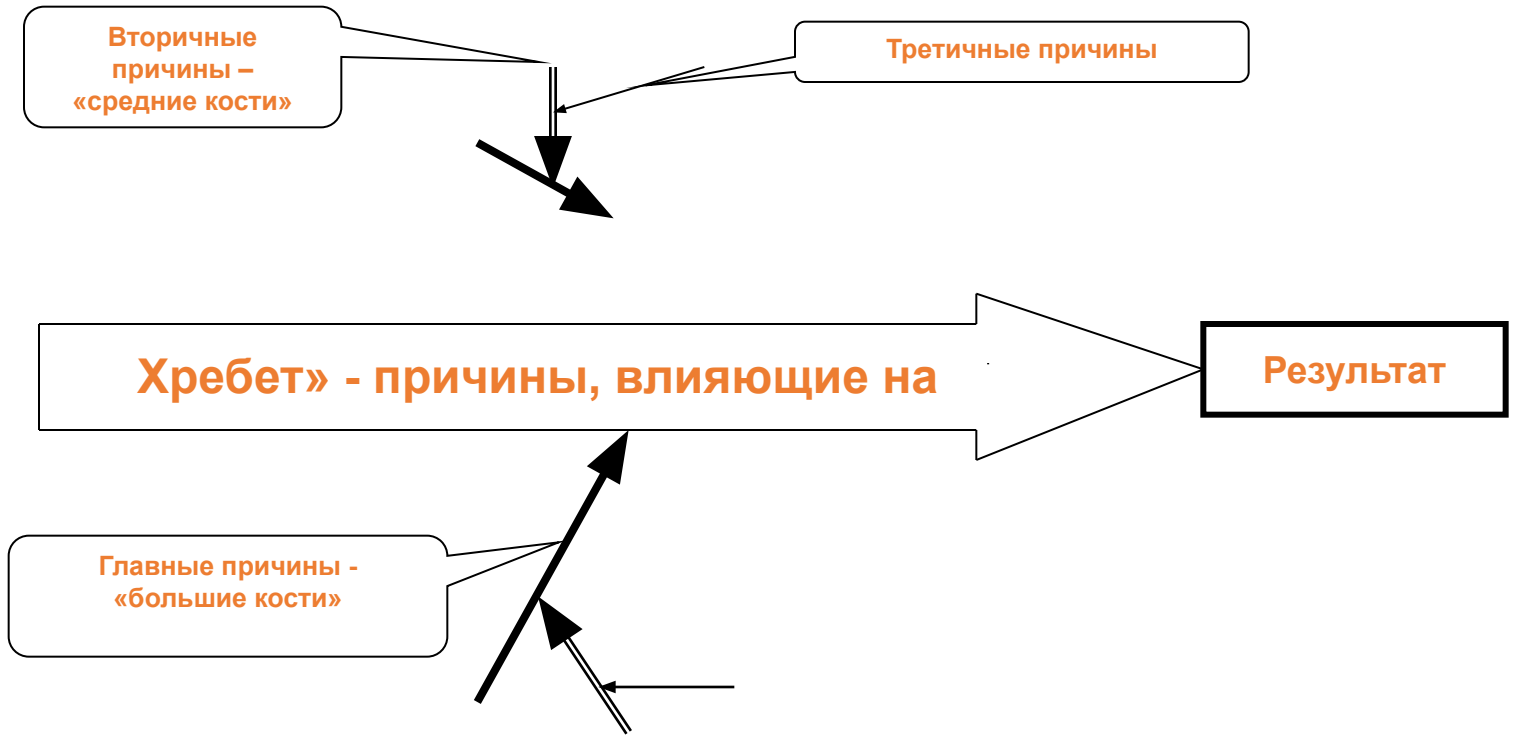


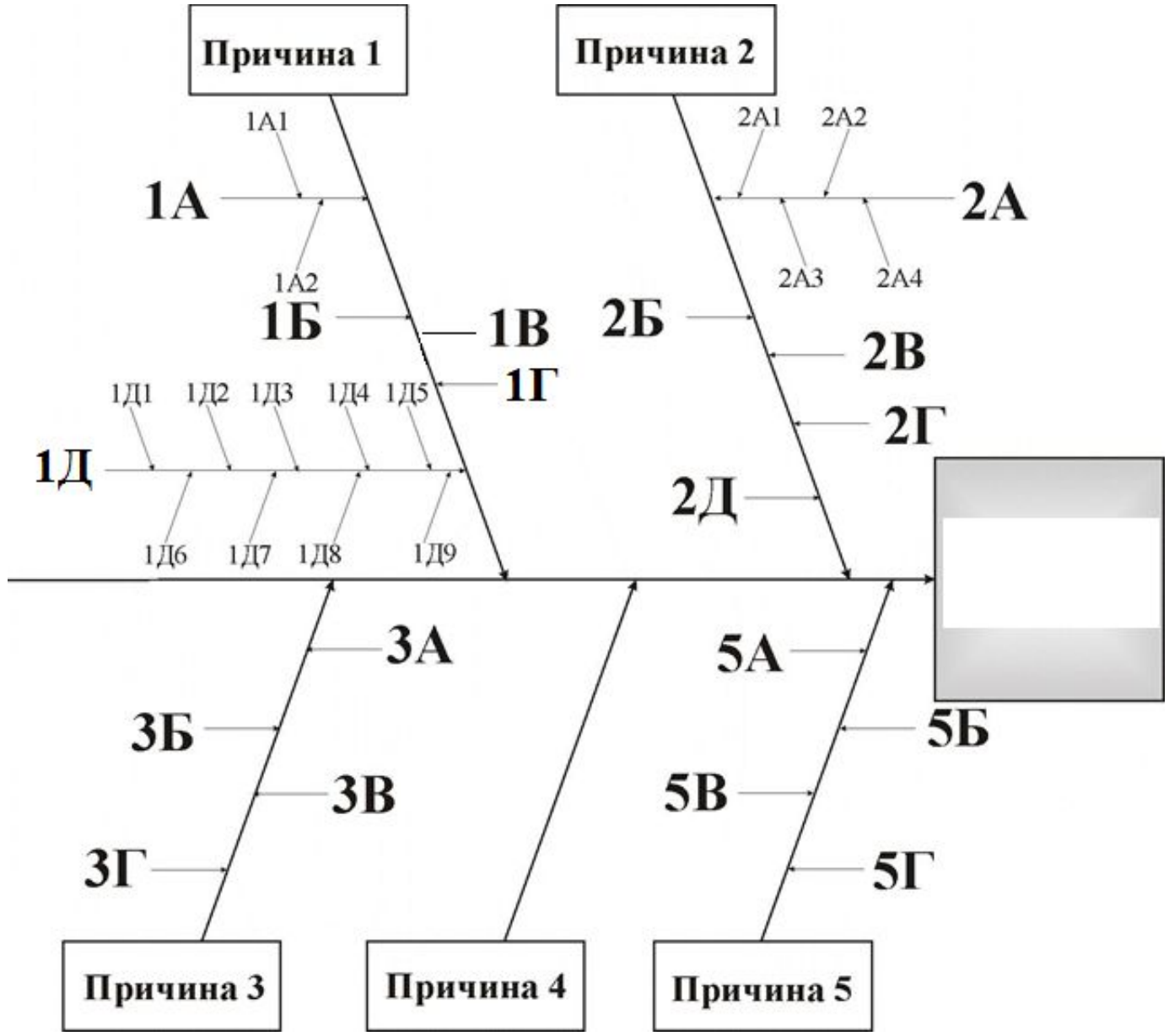

Главная причина 1
Причина 1.1.1
Причина 1.1.2
1.1.2.1
1.1.2.2
Причина 1.1
Причина 1.2
Проблема, требующая решения (ожидаемый результат)

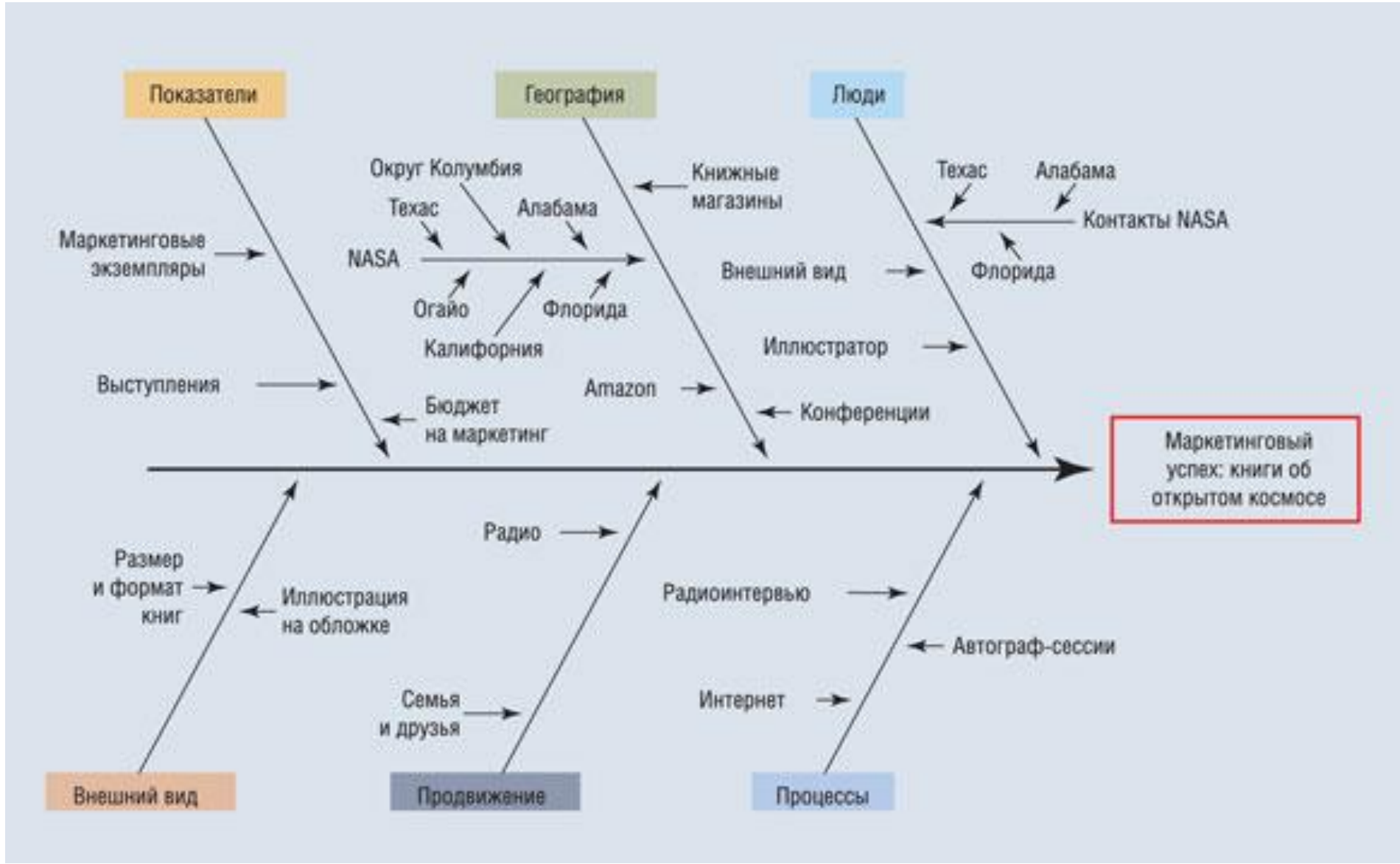
Диаграмма Исикавы

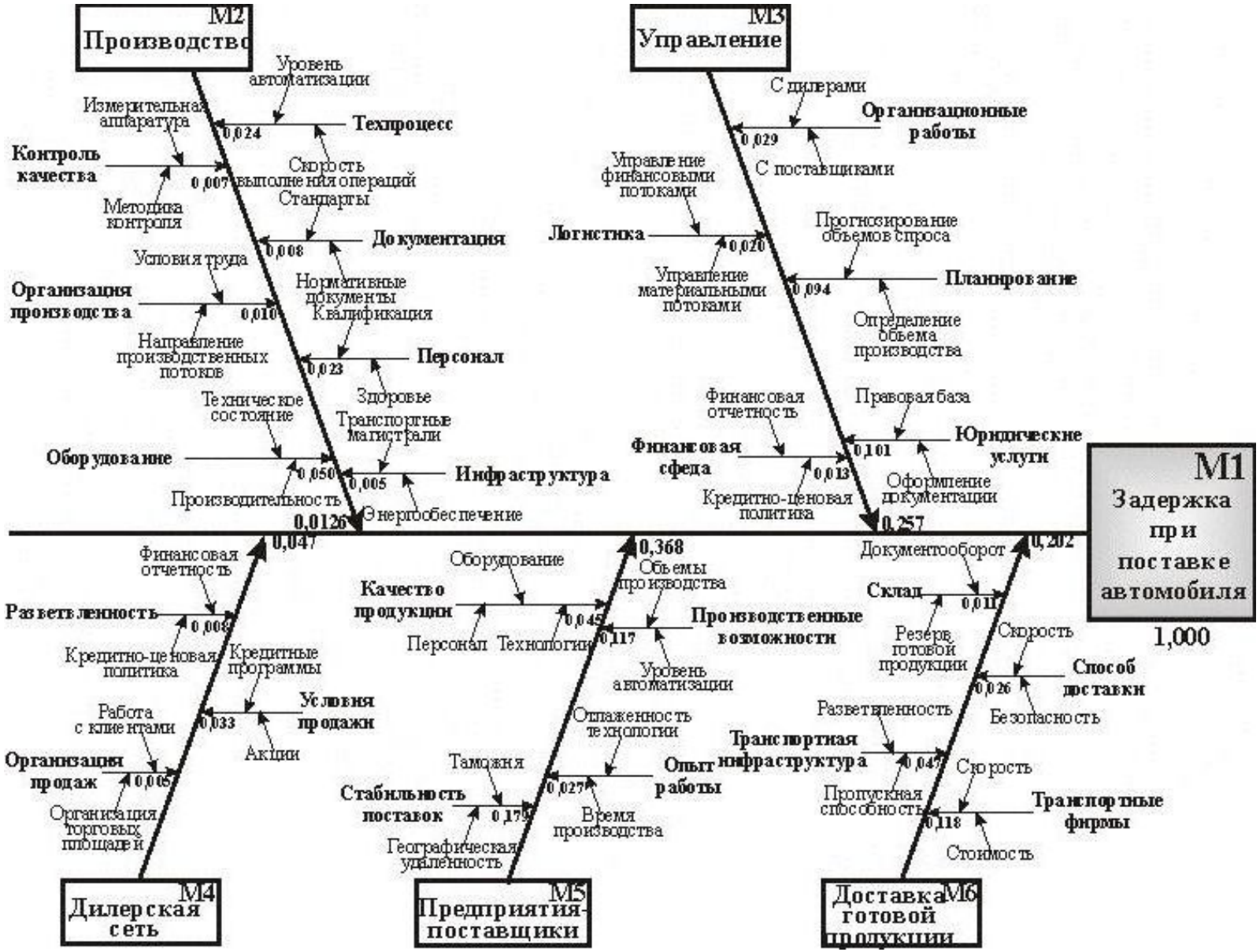
Диаграмма «причина – результат».

В классическом эта диаграмма стоится по принципу « от большего к меньшему».




Причина 1
Причина 2
1А1
1А
1А2
1Б
1В
1Г
1Д1
1Д2
1Д3
1Д4
1Д5
1Д
1Д6
1Д7
1Д8
1Д9
2А1
2А2
2А
2А3
2А4
2Б
2В
2Г
2Д
3А
3Б
3В
3Г
5А
5Б
5В
5Г
Причина 3
Причина 4
Причина 5


Показатели
География
Люди
Маркетинговые экземпляры
Округ Колумбия
Техас
Алабама
NASA
Огайо
Флорида
Калифорния
Книжные магазины
Техас
Алабама
Контакты NASA
Флорида
Внешний вид
Иллюстратор
Выступления
Бюджет на маркетинг
Amazon
Конференции
Маркетинговый успех: книги об открытом космосе
Радио
Размер и формат книг
Иллюстрация на обложке
Радиоинтервью
Автограф-сессии
Семья и друзья
Интернет
Внешний вид
Продвижение
Процессы


M1
Задержка при поставке автомобиля
1,000
M2
Производство
Уровень автоматизации
Измерительная аппаратура
Техпроцесс
0,024
Контроль качества
0,007
Скорость выполнения операций
Стандарты
Методика контроля
Документация
0,008
Условия труда
Нормативные документы
Организация производства
0,010
Квалификация
Направление производственных потоков
Персонал
0,023
Здоровье
Транспортные магистрали
Техническое состояние
Оборудование
0,050
0,005
Инфраструктура
Производительность
Энергообеспечение
0,0126
M3
Управление
С дилерами
Организационные работы
0,029
С поставщиками
Управление финансовыми потоками
Логистика
0,020
Прогнозирование объемов спроса
Управление материальными потоками
0,094
Планирование
Определение объема производства
Финансовая отчетность
Правовая база
Финансовая сфера
0,101
Юридические услуги
0,013
Оформление документации
Кредитно-ценовая политика
0,257
0,047
Финансовая отчетность
Разветвленность
0,009
Кредитно-ценовая политика
Кредитные программы
Условия продажи
Работа с клиентами
0,033
Акции
Организация продаж
0,005
Организация торговых площадей
M4
Дилерская сеть
0,368
Оборудование
Объемы производства
Качество продукции
0,045
Производственные возможности
Персонал
Технологии
0,117
Уровень автоматизации
Отлаженность технологии
Таможня
Опыт работы
Стабильность поставок
0,027
0,175
Время производства
Географическая удаленность
M5
Предприятия-поставщики
0,202
Документооборот
Склад
0,011
Резерв готовой продукции
Скорость
Способ доставки
0,026
Безопасность
Разветвленность
Транспортная инфраструктура
0,047
Скорость
Пропускная способность
Транспортные фирмы
0,118
Стоимость
Доставка готовой продукции
M6

Системный анализ и информационная безопасность

Государство, общество (институты), индивидуумы должны быть способны:

обеспечивать с определенной вероятностью
достаточные и защищенные информационные ресурсы
и информационные потоки

для поддержания своей жизнедеятельности и
жизнеспособности,
устойчивого функционирования и развития

противостоять информационным опасностям и угрозам, негативным информационным воздействиям на

индивидуальное и общественное сознание и психику людей,

а также на компьютерные сети и другие технические источники информации

вырабатывать личностные и групповые

навыки и умения безопасного поведения

поддерживать постоянную готовность к адекватным мерам в информационном противоборстве,

кем бы оно ни было навязано

Обеспечение реализации этих требований осуществляется при помощи систем защиты информации (далее СЗИ)

Следует отметить, что в дальнейшем речь будет идти о СЗИ для организационно-экономических систем

Правовые акты общего назначения

Основной закон Российской Федерации – Конституция.

Статьи Конституции закрепляют ряд прав граждан на защиту и получение информации:

- Ст. 24 – устанавливает право граждан на ознакомление с документами и нормативными актами, затрагивающими права и свободы;
- Ст. 41 – гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья граждан, ст. 42 – право на получение информации о состоянии окружающей среды
- Ст. 23 – гарантирует право на личную и семейную тайну
- Ст. 29 – право искать, получать, производить и распространять информацию любым законным способом

В Гражданском кодексе определяются понятия как банковская, коммерческая и служебная тайна:

Ст. 139 определяет, что для защиты информации, имеющей коммерческую ценность, ее обладатель имеет законные права по охране ее конфиденциальности.

В Уголовном кодексе введен раздел, посвященный преступлениям в компьютерной сфере:

- Ст. 272 – неправомерный доступ
- Ст. 273 – создание, использование и распространение вредоносных программ для ЭВМ
- Ст. 274 – нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сетей

Статья 138 УК РФ предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений;

Статья 183 УК РФ направлена на обеспечение защиты коммерческой и банковской тайны.

Основные цели и задачи систем защиты информации

1. Цели защиты информации

Закон «Об информации, информатизации и защите информации»

- Закон №149-ФЗ (принят 19,07,2006) является одним из основополагающих законов в области информационной безопасности.
- В законе юридически определены важные понятия, такие как **информация, документированная информация, информационная система, конфиденциальная информация, пользователь информации** и т.д.
- В законе выделены следующие цели защиты информации:
  - Предотвращение утечки, хищения, утраты, искажения информации
  - Предотвращения угроз безопасности личности, общества, государства
  - Предотвращение других форм незаконного вмешательства в информационные ресурсы и системы, обеспечение правового режима документированной информации
  - Защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных
  - Сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством
  - Обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем

эффективной может быть только комплексная защита, сочетающая в себе такие направления защиты, как правовая, организационная и инженерно-техническая

Комплексный характер защиты информации проистекает из комплексных действий злоумышленников, стремящихся любыми средствами добыть важную информацию.

Здесь правомерно утверждение, что оружие защиты должно быть адекватно оружию нападения

2. Основные задачи систем защиты информации

к первому виду задач

можно отнести 3 класса,

связанных с

уменьшением степени распознавания объектов:

Скрытие информации о средствах, комплексах, объектах и системах обработки информации. Эти задачи могут подразделяться на технические и организационные. Организационные задачи по скрытию информации об объектах направлены на недопущение разглашения этих сведений сотрудниками и утечки их по агентурным каналам. Технические задачи направлены на устранение или ослабление технических демаскирующих признаков объектов защиты и технических каналов утечки сведений о них. При этом скрытие осуществляется уменьшением электромагнитной, временной, структурной и признаковой доступности, а также ослаблением адекватности между структурой, топологией и характером функционирования средств, комплексов, объектов, систем обработки информации и управления

Дезинформация противника – к этому классу относятся задачи, заключающиеся в распространении заведомо ложных сведений относительно истинного назначения каких-то объектов и изделий, действительного состояния какой-то области государственной деятельности, положения дел на предприятии и т. д.

Дезинформация обычно проводится путем распространения ложной информации по различным каналам, имитацией или искажением признаков и свойств отдельных элементов объектов защиты, созданием ложных объектов, по внешнему виду или проявлениям похожих на интересующих соперника объекты

Легендирование – объединяет задачи по обеспечению получения злоумышленником искаженного представления о характере и предназначении объекта,

когда наличие объекта и направленность работ на нем полностью не скрываются,

а маскируются действительное предназначение и характер мероприятий

Ко второму виду можно отнести 10 классов задач, связанных с защитой содержания получаемой, обрабатываемой, хранимой и передаваемой информации

Введение избыточности элементов системы

Регулирование доступа к средствам, комплексам и системам обработки информации (на территорию, в помещение, к техническим средствам, к программам, к базам данных и т.п.) предполагает реализацию идентификации, проверки подлинности и контроля доступа, регистрацию субъекта, учет носителей информации в системе ее обработки.

Кроме того, к данному классу относятся задачи по установлению и регулированию контролируемых зон вокруг технических средств обработки информации, за пределами которых становятся невозможными выделение и регистрация с помощью технических средств разведки сигналов, содержащих конфиденциальную информацию

Регулирование использования элементов системы и защищаемой информации заключается в осуществлении запрашиваемых процедур (операций) при условии предъявления некоторых заранее обусловленных полномочий

Для решения данного класса задач относительно конфиденциальной информации могут осуществляться такие операции, как ее дробление и ранжирование.

- Дробление (расчленение) информации на части с таким условием, что знание какой-то одной части информации (например, знание одной операции технологии производства какого-то продукта) не позволяет восстановить всю картину, всю технологию в целом.

- Ранжирование включает, во-первых, деление засекречиваемой информации по степени секретности и, во-вторых, регламентацию допуска и разграничение доступа к защищаемой информации: предоставление индивидуальных прав отдельным пользователям на доступ к необходимой им конкретной информации и на выполнение отдельных операций.

Маскировка информации заключается в преобразовании данных, исключающем доступ посторонних лиц к содержанию информации и обеспечивающем доступ разрешенным пользователям при предъявлении ими специального ключа преобразования. Решение этой задачи осуществляется на основе криптографических, некриптографических и смежных с ними (кодовое зашумление, ортогональные преобразования) преобразований

Регистрация сведений предполагает фиксацию всех сведений о фактах, событиях, возникающих в процессе функционирования средств и систем обработки информации, относящихся к защите информации, на основании которых осуществляется решение задач оценки состояния безопасности информации с целью повышения эффективности и управления подсистемами защиты.

Уничтожение информации – представляется как процедура своевременного полного или частичного удаления (стирания) из подсистем хранения информации той ее части, которая не представляет практической, исторической или научной ценности, а также если ее дальнейшее нахождение в той или иной подсистеме становится критичным с точки зрения несанкционированного доступа.

Одной из разновидностей уничтожения информации является так называемое аварийное уничтожение, осуществляемое при явной угрозе злоумышленного доступа к информации повышенной важности. Например, для систем автоматизированной обработки информации типичной процедурой является уничтожение остаточной информации в элементах оперативного запоминающего устройства, отдельных магнитных и оптических носителях, контрольных распечатках, выданных документах после решения соответствующей задачи обработки информации.

Для криптографических систем такой задачей может быть своевременное уничтожение носителей ключевой информации для шифрования.

Обеспечение сигнализации – состоит в реализации процедуры сбора, генерирования, передачи, отображения и хранения сигналов о состоянии механизмов защиты с целью обеспечения регулярного управления ими, а также объектами и процессами обработки информации.

Этот класс задач обеспечивает обратную связь в системе управления, чем достигается обеспечение активности системы защиты.
В основном такие задачи решаются с помощью технических средств сигнализации

Обеспечение реагирования при получении по каналам обратной связи информации о состоянии системы защиты – означает принятие управленческого решения в ответ на полученный сигнал.

Реагирование на проявление дестабилизирующих факторов является признаком активности системы защиты информации, направленным на предотвращение или снижение степени воздействия факторов на информацию и тем самым повышающим устойчивость СЗИ.

Управление системой защиты информации – этот класс объединяет широкий круг задач, связанных с контролем правильности функционирования механизмов обработки и защиты информации, оценкой внутренних и внешних угроз, планированием защиты и т. д.

При этом понятие «контроль» рассматривается в узком смысле и сводится к проверкам эффективности реализации технических и, в частности, аппаратных мер защиты: соответствия элементов системы заданному их составу, текущего состояния элементов системы, работоспособности элементов системы, правильности функционирования элементов системы, отсутствия несанкционированных устройств и систем съема информации

Обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности – минимизация ошибок и сбоев в работе персонала.

В связи с этим к рассматриваемому классу относятся задачи достижения необходимого уровня теоретической подготовки и практических навыков в работе (подготовка персонала), а также задачи формирования высокой психофизиологической устойчивости к воздействию дестабилизирующих факторов и моральной устойчивости к разглашению конфиденциальных сведений (подбор персонала, мотивация и стимулирование его деятельности и др.)

К третьему виду относят задачи защиты информации от информационного воздействия и выделяют 3 класса

1. **Защита от информационного воздействия на технические средства** обработки, хранения и передачи информации может быть направлена: на уничтожение информации (например, электронное подавление средств связи), искажение или модификацию информации и логических связей (внедрение компьютерных вирусов), внедрение ложной информации в систему.

Т.е. данный класс включает задачи реализации технических средств и организационно-технических мероприятий по защите от рассмотренных направлений воздействий

2. Защита от информационного воздействия на общество предполагает разработку и реализацию методов защиты от негативного воздействия через средства массовой информации на общественное сознание людей.

Целями такого воздействия могут быть, например, навязывание общественного мнения (пропаганда), решение экономических вопросов (реклама), разрушение национальных традиций и культуры (навязывание со стороны других государств чуждых культурных ценностей) и др

3. Защита от информационного воздействия на психику человека включает широкий круг задач, направленных как непосредственно на защиту от технических средств воздействия на психику (психотронного оружия), так и на определение и формирование у человека высокой стрессоустойчивости, высоких моральных качеств и т. д., позволяющих противостоять такому воздействию.

2. Проектирование систем защиты информации

- предпроектное обследование, формирующее базовые требования к СЗИ;
- анализ требований, предъявляемых заказчиком к системе;
- проектирование программной и аппаратной компонент – преобразование требований в детальные спецификации системы;
- конструирование – выполнение организационно-технических мероприятий, связанных разработкой и тестированием компонент системы;
- верификация спроектированной системы требованиям безопасности;
- проведение испытаний и опытной эксплуатации системы;

ввод СЗИ в эксплуатацию

Применение системных принципов при проектировании

Принцип **конечной цели**
принцип **измерения**
принцип **эквифинальности**
принцип **единства**
Принцип связности
принцип **модульного построения**
принцип **иерархии**
Принцип **функциональности**
принцип **развития**
Принцип **децентрализации**
принцип **неопределенности**

Принципы проектирования СЗИ

- стоимость создания и эксплуатации системы информационной защиты должна быть меньше, чем размеры наиболее вероятного или возможного допустимого ущерба от любых потенциальных угроз;
- программная защита функциональных программ и данных должна быть комплексной и многоуровневой, ориентированной на все виды угроз с учетом их опасности;
- СИЗ должна иметь целевые, индивидуальные компоненты, предназначенные для обеспечения безопасности функционирования каждого отдельно взятого объекта и функциональной задачи с учетом их уязвимости и степени влияния на безопасность ИС в целом;
- СИЗ не должна приводить к ощутимым трудностям, помехам и снижению эффективности применения и решения основных функциональных задач информационной системы в целом

Процессы проектирования СЗИ требуют проанализировать и конкретизировать задачи, а также исходные данные и факторы, определяющие безопасность ее функционирования:

- критерии качества и их значения, характеризующие необходимый и достаточный уровень безопасности ИС в целом и каждого из ее основных, функциональных компонентов в соответствии с условиями среды применения и требованиями спецификаций заказчика;
- перечень и характеристики возможных внутренних и внешних дестабилизирующих факторов и угроз, способных влиять на безопасность функционирования программных средств и баз данных;
- требования к методам и средствам предотвращения и снижения влияния угроз безопасности системы, обусловленные возможными дефектами программ и данных, а также предумышленными внешними воздействиями;
- перечень подлежащих решению задач защиты, перекрывающих все потенциально возможные угрозы и оценки эффективности решения отдельных задач, необходимых для обеспечения равнопрочной защиты ИС с заданной эффективностью;
- оперативные методы и средства повышения безопасности функционирования программ в течение всего жизненного цикла ИС путем введения временной, программной и информационной избыточности для реализации системы защиты от актуальных видов угроз;
- ресурсы, необходимые и доступные для разработки и размещения программной системы обеспечения безопасности ИС (финансово-экономические, ограниченная квалификация специалистов и вычислительные ресурсы ЭВМ);
- стандарты, нормативные документы и методики воспроизводимых измерений показателей безопасности, а также состав и значения исходных и результирующих данных, обязательных для проведения испытаний;
- технико-экономическая оценка проекта комплекса программ обеспечения безопасности и качества выполнения функций защиты в штатных и экстремальных условиях реализации угроз применению ИС;
- оценки степени влияния средств защиты на функциональные и временные характеристики ИС при автоматизированной обработке основной информации;
- оценки комплексной эффективности защиты ИС и их сравнение с требуемой заказчиком, с учетом реальных ограничений совокупных затрат ресурсов на обеспечение защиты.

В процессе решения перечисленных задач должно быть проведено обоснование структуры и технологии функционирования СЗИ, определена общая структура системы защиты, состав ее ядра и подсистем.

Перечень основных способов и средств СЗИ

Пассивные способы обеспечения безопасности заключаются в создании на пути возникновения или распространения дестабилизирующего фактора некоторого барьера, не позволяющего соответствующему фактору принять опасные размеры.

Типичными его примерами являются блокировки, не позволяющие техническому устройству или программе выйти за опасные границы; создание физических препятствий на пути злоумышленников, экранирование помещений и технических средств и т.п

Активные способы включают в себя контур управления, воздействующий на каждом шаге функционирования ИС на ее элементы с целью решения (или способствования решению) одной или нескольких задач защиты информации.

Например, управление доступом на объект включает следующие функции защиты:

- идентификацию лиц, претендующих на доступ, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);
- опознавание (установление подлинности) объекта или субъекта по предъявленному идентификатору;
- проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
- регистрацию (протоколирование) обращений к защищаемым ресурсам;
- реагирование (сигнализация, отключение, задержка работ, отказ в процессе) при попытках несанкционированных действий.

Основные задачи систем защиты информации реализуются с применением различных методов и средств. При этом различают формальные и неформальные средства.

К *формальным* относятся такие средства, которые выполняют свои функции по защите информации формально, т.е. преимущественно без участия человека. К *неформальным* относятся средства, основу которых составляет целенаправленная деятельность людей. Формальные средства делятся на физические, аппаратные и программные

- **Физические средства** – механические, электрические, электромеханические и т.п. устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов.
- **Аппаратные средства** – различные электронные и электронно-механические и т.п. устройства, схемно встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации. Например, для защиты от утечки по техническим каналам используются генераторы шума. Физические и аппаратные средства объединяются в класс технических средств защиты информации.
- **Программные средства** – специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения автоматизированных систем с целью решении задач защиты информации. Это могут быть различные программы по криптографическому преобразованию данных, контролю доступа, защиты от вирусов и др.

Неформальные средства делятся на организационные, законодательные и морально-этические.

- **Законодательные средства** – существующие в стране или специально издаваемые нормативно-правовые акты, с помощью которых регламентируются права и обязанности, связанные с обеспечением защиты информации, всех лиц и подразделений, имеющих отношение к функционированию системы, а также устанавливается ответственность за нарушение правил обработки информации, следствием чего может быть нарушение защищенности информации.
- **Организационные средства** – специально предусматриваемые в технологии функционирования объекта организационно-технические мероприятия для решения задач защиты информации, осуществляемые в виде целенаправленной деятельности людей.
- **Морально-этические нормы** – сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе. Именно человек, сотрудник предприятия или учреждения, допущенный к секретам и накапливающий в своей памяти колоссальные объемы информации, в том числе секретной, нередко становится источником утечки этой информации или по его вине соперник получает возможность несанкционированного доступа к носителям защищаемой информации.

Стратегии применения средств защиты информации

Выработка стратегии защиты информации в самом общем виде может быть определена как поиск оптимального компромисса между потребностями в защите и необходимыми для этих целей ресурсами.

Потребности в защите обуславливаются, прежде всего, важностью и объемами защищаемой информации, а также условиями ее хранения, обработки и использования. Эти условия определяются уровнем (качеством) структурно-организационного построения объекта обработки информации, уровнем организации технологических схем обработки, местом и условиями расположения объекта и его компонентов и другими параметрами.

Размер ресурсов на защиту информации может быть ограничен определенным пределом либо обусловливается условием обязательного достижения требуемого уровня защиты. В первом случае защита должна быть организована так, чтобы при выделенных ресурсах обеспечивался максимально возможный уровень защиты, а во втором – чтобы требуемый уровень защиты обеспечивался при минимальном расходовании ресурсов.

Сформулированные задачи есть не что иное, как прямая и обратная постановки оптимизационных задач. Существуют две проблемы, затрудняющие формальное решение.

- Первая – процессы защиты информации находятся в значительной зависимости от большого числа случайных и труднопредсказуемых факторов, таких, как поведение злоумышленника, воздействие природных явлений, сбои и ошибки в процессе функционирования элементов системы обработки информации и др.
- Вторая – среди средств защиты весьма заметное место занимают организационные меры, связанные с действием человека.

В качестве примера рассмотрим несколько стратегий, определяемых по двум критериям: требуемому уровню защиты и степени свободы действий при организации защиты.

Значения первого критерия лучше всего выразить множеством тех угроз, относительно которых должна быть обеспечена защита:

- от наиболее опасных из известных (ранее появившихся) угроз;
- от всех известных угроз;
- от всех потенциально возможных угроз.

Второй критерий выбора стратегий защиты сводится к тому, что организаторы и исполнители процессов защиты имеют относительно полную свободу распоряжения методами и средствами защиты и некоторую степень свободы вмешательства в архитектурное построение системы обработки информации, а также в организацию и обеспечение технологии ее функционирования. По этому аспекту удобно выделить три различные степени свободы:

- никакое вмешательство в систему обработки информации не допускается. Такое требование может быть предъявлено к уже функционирующим системам обработки информации, и нарушение процесса их функционирования для установки механизмов защиты не допустимо;
- допускается предъявление ограниченных по степени воздействия требований к архитектурному построению системы обработки информации и технологиям ее функционирования. Возможна приостановка процессов функционирования системы обработки информации или модификация используемых технологий для установки некоторых механизмов защиты.
- требования любого уровня, обусловленные необходимостью защиты информации, принимаются в качестве обязательных условий при проектировании, конструировании и эксплуатации системы обработки информации.

Учитываемые угрозы	Влияние на системы обработки информации		
	Отсутствует	Частичное	Полное
Наиболее опасные	Оборонительная стратегия		
Все идентифицированные угрозы		Наступательная стратегия	
Все потенциально возможные			Упреждающая стратегия

Анализ информационных рисков, угрозы и уязвимости системы

При анализе рисков можно использовать возможные значения ***лингвистических переменных:***

- Малоценный информационный ресурс: от него не зависят критически важные задачи и он может быть восстановлен с небольшими затратами времени и денег.
- Ресурс средней ценности: от него зависит ряд важных задач, но в случае его утраты, он может быть восстановлен за время, менее, чем критически допустимое, стоимость восстановления высокая.
- Ценный ресурс: от него зависят критически важные задачи, в случае утраты время восстановления превышает критически допустимое, либо стоимость чрезвычайно высока.

Оценка рисков по двум факторам

В простейшем случае используется оценка двух факторов: вероятность происшествия и тяжесть возможных последствий. Обычно считается, что риск тем больше, чем больше вероятность происшествия и тяжесть последствий.

Общая идея может быть выражена формулой: РИСК = $Р_{происшествия}$ * ЦЕНА ПОТЕРИ.

Если переменные являются ***количественными величинами*** – риск это оценка математического ожидания потерь.

Если переменные являются качественными величинами, то операция умножения не определена. Таким образом, в явном виде эта формула использоваться не должна. Рассмотрим вариант использования качественных величин (наиболее часто встречающаяся ситуация).

Сначала должны быть определены значения лингвистической переменной вероятности событий, например такой шкалы:

- A – событие практически никогда не происходит;
- B – событие случается редко;
- C – вероятность события за рассматриваемый промежуток времени – около 0,5;
- D – скорее всего событие произойдет;
- E – событие почти обязательно произойдет.

Кроме того, определяется лингвистическая переменная серьезности происшествий, например:

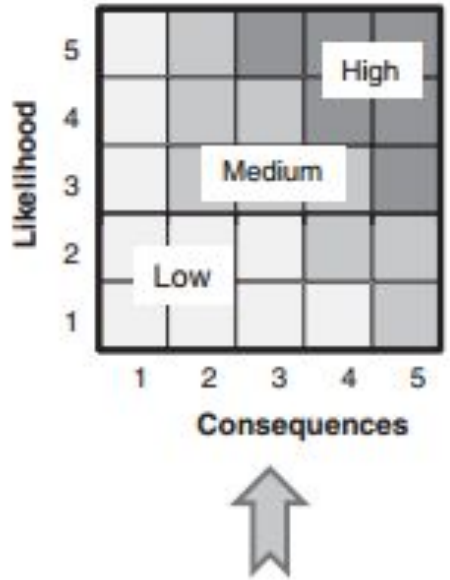
- N (Negligible) – Воздействием можно пренебречь.
- Mi (Minor) – Незначительное происшествие: последствия легко устранимы, затраты на ликвидацию последствий не велики, воздействие на информационную технологию незначительно.
- Mo (Moderate) – Происшествие с умеренными результатами: ликвидация последствий не связана с крупными затратами, воздействие на информационную технологию не велико и не затрагивает критически важные задачи.
- S (Serious) – Происшествие с серьезными последствиями: ликвидация последствий связана со значительными затратами, воздействие на информационные технологии ощутимо, воздействует на выполнение критически важных задач.
- C (Critical) – Происшествие приводит к невозможности решения критически важных задач.

Для оценки рисков определяется переменная из трех значений: низкий риск, средний риск, высокий риск.

	Negligible	Minor	Moderate	Serious	Critical
A	Низкий риск	Низкий риск	Низкий риск	Средний риск	**Средний риск**
B	Низкий риск	Низкий риск	Средний риск	Средний риск	**Высокий риск**
C	Низкий риск	Средний риск	Средний риск	Средний риск	**Высокий риск**
D	Средний риск	Средний риск	Средний риск	Средний риск	**Высокий риск**
E	**Средний риск**	**Высокий риск**	**Высокий риск**	**Высокий риск**	**Высокий риск**

Derived from
Risk Management—A Process Overview by Bob Skalamera

Likelihood	What is the likelihood the risk will happen?	
Level		Your approach and processes …
1	Not likely	… Will effectively avoid or mitigate this risk based on standard practices
2	Low likelihood	… Have usually mitigated this type of risk with minimal oversight in similar cases
3	Likely	… May mitigate this risk, but work-arounds will be required
4	Highly likely	… Cannot mitigate this risk, but a different approach might
5	Near certainty	… Cannot mitigate this type of risk; no known processes or work-arounds are available



Consequences	Given the risk is realized, what would be the magnitude of the impact?		
Level	Technical	Schedule	Cost
1	Minimal or no impact	Minimal or no impact	Minimal or no impact
2	Minor performance shortfall, same approach retained	Additional activities required, able to meet key dates	Budget increase or unit production cost increase <1%
3	Moderate performance shortfall, but work-arounds available	Minor schedule slip, will miss needed dates	Budget increase or unit production cost increase <5%
4	Unacceptable, but work-arounds available	Project critical path affected	Budget increase or unit production cost increase <10%
5	Unacceptable; no alternatives exist	Cannot achieve key project milestones	Budget increase or unit production cost increase >10%

При разработке (использовании) методик оценки рисков необходимо учитывать следующие особенности:

- Значения шкал должны быть четко определены (словесное описание) и пониматься одинаково всеми участниками процедуры экспертной оценки.
- Требуются обоснования выбранной таблицы. Необходимо убедиться, что разные инциденты, характеризующиеся одинаковыми сочетаниями факторов риска, имеют с точки зрения экспертов одинаковый уровень рисков.

Подобные методики широко применяются при проведении анализа рисков базового уровня.