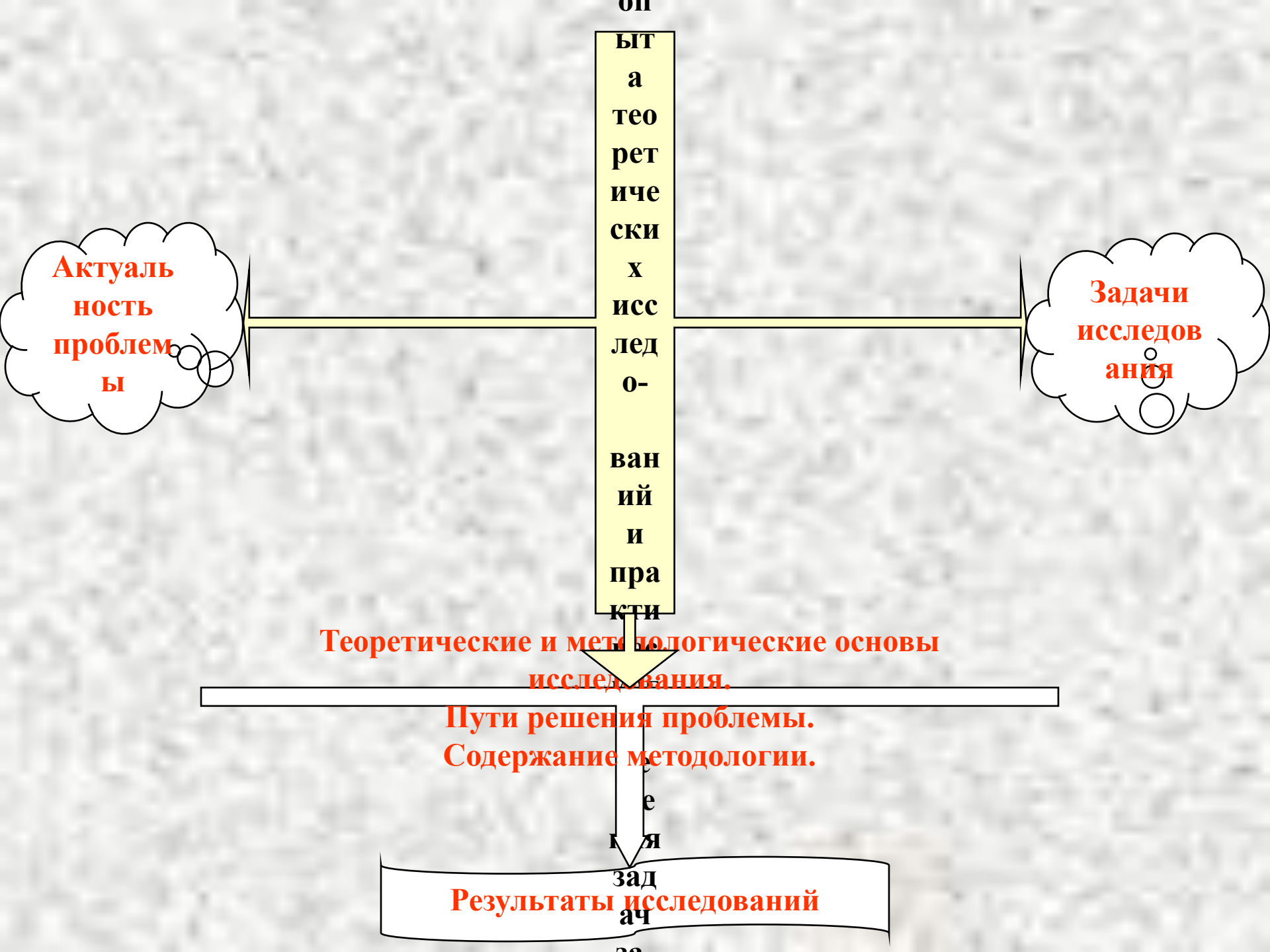
# Современные проблемы теории и практики защиты информации

# Содержание

1. Проблема, цель, задачи, основы исследования.
2. Современная постановка задачи ЗИ.
3. Унифицированная концепция ЗИ.
4. Теория ЗИ.
5. Интерпретация общеметодологических принципов развития науки применительно к современным проблемам ЗИ.
6. Обобщенная модель процессов ЗИ.
7. Методология оценки уязвимости информации.
8. Методы определения требований к ЗИ.
9. Система ЗИ.
10. Проектирование систем ЗИ.
11. Перспективы развития теории и практики ЗИ.
12. Основные научные и практические результаты.


Актуальность проблемы
Задачи исследования
Теоретические и методологические основы исследования.
Пути решения проблемы.
Содержание методологии.
Результаты исследований

**Актуальность проблемы**

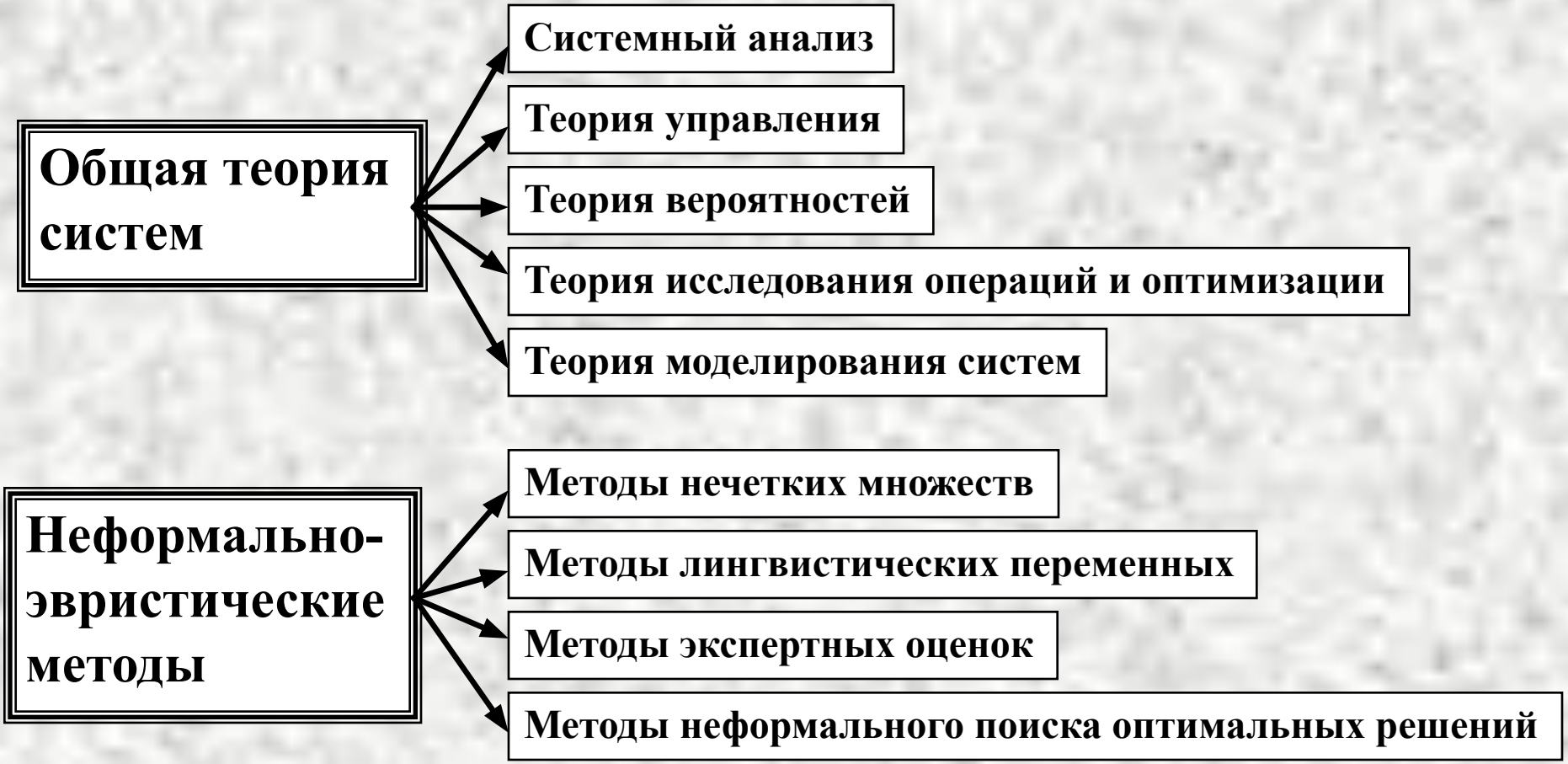
**определяется:**

1. **Вступлением современного общества в информационный этап развития.**
2. **Массовой компьютеризацией информационных процессов.**
3. **Возрастанием влияния информационной безопасности (ИБ) автоматизированных систем (АС) на эффективность их функционирования.**
4. **Необходимостью перехода к интенсивным способам защиты информации (ЗИ) в АС.**
5. **Целесообразностью развития комплексного подхода к обеспечению ИБ.**
6. **Потребностями разработки научно обоснованных нормативно-методических документов по ЗИ и стандартизации систем защиты на объектовом, региональном и государственном уровнях.**
7. **Необходимостью совершенствования кадрового обеспечения ИБ.**

# Задачи исследования

1. Определение места проблем ИБ в общей совокупности информационных проблем современного общества.
2. Анализ развития подходов к ЗИ и обоснование необходимости перехода в современных условиях к интенсивным способам защиты.
3. Формирование научно-методологических основ интенсификации процессов ЗИ.
4. Исследование угроз и разработка методологии оценки уязвимости информации в современных системах ее обработки.
5. Разработка методов определения требований к ЗИ с учетом факторов, влияющих на уровень защиты, и потенциально возможных условий функционирования АС.
6. Формирование общеметодологических принципов построения систем ЗИ и управления процессами их функционирования.
7. Выработка практических рекомендаций по интенсификации процессов ЗИ и формированию современных организационных структур, обеспечивающих эффективную реализацию комплексного подхода к обеспечению ИБ.

# Теоретические и методологические основы исследования




**Пути решения проблемы:** концептуальный
методологический
организационный
технический

# Содержание методологии

| 1. Научно-методологический базис защиты информации | 2. Методология оценки уязвимости информации | 3. Методология определения требований к защите информации | 4. Методы проектирования систем защиты информации | 5. Технология организационного обеспечения защиты информации |
|---|---|---|---|---|
| **Классическая основа** | | | | |
| 1. Методы системного анализа<br>2. Концептуальные основы моделирования систем<br>3. Концептуальные основы решения слабо структурированных проблем | 1. Методы теориии вероятностей | 1. Концептуальные основы моделирования систем<br>2. Методы экспертных оценок<br>3. Методы кластерного анализа<br>4. Концептуальные основы теории информации | 1. Общие понятия теории исследования операций и оптимизации<br>2. Концептуальные основы теории управления | 1. Концептуальные основы теории управления<br>2. Методы экспертных оценок |

# Современная постановка задачи ЗИ

**Информационный период развития общества**

**Возрастание роли информации, информационных ресурсов и технологий в жизни граждан, общества и государства в XXI веке выводят вопросы ИБ на первый план в системе обеспечения национальной безопасности.**

**Современные средства и унифицированные методы**

**Проблемы ЗИ являются производными относительно более общих проблем информатизации, поэтому концептуальные подходы к их решению должны увязываться с концепциями информатизации, которые базируются на современных средствах и унифицированных методах.**

**Многоаспектная комплексная защита**

**История развития подходов к решению проблем ЗИ включает три периода: эмпирический, концептуально-эмпирический и теоретико-концептуальный. Современный теоретико-концептуальный подход заключается в разработке основ теории ЗИ, постановке задачи многоаспектной комплексной защиты и формировании унифицированной концепции ЗИ.**

**Возрастание значимости системных вопросов**

**Взгляд на ЗИ как комплексную проблему приводит к возрастанию значимости системных вопросов:**

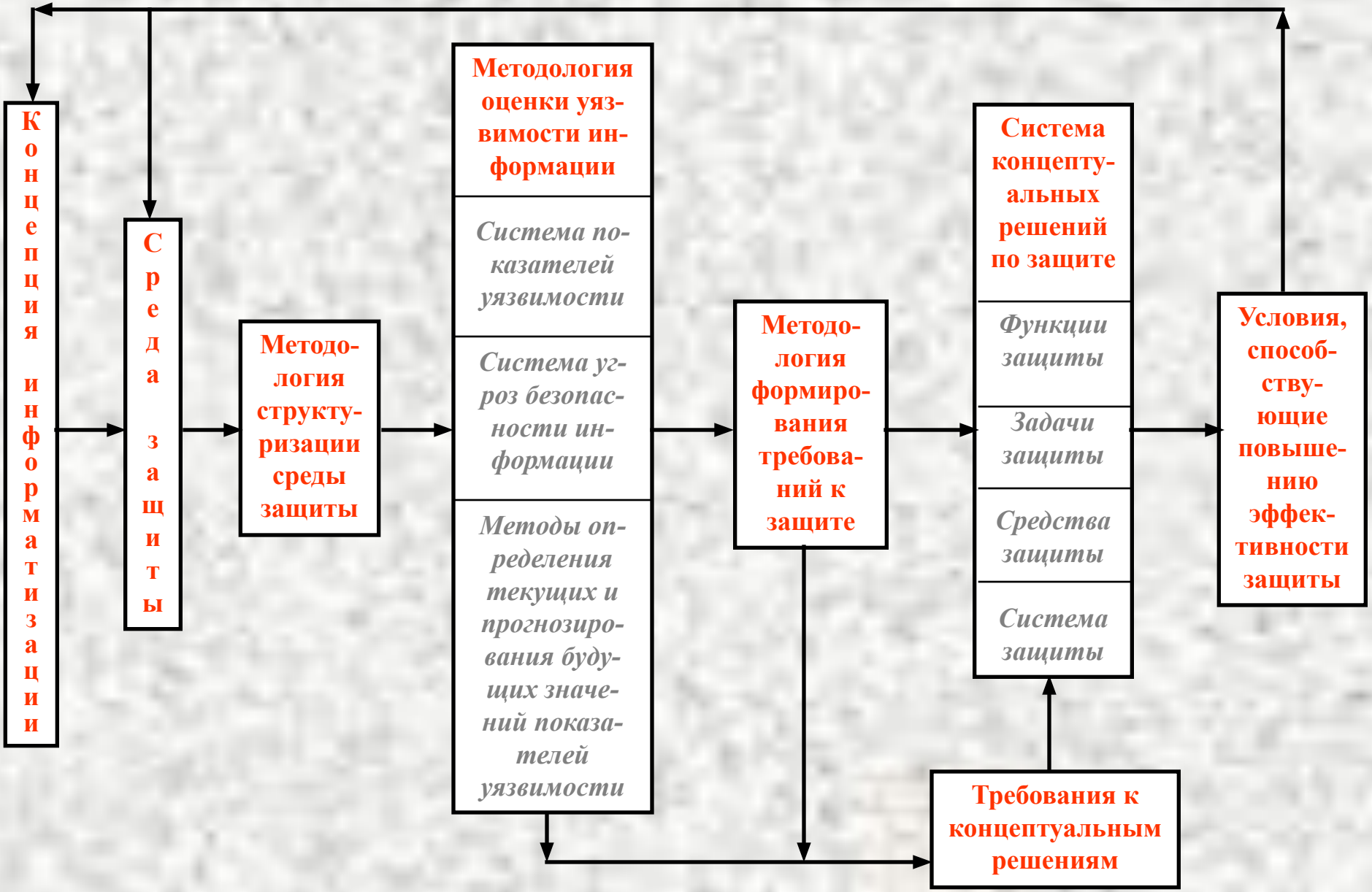
- **формирование и обоснование общей политики защиты;**
- **оптимизация процессов проектирования и функционирования комплексных систем защиты;**
- **подбор, обучение и расстановка соответствующих кадров специалистов;**
- **сбор и аналитико-синтетическая обработка данных о функционировании реальных систем защиты.**

**Переход к интенсивным способам защиты**

**Переход к интенсивным способам ЗИ предполагает:**

- **структурированное описание средств защиты;**
- **всесторонний количественный анализ степени уязвимости информации на объекте;**
- **научно обоснованное определение требуемого уровня защиты;**
- **построение оптимальных систем защиты на основе единой унифицированной методологии.**

# Унифицированная концепция ЗИ



# Теория защиты информации -

**система основных идей,
относящихся к защите информации
в современных системах ее обработки,
дающая целостное представление о
сущности проблемы защиты,
закономерностях ее развития и существенных
связях с другими отраслями знания,
формирующаяся и развивающаяся на основе
опыта практического решения задач защиты и
определяющая основные ориентиры в
направлении совершенствования
практики защиты информации.**

**Теория защиты информации**

1. Полные и систематизированные сведения о происхождении, сущности и содержании проблемы защиты.

2. Систематизированные результаты ретроспективного анализа развития теоретических исследований и разработок, а также опыта практического решения задач защиты, полно и адекватно отражающие наиболее устойчивые тенденции в этом развитии.

3. Научно обоснованная постановка задачи ЗИ в современных системах ее обработки, полно и адекватно учитывающая текущие и перспективные концепции построения систем и технологий обработки, потребности в ЗИ и объективные предпосылки их удовлетворения.

4. Общие стратегические установки на организацию ЗИ, учитывающие все многообразие потенциально возможных условий защиты.

5. Методы, необходимые для адекватного и наиболее эффективного решения всех задач защиты и содержащие как общеметодологические подходы, так и конкретные приложения.

6. Методологическая и инструментальная база, содержащая необходимые методы и инструментальные средства решения любой совокупности задач защиты в рамках любой выбранной стратегической установки.

7. Научно обоснованные предложения по организации и обеспечению работ по ЗИ.

8. Научно обоснованный прогноз перспективных направлений развития теории и практики ЗИ.

# Интерпретация общеметодологических принципов развития науки применительно к современным проблемам ЗИ

# 1. Строгая целевая направленность

**Главная цель - формирование научно-технических предпосылок, необходимых для перехода от экстенсивных способов решения проблем ЗИ к интенсивным, т.е.:**

**1) дальнейшее развитие основ теории защиты;**

**2) формирование регулярных методологий анализа степени опасности для информации, обоснование целесообразного уровня защиты; создание методологии синтеза систем защиты, оптимальных по всей совокупности существенно значимых критериев, оптимального управления системой в процессе ее функционирования.**

# 2. Неукоснительное следование главной задаче науки - за внешними проявлениями вскрыть внутреннее движение

**Необходимо:**

1) **подвергнуть тщательной аналитико-синтетической обработке всю совокупность статистических данных, относящихся к ЗИ в современных АС;**
2) **выявить устойчивые тенденции в эволюционном развитии теории и практики ЗИ;**
3) **осуществить прогноз наиболее вероятных направлений развития выявленных тенденций.**

# 3. Упреждающая разработка общих концепций

1) уточнение и строгое научное обоснование УКЗИ - унифицированной концепции защиты информации;

2) формирование на базе кортежа концептуальных решений по ЗИ единой методологии создания, организации и обеспечения функционирования систем ЗИ, соответствующих заданным требованиям к защите.

# 4. Формирование концепций на основе реальных фактов

1) формирование структуры и содержания информационного кадастра по ЗИ;
2) организация систематического и целенаправленного сбора и накопления всех данных, относящихся к ЗИ;
3) регулярная обработка всех накопленных данных в целях обновления и пополнения информационного кадастра по ЗИ;
4) периодический анализ данных информационного кадастра в целях выявления новых фактов относительно различных аспектов ЗИ.

# 5. Учет всех существенно значимых факторов, влияющих на изучаемую проблему

1) рассмотрение ЗИ как комплексной проблемы в целевом, инструментальном и организационном аспектах;
2) рассмотрение проблемы комплексной защиты как составляющей части более общей проблемы управления информацией;
3) рассмотрение проблемы управления информацией как составляющей части глобальной проблемы информатизации современного общества.

# 6. Строгий учет диалектики взаимосвязей количественных и качественных изменений в развитии изучаемых явлений

**Необходимо предметно обосновать, что к настоящему времени в развитии проблем ЗИ произошли (накоплены) такие количественные изменения (масштабы работ, объемы расходуемых ресурсов, арсеналы используемых средств), на основе которых вполне созрела необходимость качественных изменений в подходах к организации и обеспечению защиты в общегосударственном масштабе.**

# 7. Своевременное видоизменение постановки задачи

**Интерпретация требований данного принципа заключается в разработке и обосновании необходимости, сущности и содержания перехода от экстенсивных к интенсивным способам решения всех проблем ЗИ.**

# Теоретико-прикладные принципы:

- построение адекватных моделей изучаемых систем и процессов;
- унификация разрабатываемых решений;
- максимальная структуризация изучаемых систем и разрабатываемых решений;
- радикальная эволюция в реализации разработанных концепций.

# Обобщенная модель процессов ЗИ

**Принятые сокращения:**

**{K} - множество показателей уязвимости (защищенности информации);**

**$\{P^{(c)}\}$ - множество параметров внешней среды, оказывающих влияние на функционирование АС;**

**$\{R^{(c)}\}$ - множество ресурсов АС, участвующих в обработке защищаемой информации;**

**$\{P^{(y)}\}$ - множество внутренних параметров АС и системы ЗИ, которыми можно управлять непосредственно в процессе обработки защищаемых данных;**

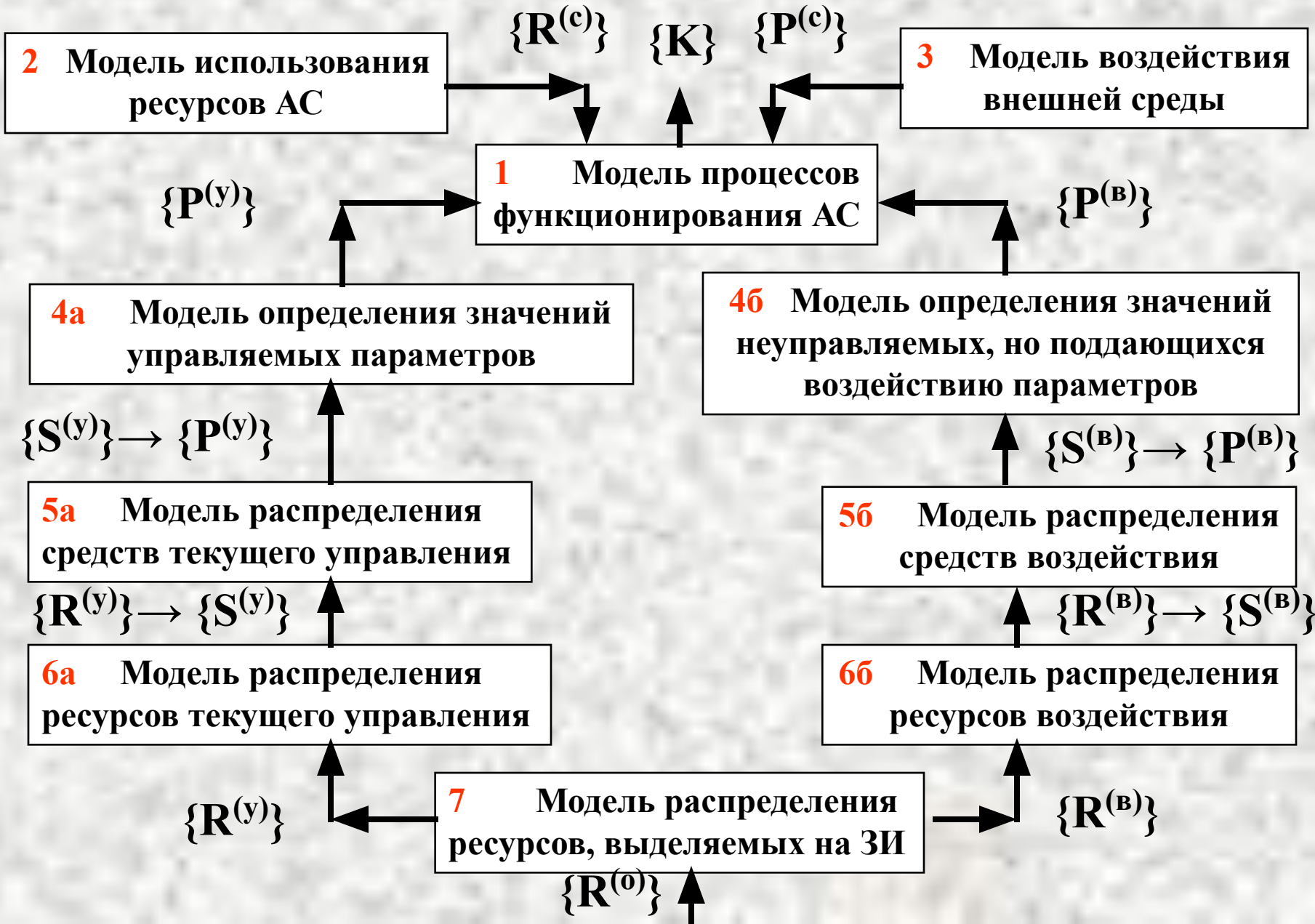
**$\{P^{(в)}\}$ - множество внутренних параметров АС, не подлежащих непосредственному управлению, но поддающихся воздействию;**

**$\{S^{(y)}\}$ и $\{R^{(y)}\}$ - множества средств и ресурсов текущего управления;**

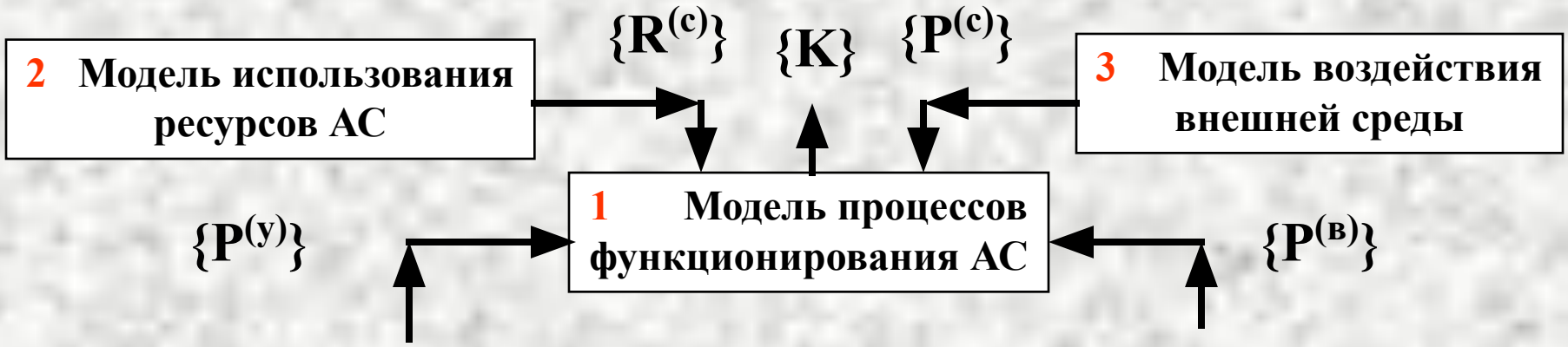
**$\{S^{(в)}\}$ и $\{R^{(в)}\}$ - множества средств и ресурсов воздействия;**

**$\{R^{(o)}\}$ - множество общих ресурсов управления.**

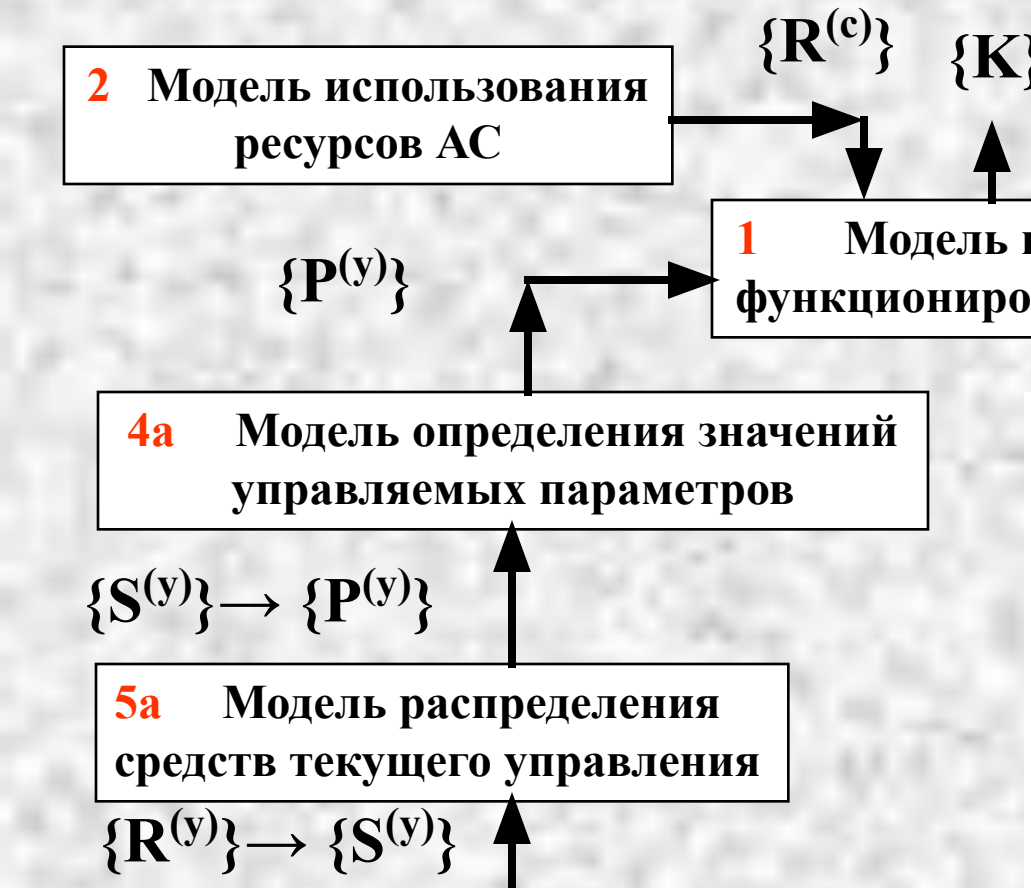
# Обобщенная модель процессов ЗИ



# Модификации обобщенной модели




# 1 - Модель функционирования АС при отсутствии управления ЗИ



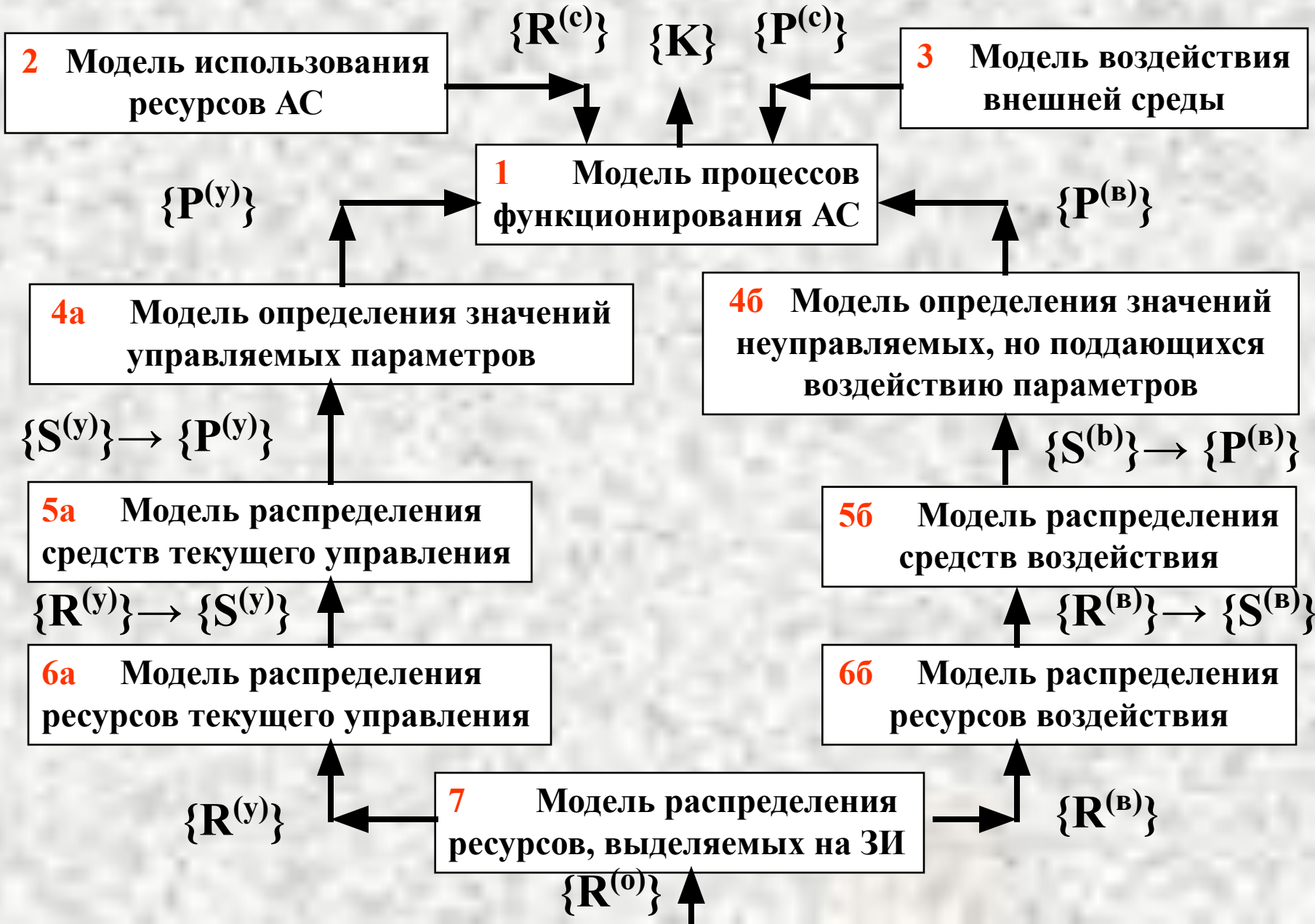

# 2 - Модель текущего управления ЗИ


# 3 - Модель управления ресурсами, выделяемыми на ЗИ


# 4 - Модель управления средствами воздействия на параметры, не допускающие текущего управления


# 5 - Модель управления ресурсами, выделенными на развитие АС

# 6 - Полная модель защиты



## Задача анализа

$$\{K\} = F\,[\{P^{(у)}\}, \{P^{(в)}\}, \{R^{(с)}\}, \{P^{(с)}\}]$$

## Задачи синтеза

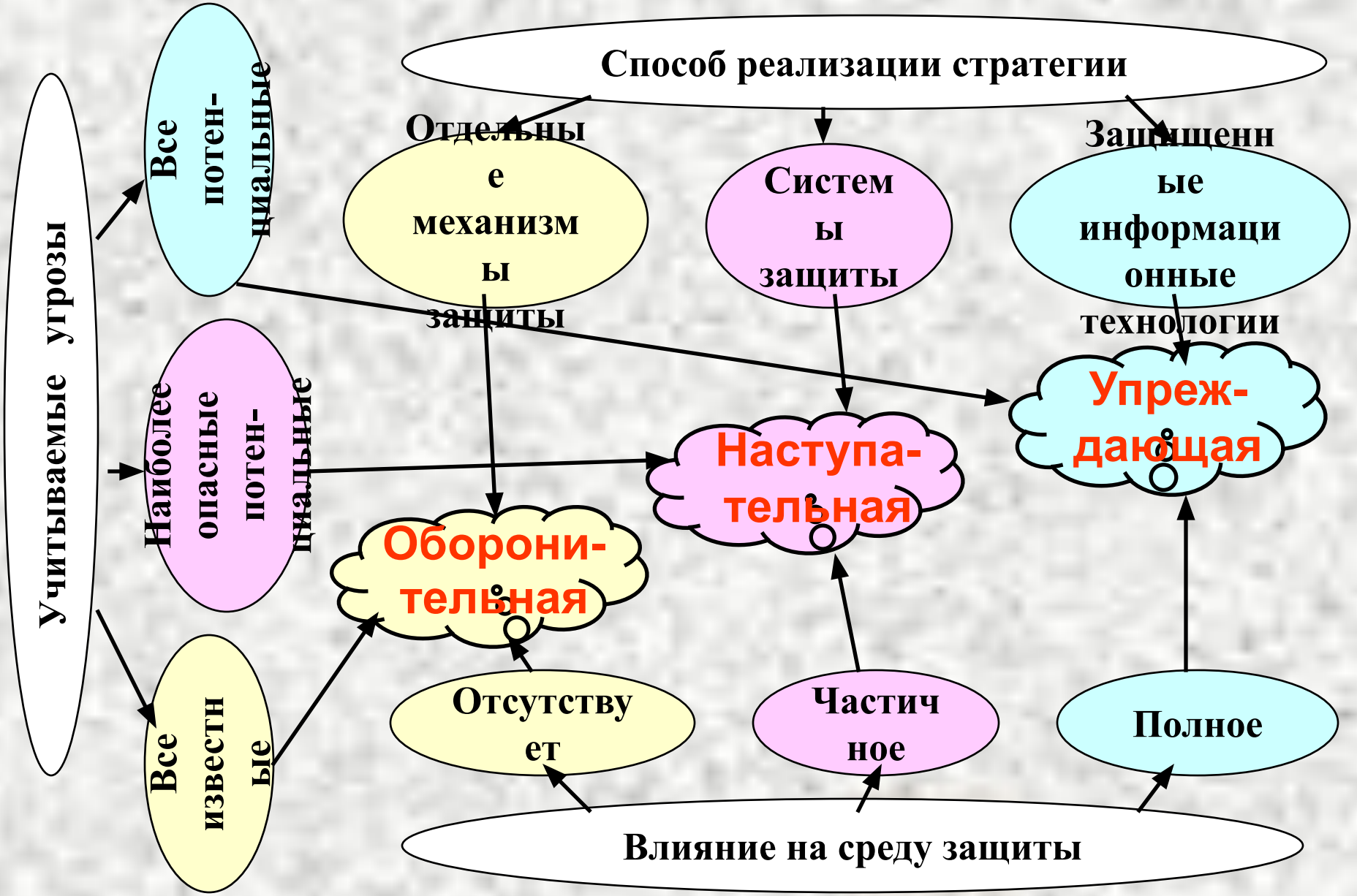
1. Найти такие $\{R^{(у)}\}$ и $\{R^{(в)}\}$, чтобы при заданных $\{R^{(с)}\}$ и $\{P^{(с)}\}$ $\{K\}$-> max.

   При этом $\{R^{(у)}\} + \{R^{(в)}\} \leq \{\overline{R^{(о)}}\}$, $\{\overline{R^{(о)}}\}$ - заданные ресурсы.

2. Выбрать такие $\{R^{(у)}\}$ и $\{R^{(в)}\}$, чтобы при заданных $\{R^{(с)}\}$ и $\{P^{(с)}\}$ условие $\{K\} \geq \{\overline{K}\}$ выполнялось при $\{R^{(о)}\} = \{R^{(у)}\} + \{R^{(в)}\}$ -> min.

   $\{\overline{K}\}$ - заданный уровень защищенности.

# Стратегии защиты информации



# Методология оценки уязвимости информации

# Системная классификация угроз

## Виды угроз

**Нарушение физической целостности**

**→ Уничтожение (искажение)**

**Нарушение логической структуры**

**→ Искажение структуры**

**Нарушение содержания**

**→ Несанкционированная модификация**

**Нарушение конфиденциальности**

**→ Несанкционированное получение**

**Нарушение права собственности**

**→ Присвоение чужого права**

# Системная классификация угроз

## Природа происхождения угроз

**Случайная** → **Отказы**

→ **Сбои**

→ **Ошибки**

→ **Стихийные бедствия**

→ **Побочные влияния**

**Преднамеренная** → **Злоумышленные действия людей**

# Системная классификация угроз

## Предпосылки появления угроз

**Объективные** → **Количественная недостаточность элементов системы**

→ **Качественная недостаточность элементов системы**

**Субъективные** → **Разведорганы иностранных государств**

→ **Промышленный шпионаж**

→ **Уголовные элементы**

→ **Недобросовестные сотрудники**

# Системная классификация угроз

## Источники угроз

**Люди** → **Посторонние лица**
→ **Пользователи**
→ **Персонал**

**Технические устройства** → **Регистрации**
→ **Передачи**
→ **Хранения**
→ **Переработки**
→ **Выдачи**

**Модели, алгоритмы, программы** → **Общего назначения**
→ **Прикладные**
→ **Вспомогательные**

**Технологические схемы обработки** → **Ручные**
→ **Интерактивные**
→ **Внутримашинные**
→ **Сетевые**

**Внешняя среда** → **Состояние атмосферы**
→ **Побочные шумы**
→ **Побочные сигналы**

# Содержание показателей уязвимости

| Вид защиты информации | Вид дестабилизирующего воздействия | |
|---|---|---|
| | Случайный | Злоумышленный |
| Предупреж-дение уничто-жения или искажения | Вероятность того, что под воздействием случайных факторов информация будет искажена или уничтожена. Математическое ожидание объема уничтоженной или искаженной информации. | Вероятность того, что злоумышленнику удастся уничтожить или исказить информацию. Математическое ожидание объема уничтоженной или искаженной информации. |

# Содержание показателей уязвимости

| Вид защиты информации | Вид дестабилизирующего воздействия | |
|---|---|---|
| | Случайный | Злоумышленный |
| Предупреждение несанкционированной модификации | Вероятность того, что под воздействием случайных факторов информация будет модифицирована при сохранении синтаксических характеристик. Математическое ожидание объема модифицированной информации. | Вероятность того, что злоумышленнику удастся модифицировать информацию при сохранении синтаксических характеристик. Математическое ожидание объема модифицированной информации. |

# Содержание показателей уязвимости

| Вид защиты информации | Вид дестабилизирующего воздействия | |
|---|---|---|
| | Случайный | Злоумышленный |
| Предупреждение несанкционированного получения | Вероятность того, что под воздействием случайных факторов защищаемая информация будет получена лицами или процессами, не имеющими на это полномочий. Математическое ожидание объема несанкционированно полученной информации. | Вероятность того, что злоумышленнику удастся получить ( похитить ) защищаемую информацию. Математическое ожидание объема похищаемой информации. |

# Содержание показателей уязвимости

| Вид защиты информации | Вид дестабилизирующего воздействия | |
|---|---|---|
| | Случайный | Злоумышленный |
| Предупреждение несанкционированного размножения (копирования) | Случайное несанкционированное размножение ( копирование) информации в корыстных целях является маловероятным. | Вероятность того, что злоумышленнику удастся несанкционированно снять копию с защищаемой информации без оставления следов злоумышленных действий. Математическое ожидание объема несанкционированно скопированной информации. Математическое ожидание числа несанкционированно снятых копий. |

# Классификация каналов несанкционированного получения информации (КНПИ)

**1 кл - проявляются безотносительно к обработке информации и без доступа злоумышленника к элементам АС**

**2 кл - проявляются в процессе обработки информации без доступа злоумышленника к элементам АС**

**3 кл - проявляются безотносительно к обработке информации с доступом злоумышленника к элементам АС, но без изменения последних**

**4 кл - проявляются в процессе обработки информации с доступом злоумышленника к элементам АС, но без изменения последних**

**5 кл - проявляются безотносительно к обработке информации с доступом злоумышленника к элементам АС с изменением последних**

**6 кл - проявляются в процессе обработки информации с доступом злоумышленника к элементам АС с изменением последних**

# Уязвимость информации

$$P_{ijkl} = P_{ikl}^{(д)} * P_{ijl}^{(к)} * P_{ijkl}^{(н)} * P_{ijl}^{(и)}$$

$P_{ijkl}$ – вероятность несанкционированного получения информации нарушителем k-й категории по j-ому КНПИ в l-ой зоне i-го структурного компонента АС;

$P_{ikl}^{(д)}$ – вероятность доступа нарушителя k-й категории в l-ую зону i-го компонента АС;

$P_{ijl}^{(к)}$ – вероятность наличия (проявления) j-ого КНПИ в l-ой зоне i-го компонента АС;

$P_{ijkl}^{(н)}$ – вероятность доступа нарушителя k-й категории к j-ому КНПИ в l-ой зоне i-го компонента АС при условии доступа нарушителя в зону;

$P_{ijl}^{(и)}$ – вероятность наличия защищаемой информации в j-ом КНПИ в l-ой зоне i-го компонента АС в момент доступа туда нарушителя.

## Базовый показатель уязвимости информации

$$P_{ijk}^{(б)} = 1 - \prod_{l=1}^{5} [1 - P_{ijkl}] = 1 - \prod_{l=1}^{5} [1 - P_{ikl}^{(д)} * P_{ijl}^{(к)} * P_{ijkl}^{(н)} * P_{ijl}^{(и)}]$$

# Классификация причин несанкционированного получения информации

| | |
|---|---|
| отказы | Основной аппаратуры; программ; людей; носителей информации; систем питания; систем обеспечения нормальных условий работы аппаратуры и персонала; систем передачи данных; вспомогательных материалов |
| сбои | Основной аппаратуры; программ; людей; носителей информации; систем питания; систем обеспечения нормальных условий работы аппаратуры и персонала; систем передачи данных; вспомогательных материалов |
| ошибки | Основной аппаратуры; программ; людей; систем передачи данных |
| стихийные бедствия | Пожар; наводнение; землетрясение; ураган; взрыв; авария |
| злоумышленные действия | Хищения; подмена; подключение; поломка (повреждение); диверсия |
| побочные влияния | Электромагнитные излучения устройств АС; паразитные наводки; внешние электромагнитные излучения; вибрация; внешние атмосферные явления |

# Методы определения требований к защите информации

# Методы определения требований к ЗИ

**Задачи:**

1. **Разработка методов оценки параметров защищаемой информации.**
2. **Формирование перечня и классификация факторов, влияющих на требуемый уровень защиты.**
3. **Структуризация возможных значений факторов.**
4. **Структуризация поля потенциально возможных вариантов условий защиты.**
5. **Оптимальное деление поля возможных вариантов на типовые классы.**
6. **Структурированное описание требований к защите в пределах выделенных классов.**

# Методы определения требований к ЗИ

**Оценка параметров защищаемой информации**

**Показатели, характеризующие информацию как обеспечивающий ресурс**

- **важность**
- **полнота**
- **адекватность**
- **релевантность**
- **толерантность**

**Показатели, характеризующие информацию как объект труда**

- **способ кодирования**
- **объем**

# Методы определения требований к ЗИ

## Классификация информации по важности

| Важность информации | | Относительно обработки | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| Относительно назначения | 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| | 2 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | 3 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| | 4 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| | 5 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| | 6 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| | 7 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| | 8 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| | 9 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |

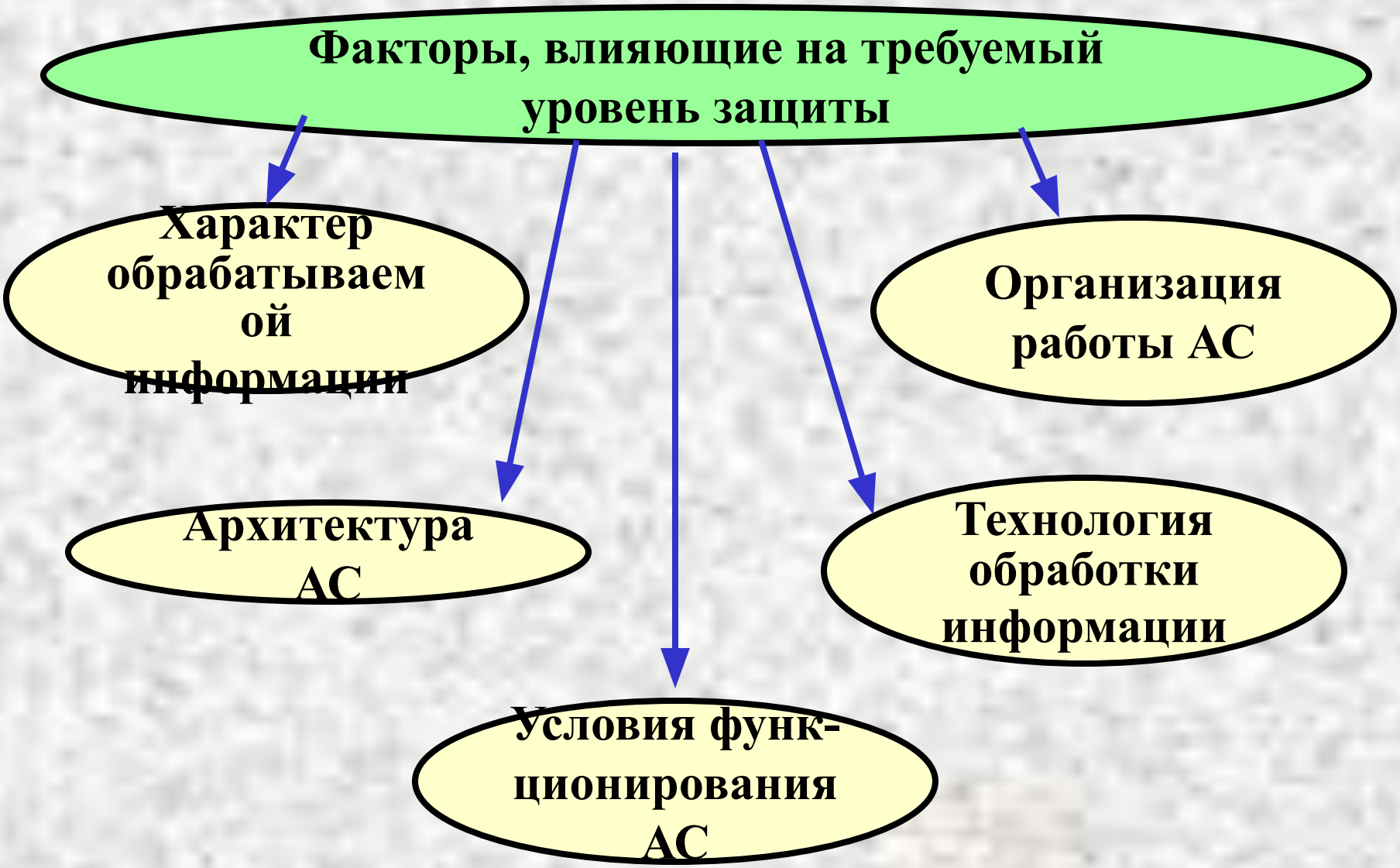
- Малая важность
- Обычная важность
- Полусредняя важность
- Средняя важность
- Повышенная важность
- Большая важность
- Чрезвычайная важность

# Методы определения требований к ЗИ

## Адекватность информации

| Тип характеристики | | | Качество определения значения характеристик | | |
|---|---|---|---|---|---|
| | | | хорошее | среднее | плохое |
| Измеряемая | Непосредственно | Количественно | 1 | 2 | 3 |
| | | Качественно | 2 | 3 | 4 |
| | Косвенно | Аналитически | 3 | 4 | 5 |
| | | Логически | 4 | 5 | 6 |
| Неизмеряемая | Имеющая аналоги | В данной среде | 5 | 6 | 7 |
| | | В схожей средей | 6 | 7 | 8 |
| | Не имеющая аналогов | Конкретного | 7 | 8 | 9 |
| | | Даже отдаленного | 8 | 9 | 10 |

# Методы определения требований к ЗИ



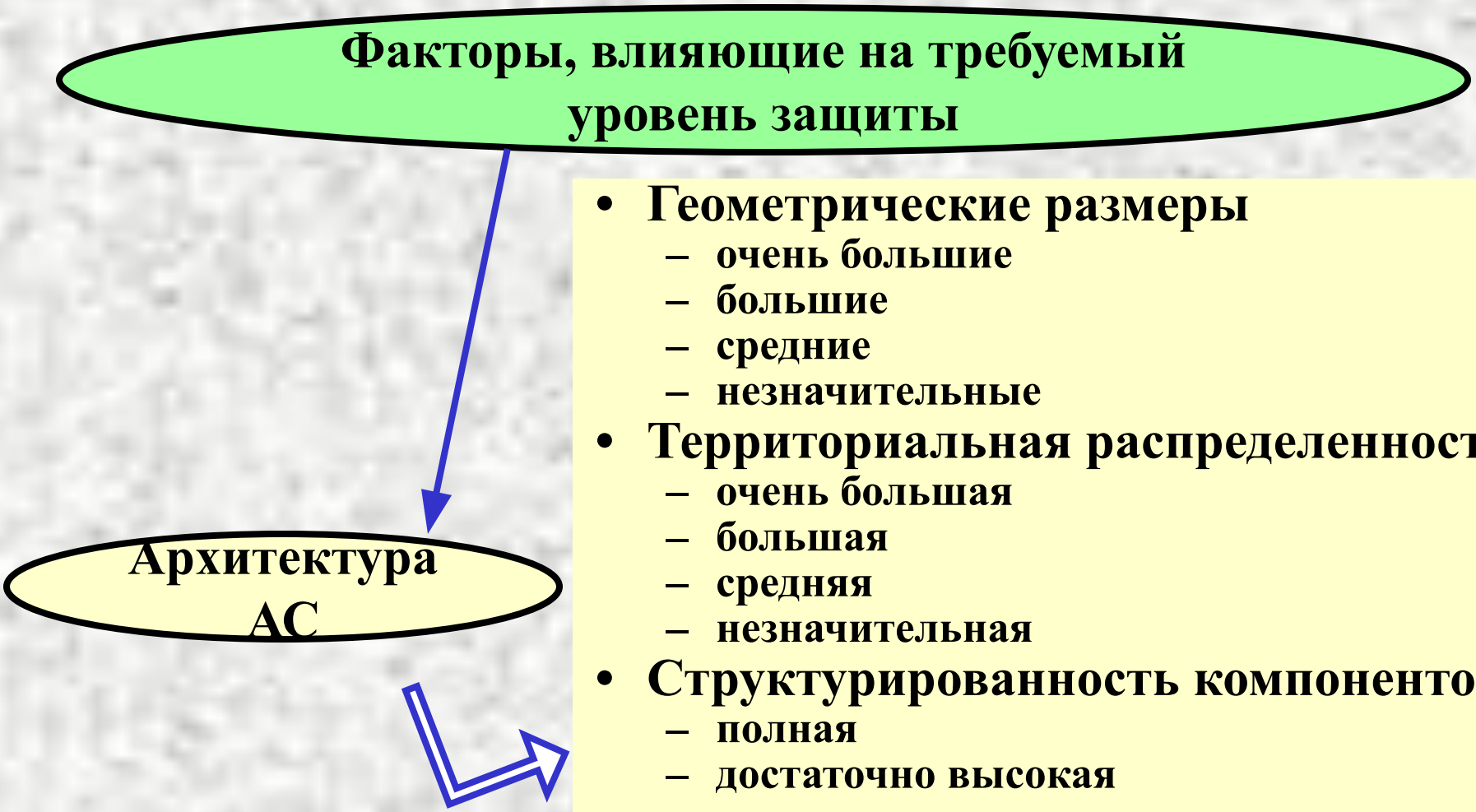
# Методы определения требований к ЗИ

**Факторы, влияющие на требуемый уровень защиты**

**Характер обрабатываемой информации**

- **Конфиденциальность**
  - **очень высокая**
  - **высокая**
  - **средняя**
  - **невысокая**
- **Объем**
  - **очень большой**
  - **большой**
  - **средний**
  - **малый**
- **Интенсивность обработки**
  - **очень высокая**
  - **высокая**
  - **средняя**
  - **низкая**

# Методы определения требований к ЗИ



# Методы определения требований к ЗИ

**Факторы, влияющие на требуемый уровень защиты**

**Условия функ-ционирования АС**

- **Расположение в населенном пункте**
  - **очень неудобное**
  - **создает значительные трудности для защиты**
  - **создает определенные трудности**
  - **хорошее**
- **Расположение на территории объекта**
  - **хаотично разбросанное**
  - **разбросанное**
  - **распределенное**
  - **компактное**
- **Обустроенность**
  - **очень плохая**
  - **плохая**
  - **средняя**
  - **хорошая**

# Методы определения требований к ЗИ

**Факторы, влияющие на требуемый уровень защиты**

**Технология обработки информации**

- **Масштаб обработки**
  - очень большой
  - большой
  - средний
  - незначительный
- **Стабильность информации**
  - регулярная
  - достаточно упорядоченная
  - частично стабильная
  - отсутствует
- **Доступность информации**
  - общедоступная
  - с незначительными ограничениями
  - с существенными ограничениями
  - с регулярным доступом
- **Структурированность информации**
  - полная
  - достаточно высокая
  - частичная
  - полностью отсутствует

# Методы определения требований к ЗИ

**Факторы, влияющие на требуемый уровень защиты**

**Организация работы АС**

- **Общая постановка дела**
  - **хорошая**
  - **средняя**
  - **слабая**
  - **очень плохая**
- **Укомплектованность кадрами**
  - **полная**
  - **средняя**
  - **слабая**
  - **очень слабая**
- **Уровень подготовки и воспитания кадров**
  - **высокий**
  - **средний**
  - **низкий**
  - **очень низкий**
- **Уровень дисциплины**
  - **высокий**
  - **средний**
  - **низкий**
  - **очень низкий**

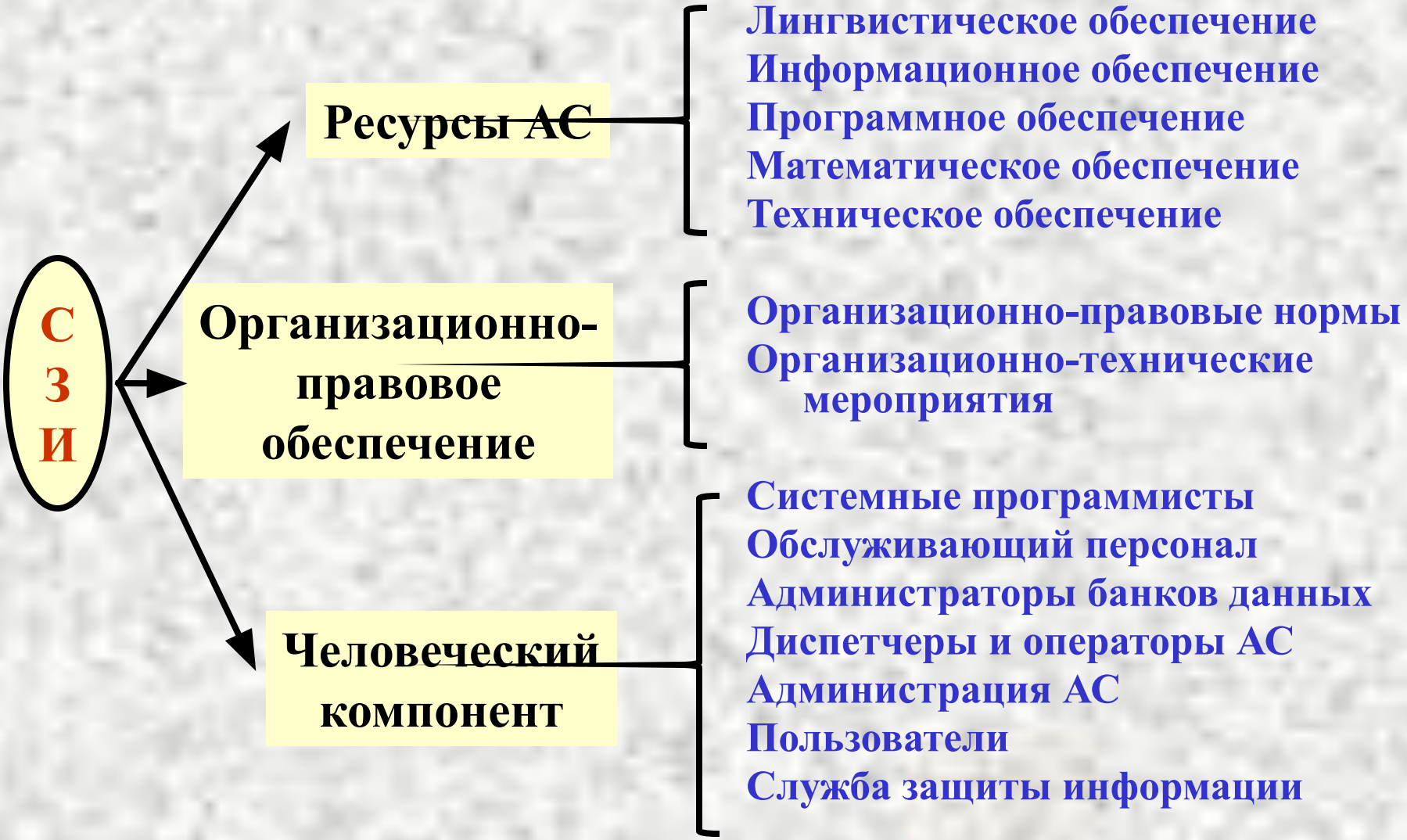
# Методы определения требований к ЗИ

## Классификационная структура типовых систем ЗИ

| Уровень защиты | Стратегии защиты | | |
|---|---|---|---|
| | оборонительная | наступательная | упреждающая |
| Слабый | 1 | | |
| Средний | 2 | 2 | |
| Сильный | 3 | 3 | 3 |
| Очень сильный | | 4 | 4 |
| Особый | | 5 | 5 |

# Система защиты информации

# Общая структурная схема системы защиты информации (СЗИ)



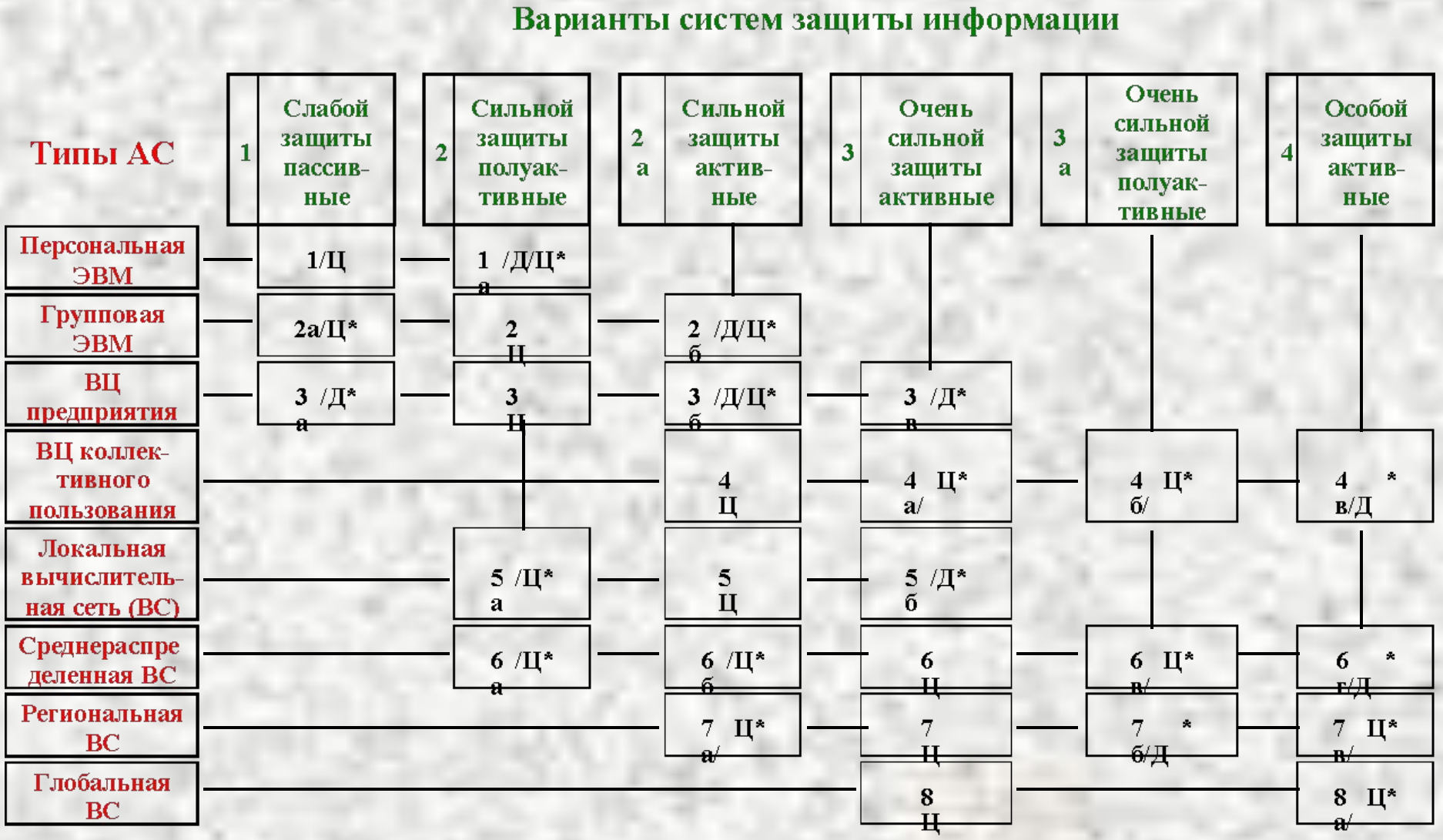
# Допустимые и целесообразные типы СЗИ для различных категорий

| Варианты СЗИ | | Тип СЗИ | | |
|---|---|---|---|---|
| | | Пассивные | Полуактивные | Активные |
| Категории СЗИ | Слабой защиты | Д<br>Ц [1] | Д<br>Ц* | Д<br>НЦ |
| | Сильной защиты | НД | Д<br>Ц [2] | Д<br>Ц* [2а] |
| | Очень сильной защиты | НД | Д*<br>Ц* [3а] | Д<br>Ц$^{О*}$ [3] |
| | Особой защиты | НД | НД | О [4] |

О - обязательно  Ц - целесообразно  Д - допустимо  НД - недопустимо

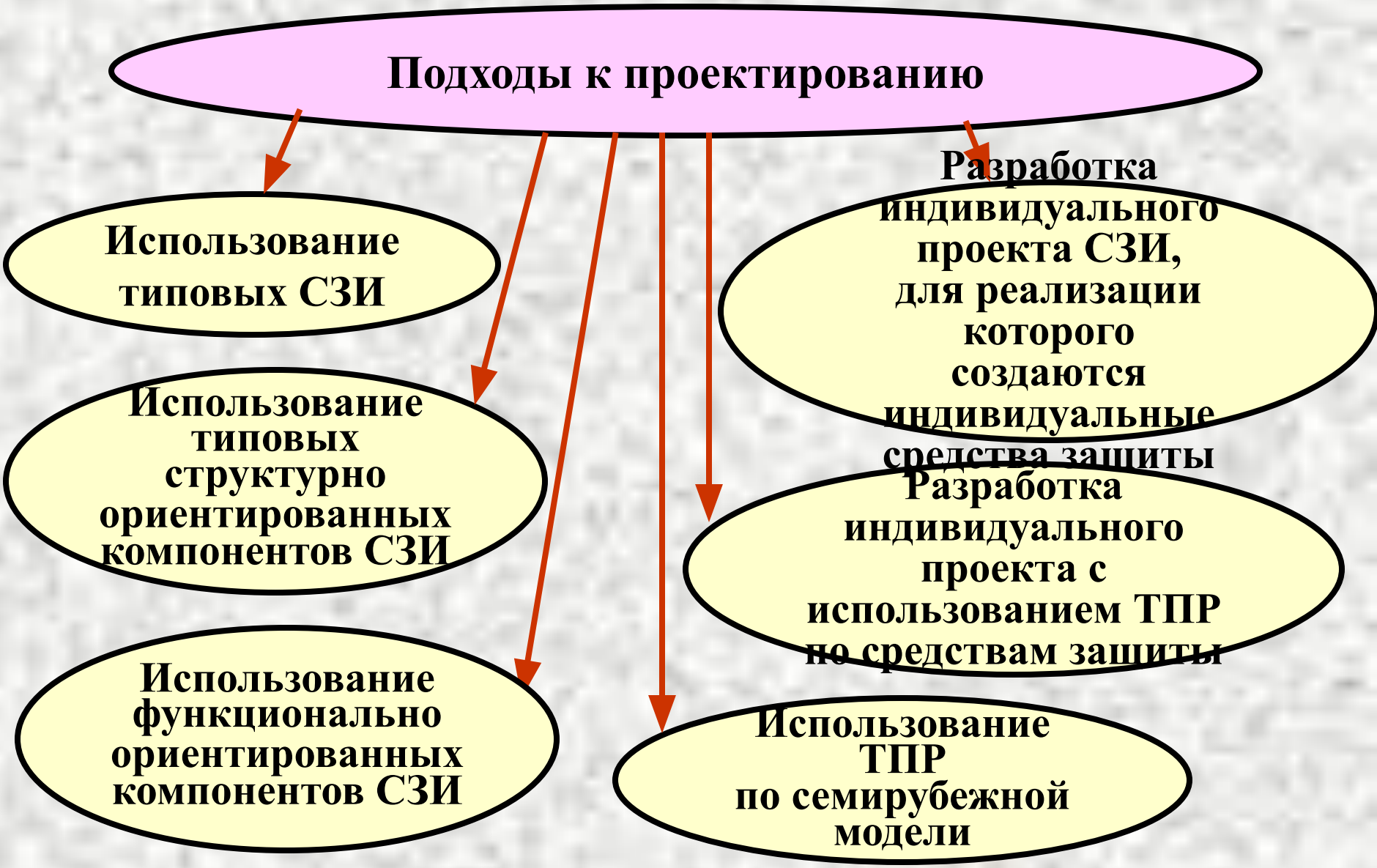
* -

# Итоговая классификация СЗИ



# Проектирование систем защиты информации

# Проектирование СЗИ



# Проектирование СЗИ

**Подходы к проектированию**

**Использование типовых СЗИ**

**Выбирается один из имеющихся типовых проектов полной СЗИ. Осуществляется привязка типового проекта к условиям конкретной АС.**

**Целесообразно применять, когда**

**1. Требования к ЗИ не очень высокие.**
**2. Строго определенная структура АС.**
**3. Архитектура АС близка к одной из типовых.**
**4. Требования и условия защиты во всех однотипных ТСК однородны.**

# Проектирование СЗИ

**Подходы к проектированию**

**Использование типовых структурно ориентированных компонентов СЗИ**

**Для каждого ТСК АС выбирается один из типовых проектов компонента СЗИ. Осуществляется привязка проектов к условиям ТСК. Производится объединение всех компонентов в СЗИ.**

**Целесообразно применять, когда**

**1. Требования к ЗИ не очень высокие.**
**2. Строго определенная структура АС.**
**3. Архитектура АС близка к одной из типовых.**
**4. Требования и/или условия защиты в различных ТСК различны.**

# Проектирование СЗИ

**Подходы к проектированию**

**Использование функционально ориентированных компонентов СЗИ**

**Для каждой группы компонентов АС выбираются по одному из типовых функционально ориентированных компонентов СЗИ. Осуществляется привязка проектов к условиям группы. Производится объединение компонентов в подсистему СЗИ. Все подсистемы объединяются в СЗИ.**

**Целесообразно применять, когда**

**1. Требования к ЗИ не очень высокие.**
**2. В АС выделяются компактно расположенные компоненты.**
**3. Требования и условия защиты в различных частях АС различны.**

# Проектирование СЗИ

**Подходы к проектированию**

**Использование ТПР по семирубежной модели**

**На плане территориального размещения АС намечаются рубежи защиты. Для каждого рубежа выбирается один из типовых проектов подсистемы СЗИ. Осуществляется привязка проектов к условиям каждого реального рубежа. Все подсистемы объединяются в СЗИ.**

**Целесообразно применять, когда**

**1. Требования к ЗИ не слишком высокие.**
**2. Компоненты АС распределены на значительной территории.**
**3. АС имеет сетевую структуру.**
**4. Требования и условия защиты в различных компонентах АС различны.**

# Проектирование СЗИ

**Подходы к проектированию**

**Разработка индивидуального проекта с использованием ТПР по средствам защиты**

**Разрабатывается проект индивидуальной СЗИ, для реализации которого используются ТПР по основным средствам защиты.**

**<u>Целесообразно применять, когда</u>**
**1. Требования к ЗИ очень высокие.**
**2. АС имеет ярко выраженные особенности.**

# Проектирование СЗИ

**Подходы к проектированию**

**Разработка индивидуального проекта СЗИ, для реализации которого создаются индивидуальные средства защиты**

**Разрабатывается проект индивидуальной СЗИ. Разрабатываются средства для реализации проекта. Осуществляется наладка СЗИ.**

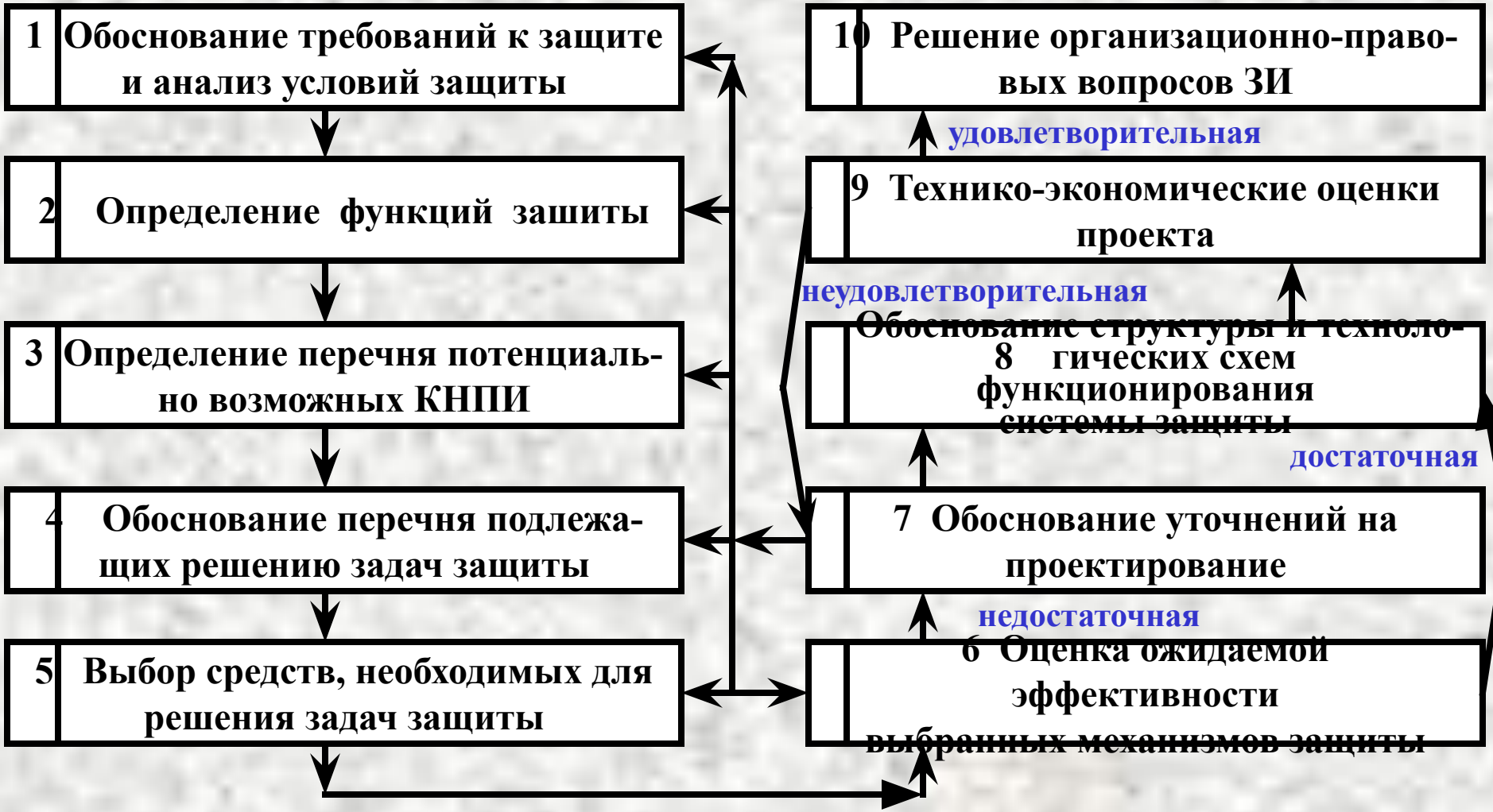
**Целесообразно применять, когда**

**1. Требования к ЗИ очень высокие.**

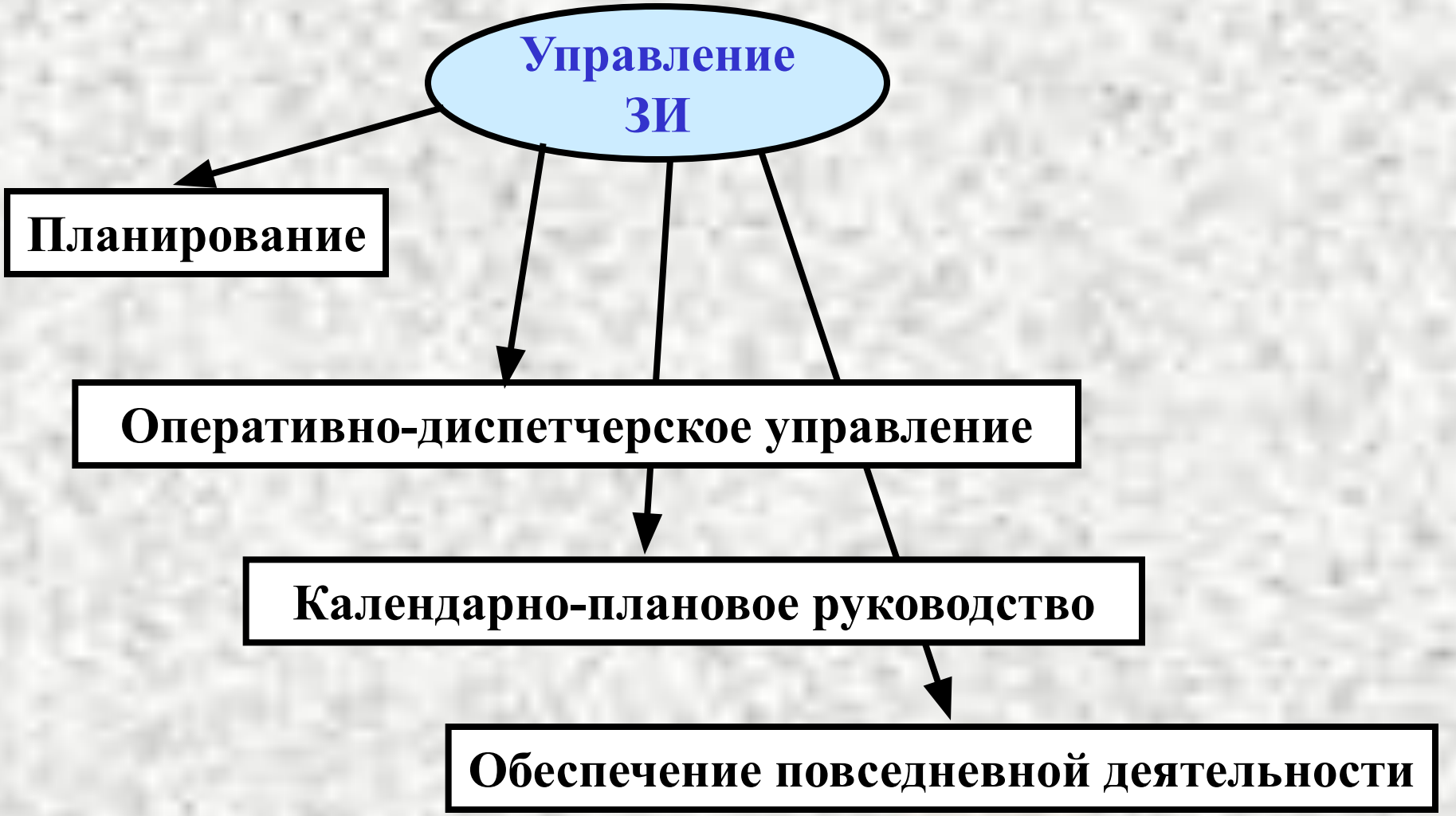
**2. Защищаемая информация имеет особую важность.**

**3. АС является уникальной.**

# Проектирование СЗИ
# Последовательность и содержание проектирования



# Проектирование СЗИ



# Проектирование СЗИ
# Управление ЗИ

**Планирование**

**Краткосрочное:**

**Анализ планов обработки информации; анализ условий ЗИ; оценка уязвимости информации в процессе функционирования АС; определение потребностей в средствах защиты (СЗ); оценка потенциальных возможностей механизмов зашиты; распределение СЗ; формирование графика использования СЗ; оценка ожидаемой эффективности использования СЗ.**

**Среднесрочное:**

**Анализ выполнения работ в АС; прогнозирование условий ЗИ; определение требований к ЗИ; анализ СЗ и ресурсов защиты, которые могут быть использованы; определение заданий на ЗИ в ближайший интервал; ориентировочное определение заданий на ЗИ в последующие интервалы; распределение СЗ и ресурсов защиты.**

**Долгосрочное:**

**Анализ ожидаемых структур и технологических схем функционирования АС; анализ ожидаемого функционального использования АС; ориентировочное определение требований к ЗИ; оценка ожидаемых ресурсов защиты; оценка ожидаемого арсенала СЗИ; обоснование структуры и технологии функционирования СЗИ; разработка и уточнение программ развития СЗ и порядка их использования; оценка ожидаемой эффективности защиты.**

# Проектирование СЗИ
## Управление ЗИ

**Краткосрочное**:

**Оперативно-диспетчерское управление** → **Регулярное использование СЗ; сбор, обработка и регистрация оперативной информации; распознавание сложившейся ситуации; принятие решений на вмешательство в функционирование СЗИ; реализация принятых решений; анализ и прогнозирование развития ситуации; разработка предложений по корректировке планов защиты.**

# Проектирование СЗИ
# Управление ЗИ

**Календарно-плановое руководство**

**Краткосрочное:**

**Текущая оценка состояния ЗИ; оценка требований к защите, определяемых нерегламентированными задачами; оценка влияния на защиту изменения условий функционирования АС; корректировка текущих планов защиты; разработка предложений по совершенствованию планирования защиты.**

**Среднесрочное:**

**Анализ соответствия фактического и требуемого уровней защиты; анализ изменения требований к защите; анализ изменения условий функционирования АС; корректировка среднесрочных планов защиты; разработка предложений по совершенствованию механизмов и развитию СЗ.**

**Долгосрочное:**

**Анализ уровня обеспечения ЗИ; анализ качества функционирования механизмов защиты; анализ ожидаемых изменений в функциональном использовании АС; анализ ожидаемых изменений условий функционирования АС; разработка предложений по совершенствованию структуры и технологии функционирования АС; организация разработки, производства и внедрения СЗ; совершенствование механизмов защиты.**

# Проектирование СЗИ
# Управление ЗИ

**Обеспечение повседневной деятельности**

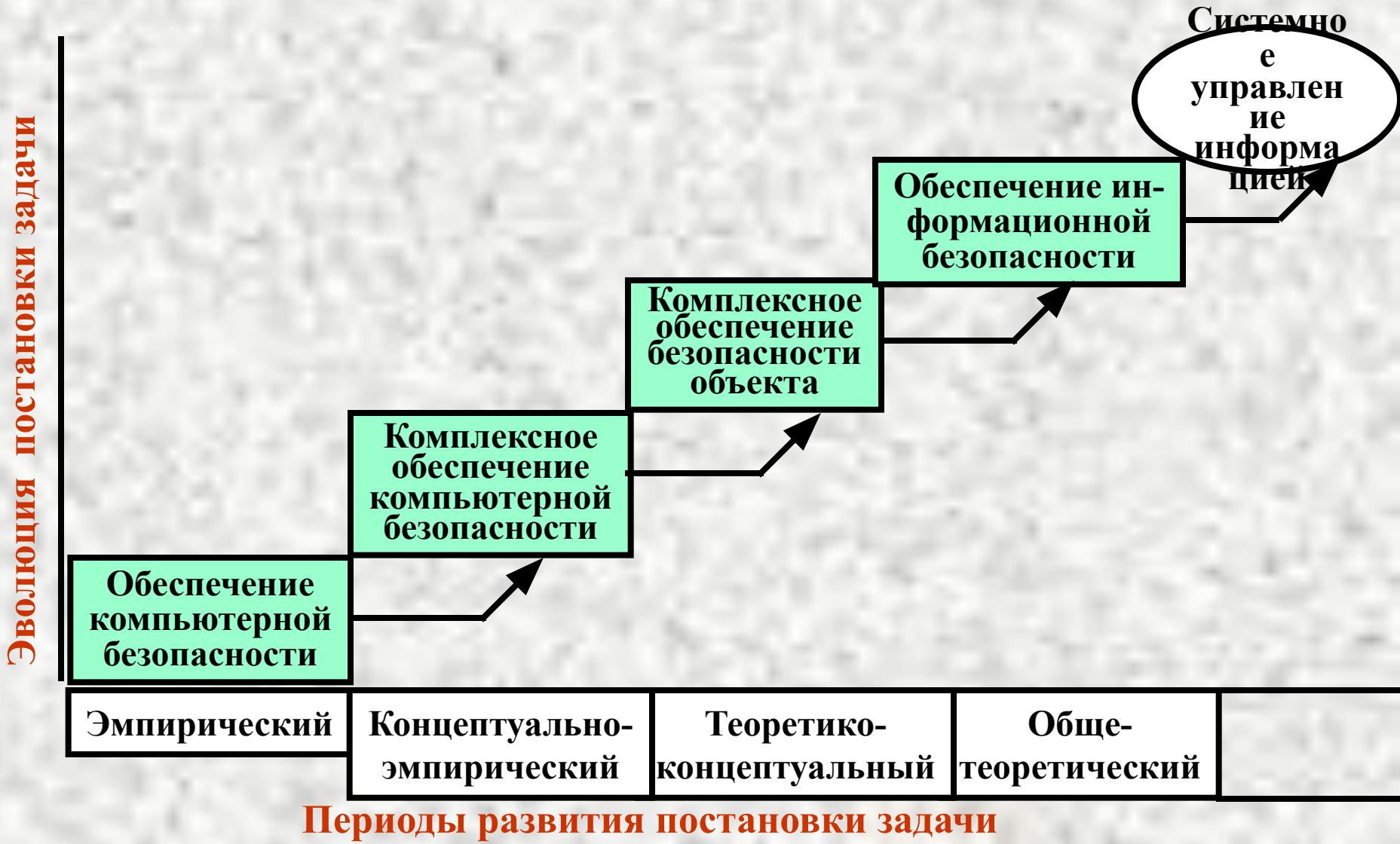
**Краткосрочное**:

**Сбор дополнительной информации; базовая обработка информации и формирование исходных данных; выдача информации.**

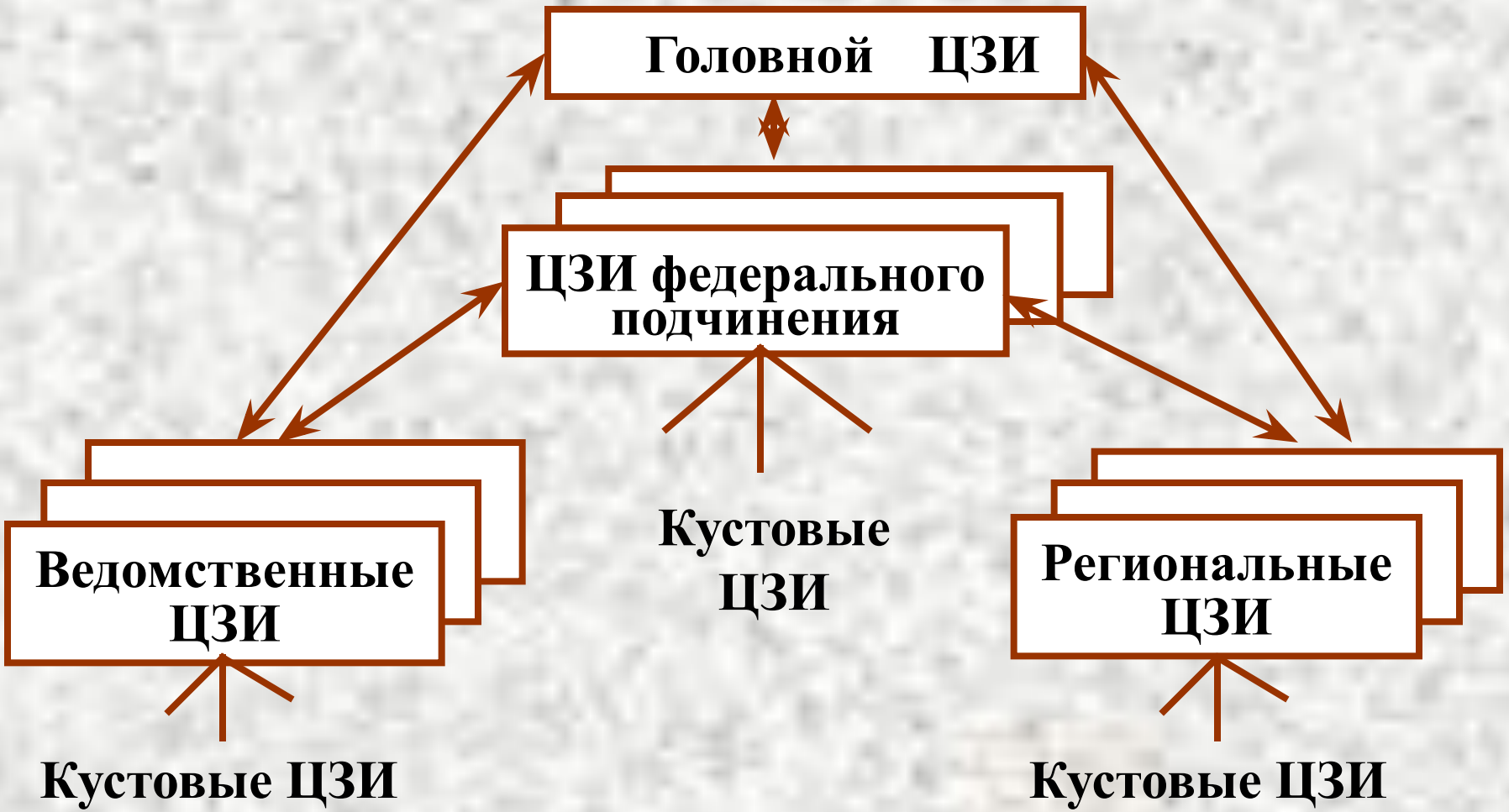
**Среднесрочное**:

**Аналитико-синтетическая обработка данных; формирование массива регламентных данных; выдача информации.**

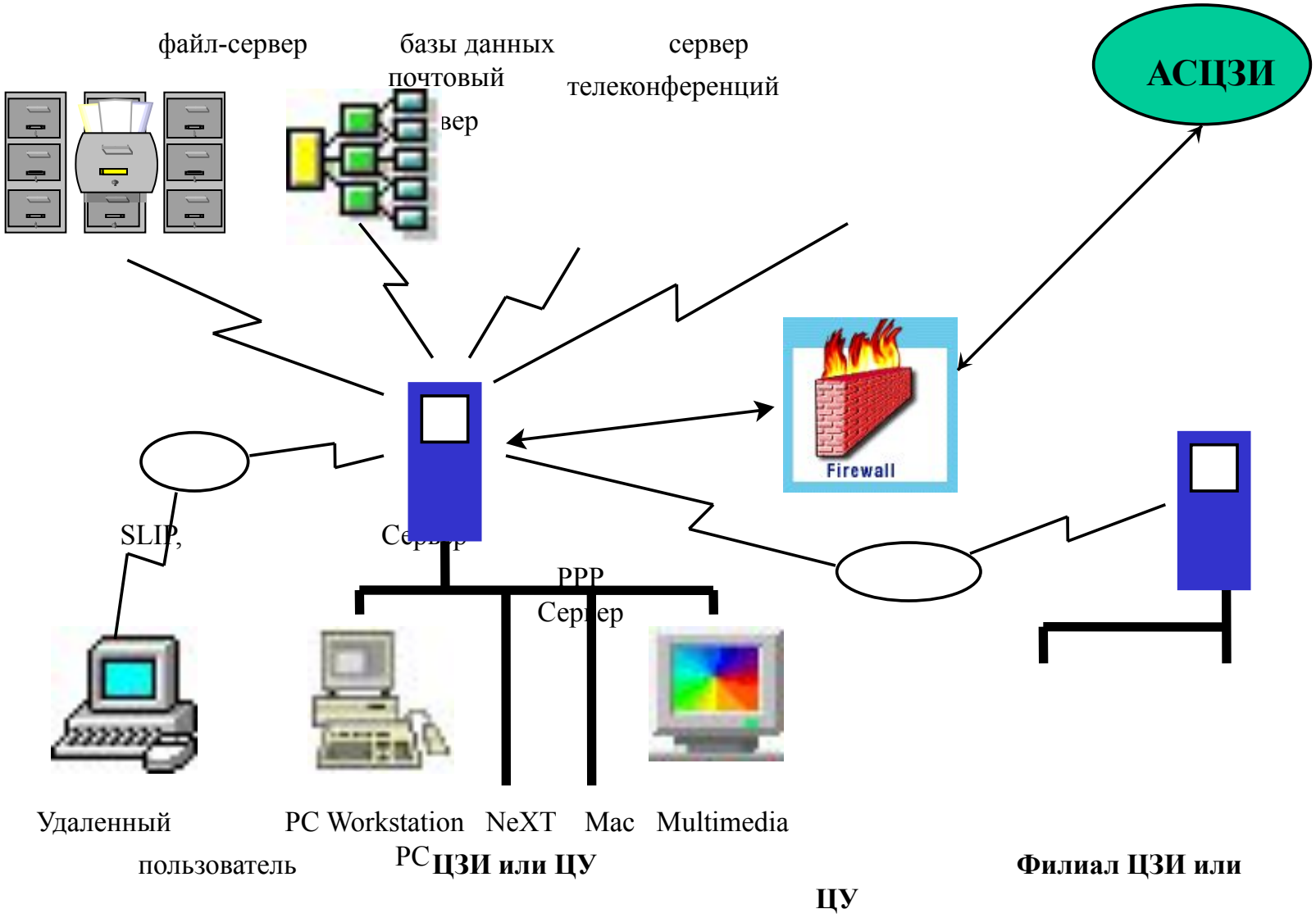
# Перспективы развития теории и практики защиты информации



# Центры защиты информации (ЦЗИ)



# Автоматизированная система ЦЗИ



# Региональные учебно-научные центры информационной безопасности в системе высшей школы

**Головной центр - Московский инженерно-физический институт (государственный университет)**

**Центральный федеральный округ**

**Московский государственный технический университет (ТУ)**

**Российский государственный гуманитарный университет**

**Московский государственный авиационный институт (ТУ)**

**Московский государственный институт электроники и математики (ТУ)**

**Рязанская государственная радиотехническая академия**

**Воронежский государственный ТУ**

**Дальневосточный федеральный округ**

**Дальневосточный ГУ**

**Приволжский федеральный округ**

**Казанский государственный ТУ**

**Нижегородский государственный ТУ**

**Северо-Западный федеральный округ**

**Санкт-Петербургский государственный ТУ**

**Сыктывкарский ГУ**

**Южный федеральный округ**

**Волгоградский государственный ТУ**

**Кубанский государственный университет**

**Таганрогский государственный радиотехнический университет**

**Уральский федеральный округ**

**Южно-Уральский государственный университет**

**Сибирский федеральный округ**

**Красноярский государственный ТУ**

**Новосибирский государственный ТУ**

**Омский государственный ТУ**

**Томский государственный университет систем управления и радиоэлектроники**

# Основные научные результаты

# Основные научные результаты

1. **Обоснована современная постановка задачи защиты информации, суть которой состоит в переходе от экстенсивных к интенсивным методам решения проблем, базирующимся на целенаправленной реализации всех достижений теории и практики защиты - структурированном описании среды защиты, всестороннем количественном анализе степени уязвимости информации на объекте, научно обоснованном определении требуемого уровня защиты на каждом конкретном объекте и в конкретных условиях его функционирования, построении оптимальных систем защиты на основе единой унифицированной методологии.**

# Основные научные результаты

2. **Как основа интенсификации решения проблем защиты сформирован научно-методологический базис научного направления - теории защиты информации, использующий достижения методов нечетких множеств, лингвистических переменных, неформального оценивания, неформального поиска оптимальных решений. Проведена системная классификация моделей защиты информации и предложена обобщенная модель систем и процессов защиты. Структурирован процесс создания оптимальных систем защиты информации в виде кортежа концептуальных решений, составляющих существо развитой унифицированной концепции защиты информации.**

# Основные научные результаты

3. На основе неформально-эвристических методов предложены подходы и разработаны системные классификации угроз информации, потенциально возможных условий защиты, основных типов архитектурного построения систем защиты, позволяющие осуществить масштабную стандартизацию систем и процессов защиты информации, что является чрезвычайно важным с прагматической точки зрения, так как дает возможность получать решения, близкие к оптимальным, в условиях существенно ограниченных ресурсов.

# Основные научные результаты

4. Определены наиболее вероятные перспективы дальнейшего развития теории и практики защиты информации, связанные с совершенствованием теоретических основ защиты, практической реализацией идеи интенсификации защиты информации и переводом ее на индустриальную основу, а также с постепенной трансформацией задачи защиты информации в задачу обеспечения информационной безопасности объектов, регионов и государства в целом.