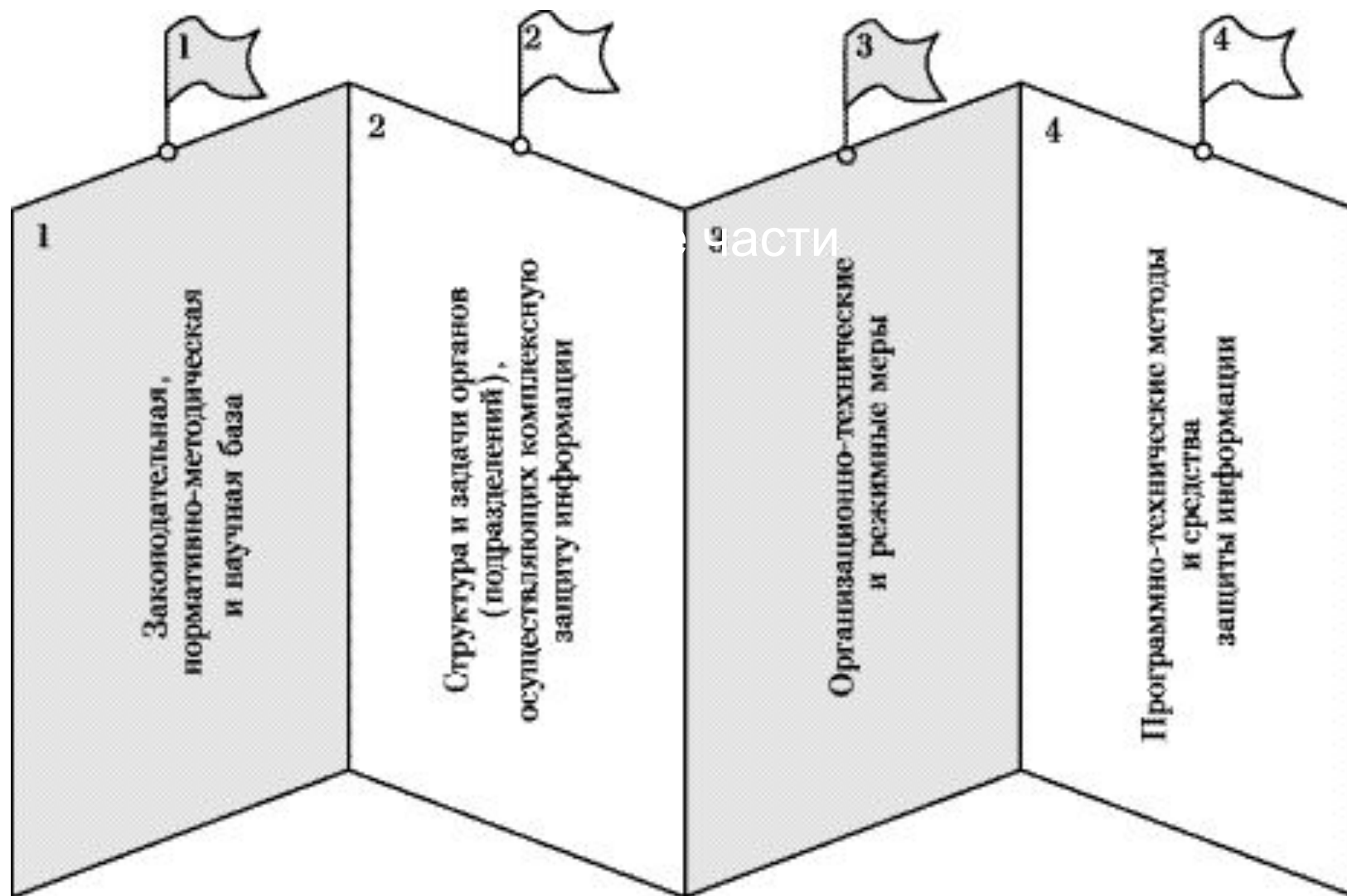


ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

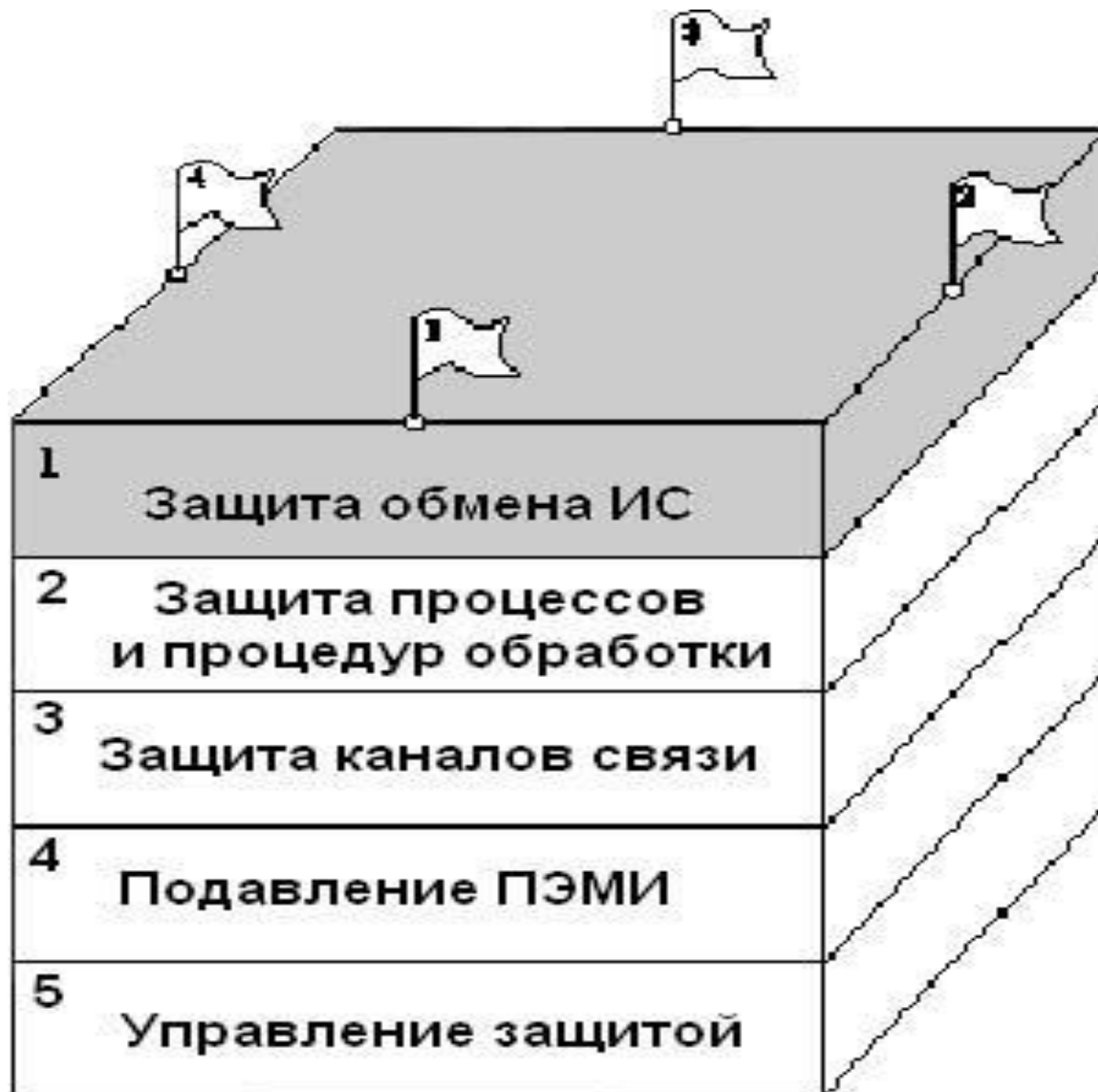
Рекомендуемая литература

1. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации: Учебное пособие. – М.: ИНФРА М_РИОР, 2014. – 265 с.
2. Баранова Е.К., Бабаш А.В. Моделирование системы защиты информации. Практикум. - М.: ИНФРА М_РИОР, 2015. – 190 с.
3. Завгородний В.И. Комплексная защита в компьютерных системах: Учебное пособие. – М.: Логос; ПБОЮЛ Н.А.Егоров, 2001. - 264 с.
4. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб.пособие для вузов – М.: Горячая линия – Телеком, 2004. - 280 с.
5. Мельников В.В. Безопасность информации в автоматизированных системах. – М.: Финансы и статистика, 2003. – 368 с.
6. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия.- СПб: БХВ-Петербург, 2002.
7. Соколов А.В., Степанюк О.М. Методы информационной защиты объектов и компьютерных сетей. - М.: ООО "Фирма "Издательство АСТ"; СПб: ООО "Издательство "Полигон", 2000. – 272 с.
8. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия. – М.: "Дашков и К", 2006. - 234 с.
9. Шумский А.А. Системный анализ в защите информации: учеб.пособие для студентов вузов, обучающихся по специальностям в обл.информ.безопасности / А.А.Шумский, А.А. Шелупанов – М.: Гелиос АРВ, 2005.- 224 с.

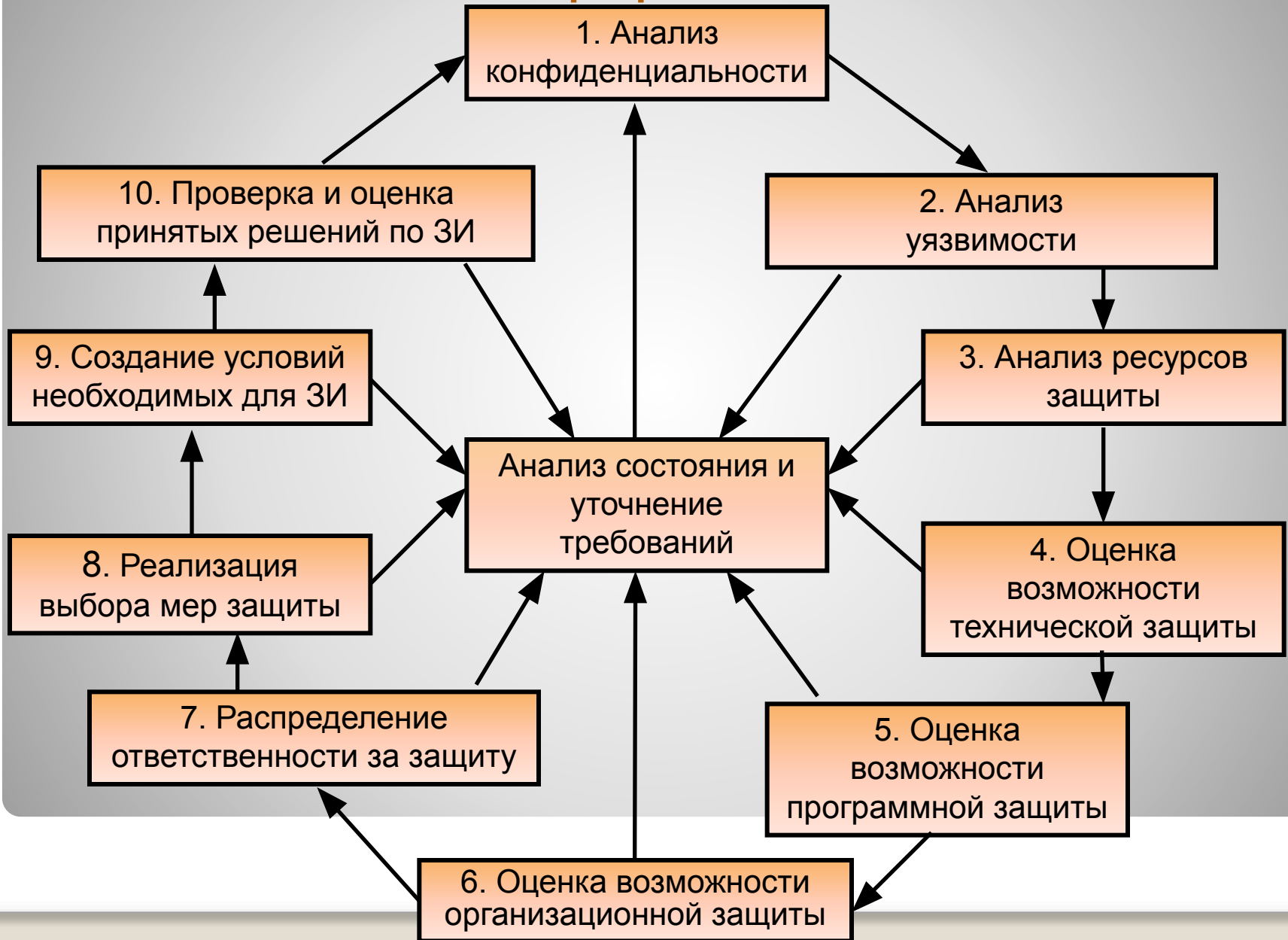
Организация системы защиты информации



Основные направления в общей проблеме обеспечения безопасности



Этапы разработки СЗИ





Параллельная разработка ИС и СЗИ

**Системный подход к построению
защищенных ИС**

Многоуровневая структура СЗИ

**Иерархическая система управления
СЗИ**

**Блочная архитектура защищенных
ИС**

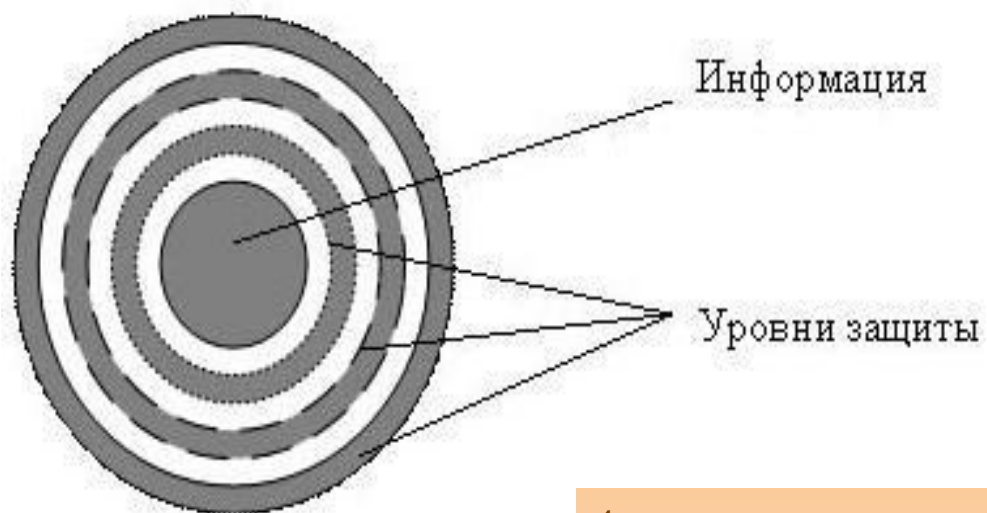
Возможность развития СЗИ

**Дружественный интерфейс
пользователя**

Концепция создания защищенных ИС

Многоуровневая структура СЗИ

Для отдельного объекта можно выделить
6-7 уровней (рубежей) защиты:



1. охрана по периметру территории объекта;
2. охрана по периметру здания;
3. охрана помещения;
4. защита аппаратных средств;
5. защита программных средств;
6. защита информации.

1. Регламентация
действий
пользователей

2. Установление
юридической
ответственности за
выполнение правил ИБ

3. Явный и скрытый
контроль за порядком
информационного
обмена

4. Блокирование
каналов утечки
информации

5. Выявление
закладных устройств в
ТС и ПО

6. Непрерывный
контроль и управление
СЗИ

7. Обнаружение
зондирований,
навязываний ложной
информации
и излучений

8. Санкционированный
доступ в физическое и
информационное
пространство

9. Обнаружение
возгораний,
затоплений и иных ЧС

10. Обеспечение
резервирования
информации

11. Организация
оборота физических
носителей
защищаемой
информации

12. Обеспечение
достоверности
электронного
документооборота,
ЭЦП

13. Шифрование
информации на любых
этапах
обработки

14. Восстановление
ключевых структур
при компрометации

15. Генерация,
распределение и
хранение ключей
и паролей

16. Регистрация
событий и обнаружение
нарушений

17. Расследование во
взаимодействии с ПОО
нарушений политики
безопасности

Сущность и задачи ОУСЗИ

Стратегии организации защиты информации

Стратегия – общая направленность в организации деятельности с учетом объективных потребностей, возможных условий осуществления и возможностей предприятия.

Виды стратегий

Оборонительная

защита от уже известных угроз, осуществляемая автономно, без влияния на существующую ИС

Наступательная

защита от всего множества потенциальных угроз

Упреждающая

создание информационной среды, в которой угрозы не имеют условий для возникновения

Основные характеристики стратегий организации защиты информации

Наименование характеристики	Стратегии комплексной защиты информации		
	Оборонительная	Наступательная	Упреждающая
Возможный уровень защиты	Достаточно высок, но только в отношении известных угроз	Очень высок, но только в пределах существующих представлений о природе угроз и возможностях их проявления	Уровень защиты гарантированно очень высок
Необходимые условия реализации	Наличие методов и средств реализации	1. Наличие перечня и характеристик полного множества потенциально возможных угроз 2. Развитый арсенал методов и средств защиты 3. Возможность влиять на архитектуру ИС и технологию обработки информации	Наличие защищенных информационных технологий
Ресурсоемкость	Незначительная по сравнению с другими стратегиями	Значительная (с ростом требований по защите растет по экспоненте)	1. Высокая в плане капитальных затрат 2. Незначительная в каждом конкретном случае при наличии унифицированной защищенной ИТ
Рекомендации по применению	Невысокая степень секретности защищаемой информации и не очень большие ожидаемые потери	Достаточно высокая степень секретности защищаемой информации и возможность значительных потерь при нарушении защиты	Перспективная

Этапы построения СЗИ для различных стратегий

Наименование этапов построения	Стратегии комплексной защиты информации		
	Оборонительная	Наступательная	Упреждающая
Формирование среды защиты		1. Структурированная архитектура ИС 2. Структурированная технология обработки ЗИ 3. Четкая организация работ по защите	Защищенная информационная технология в унифицированном исполнении
Анализ средств защиты	1. Представление организационной структуры ИС в виде графа, узлы – типовые структурные компоненты, а дуги – взаимосвязи между компонентами 2. Представление технологии обработки ЗИ в виде строго определенной схемы 3. Определение параметров ЗИ и условий ее обработки		
Оценка уязвимости информации	1. Определение значений вероятности нарушения защиты информации в условиях ее обработки 2. Оценка размеров возможного ущерба при нарушении защиты		
Определение требований к защите	Определение вероятности нарушения защиты информации, которая должна быть обеспечена при обработке защищаемой информации		
Построение системы комплексной защиты	Определение технических средств, которые должны быть использованы при обработке ЗИ	Выбор типового варианта или проектирование индивидуальной системы КЗИ	Определение механизмов защиты, которые должны быть задействованы при создании КЗИ
Требования к среде защиты		Определяется в зависимости от требований к защите информации	Реализуется на базе унифицированной защищенной ИТ

Простота механизма
защиты

Постоянство защиты

Полнота контроля

Открытость
проектирования

Идентификация

Разделение полномочий

Минимизация
полномочий

Надежность

Максимальная
обособленность

Защита памяти

Непрерывность

Гибкость

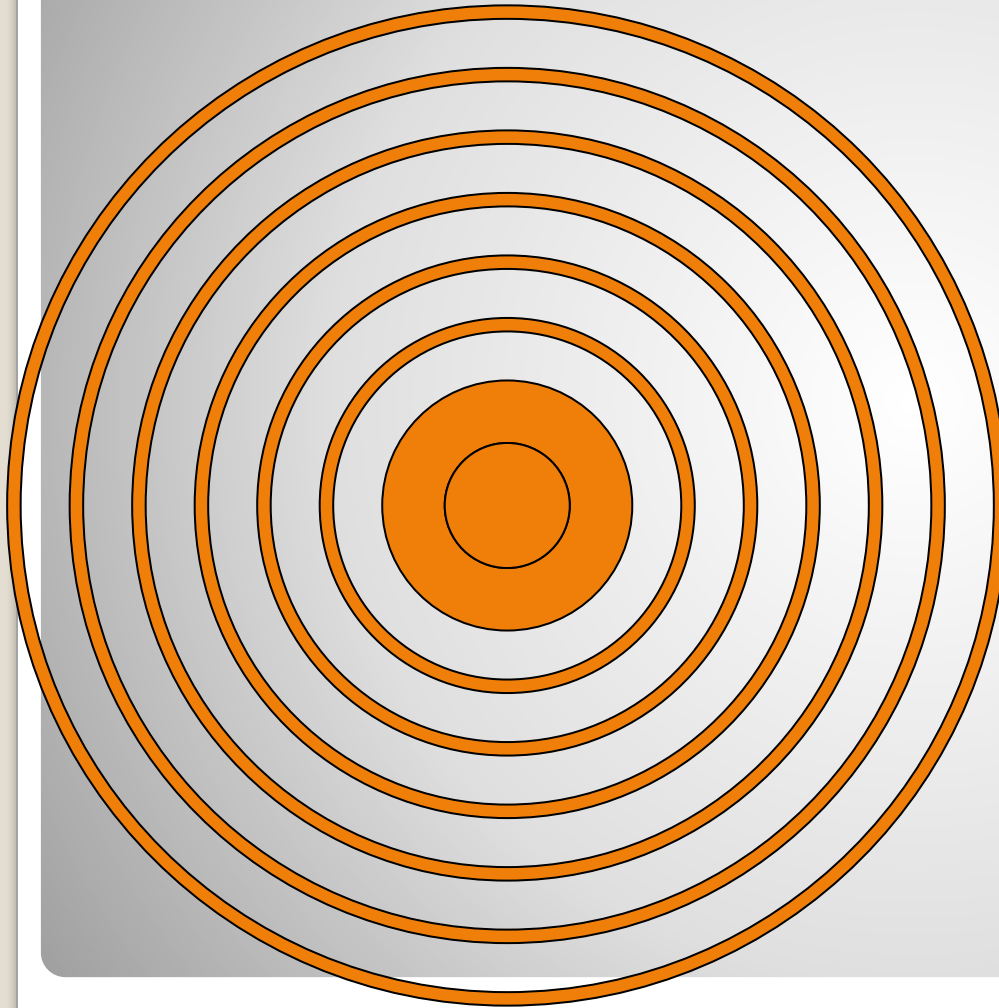
Неизбежность
наказания нарушений

Экономичность

Специализированность

Общие принципы построения КЗИ

Структура КЗИ



~~Инфо~~

~~Диаг~~

~~Воспи~~

~~Проф~~

~~Ранни~~

~~Охра~~

~~Техн~~

Инже

нерн

ые

соору

жени

я

Основные характеристики КЗИ

- **Надежность**
эшелонированность, многоуровневость
- **Отказоустойчивость**
минимизация последствий отказов рубежей защиты
- **Равнопрочность**
нарушитель должен преодолевать рубежи защиты с одинаковой трудностью, независимо от направления атаки

Этапы разработки КЗИ

I. Определение информации, подлежащей защите

II. Выявление полного множества угроз и критериев утечки информации

III. Проведение оценки уязвимости и рисков информации по имеющимся угрозам и каналам утечки

IV. Определение требований к комплексной защите

V. Осуществление выбора средств защиты информации и их характеристик

VI. Внедрение и организация использования выбранных мер, способов и средств защиты

VII. Осуществление контроля целостности и управление системой защиты

Постоянный анализ и уточнение требований к КЗИ

Правовые

Организационные

Инженерно-
технические

Программно-
аппаратные

Криптографические

Обязательные элементы КЗИ

Контрольные вопросы

1. Основные направления обеспечения информационной безопасности на предприятии
2. Этапы и общие принципы разработки СЗИ на предприятии.
3. Многоуровневая структура СЗИ на предприятии.
4. Сущность и задачи ОУСЗИ
5. Стратегии организации защиты информации на предприятии.
6. Этапы разработки комплексной системы защиты информации на предприятии.

Организация защиты конфиденциальных документов

Безопасность ценных информационных ресурсов

Цель ИБ – безопасность информационных ресурсов
в любой момент времени
в любой обстановке.

Первоначально всегда необходимо решить
следующие вопросы:

*Что защищать?
Почему защищать?
От кого защищать?
Как защищать?*

Главные опасности:

- утрата конфиденциального документа;
- разглашение конфиденциальных сведений;
- утечка по техническим каналам.

В настоящее время главные опасности:

- незаконные тайные операции с электронными документами без кражи из БД;
- незаконное использование информационных ресурсов для извлечения материальной выгоды.



The diagram features a large orange triangle on a gray background. Three white rounded rectangular boxes with orange borders are positioned to the right of the triangle, each containing text. The boxes are stacked vertically, corresponding to the top, middle, and bottom sections of the triangle.

**Электронные информационные
системы**

**Весь комплекс управления
предприятием
в единстве его функциональных и
структурных систем**

**Традиционные документационные
процессы**

Архитектура СЗИ

Управление
предприятием

Прогнозирование и
планирование

Финансовая
деятельность

Производственная
деятельность

Торговая
деятельность

Переговоры и
совещания по
направлениям
деятельности

Организация
безопасности
предприятия

Управление
персоналом

Использование
новых технологий

Научная и
исследовательская
деятельность

Участие в торгах и
аукционах

Изучение
направлений
интересов
конкурентов

Формирование
состава клиентов,
компаньонов и т.д.

Формирование
ценовой политики

Основные направления формирования ценной информации

Выявление конфиденциальных сведений

Основополагающая часть организации системы защиты информации – процесс выявления и регламентации состава конфиденциальной информации.

Критерии анализа информационных ресурсов:

- ✓ степень заинтересованности конкурентов;
- ✓ степень ценности (стоимостной, правовой аспект).

Перечень конфиденциальных сведений

Перечень – классифицированный список типовой и конкретно ценной информации о выполняемых работах, производимой продукции, научных и деловых идеях, технологических новшествах.

Перечень конфиденциальных сведений:

- ✓ закрепляет факт отнесения сведений к защищаемой информации;
- ✓ определяет срок, период недоступности этих сведений,
- ✓ уровень конфиденциальности (гриф);
- ✓ список должностей, которым дано право использовать эти сведения в работе.

Документирование конфиденциальных сведений

Основные отличия документированных конфиденциальных сведений

1. Обязательность получения разрешения на документирование конфиденциальной информации от полномочного руководителя
2. Установление грифа (уровня) конфиденциальности сведений, подлежащих включению в документ
3. Оформление и учет носителя для документирования, выделенного комплекса конфиденциальных сведений.
4. Учет подготовленного черновика документа
5. Составление черновика и вариантов текста документа
6. Получение разрешения на изготовление документа от полномочного руководителя
7. Изготовление проекта конфиденциального документа
8. Издание конфиденциального документа.

Документирование на случайном носителе

Подготовка к изданию документа, не обоснованная деловой необходимостью или не разрешенного документирования

Включение в документ избыточной информации

Случайное (умышленное) занижение грифа конфиденциальности

Изготовление документа в условиях, не гарантирующих конфиденциальности обрабатываемой информации

Утеря оригинала, черновика, варианта или редакции документа

Попытка подмены утраченного материала

Сообщение содержимого проекта документа постороннему лицу

Несанкционированное копирование

Утечка информации по техническим каналам

Ошибочные действия пользователей

Угрозы конфиденциальным документам

Носители
конфиденциальных
сведений

```
graph TD; A[Носители конфиденциальных сведений] --> B[Традиционные текстовые]; A --> C[Чертежно-графические]; A --> D[Машиночитаемые документы]; B --> C; B --> D; C --> E[Аудио и видео документы]; C --> F[Фотодокументы];
```

Традиционные текстовые

Чертежно-графические

Машиночитаемые документы

Аудио и видео документы

Фотодокументы

Конфиденциальный документ
– необходимым образом оформленный носитель документированной информации, содержащий сведения ограниченного доступа или использования, которые составляют интеллектуальную собственность юридического (физического) лица.

Закрепление факта присвоения носителю категории ограничения доступа

Присвоение носителю учетного номера и включение его в справочно-информационный банк для обеспечения контроля за использованием и проверки наличия

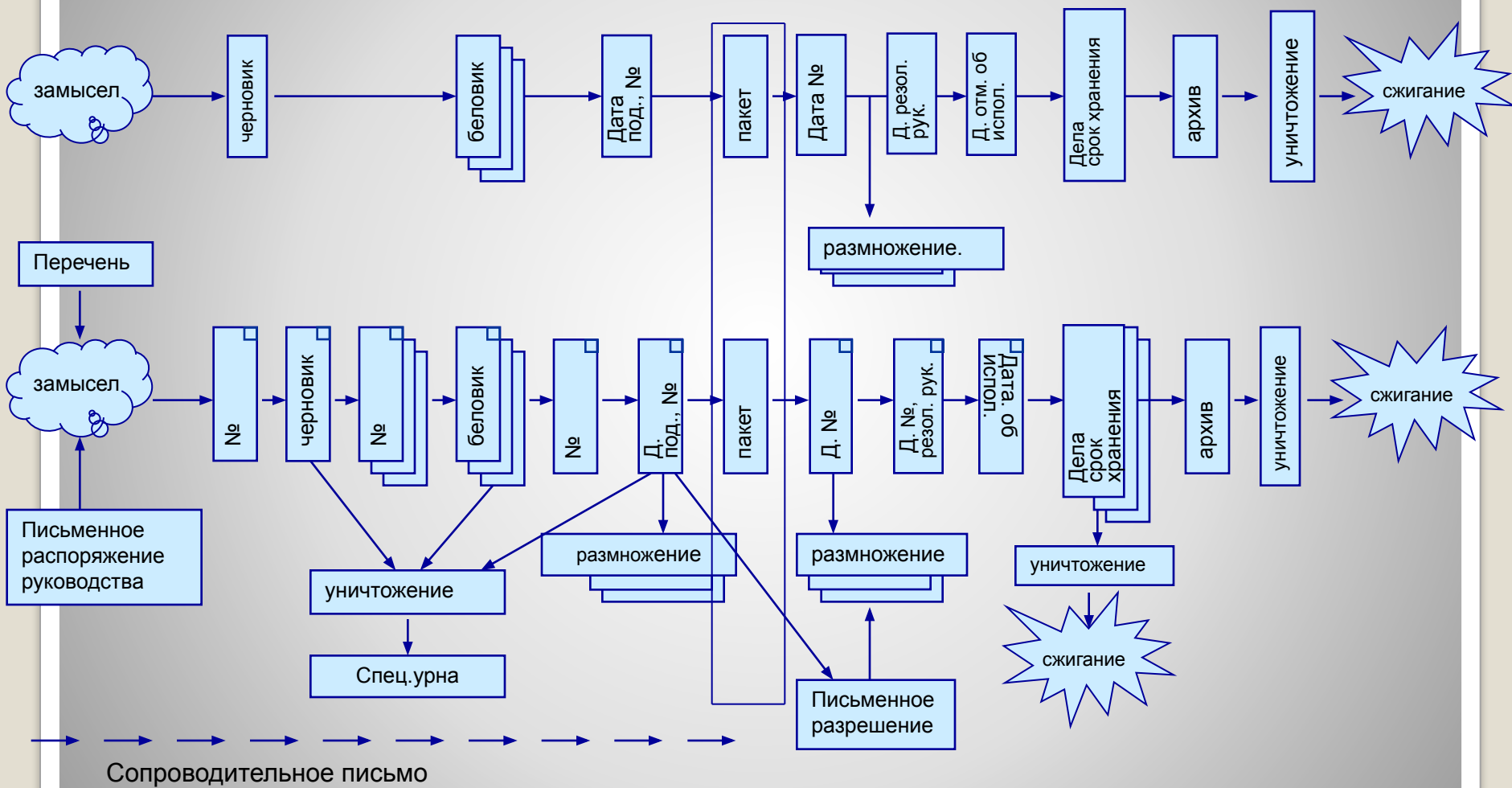
Документирование фактов перемещения носителей между руководителями и сотрудниками

Закрепление персональной ответственности за сохранность носителя

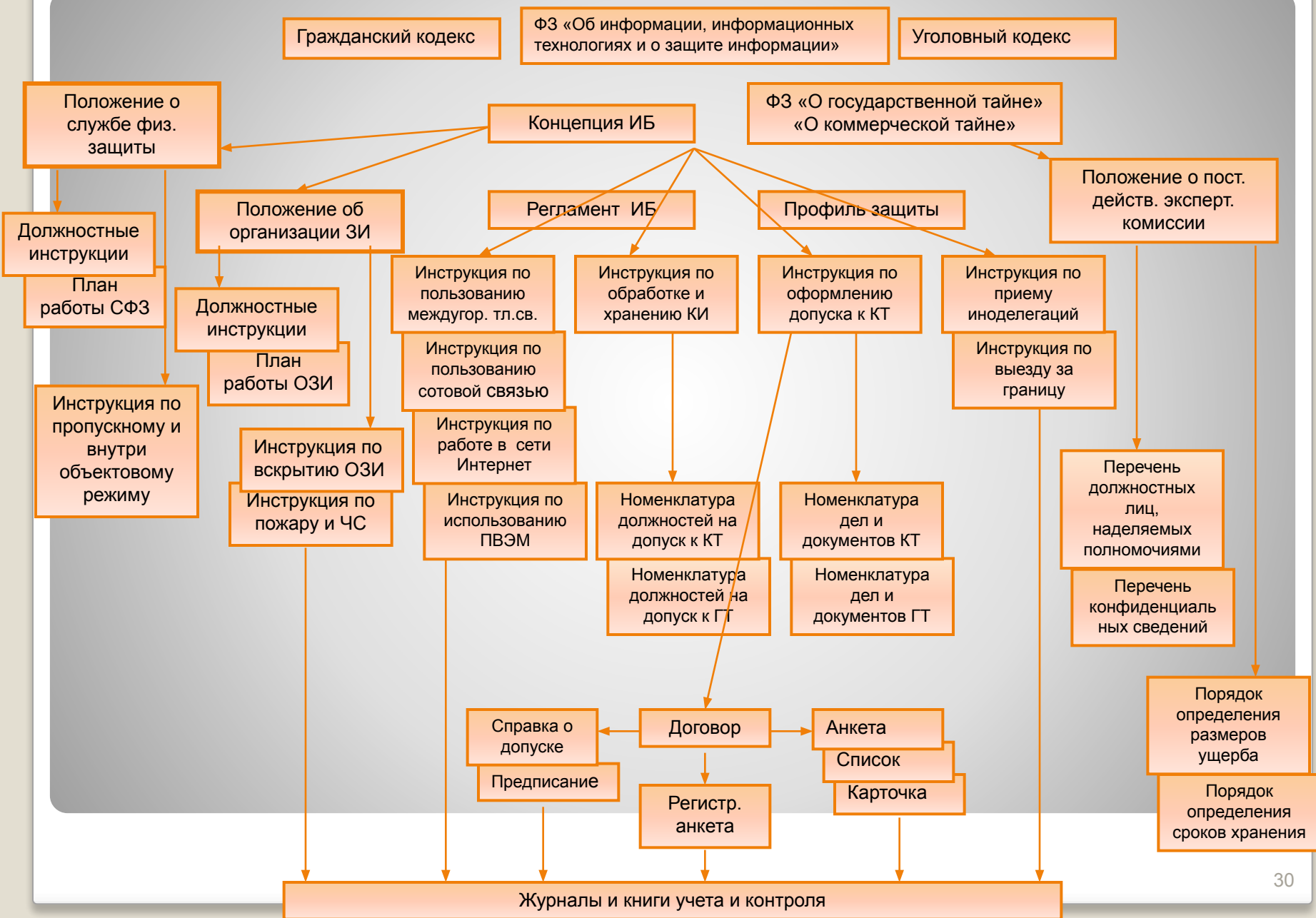
Контроль работы исполнителей над документами и своевременное уничтожение при потере практической ценности

Задачи учета конфиденциальных документов

Жизненный цикл конфиденциального документа



Документированная система защиты



Контрольные вопросы

1. Архитектура системы защиты конфиденциального документооборота на предприятии.
2. Основные направления формирования конфиденциальных документов на предприятии.
3. Предпосылки отнесения информации к категории конфиденциальной и выявление конфиденциальных сведений на предприятии.
4. Порядок документирования конфиденциальных сведений.
5. Основные носители конфиденциальных сведений и угрозы конфиденциальному документообороту.
6. Жизненный цикл конфиденциального документа.
7. Структура документированной системы защиты в РФ.

Организация режима обеспечения комплексной защиты информации

Разработка Политики безопасности

Политика безопасности информации – совокупность нормативных документов, определяющих (или устанавливающих) порядок обеспечения безопасности информации на конкретном предприятии, а также выдвигающих требования по поддержанию подобного порядка.

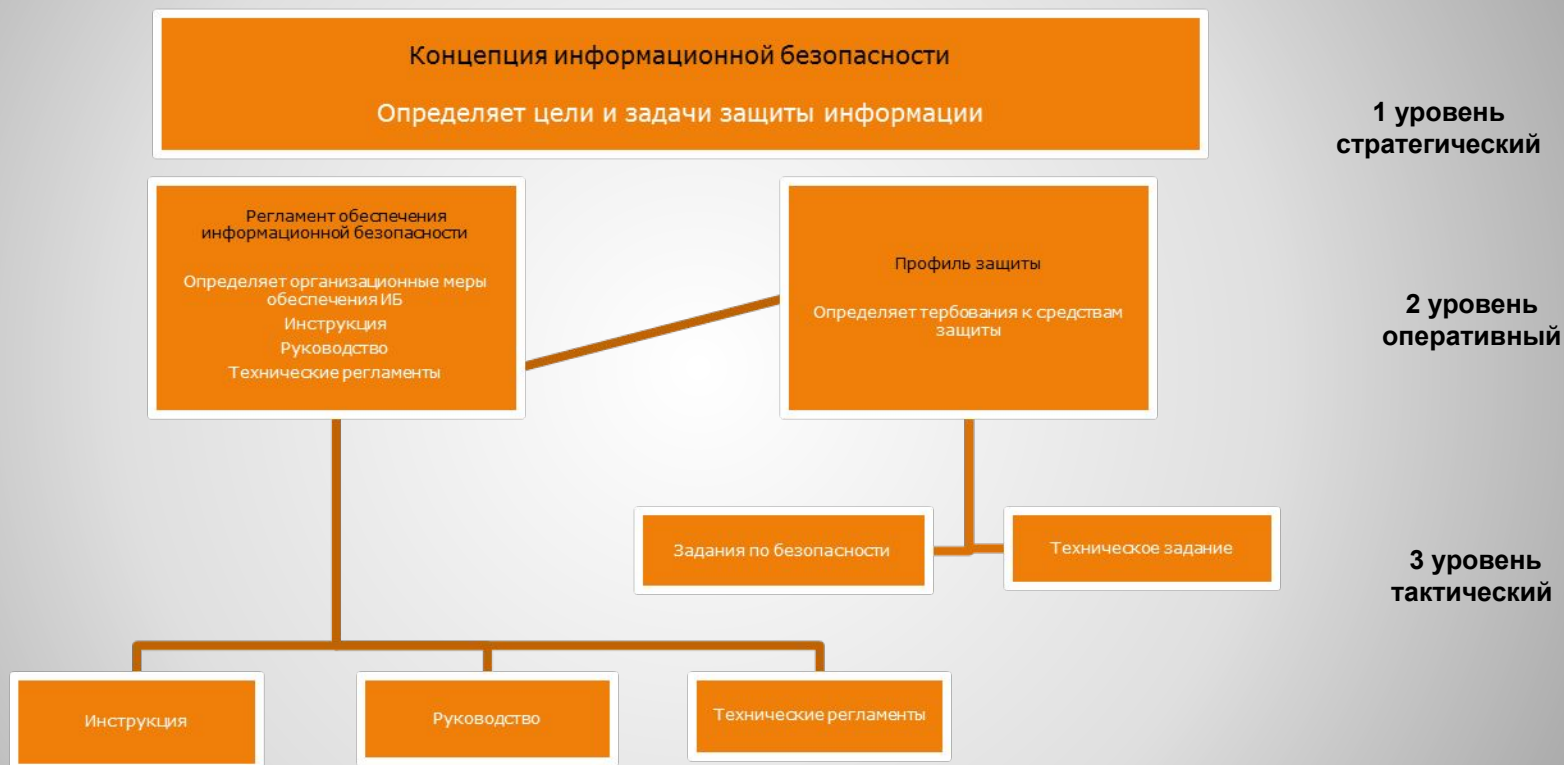
Формирование системы взглядов
на проблему
обеспечения безопасности
информации и пути
ее решения с учетом
современных тенденций
развития технологий и
методов защиты
информации

Формулирование рекомендаций
по повышению
степени защищенности
информационной
системы

Выработка общих требований к
средствам
защиты информации

Цели политики безопасности

Уровни Политики безопасности информации





**Определение общих положений
Концепции**

**Уяснение основных направлений
обеспечения безопасности информации и
описание требований к безопасности
информации**

Разработка специальных глав Концепции

**Разработка
Концепции безопасности информации**



Подготовка к разработке Регламента

**Определение общих положений
Регламента**

**Определение обязанностей персонала по
обеспечению безопасности информации**

**Определение правил использования
компьютеров и информационных систем**

**Разработка Регламента
обеспечения безопасности информации**

Разделы Профиля защиты:

- ✓ «Введение ПЗ»;
- ✓ «Описание Объекта Оценки»;
- ✓ «Среда безопасности ОО»;
- ✓ «Цели безопасности»;
- ✓ «Требования безопасности ИТ»;
- ✓ «Обоснование».

**Формулировка
необходимости ИБ**

**Описание среды, в
которой находится
КИС**

**Описание
предположений о
существующем
состоянии
безопасности**

**Описание политики
безопасности,
которая
должна
выполняться**

**Описание целей
безопасности**

**Функциональные
требования к
безопасности
и требования
доверия к
безопасности**

**Обоснование
достаточности
функциональных
требований и
требований доверия к
безопасности**

Профиль защиты включает:

АСПЕКТЫ СРЕДЫ БЕЗОПАСНОСТИ АИС

Угрозы

Политика
безопасности

Предположения
безопасности

Цели безопасности

Для АИС

Для среды
функционирования

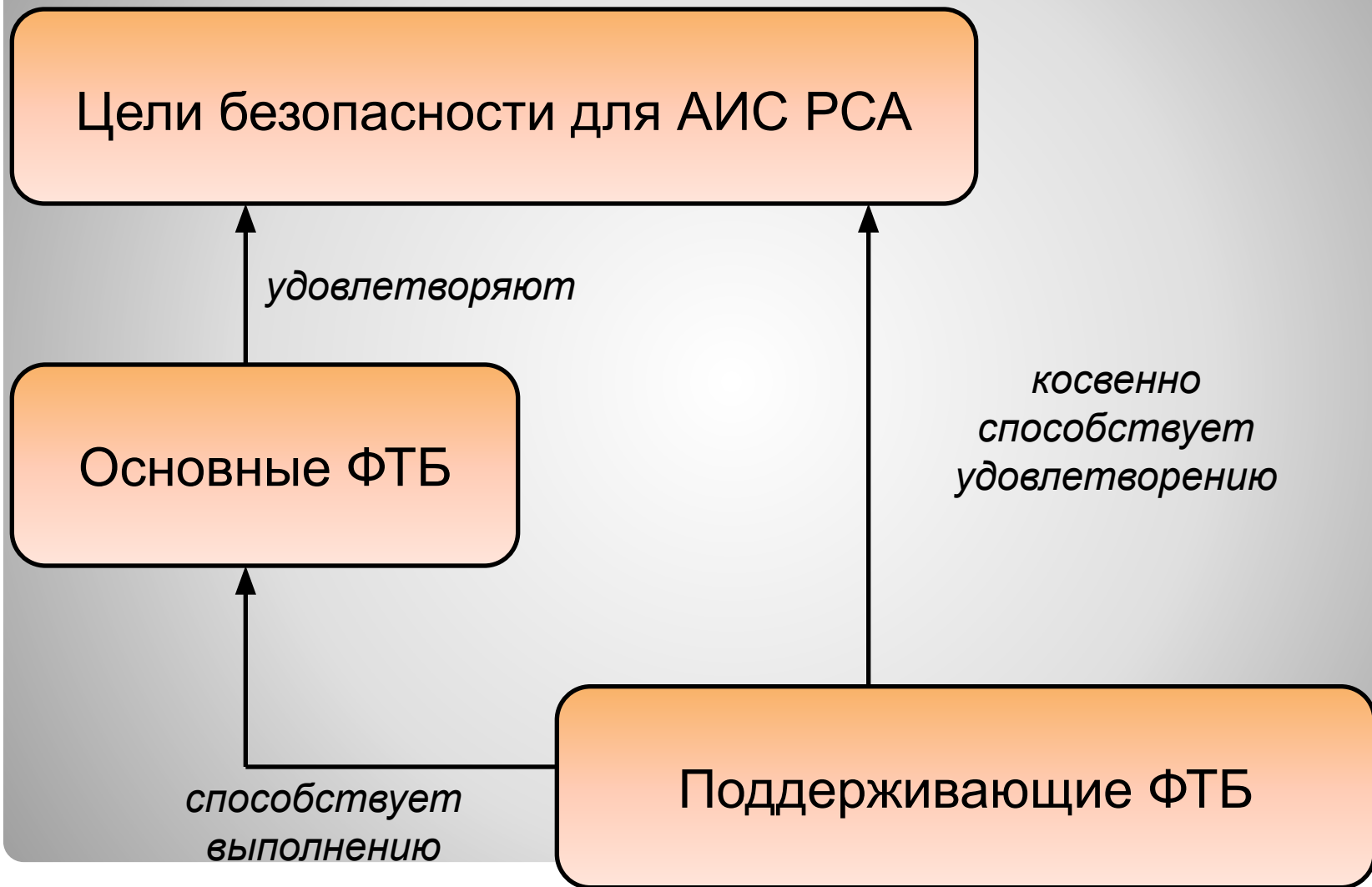
Для АИС

Для среды
функционирования

Не ИТ-требования
безопасности

Требования безопасности к СОБИ

Взаимосвязь основных и дополнительных ФТБ



Контрольные вопросы

1. Цели и задачи Политики информационной безопасности на предприятии
2. Уровни Политики информационной безопасности на предприятии.
3. Разработка Концепции безопасности информации и
Регламента обеспечения безопасности информации на предприятии.
4. Понятие Профиль защиты и его составляющие.

Организация системы физической защиты информации

Система физической защиты – типовые задачи и способы ее реализации

Система физической защиты (СФЗ) – совокупность людей, процедур и оборудования защищающих имущество (объекты) от хищений, диверсий и иных неправомерных действий.

Предотвращение
диверсий,
направленных
на вывод из строя
оборудования

Предотвращение
хищений
материальных
средств,
имущества либо
информации

Защита сотрудников
объекта

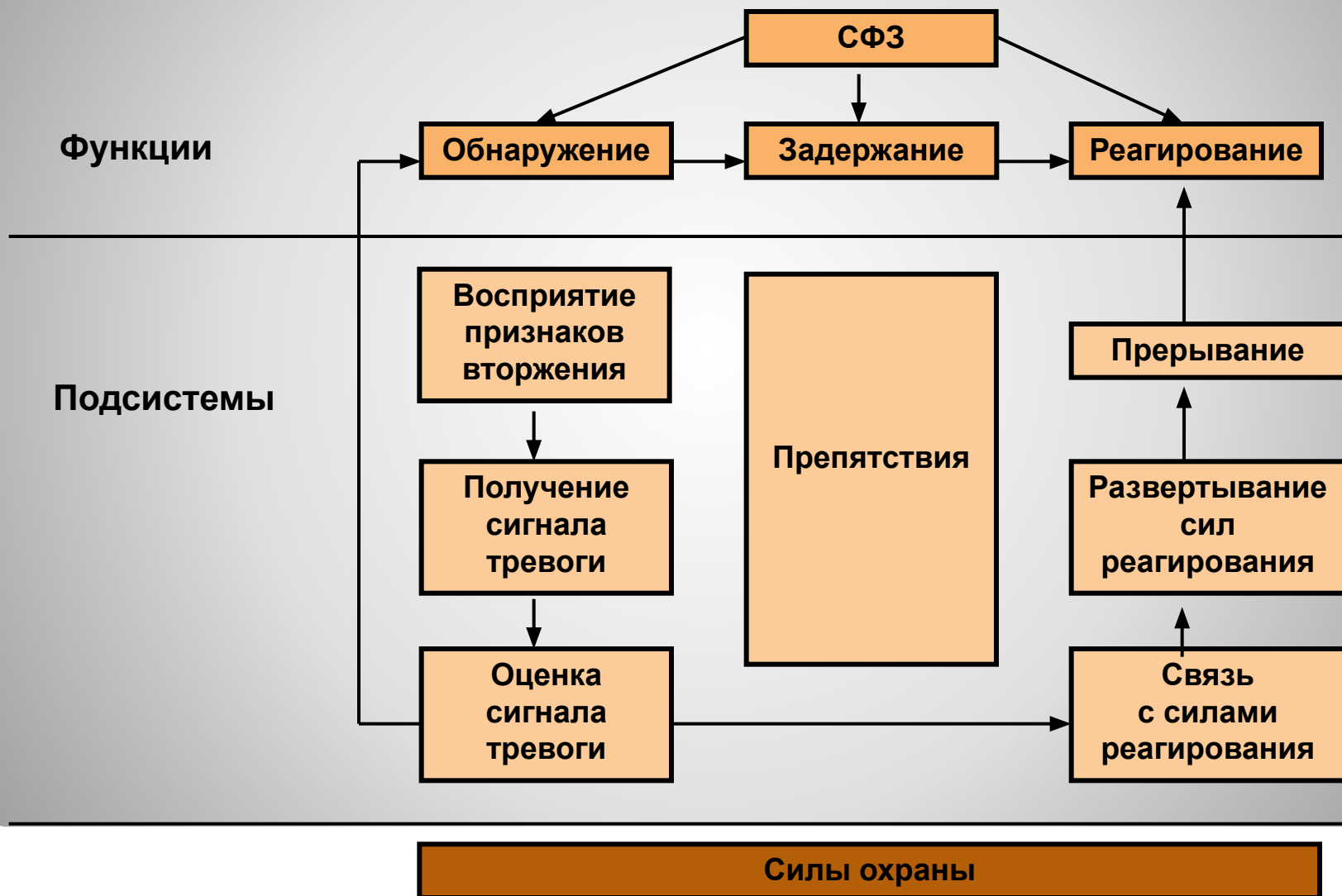
Типовые задачи СФЗ

Способы организации СФЗ

Сдерживание

**Обнаружение, задержка,
реагирование –
триединая задача
эффективной СФЗ**

Функции и подсистемы СФЗ



Связь между функциями СФЗ



- | | |
|------------------|---|
| T_o | – время срабатывания датчика |
| T_A | – время принятия решения об отражении акции |
| $T_{\text{пер}}$ | – время прерывания вторжения |
| T_c | – время совершения акции нарушителем |

Сдерживание

Сдерживание –
реализация мер,
воспринимаемых
потенциальным нарушителем
как труднопреодолимые,
устрашающие
(предупреждающие) и
превращающие объект в
непривлекательную цель.

Результат сдерживания
– *нарушитель прекращает
нападение, лучше если не
предпринимает вовсе.*

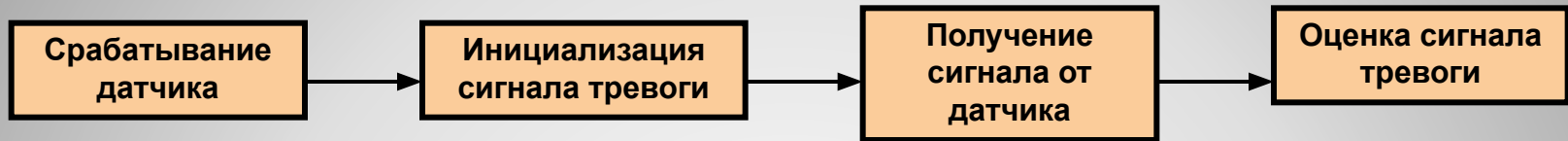
Обнаружение

Обнаружение – выявление
скрытой или открытой акции
нарушителя по
проникновению в
пространство объекта.

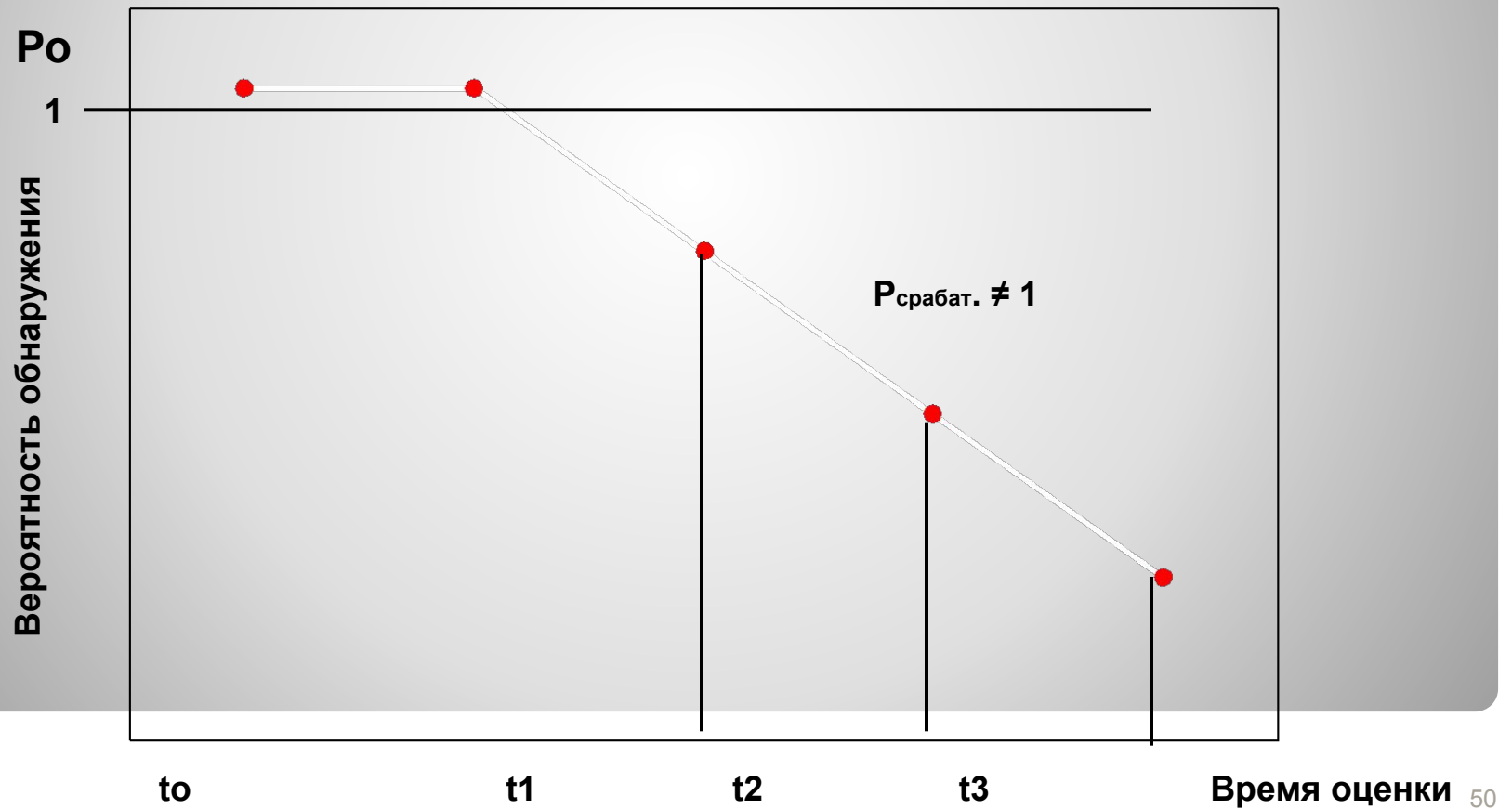
**Показатели эффективности
обнаружения :**

- вероятность выявления
акции;
- время оценивания акции;
- время передачи сообщения
об акции;
- частота ложных тревог.

Организация подсистемы обнаружения



Связь времени оценки и вероятности обнаружения:



Задержка

Задержка – замедление продвижения нарушителя к цели.

Пути (способами) являются:

- ✓ физические барьеры, препятствия; замки;
- ✓ персонал охраны (постоянной готовности, ждущий режим)

Показатель эффективности задержки
– общее время преодоления каждого элемента задержки после обнаружения.

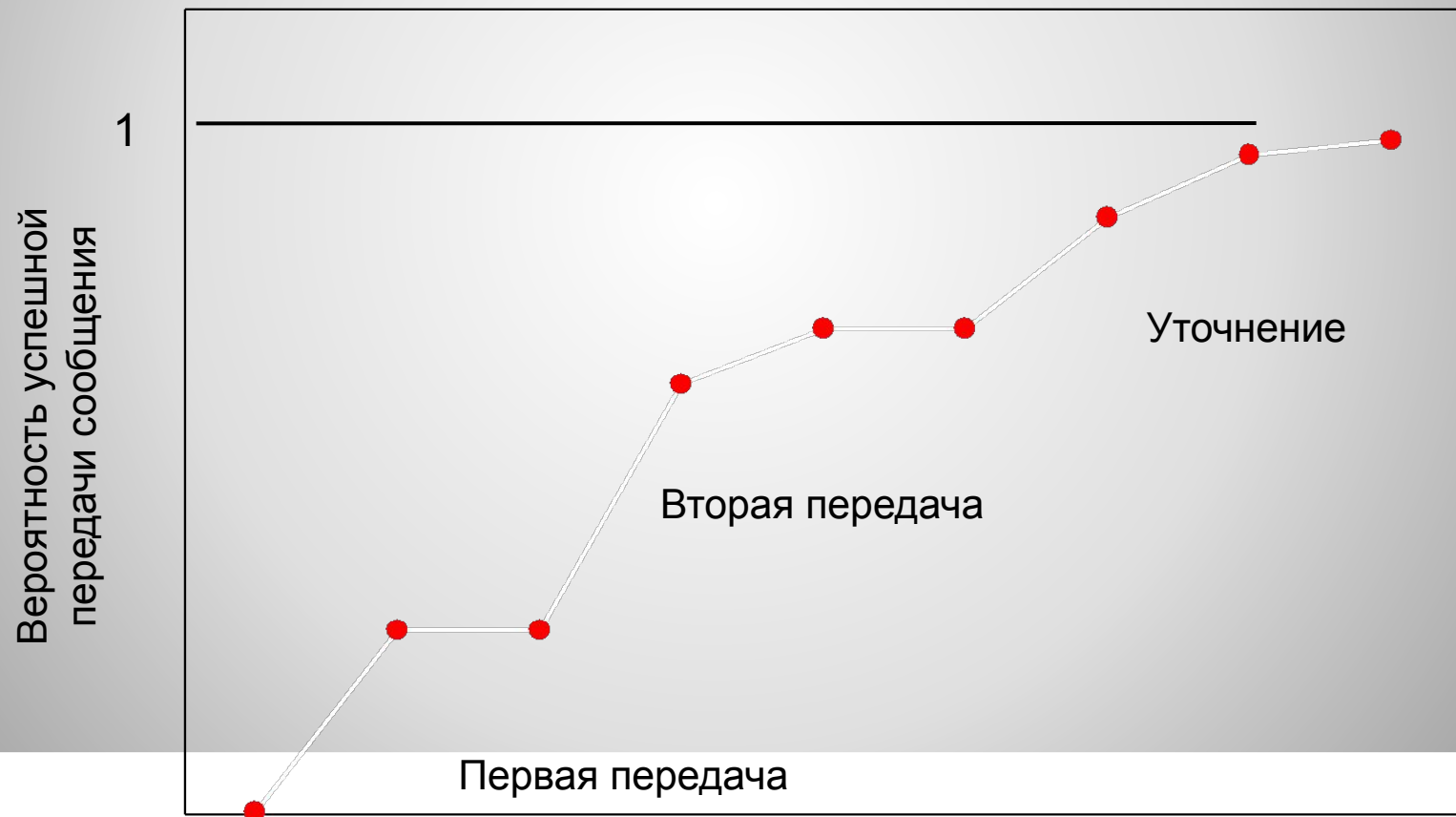
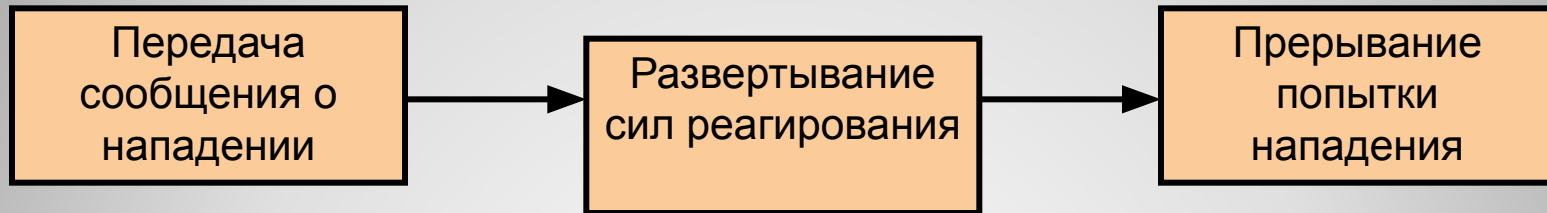
Реагирование

Реагирование – действия сил защиты по воспрепятствованию успеху нарушителя, прерывание действий нарушителя.

Показатели эффективности реагирования:

- ✓ время между получением информации об обнаружении и прерывание акции нарушителя;
- ✓ вероятность своевременного развертывания сил реагирования.

Подсистемы реагирования



$$T_R = \sum_{i=k}^m T_i > T_G \quad P_1 = 1 - \prod_{i=k}^{k-1} P_{NDi}$$

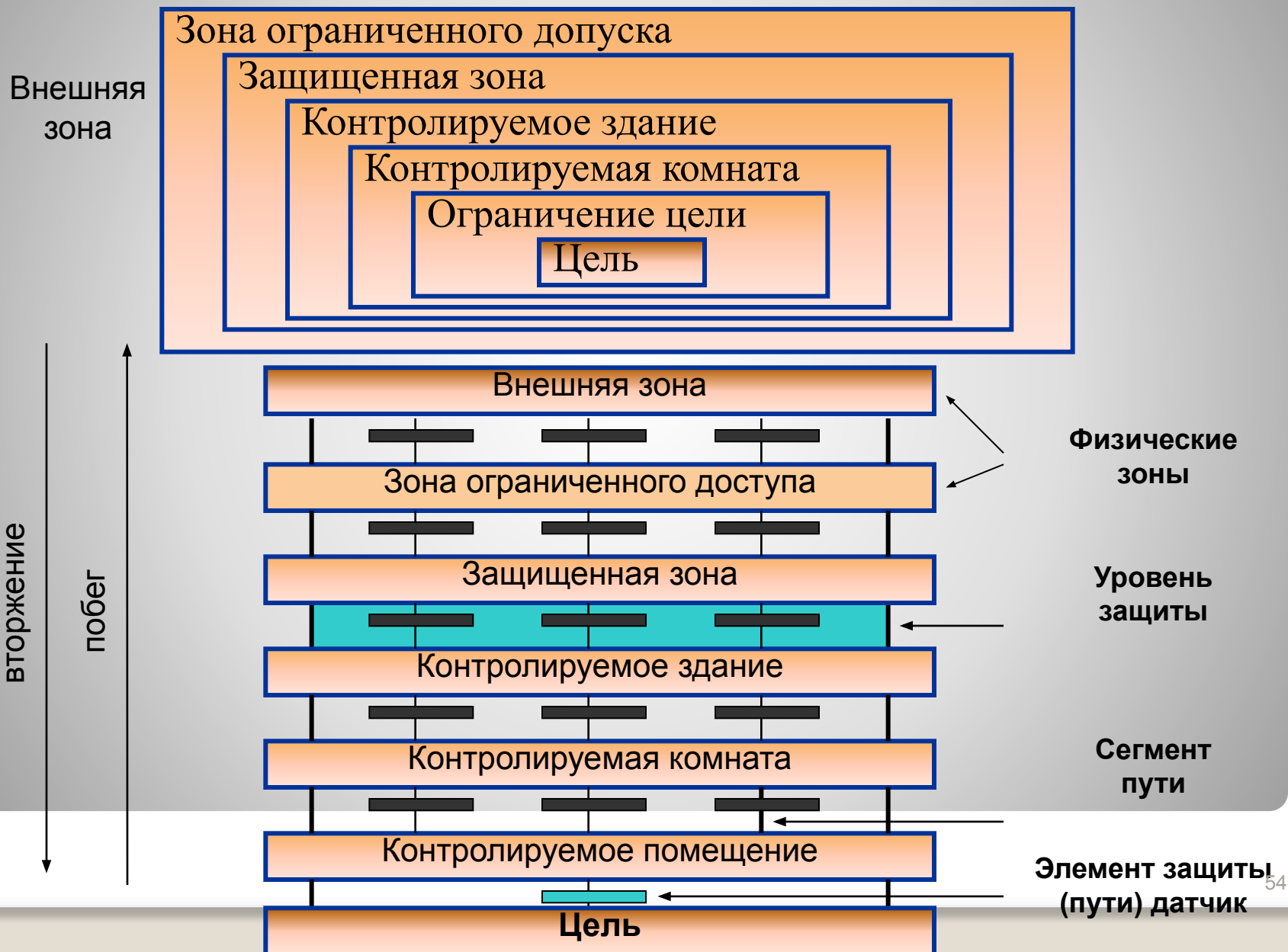
m – общее число элементов задержки по пути

k – точки, где $T_R > T_G$

T_i – время задержки i -го элемента

P_{NDi} – вероятность, того, что i -ый элемент не обнаружил нарушителя

Диаграмма последовательности действий нарушителя



Силы реагирования

Комплектование охраны

Организационная структура и численность подразделений ведомственной охраны, осуществляющих защиту объектов, определяются в зависимости от:

- ✓ особенностей охраняемого объекта,
- ✓ степени оборудования их инженерно-техническими средствами защиты,
- ✓ а также иных условий, связанных с обеспечением надежной защиты объектов.

К техническим средствам охраны относятся:

- ✓ системы охранной сигнализации (СОС) периметра;
- ✓ системы охранной сигнализации зданий и сооружений;
- ✓ системы контроля и управления доступом (СКУД);
- ✓ системы телевизионного наблюдения (СТН);
- ✓ системы охранного освещения (СОО);
- ✓ системы связи и оповещения (ССО).

К инженерным средствам охраны относятся:

- ✓ ограждение периметра объекта охраны и внутренних зон ограниченного доступа;
- ✓ контрольно-пропускные пункты (КПП) с соответствующим досмотровым оборудованием;
- ✓ въездные ворота, калитки, шлагбаумы.

Инженерно-технические средства охраны

Контрольные вопросы

1. Система физической защиты: основные задачи и способы их решения на предприятии.
2. Функции и подсистемы СФЗ.
3. Организация подсистемы сдерживания и обнаружения СФЗ.
4. Организация подсистемы задержки и реагирования СФЗ.
5. Сценарии последовательности действий нарушителя СФЗ.
6. Организация инженерно-технических средств охраны.

МЕЖДУНАРОДНЫЕ СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Формирование в
мире единого
подхода
к системам
управления ИБ
уровня корпорации

Структура общих
требований ИБ

Внедрение
принципов ИБ в
организационную
структуру
компании

Разработка и
внедрение
эффективной
политики
безопасности

**Основные цели и задачи
британского стандарта ISO 17799**

*Информационные технологии — Технологии безопасности — Практические
правила менеджмента информационной безопасности*

Международное
признание

Отношение
бизнес-партнеров

Управление
информационной
безопасностью
корпорации

Повышение
защищенности
информационной
системы

Эффективная
политика
информационной
безопасности

Преимущества ISO 17799

Политика
безопасности

Организационные
меры
по обеспечению
безопасности

Классификация и
управление
ресурсами

Безопасность
персонала

Физическая
безопасность

Управление
коммуникациями и
процессами

Контроль доступа

Разработка и
техническая
поддержка
вычислительных
систем

Управление
инцидентами
информационной
безопасности

Управление
непрерывностью
бизнеса

Соответствие
системы основным
требованиям

Содержание стандарта ISO 17799

Методология
управления ИБ

Компоненты
информационных
технологий

Каталоги угроз
безопасности и
контрмер

германского стандарта BSI

*Руководство по защите информационных технологий
для базового уровня защищенности*

Система
управления
информационной
безопасностью
(СУИБ)

Обязанности
руководства
компании

Внутренний аудит
СУИБ

Проверки СУИБ
руководством
компании

Совершенствование
СУИБ

Содержание международного стандарта ISO 27001

*Информационные технологии - Методы обеспечения безопасности - Системы
управления информационной безопасностью – Требования*

Системы менеджмента защиты информации

Бизнес ориентация
стандарта

Ориентация на
лучшие западные
стандарты

Конфиденциальность,
целостность,
доступность

Анализ и управление
рисками

Аудит безопасности

Модели зрелости
процессов
менеджмента ИБ

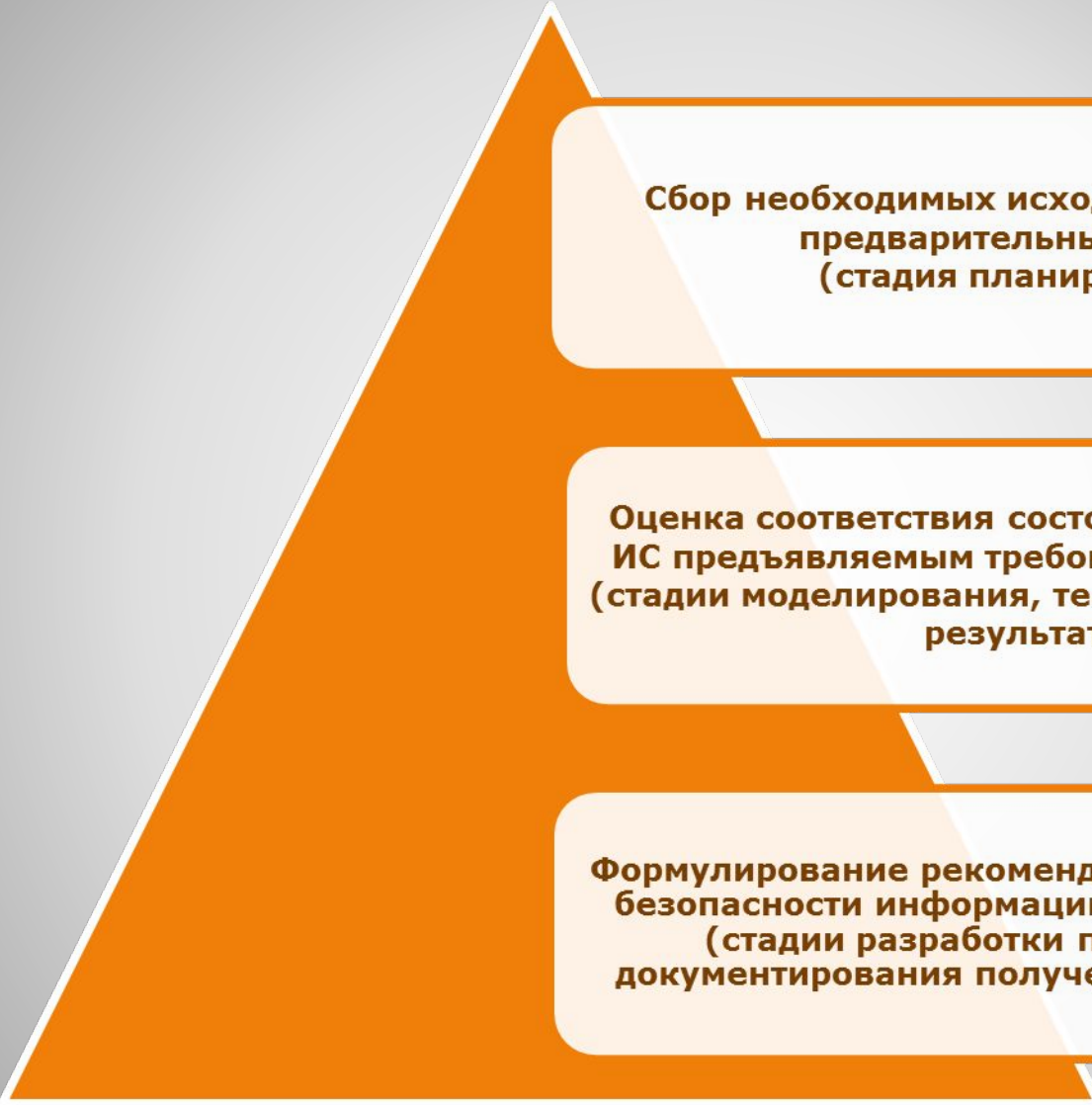
Менеджмент
информационной
безопасности

**Особенности стандарта ЦБ РФ – обеспечение ИБ организаций
банковской системы РФ**

ПРОВЕДЕНИЕ КОМПЛЕКСНОГО ОБСЛЕДОВАНИЯ ЗАЩИЩЕННОСТИ ИС

**Методологическое обследование
процессов, методов и средств
обеспечения безопасности
информации при выполнении
информационной системой своего
главного предназначения –
информационное обеспечение
бизнеса.**

Цель проведения обследования (аудита)



**Сбор необходимых исходных данных и их
предварительный анализ
(стадия планирования)**

**Оценка соответствия состояния защищенности
ИС предъявляемым требованиям и стандартам
(стадии моделирования, тестирования и анализа
результатов)**

**Формулирование рекомендаций по повышению
безопасности информации в обследуемой ИС
(стадии разработки предложений и
документирования полученных результатов)**

Стадии проведения аудита ИБ

Виды обследования

Периоды жизненного цикла обследуемого объекта	Виды обследования (аудита)				
	Первичный	Технический	Аттестация	Сюрвей	Контрольный
Принятие решения о создании корпоративной ИС	х				
Определение требований к создаваемой корпоративной ИС		х			
Проектирование и ввод в эксплуатацию корпоративной ИС			х	х	
Штатная эксплуатация средств корпоративной ИС					х
Ремонт (плановый и внеплановый), устранение неисправностей			х		х
Нештатные ситуации, приводящие к ущербу				х	х
Устранение последствий нештатных ситуаций					х
Принятие решений о модернизации корпоративной ИС	х	х	х		
Модернизация корпоративной ИС				х	
Эксплуатация модернизированной ИС					х
Вывод из эксплуатации и замена корпоративной ИС					х

Сюрвей - аудит застрахованных или подлежащих страхованию объектов

Анализ угроз безопасности информации

ОБЪЕКТ ЗАЩИТЫ

информационные ресурсы, содержащие сведения ограниченного доступа

ЦЕЛЬ ИБ

исключение нанесения материального, морального и иного ущерба
собственникам информации в результате нарушения:

конфиденциальности

доступности

целостности

Хищение

Утрата

Блокирование

Уничтожение

Модификация

Отрицание подлинности

Навязывание ложной

Угрозы информационной безопасности

Планирование
проведения
обследования

Проведение
комплексного
обследования

Оценка эффективности
существующей
системы защиты ИС с
применением
специализированных
инструментариев

Состав работ по проведению аудита

Контрольные вопросы

1. Международные стандарты в области информационной безопасности.
2. Цели, задачи и стадии проведения аудита информационной безопасности.
3. Виды аудита информационной безопасности, применяемые на различных стадиях жизненного цикла обследуемого объекта.
4. Состав работ по проведения аудита информационной безопасности.