КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

РАЗДЕЛ 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И УРОВНИ ЕЕ ОБЕСПЕЧЕНИЯ

Постулаты

1. Информация — это всеобщее свойство материи.
2. Любое взаимодействие в природе и обществе основано на информации.
3. Всякий процесс совершения работы есть процесс информационного взаимодействия.
4. Информация—продукт отражения действительности.
5. Действительность отражается в пространстве и времени.
6. Ничего не происходит из ничего.
7. Информация сохраняет свое значение в неизменном виде до тех пор, пока остается в неизменном виде носитель информации — ПАМЯТЬ.
8. Ничто не исчезает просто так.

Что храним, то и имеем

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ -*это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств».*

(Закон РФ «Об участии в международном информационном обмене»)

Информационная безопасность – это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

Безопасность автоматизированной системы обработки информации (АСОИ) – свойство защищенности системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, изменения или разрушения ее компонентов.

Исходя из вышесказанного, отметим следующие важные выводы:

- задачи по обеспечению информационной безопасности для разных категорий субъектов могут существенно различаться;

- информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации – это принципиально более широкое понятие.

Объектно-ориентированный подход является основой современной технологии программирования, испытанным методом борьбы со сложностью систем. Представляется естественным и, более того, необходимым, стремление распространить этот подход и на системы информационной безопасности, для которых, как и для программирования в целом, имеет место упомянутая проблема сложности.

Любой разумный метод борьбы со сложностью опирается на *принцип «divide et impera» - «разделяй и властвуй»*. *Этот* ***принцип*** *означает, что* сложная система *(информационной безопасности) на верхнем уровне должна состоять из небольшого числа относительно* независимых ***компонентов***. *Относительная независимость здесь и далее понимается как минимизация числа связей между компонентами. Затем* **декомпозиции** *подвергаются выделенные на первом этапе* ***компоненты***, *и так далее до заданного* ***уровня детализации***. *В результате система оказывается представленной в виде иерархии с несколькими уровнями абстракции.* ***Структурный подход*** *опирается на* ***алгоритмическую*** **декомпозицию**, *когда выделяются* ***функциональные элементы*** *системы.*

Защита информации (ГОСТ Р 50922-2006) – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Национальный стандарт РФ ГОСТ Р 50922-2006 "Защита информации Основные термины и определения" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. N 373-ст)

Решение проблемы информационной безопасности, как правило, начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем. Это обусловлено тем, что для разных категорий субъектов характер решаемых задач может существенно различаться. Например, задачи, решаемые администратором локальной сети по обеспечению информационной безопасности, в значительной степени отличаются от задач, решаемых пользователем на домашнем компьютере, не связанном сетью.

Объектно-ориентированный подход использует объектную *декомпозицию*, то есть поведение системы описывается в терминах взаимодействия *объектов*.
Необходимо ввести понятие *класса и объекта*.

Класс - это абстракция множества сущностей реального мира, объединенных общностью структуры и поведения.
Объект - это элемент класса, то есть абстракция определенной сущности.

Подчеркнем, что **объекты** *активны, у них есть не только внутренняя структура, но и поведение, которое описывается так называемыми* **методами объекта**.

ОСНОВНЫЕ КОНЦЕПТУАЛЬНЫЕ ИНФОРМАЦИИ

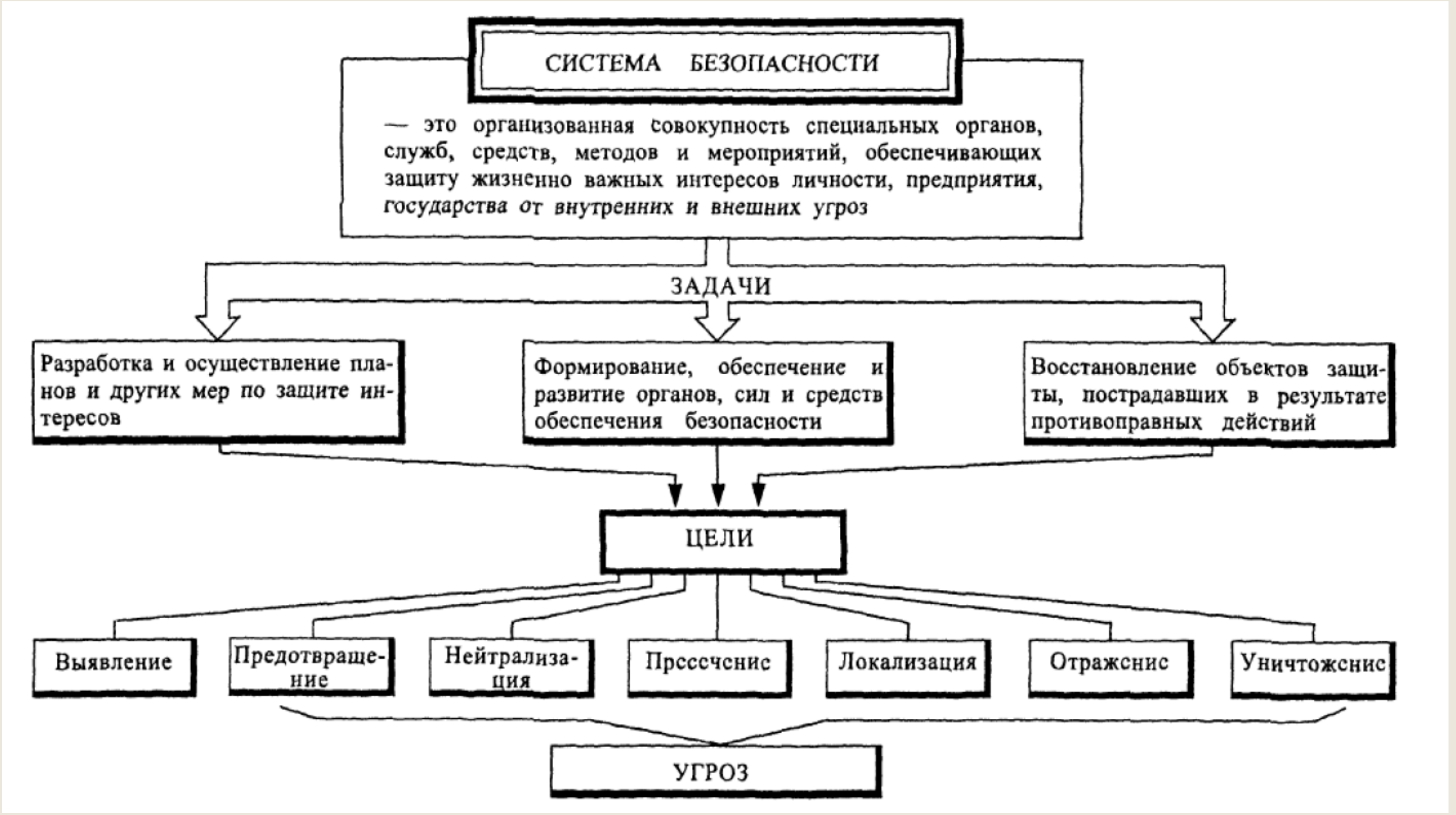
✓весьма развитый арсенал технических средств защиты информации, производимых на промышленной основе;

✓значительное число фирм, специализирующихся на решении вопросов защиты информации;

✓достаточно четко очерченная система взглядов на эту проблему;

✓наличие значительного практического опыта и другое.

ПОЛОЖЕНИЯ СИСТЕМЫ ЗАЩИТЫ


СИСТЕМА БЕЗОПАСНОСТИ
— это организованная совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия, государства от внутренних и внешних угроз
ЗАДАЧИ
Разработка и осуществление планов и других мер по защите интересов
Формирование, обеспечение и развитие органов, сил и средств обеспечения безопасности
Восстановление объектов защиты, пострадавших в результате противоправных действий
ЦЕЛИ
Выявление
Предотвращение
Нейтрализация
Пресечение
Локализация
Отражение
Уничтожение
УГРОЗ


ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
— состояние защищенности информационной среды общества от внутренних и внешних угроз, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства
УГРОЗЫ
ОЗНАКОМЛЕНИЕ (получение)
Противоправные действия, приводящие к значительному или полному разрушению информационных ресурсов
ИСКАЖЕНИЕ (модификация)
Случайные или преднамеренные действия, приводящие к частичному изменению содержания
РАЗРУШЕНИЕ (уничтожение)
Противоправное действие, не приводящее к изменению или разрушению информации
ЦЕЛИ
Обеспечение конфиденциальности, целостности и доступности

РАЗДЕЛ 2. СОСТАВЛЯЮЩИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

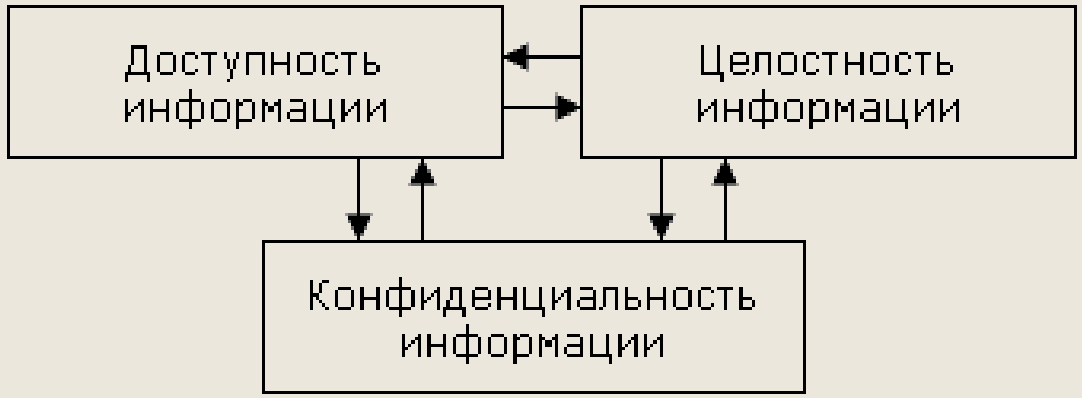
Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением трех задач:

1) Обеспечением доступности информации.
2) Обеспечением целостности информации.
3) Обеспечением конфиденциальности информации.

Доступность – это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

Целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

Конфиденциальность – гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.




УГРОЗЫ ИНФОРМАЦИИ
Проявляются в нарушении
КОНФИДЕНЦИАЛЬНОСТИ
- Разглашение
- Утечка
- НСД
ДОСТОВЕРНОСТИ
- Фальсификация
- Подделка
- Мошенничество
ЦЕЛОСТНОСТИ
- Искажение
- Ошибки
- Потери
ДОСТУПНОСТИ
- Нарушение связи
- Воспрещение получения


КЛАССИФИКАЦИЯ УГРОЗ
Угроза – потенциально возможное или реальное действие злоумышленников, способное нанести моральный или материальный ущерб
По объектам
Персонал
Материальные и финансовые ценности
Информация
По величине ущерба
Предельный
Значительный
Незначительный
По вероятности возникновения
Весьма вероятные
Вероятные
Маловероятные
По причинам появления
Стихийные
Преднамеренные
По ущербу
Материальный
Моральный
По отношению к объекту
Внутренние
Внешние
По характеру воздействия
Активные
Пассивные


НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
- нормативно-правовые категории, определяющие комплексные меры защиты информации
ПРАВОВАЯ ЗАЩИТА
- Специальные правовые акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе
ОРГАНИЗАЦИОННАЯ ЗАЩИТА
- Регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая нанесение ущерба
ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА
- Использование различных технических средств, препятствующих нанесению ущерба


КЛАССИФИКАЦИЯ
ИТЗ по используемым средствам
ФИЗИЧЕСКИЕ
Устройства, инженерные сооружения и организационные меры, затрудняющие или исключающие проникновение злоумышленников к источникам конфиденциальной информации
АППАРАТНЫЕ
Механические, электрические, электронные и др. устройства, предназначенные для защиты информации от утечки и разглашения и противодействия техническим средствам промышленного шпионажа
ПРОГРАММНЫЕ
Система специальных программ, включаемых в состав общего и специального обеспечения, реализующих функции защиты информации и сохранения целостности и конфиденциальности
КРИПТОГРАФИЧЕСКИЕ
Технические и программные средства шифрования
КОМБИНИРОВАННЫЕ
Совокупная реализация аппаратных и программных средств и криптографических методов защиты информации


ДЕЙСТВИЯ,
приводящие к незаконному овладению конфиденциальной информацией
РАЗГЛАШЕНИЕ
Уменьшенные или неосторожные действия должностных лиц и граждан, которым соответствующие сведения были доверены в установленном порядке, приведшие к ознакомлению с ними лиц, не допущенных к ним
Выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и других иных способах и реализуется по каналам распространения и средствам массовой информации
УТЕЧКА
Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена
Возможна по различным каналам утечки информации, в том числе визуально-оптическим, акустическим, электромагнитным и материально-вещественным
НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП
Противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым сведениям
Реализуется различными способами, в том числе такими, как сотрудничество, выведывание, подслушивание, наблюдение, хищение, копирование, подделка, уничтожение, перехват, фотографирование и др

РАЗДЕЛ 3. СИСТЕМА ФОРМИРОВАНИЯ РЕЖИМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Постулаты безопасности

1. Если не уверен в безопасности, считай, что опасность существует реально.
2. Безопасности бесплатной не бывает.
3. Безопасности не бывает много.
4. Безопасность должна быть только комплексной.
5. Информационная безопасность может быть обеспечена только системой нормативно-правовых мер, ориентированных на обеспечение комплексной защиты информации от внутренних и внешних угроз.
6. Никакая система безопасности не обеспечивает требуемого уровня без надлежащей подготовки руководителей, сотрудников и клиентов.
7. В безопасности должен быть заинтересован каждый.

Подальше положишь — поближе возьмешь

Направления обеспечения информационной безопасности — это категории,

Задачи информационной безопасности:

- защита технических и программных средств информатизации от ошибочных действий персонала и техногенных воздействий, а также стихийных бедствий;
- защита технических и программных средств информатизации от преднамеренных воздействий.


НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
- нормативно-правовые категории, определяющие комплексные меры защиты информации
ПРАВОВАЯ ЗАЩИТА
- Специальные правовые акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе
ОРГАНИЗАЦИОННАЯ ЗАЩИТА
- Регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая нанесение ущерба
ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА
- Использование различных технических средств, препятствующих нанесению ущерба

Выделим три уровня формирования режима информационной безопасности:

- законодательно-правовой (правовая защита);
- административный (организационный);
- программно-технический (инженерно-техническая защита).

Программно-технические меры, то есть меры, направленные на контроль компьютерных сущностей - оборудования, программ и/или данных, образуют последний и самый важный рубеж информационной безопасности.

Центральным для программно-технического уровня является понятие сервиса безопасности.

Основными сервисами обеспечения безопасности являются:

- *идентификация и аутентификация;*
- *управление доступом;*
- *протоколирование и аудит;*
- *шифрование;*
- *контроль целостности;*
- *экранирование;*
- *анализ защищенности;*
- *обеспечение отказоустойчивости;*
- *обеспечение безопасного восстановления;*
- *туннелирование;*
- *управление.*

1. Законодательно-правовой уровень включает комплекс законодательных и иных правовых актов, устанавливающих правовой статус субъектов информационных отношений, субъектов и объектов защиты, методы, формы и способы защиты, их правовой статус.
2. Административный уровень включает комплекс взаимо-координируемых мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации.
3. Программно-технический уровень включает три подуровня: физический, технический (аппаратный) и программный.

АДУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Доверяй, но проверяй

Аудит (контроль) состояния защиты информации — специальная проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам. Собственник информационных ресурсов или уполномоченные им лица имеют право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований. *(Закон РФ «Об информации, информатизации и защите информации»)*

Постулаты

1. Безопасных технических средств нет.
2. Источниками образования технических каналов утечки информации являются физические преобразователи.
3. Любой электронный элемент при определенных условиях может стать источником образования канала утечки информации.
4. Любой канал утечки информации может быть обнаружен и локализован. «На каждый яд есть противоядие».
5. Канал утечки информации легче локализовать, чем обнаружить.

Основными направлениями деятельности в области аудита безопасности информации являются

1 Аттестация объектов информатизации по требованиям безопасности информации

a. аттестация автоматизированных систем, средств связи, обработки и передачи информации;

b. аттестация помещений, предназначенных для ведения конфиденциальных переговоров;

c. аттестация технических средств, установленных в выделенных помещениях.

Основными направлениями деятельности в области аудита безопасности информации являются

2 Контроль защищенности информации ограниченного доступа

a. выявление технических каналов утечки информации и способов несанкционированного доступа к ней;

b. контроль эффективности применяемых средств защиты информации.

3 Специальные исследования технических средств на наличие побочных электромагнитных излучений и наводок (ПЭМИН)

a. персональные ЭВМ, средства связи и обработки информации;

b. локальные вычислительные системы;

c. оформления результатов исследований в соответствии с требованиями Гостехкомиссии России.

Основными направлениями деятельности в области аудита безопасности информации являются

4 Проектирование объектов в защищенном исполнении

a. разработка концепции информационной безопасности;

b. проектирование автоматизированных систем, средств связи, обработки и передачи информации в защищенном исполнении;

c. проектирование помещений, предназначенных для ведения конфиденциальных переговоров.

Аудит выделенных помещений

- ✓ подготовительный этап;
- ✓ этап непосредственного проведения аудита;
- ✓ заключительный этап.

Выводы:

1. Аудит информационной безопасности фирмы — это мощное средство оценки состояния защиты информации.

2. Аудит может проводиться как собственными силами СБ фирмы, так силами специальных лицензированных аудиторских фирм.

3. Регулярность, периодичность и масштабность аудита определяются реальной обстановкой общей безопасности предприятия.

РАЗДЕЛ 4. НОРМАТИВНО-ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РФ

Правовые меры обеспечения безопасности и защиты информации являются основой порядка деятельности и поведения сотрудников предприятия и определяют меры их ответственности за нарушение установленных норм.


ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИИ
– это специальные правовые акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе
МЕЖДУНАРОДНОЕ ПРАВО
Договоры, конвенции, декларации
Патенты
Авторские права
Лицензии
ВНУТРИГОСУДАРСТВЕННОЕ ПРАВО
Государственные
Конституция
Законы (кодексы)
Указы
Постановления
Ведомственные
Приказы
Руководства
Положения
Инструкции

К *нормативно-правовым* мерам защиты относятся действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей.

Нормативно-правовые меры направлены на решение следующих вопросов:

- отнесение информации к категориям открытого и ограниченного доступа;
- определение полномочий по доступу к информации;
- права должностных лиц на установление и изменение полномочий;
- способы и процедуры доступа;
- порядок контроля, документирования и анализа действий персонала;
- ответственность за нарушение установленных требований и правил;
- проблема доказательства вины нарушителя;
- соответствующие карательные санкции.

В настоящее время защита секретной информации в автоматизированных системах осуществляется Федеральной службой по техническому и экспортному контролю *(ФСТЭК), созданной по Указу Президента РФ от 09.03.2004 г. № 314 «О системе и структуре федеральных органов исполнительной власти».*

Важнейшие законодательные нормативно-правовые документы разработаны с учетом следующих видов тайн:

- *государственная тайна* – Закон о государственной тайне, ст. 275, 276, 283, 284 УК РФ;
- *служебная и коммерческая тайна* – ст. 139 и 727 ГК РФ, ст. 155 и 183 УК РФ;
- *банковская тайна* – ст. 25 Закона о банках и банковской деятельности в РСФСР, ст. 857 ГК, ст. 183 УК РФ;
- *личная и семейная тайна* – ст. 150 ГК, ст. 137 УК РФ;
- *тайна переписки и телефонных переговоров* – ст. 138 УК РФ;
- *тайна голосования* - ст. 142 УК РФ.

Основополагающими документами по информационной безопасности в РФ являются

- ✓ *Конституция РФ (создана 12 декабря 1993 года, вступила в силу с 25 декабря 1993 года. Действующая редакция: от 6 октября 2022 года)*

и

- ✓ *Стратегии национальной безопасности РФ (№ 400 от 02.07.2021г.).*

Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации

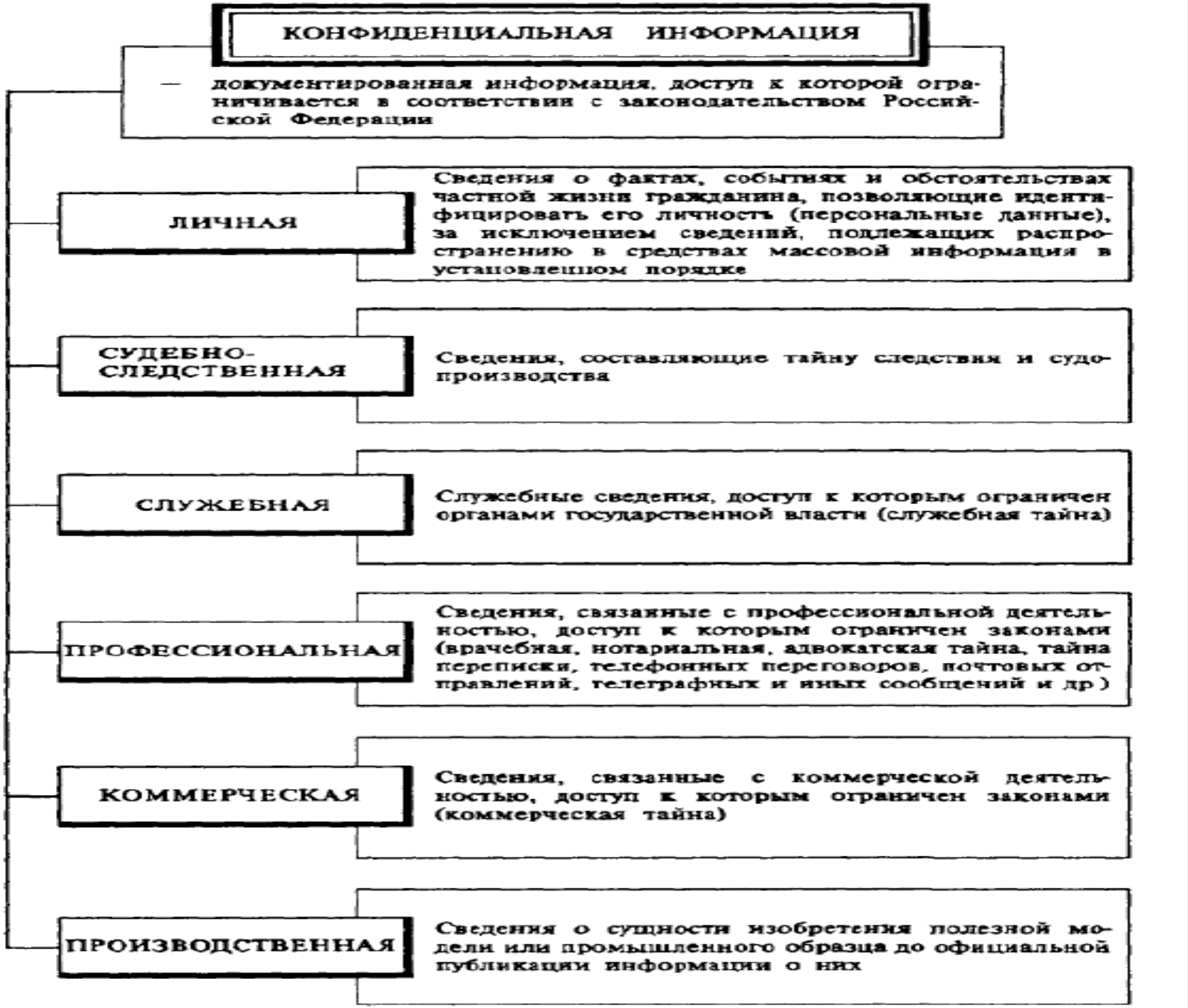
1) Закон Российской Федерации от 21 июля 1993 года №5485-1 «О государственной тайне» с изменениями и дополнениями, внесенными после его принятия, регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации

2) Закон РФ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года №149-ФЗ – является одним из основных базовых законов в области защиты информации, который регламентирует отношения, возникающие при формировании и использовании информационных ресурсов Российской Федерации на основе сбора, накопления, хранения, распространения и предоставления потребителям документированной информации, а также при создании и использовании информационных технологий, при защите информации и прав субъектов, участвующих в информационных процессах и информатизации.

Закон определяет пять категорий государственных информационных ресурсов:

- открытая общедоступная информация во всех областях знаний и деятельности;
- информация с ограниченным доступом;
- информация, отнесенная к государственной тайне;
- конфиденциальная информация (коммерческую тайна, профессиональная тайна, служебная тайна или иная тайна);
- персональные данные о гражданах (относятся к категории конфиденциальной информации, но регламентируются отдельным законом).


КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ
— документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации
ЛИЧНАЯ
Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленном порядке
СУДЕБНО-СЛЕДСТВЕННАЯ
Сведения, составляющие тайну следствия и судопроизводства
СЛУЖЕБНАЯ
Служебные сведения, доступ к которым ограничен органами государственной власти (служебная тайна)
ПРОФЕССИОНАЛЬНАЯ
Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и др.)
КОММЕРЧЕСКАЯ
Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен законами (коммерческая тайна)
ПРОИЗВОДСТВЕННАЯ
Сведения о сущности изобретения полезной модели или промышленного образца до официальной публикации информации о них

СЛУЖЕБНАЯ	Служебные сведения, доступ к которым ограничен органами государственной власти (служебная тайна)
ПРОФЕССИОНАЛЬНАЯ	Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и др.)
КОММЕРЧЕСКАЯ	Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен законами (коммерческая тайна)
ПРОИЗВОДСТВЕННАЯ	Сведения о сущности изобретения полезной модели или промышленного образца до официальной публикации информации о них

ISO/IEC 27799 Информационные технологии для охраны здоровья

Настоящий международный стандарт содержит рекомендации для медицинских организаций и других субъектов, обрабатывающих персональные данные о здоровье, о том, как наилучшим образом защитить конфиденциальность, целостность и доступность такой информации. Стандарт **ISO/IEC 27799** основывается на общих рекомендациях, содержащихся в стандарте ISO/IEC 27002: 2013, и расширяет их, принимая во внимание особые потребности управления информационной безопасностью в секторе здравоохранения и его уникальные операционные среды.

ГОСТ Р ИСО 27799-2015

К *морально-этическим* мерам противодействия угрозам безопасности относятся всевозможные нормы поведения, которые традиционно сложились или складываются в обществе по мере распространения компьютеров в стране. Эти нормы большей частью не являются обязательными, как законодательно утвержденные, но их несоблюдение обычно ведет к падению престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаными (например, общепризнанные нормы честности, патриотизма и т.д.), так и оформленными в некий свод (кодекс) правил или предписаний.

Например, "Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США" рассматривает как неэтичные действия, которые умышленно или неумышленно:

- нарушают нормальную работу компьютерных систем;
- вызывают неоправданные затраты ресурсов (машинного времени, памяти, каналов связи и т.п.);
- нарушают целостность информации (хранимой и обрабатываемой);
- нарушают интересы других законных пользователей и т.п.

Ответственность за нарушения, в частности в сфере информационной безопасности

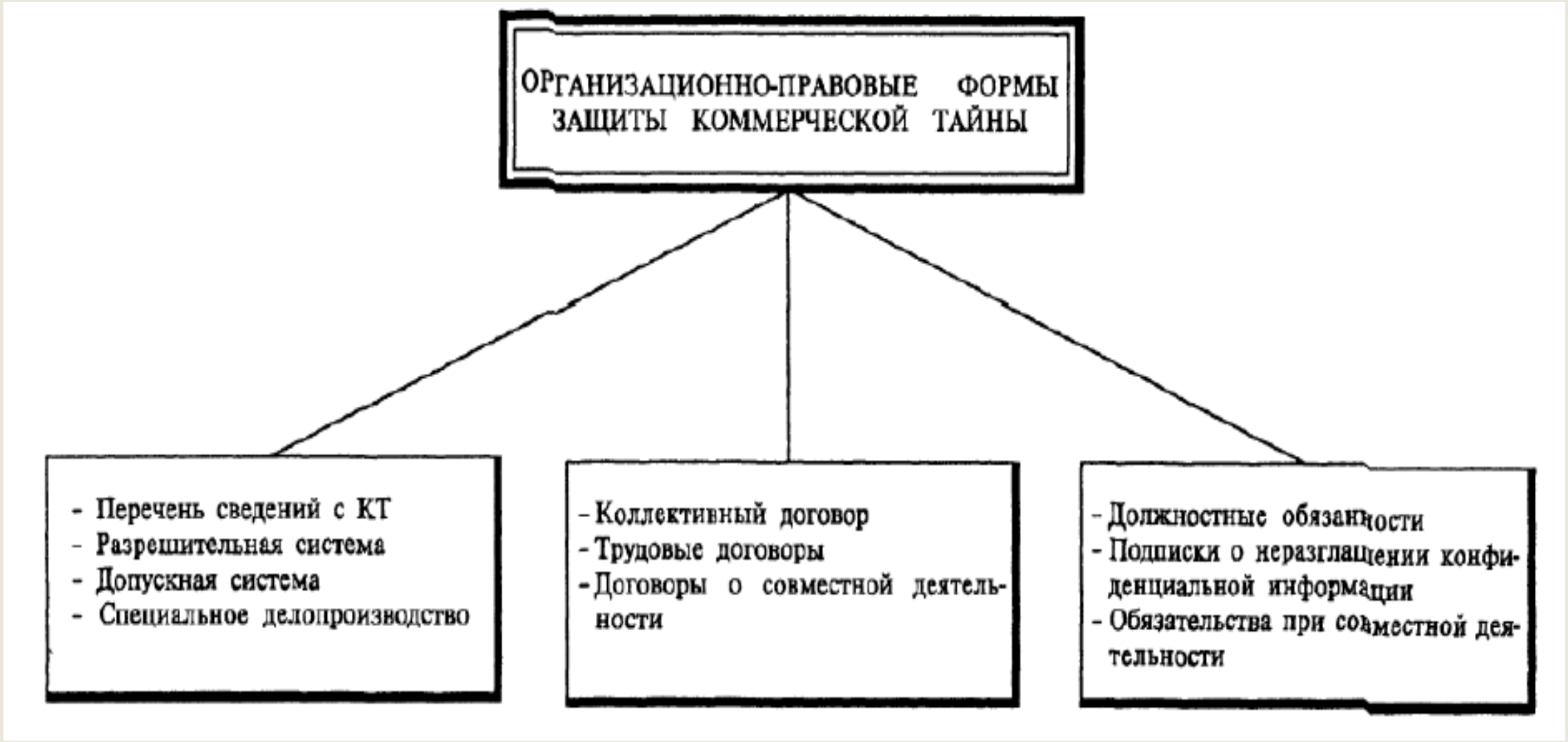
Основными документами в этом направлении являются:

- Уголовный кодекс Российской Федерации (от 13.06.1996 № 63-ФЗ (ред. от 04.08.2023));
- Кодекс Российской Федерации об административных правонарушениях (от 30.12.2001 № 195-ФЗ (ред. от 04.08.2023) (с изм. и доп., вступ. в силу с 01.10.2023).).

Организационная защита — это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

Организационная защита обеспечивает:

- ✓ организацию охраны, режима, работу с кадрами, с документами;
- ✓ использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности.


ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ФОРМЫ ЗАЩИТЫ КОММЕРЧЕСКОЙ ТАЙНЫ
- Перечень сведений с КТ
- Разрешительная система
- Допускная система
- Специальное делопроизводство
- Коллективный договор
- Трудовые договоры
- Договоры о совместной деятельности
- Должностные обязанности
- Подписки о неразглашении конфиденциальной информации
- Обязательства при совместной деятельности

РАЗДЕЛ 6. АДМИНИСТРАТИВНЫЙ УРОВЕНЬ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Если есть угроза — должны быть и средства защиты и противодействия.

Административный уровень является промежуточным между законодательно-правовым и программно-техническим уровнями формирования режима информационной безопасности.

Законы и стандарты в области информационной безопасности являются лишь отправным нормативным базисом информационной безопасности. Основой практического построения комплексной системы безопасности является административный уровень, определяющий главные направления работ по защите информационных систем.

Административные меры защиты - это меры организационного характера. Они регламентируют:

- процессы функционирования системы обработки данных,
- использование ее ресурсов,
- деятельность персонала,
- порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности.

Административные меры включают:

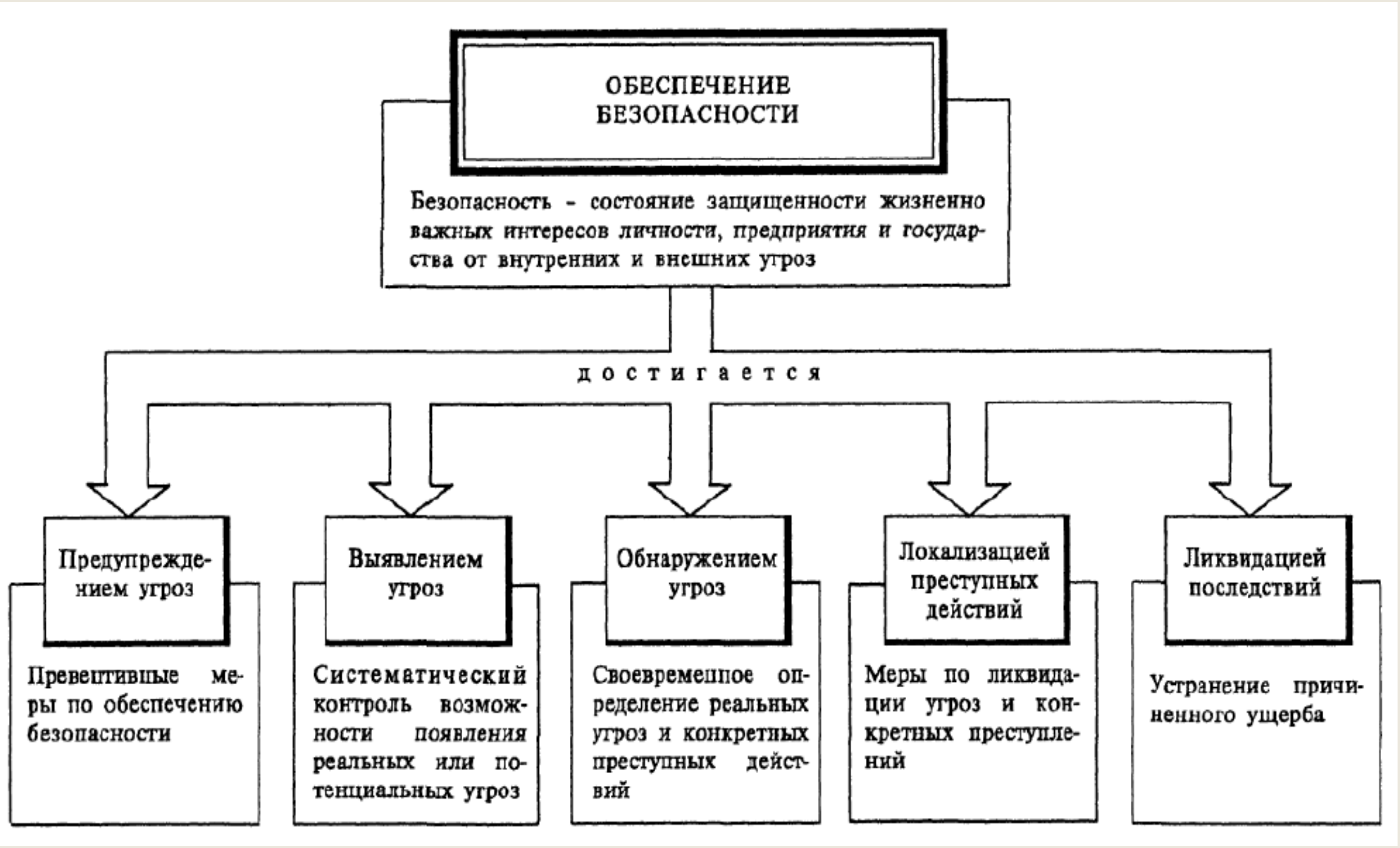
- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов систем обработки данных;
- мероприятия по разработке правил доступа пользователей к ресурсам системы (разработка политики безопасности);
- мероприятия, осуществляемые при подборе и подготовке персонала системы;
- организацию охраны и надежного пропускного режима;
- организацию учета, хранения, использования и уничтожения документов и носителей с информацией;
- распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.);
- организацию явного и скрытого контроля за работой пользователей;
- мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и программного обеспечения и т.п.

Целью административного уровня является разработка программы работ в области информационной безопасности и обеспечение ее выполнения в конкретных условиях функционирования информационной системы.

Задачей административного уровня является разработка и реализация практических мероприятий по созданию системы информационной безопасности учитывающей особенности защищаемых информационных систем.

Содержанием административного уровня являются следующие мероприятия:

- разработка политики безопасности;
- проведение анализа угроз и расчета рисков;
- выбор механизмов и средств обеспечения информационной безопасности.


ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ
Безопасность - состояние защищенности жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз
достигается
Предупреждением угроз
Превентивные меры по обеспечению безопасности
Выявлением угроз
Систематический контроль возможности появления реальных или потенциальных угроз
Обнаружением угроз
Своевременное определение реальных угроз и конкретных преступных действий
Локализацией преступных действий
Меры по ликвидации угроз и конкретных преступлений
Ликвидацией последствий
Устранение причиненного ущерба

Разработка политики информационной безопасности

Политика безопасности – это комплекс предупредительных мер по обеспечению информационной безопасности организации. Политика безопасности включает правила, процедуры и руководящие принципы в области безопасности, которыми руководствуется организация в своей деятельности. Кроме этого, политика безопасности включает в себя требования в адрес субъектов информационных отношений, при этом в политике безопасности излагается политика ролей субъектов информационных отношений.


Информационная безопасность – невозможность нанесения вреда свойствам объекта безопасности, обуславливаемым информацией и информационной инфраструктурой (защищенность от угроз)
Политика безопасности
Объект информационной безопасности
Угрозы объекту информационной безопасности
Обеспечение информационной безопасности
Методы обеспечения информационной безопасности
Деятельность по обеспечению информационной безопасности (по недопущению вреда объекту информационной безопасности)
Средства осуществления деятельности по обеспечению информационной безопасности
Субъекты обеспечения информационной безопасности

Разработка политики информационной безопасности

Основные направления разработки политики безопасности:

- определение объема и требуемого уровня защиты данных;
- определение ролей субъектов информационных отношений.

Политика информационной безопасности является методологической основой практических мер по обеспечению информационной безопасности и включает следующие группы сведений:

- основные положения информационной безопасности организации;
- область применения политики безопасности;
- цели и задачи обеспечения информационной безопасности организации;
- распределение ролей и ответственности субъектов информационных отношений организации и их общие обязанности.

В состав автоматизированной информационной системы входят следующие компоненты:

- **аппаратные средства** – компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства – дисководы, принтеры, контроллеры), кабели, линии связи и пр.;
- **программное обеспечение** – приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и пр.;
- **данные** – хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и пр.;
- **персонал** – обслуживающие сотрудники и пользователи.

Обеспечения информационной безопасности разграничение прав и обязанностей целесообразно провести по следующим группам (ролям):

- специалист по информационной безопасности;
- владелец информации;
- поставщики аппаратного и программного обеспечения;
- менеджер отдела;
- операторы;
- аудиторы.

Политики безопасности должны:

- указывать цели и причины, по которым нужна политика;
- описывать, что именно охватывается этими политиками;

определить роли, обязанности и контакты;

- определить, как будут обрабатываться нарушения безопасности;

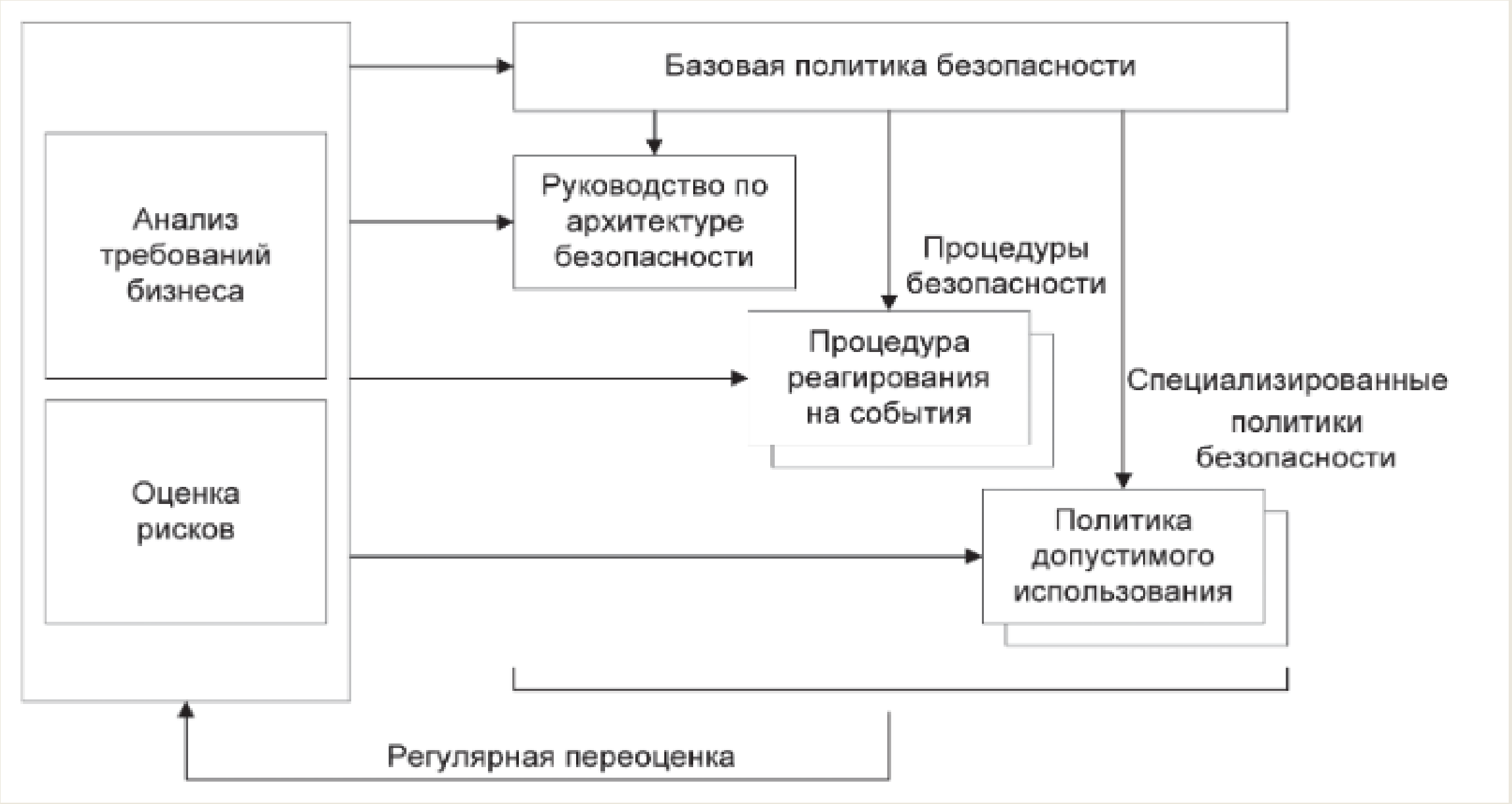
Политики безопасности должны быть:

- реальными и осуществимыми;
- краткими и доступными для понимания;
- сбалансированными по защите и производительности.

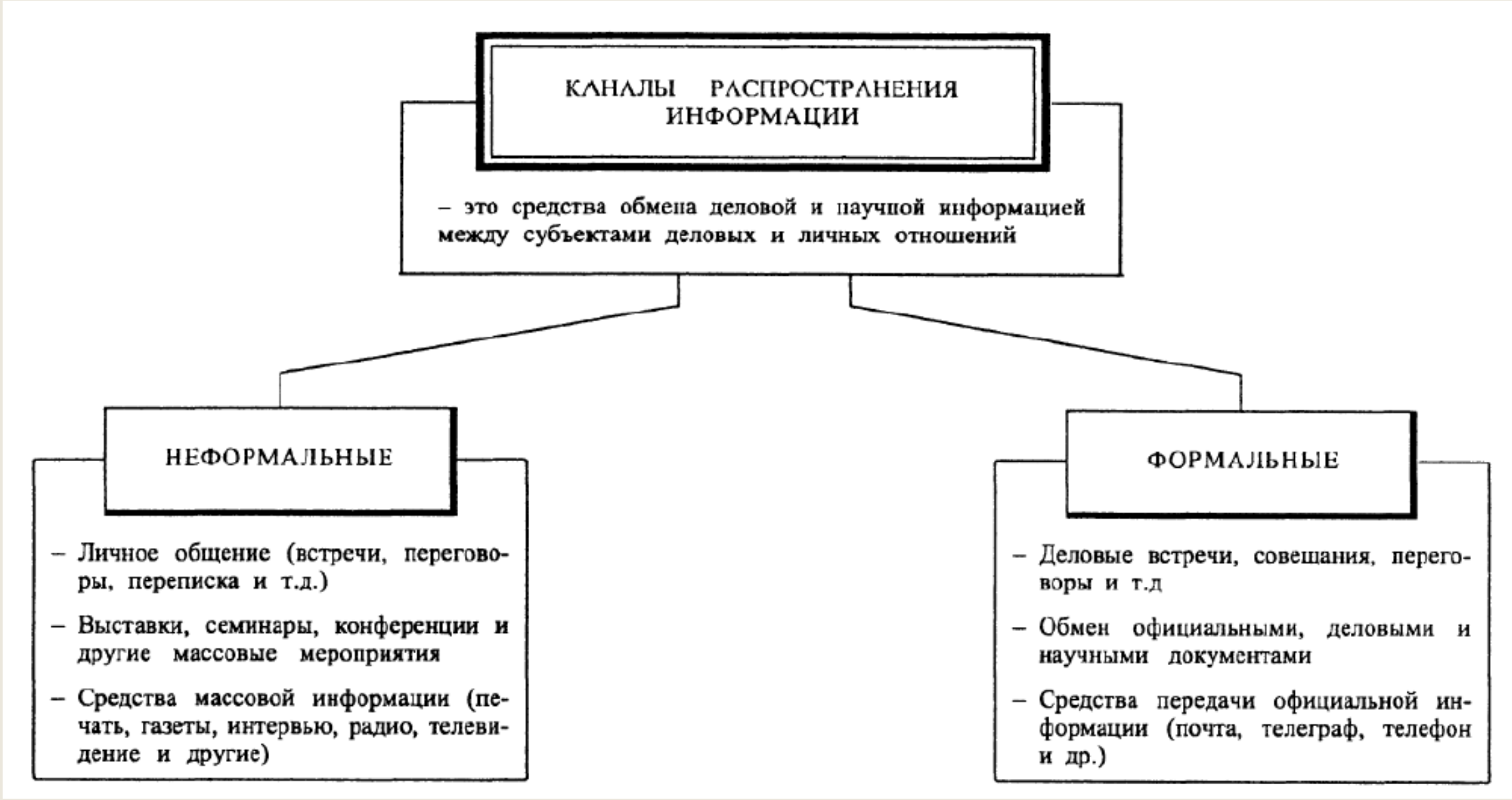
Первыми шагами по разработке политики безопасности являются следующие:

- создание команды по разработке политики;
- принятие решения об области действия и целях политики;
- принятие решения об особенностях разрабатываемой политики;
- определение лица или органа для работы в качестве официального интерпретатора политики.

Схема разработки политики безопасности



Классы угроз информационной безопасности



Классы угроз информационной безопасности

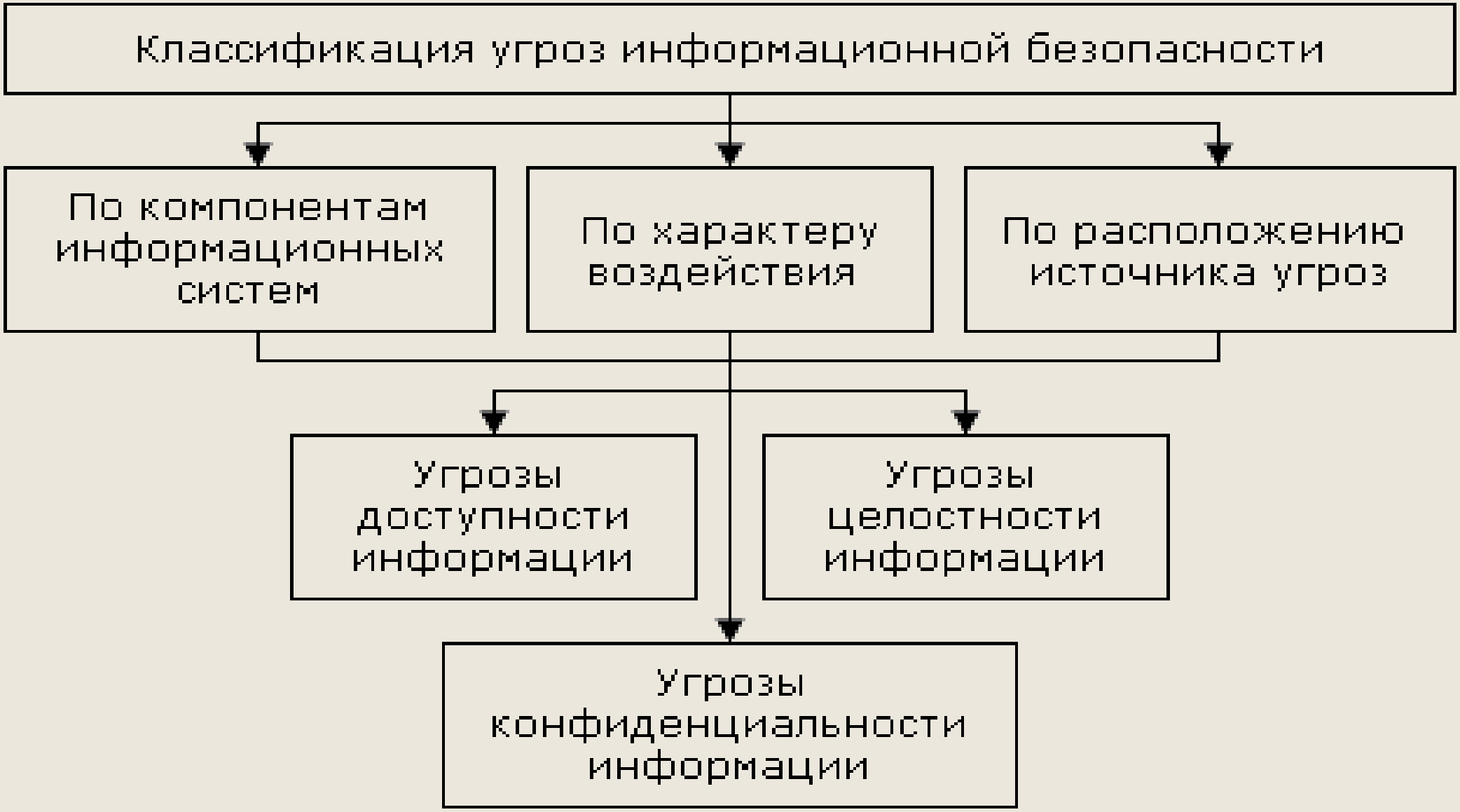
Угроза информационной безопасности – это потенциальная возможность нарушения режима информационной безопасности. Преднамеренная реализация угрозы называется атакой на информационную систему. Лица, преднамеренно реализующие угрозы, являются злоумышленниками.

Классы угроз информационной безопасности

По признакам:

- по составляющим информационной безопасности (доступность, целостность, конфиденциальность), против которых, в первую очередь, направлены угрозы;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, персонал);
- по характеру воздействия (случайные или преднамеренные, действия природного или техногенного характера);
- по расположению источника угроз (внутри или вне рассматриваемой информационной системы).

Классы угроз информационной безопасности



Каналы несанкционированного доступа к информации

Каналы НСД классифицируются по компонентам автоматизированных информационных систем:

Через человека:

- хищение носителей информации;
- чтение информации с экрана или клавиатуры;
- чтение информации из распечатки.

Каналы несанкционированного доступа к информации

Каналы НСД классифицируются по компонентам автоматизированных информационных систем:

Через программу:

- перехват паролей;
- расшифровка зашифрованной информации;
- копирование информации с носителя.

Каналы несанкционированного доступа к информации

Каналы НСД классифицируются по компонентам автоматизированных информационных систем:

Через аппаратуру:

- подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации;
- перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и пр.

ИНЖЕНЕРНО ТЕХНИЧЕСКАЯ ЗАЩИТА

Организационные меры являются решающим звеном формирования и реализации комплексной защиты информации и создания системы безопасности предприятия.

Инженерно-техническая защита (ИТЗ) по определению — это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации.

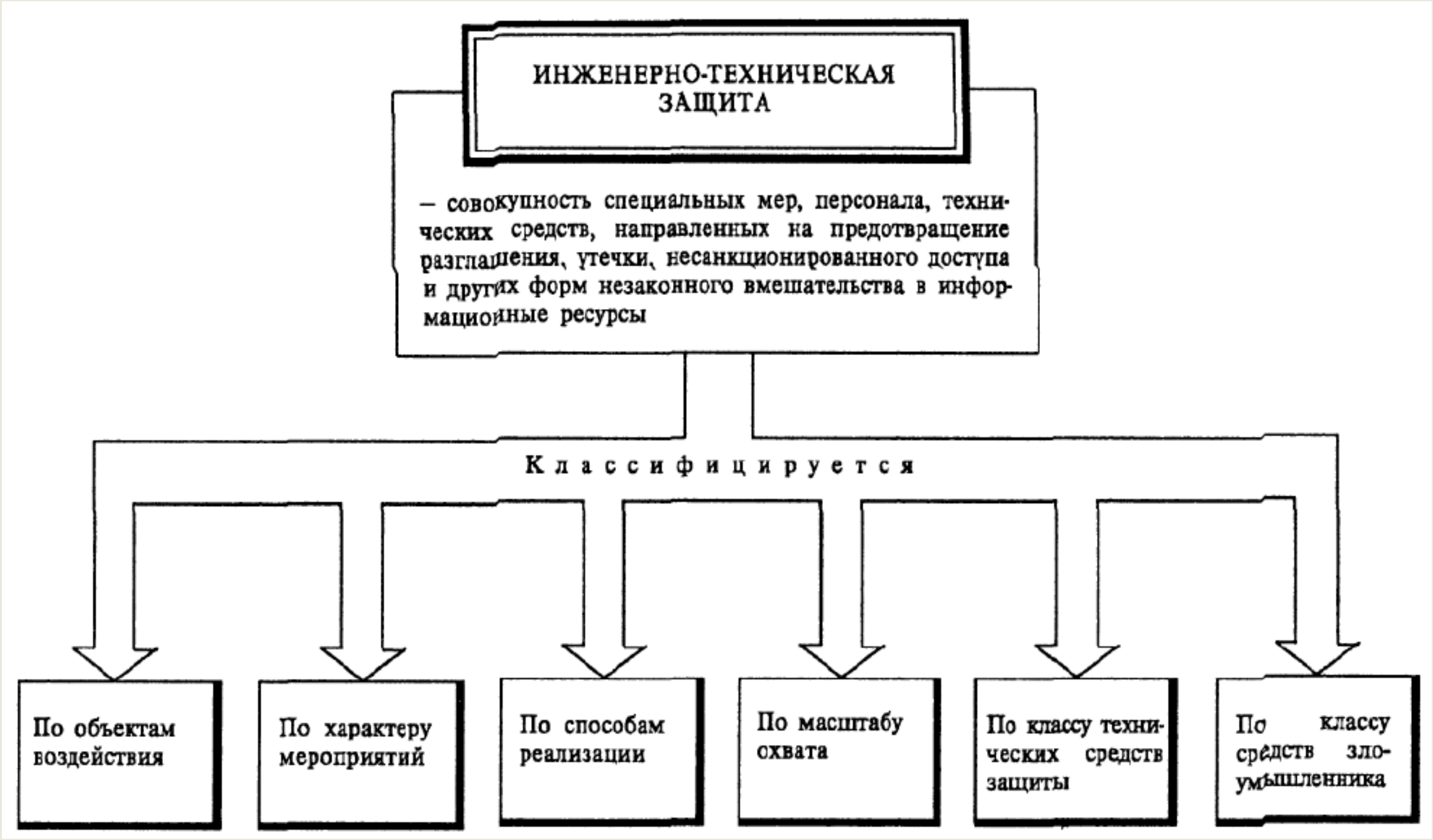
Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, которые самостоятельно или в комплексе с другими средствами, реализуют следующие способы защиты:

- идентификацию (распознавание) и аутентификацию (проверку подлинности) субъектов (пользователей, процессов),
- разграничение доступа к ресурсам,
- регистрацию и анализ событий,
- криптографическое закрытие информации,
- резервирование ресурсов и компонентов систем обработки информации и др.

Программные меры защиты основаны на использовании антивирусных средств.


КЛАССИФИКАЦИЯ
ИТЗ по используемым средствам
ФИЗИЧЕСКИЕ
Устройства, инженерные сооружения и организационные меры, затрудняющие или исключающие проникновение злоумышленников к источникам конфиденциальной информации
АППАРАТНЫЕ
Механические, электрические, электронные и др. устройства, предназначенные для защиты информации от утечки и разглашения и противодействия техническим средствам промышленного шпионажа
ПРОГРАММНЫЕ
Система специальных программ, включаемых в состав общего и специального обеспечения, реализующих функции защиты информации и сохранения целостности и конфиденциальности
КРИПТОГРАФИЧЕСКИЕ
Технические и программные средства шифрования
КОМБИНИРОВАННЫЕ
Совокупная реализация аппаратных и программных средств и криптографических методов защиты информации


ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА
– совокупность специальных мер, персонала, технических средств, направленных на предотвращение разглашения, утечки, несанкционированного доступа и других форм незаконного вмешательства в информационные ресурсы
Классифицируется
По объектам воздействия
По характеру мероприятий
По способам реализации
По масштабу охвата
По классу технических средств защиты
По классу средств злоумышленника

Взаимосвязь перечисленных мер обеспечения безопасности можно пояснить следующим образом:

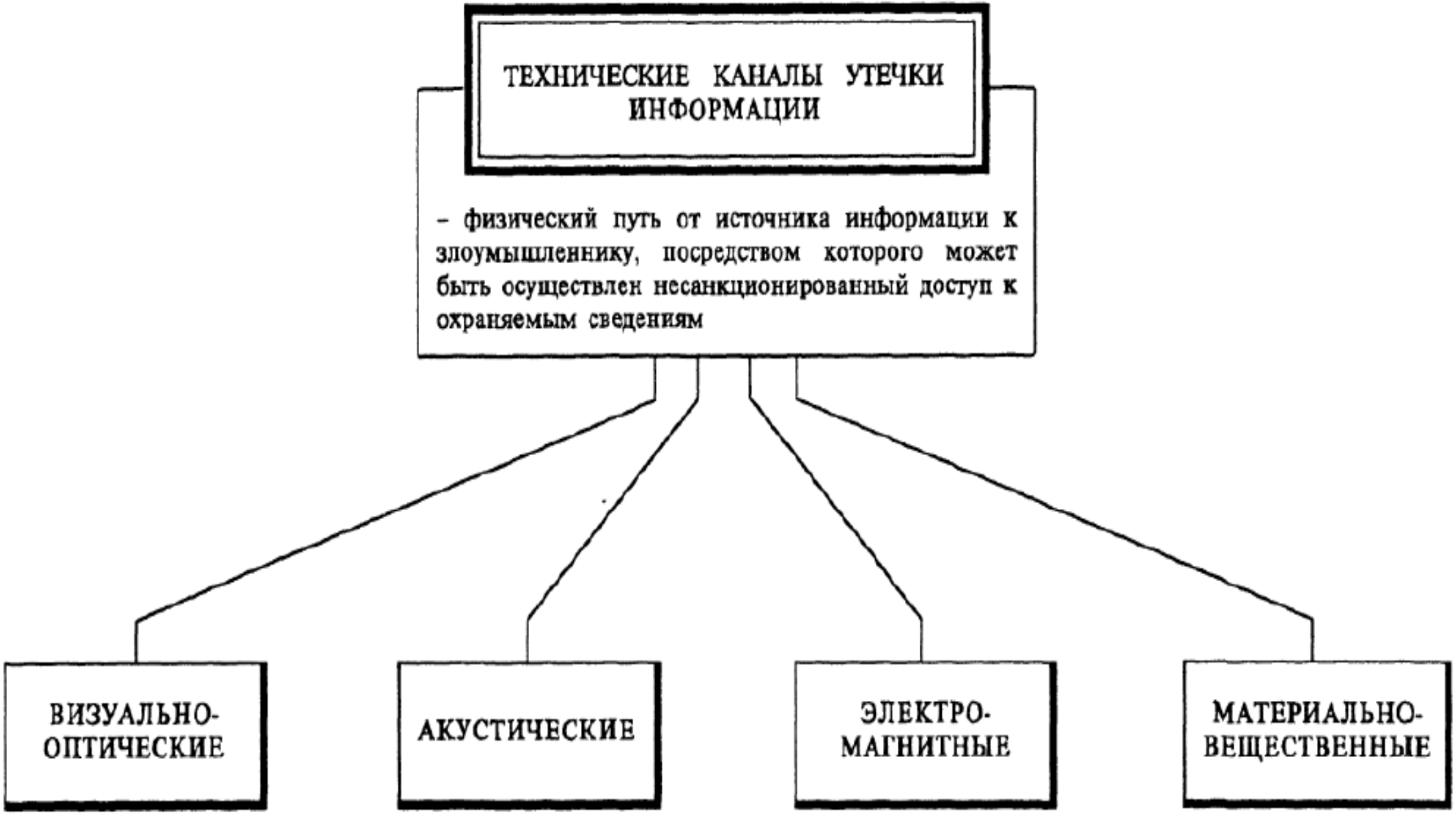
1. Организационные меры обеспечивают исполнение существующих нормативных актов и строятся с учетом существующих правил поведения, принятых в стране и/или организации.
2. Воплощение организационных мер требует создания нормативных документов.
3. Для эффективного применения организационные меры должны быть поддержаны физическими и техническими средствами.
4. Применение и использование технических средств защиты требует соответствующей организационной поддержки.

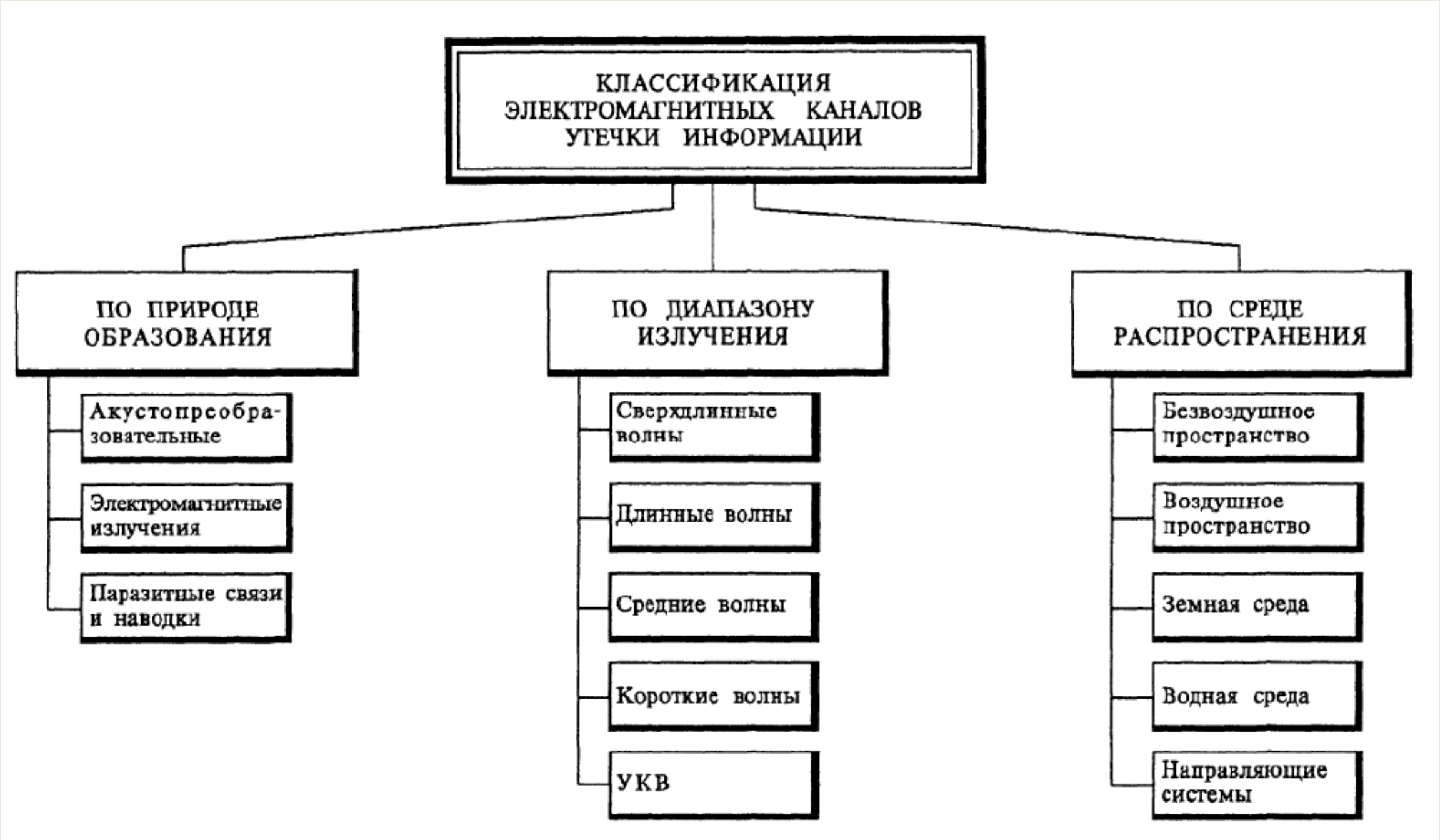
РАЗДЕЛ 5. ПРОБЛЕМАТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

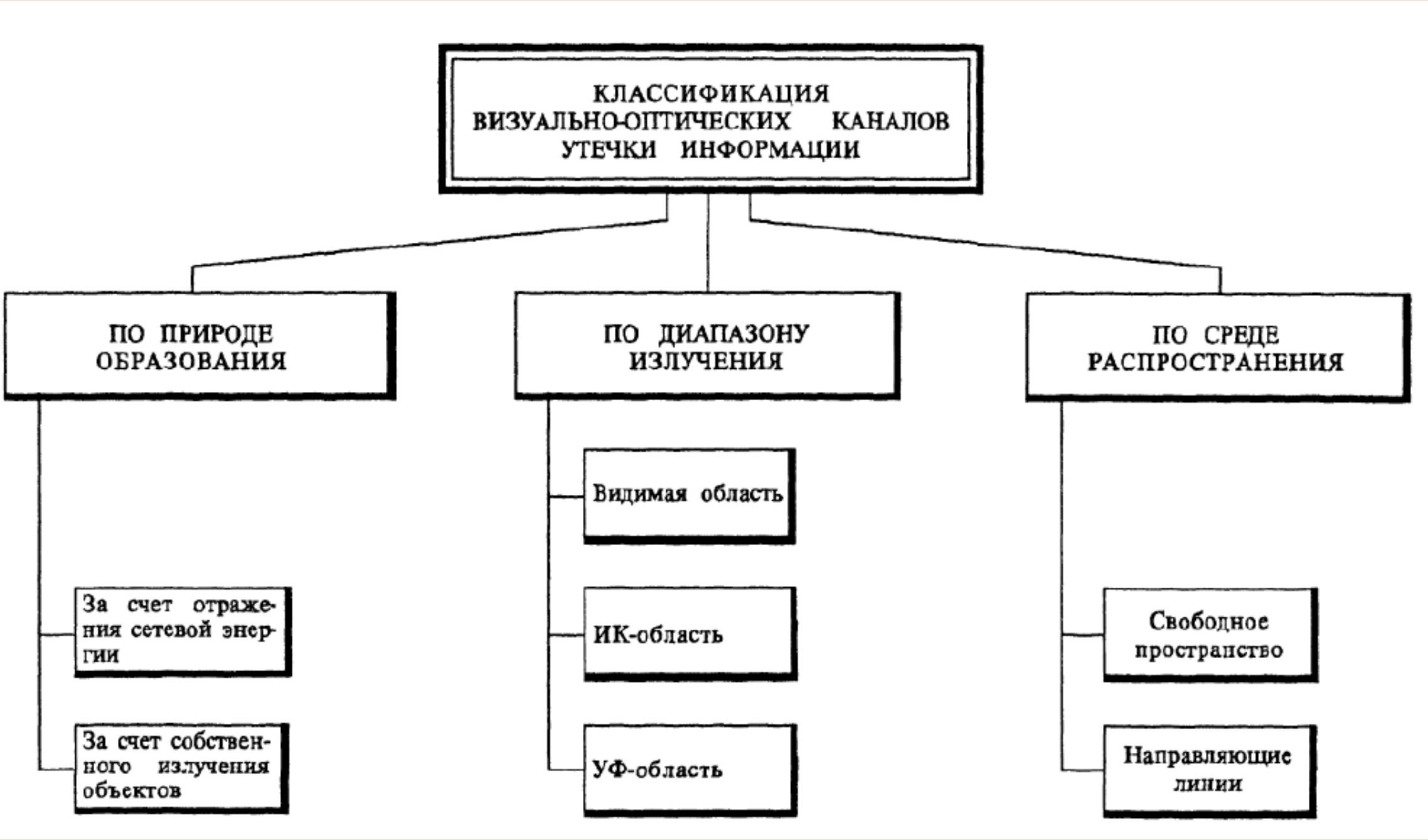
Защита информации от утечки по техническим каналам *— это комплекс организационных, организационно-технических и технических мероприятий, исключающих или ослабляющих бесконтрольный выход конфиденциальной информации за пределы контролируемой зоны.*

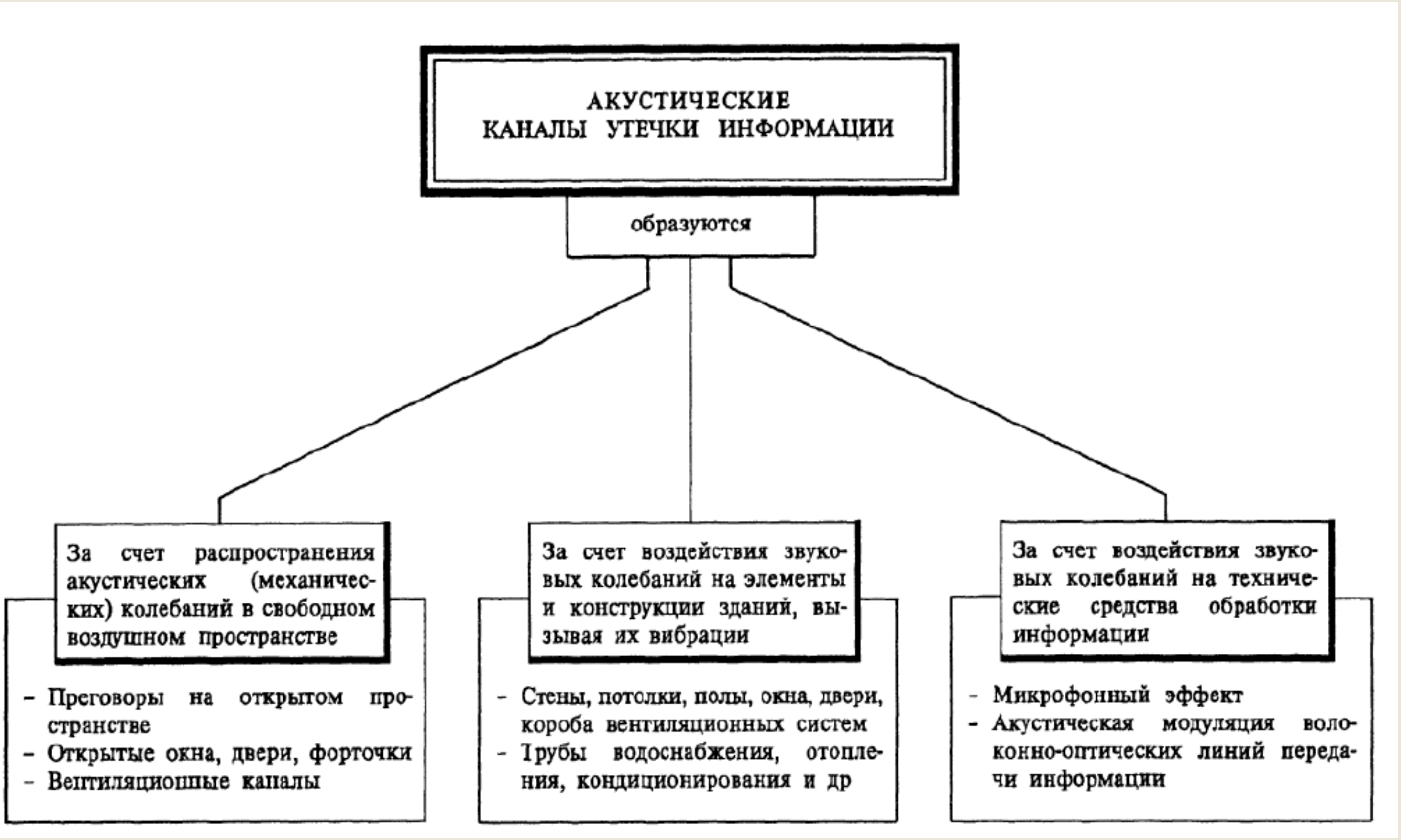
Под ***каналом утечки информации*** будем понимать физический путь от источника конфиденциальной информации к злоумышленнику, по которому возможна утечка или несанкционированное получение охраняемых сведений.

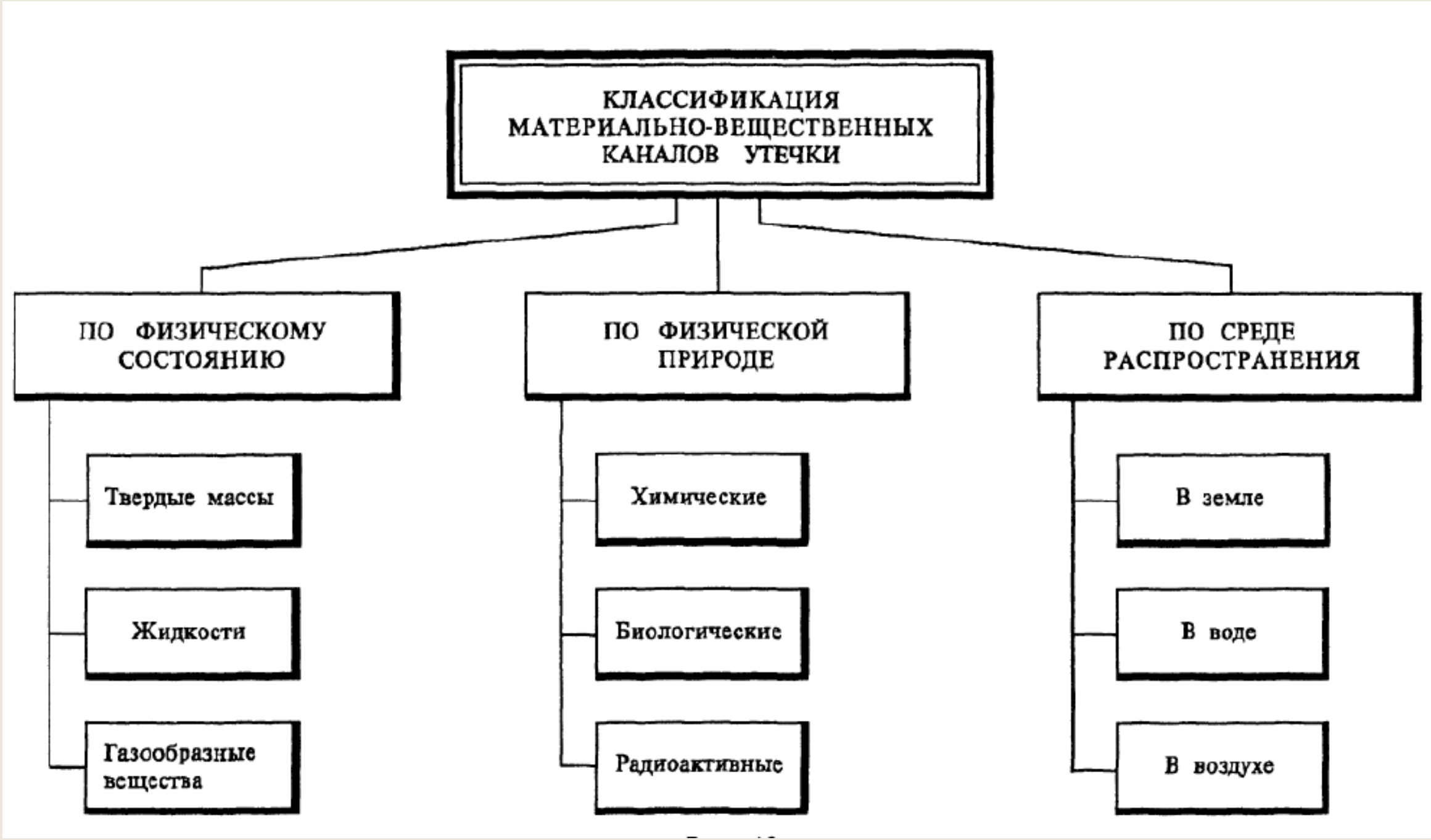

УТЕЧКА
Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена
Образуется за счет неконтроли-руемых физических полей
АКУСТИЧЕСКИХ
СВЕТОВЫХ
ЭЛЕКТРО-МАГНИТНЫХ
РАДИАЦИОННЫХ, ТЕПЛОВЫХ и др.


ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ
– физический путь от источника информации к злоумышленнику, посредством которого может быть осуществлен несанкционированный доступ к охраняемым сведениям
ВИЗУАЛЬНО-ОПТИЧЕСКИЕ
АКУСТИЧЕСКИЕ
ЭЛЕКТРО-МАГНИТНЫЕ
МАТЕРИАЛЬНО-ВЕЩЕСТВЕННЫЕ


КЛАССИФИКАЦИЯ ЭЛЕКТРОМАГНИТНЫХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ
ПО ПРИРОДЕ ОБРАЗОВАНИЯ
Акустопрсобразовательные
Электромагнитные излучения
Паразитные связи и наводки
ПО ДИАПАЗОНУ ИЗЛУЧЕНИЯ
Сверхдлинные волны
Длинные волны
Средние волны
Короткие волны
УКВ
ПО СРЕДЕ РАСПРОСТРАНЕНИЯ
Безвоздушное пространство
Воздушное пространство
Земная среда
Водная среда
Направляющие системы


КЛАССИФИКАЦИЯ ВИЗУАЛЬНО-ОПТИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ
ПО ПРИРОДЕ ОБРАЗОВАНИЯ
ПО ДИАПАЗОНУ ИЗЛУЧЕНИЯ
ПО СРЕДЕ РАСПРОСТРАНЕНИЯ
За счет отражения сетевой энергии
За счет собственного излучения объектов
Видимая область
ИК-область
УФ-область
Свободное пространство
Направляющие линии


АКУСТИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ
образуются
За счет распространения акустических (механических) колебаний в свободном воздушном пространстве
- Преговоры на открытом пространстве
- Открытые окна, двери, форточки
- Вентиляционные каналы
За счет воздействия звуковых колебаний на элементы и конструкции зданий, вызывая их вибрации
- Стены, потолки, полы, окна, двери, короба вентиляционных систем
- Трубы водоснабжения, отопления, кондиционирования и др
За счет воздействия звуковых колебаний на технические средства обработки информации
- Микрофонный эффект
- Акустическая модуляция волоконно-оптических линий передачи информации


КЛАССИФИКАЦИЯ МАТЕРИАЛЬНО-ВЕЩЕСТВЕННЫХ КАНАЛОВ УТЕЧКИ
ПО ФИЗИЧЕСКОМУ СОСТОЯНИЮ
ПО ФИЗИЧЕСКОЙ ПРИРОДЕ
ПО СРЕДЕ РАСПРОСТРАНЕНИЯ
Твердые массы
Жидкости
Газообразные вещества
Химические
Биологические
Радиоактивные
В земле
В воде
В воздухе

Защита информации от утечки по техническим каналам в общем плане сводится к следующим действиям:

1. Своевременному определению возможных каналов утечки информации.

2. Определению энергетических характеристик канала утечки на границе контролируемой зоны (территории, кабинета).

3. Оценке возможности средств злоумышленников обеспечить контроль этих каналов.

4. Обеспечению исключения или ослабления энергетики каналов утечки соответствующими организационными, организационно-техническими или техническими мерами и средствами.

При защите информации от утечки по любому из рассмотренных каналов следует придерживаться следующего порядка действий:

1. Выявление возможных каналов утечки.
2. Обнаружение реальных каналов.
3. Оценка опасности реальных каналов.
4. Локализация опасных каналов утечки информации.
5. Систематический контроль за наличием каналов и качеством их защиты.

ПОДХОДЫ К ФОРМИРОВАНИЮ ЗАЩИЩЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

РАЗДЕЛ 7. СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РФ

ФСТЭК и ее роль в обеспечении информационной безопасности в РФ

п/п	Наименование
1.	Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссии России от 30.03.1992
2.	Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утвержден решением председателя Гостехкомиссии России от 30.03.1992
3.	Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. Утвержден решением председателя Гостехкомиссии России от 30.03.1992
4.	Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссии России от 30.03.1992

п/п	Наименование
5.	Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден решением председателя Гостехкомиссии России от 30.03.1992
6.	Положение о сертификации средств защиты информации по требованиям безопасности информации. Утверждено приказом председателя Гостехкомиссии России от 27.10.1995 N 199
7.	Руководящий документ. Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден приказом Гостехкомиссии России от 04.06.1999 N 114
8.	Специальные требования и рекомендации по технической защите конфиденциальной информации. Утверждены приказом Гостехкомиссии России от 02.03.2001 N 282.ДСП

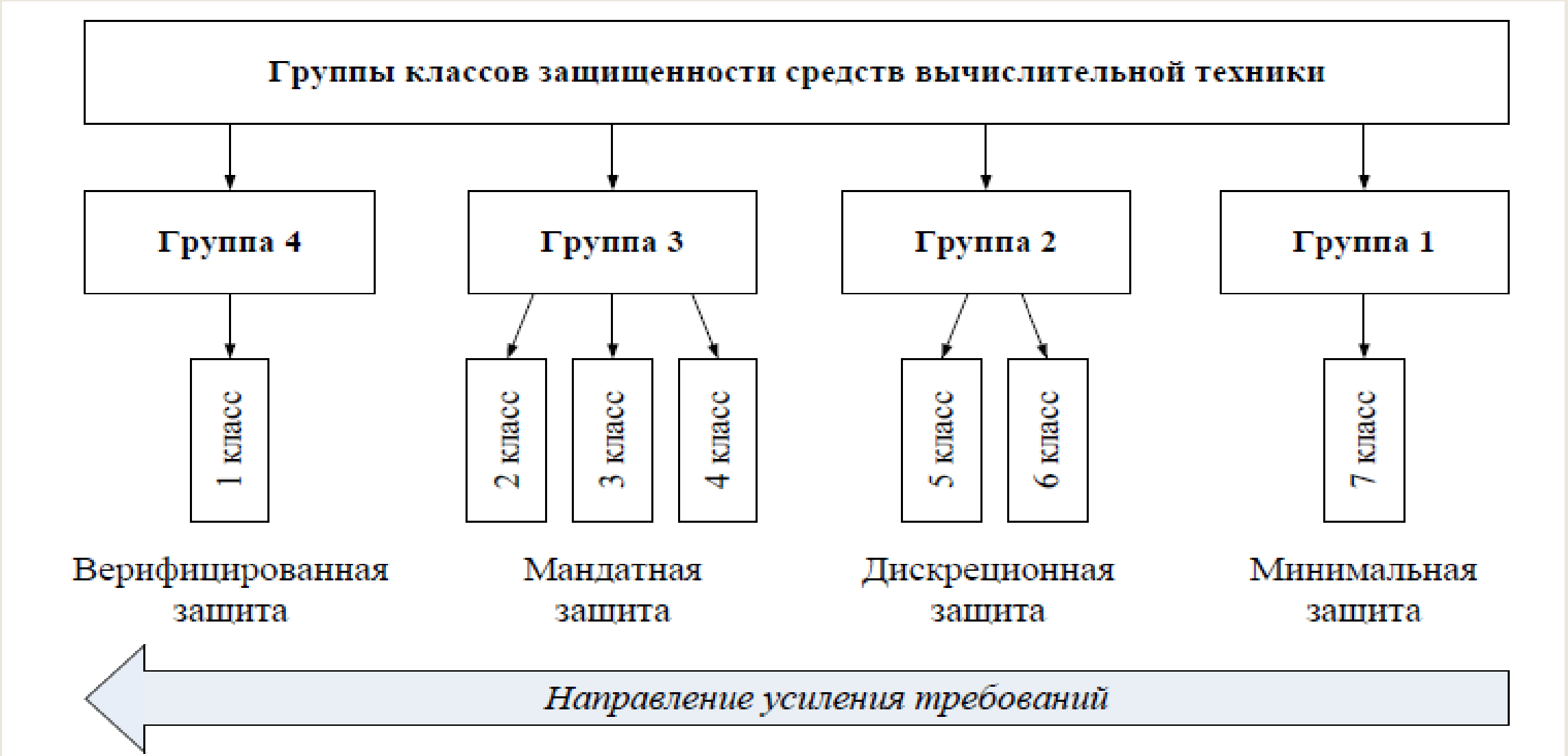
п/п	Наименование
9.	Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.ДСП
10.	Временная методика оценки защищенности конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.ДСП
11.	Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.ДСП

п/п	Наименование
12.	Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электро-акустических преобразований во вспомогательных технических средствах и системах. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.ДСП
13.	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 15.02.2008.ДСП
14.	Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 06.12.2011 N 638.ДСП
15.	Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи. Утвержден приказом ФСТЭК России от 15.03.2012 N 27.ДСП
16.	Требования к средствам антивирусной защиты. Утверждены приказом ФСТЭК России от 20.03.2012 N 28.ДСП

п/п	Наименование
17.	Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11.02.2013 N 17
18.	Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18.02.2013 N 21
19.	Требования к средствам доверенной загрузки. Утверждены приказом ФСТЭК России от 27.09.2013 N 119.ДСП
20.	Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11.02.2014

п/п	Наименование
21.	Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Утверждены приказом ФСТЭК России от 14.03.2014 N 31
22.	Требования к средствам контроля съемных машинных носителей информации. Утверждены приказом ФСТЭК России от 28.07.2014 N 87.ДСП
23.	Требования к межсетевым экранам. Утверждены приказом ФСТЭК России от 09.02.2016 N 9.ДСП
24.	Требованиям безопасности информации к операционным системам, утвержденным приказом ФСТЭК России от 19.08.2016 г. N 119.ДСП
25.	ГОСТ РО 0043-003-2012 Защита информации. Аттестация объектов информатизации. Общие положения. ДСП
26.	ГОСТ РО 0043-004-2013 Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний. ДСП

Документы по оценке защищенности автоматизированных систем в РФ



Документы по оценке защищенности автоматизированных систем в РФ

Самый низкий класс – седьмой, самый высокий – первый. Классы подразделяются на четыре группы, отличающиеся уровнем защиты:

- первая группа содержит только один седьмой класс, к которому относят все СВТ, не удовлетворяющие требованиям более высоких классов;
- вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- четвертая группа характеризуется верифицированной защитой и включает только первый класс.

Документы по оценке защищенности автоматизированных систем в РФ

К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- режим обработки данных в АС – коллективный или индивидуальный.

Третья группа

АС, в которых работает ***один пользователь***, допущенный ***ко всей информации*** АС, размещенной на носителях одного уровня конфиденциальности

3 А
информация,
составляющая гостайну

3 Б
служебная тайна
или персональные данные

Вторая группа

АС, в которых ***пользователи имеют одинаковые права доступа*** (полномочия) ***ко всей информации*** АС, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности

2 А
информация,
составляющая гостайну

2 Б
служебная тайна
или персональные данные

Первая группа

многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация ***разных уровней конфиденциальности*** и ***не все*** пользователи ***имеют право доступа ко всей информации*** АС

1 А **1 Б** **1 В** **1 Г** **1 Д**

АС, в которых циркулирует информация, составляющая гостайну: 1А, 1Б и 1В.

1 В - в случае обработки секретной информации с грифом не выше «секретно»
1 Б - в случае обработки секретной информации с грифом не выше «совершенно секретно»
1 А - в случае обработки секретной информации с грифом «особая важность»
1 Г - АС, в которых циркулирует служебная тайна
1 Д - АС, в которых циркулируют персональные данные

Документы по оценке защищенности автоматизированных систем в РФ

Всего выделяется пять показателей защищенности межсетевых экранов (МЭ):

- управление доступом;
- идентификация и аутентификация;
- регистрация событий и оповещение;
- контроль целостности;
- восстановление работоспособности.

Документы по оценке защищенности автоматизированных систем в РФ

На основании показателей защищенности определяются следующие пять классов защищенности МЭ:

- простейшие фильтрующие маршрутизаторы – 5 класс;
- пакетные фильтры сетевого уровня – 4 класс;
- простейшие МЭ прикладного уровня – 3 класс;
- МЭ базового уровня – 2 класс;
- продвинутые МЭ – 1 класс.

РАЗДЕЛ 7. СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РФ

Требования безопасности к информационным системам

Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» относится к оценочным стандартам.

Как и «Оранжевая книга», «Общие критерии» содержат два основных вида требований безопасности:

- функциональные – соответствуют активному аспекту защиты – предъявляемые к функциям безопасности и реализующим их механизмам;
- требования доверия – соответствуют пассивному аспекту – предъявляемые к технологии и процессу разработки и эксплуатации.

Угрозы безопасности в стандарте характеризуются следующими параметрами:

- источник угрозы;
- метод воздействия;
- уязвимые места, которые могут быть использованы;
- ресурсы (активы), которые могут пострадать.

Для структуризации пространства требований, в «Общих критериях» введена иерархия класс – семейство – компонент – элемент.

Классы определяют наиболее общую, «предметную» группировку требований (например, функциональные требования подотчетности).

Семейства в пределах класса различаются по строгости и другим тонкостям требований.

Компонент – минимальный набор требований, фигурирующий как целое.

Элемент – неделимое требование.

Все функциональные требования объединены в группы на основе выполняемой ими роли или обслуживаемой цели безопасности.

Всего в «Общих критериях» представлено 11 функциональных классов, 66 семейств, 135 компонентов. Это гораздо больше, чем число аналогичных понятий в «Оранжевой книге».

«Общие критерии» включают следующие классы функциональных требований:

1. Идентификация и аутентификация.
2. Защита данных пользователя.
3. Защита функций безопасности (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов).
4. Управление безопасностью (требования этого класса относятся к управлению атрибутами и параметрами безопасности).
5. Аудит безопасности (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности).
6. Доступ к объекту оценки.
7. Использование ресурсов (требования к доступности информации).
8. Приватность (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных).
9. Криптографическая поддержка (управление ключами).
10. Связь (аутентификация сторон, участвующих в обмене данными).
11. Доверенный маршрут/канал (для связи с сервисами безопасности).

Классы требований доверия безопасности:

1) Разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до реализации).
2) Поддержка жизненного цикла (требования к модели жизненного цикла, включая порядок устранения недостатков и защиту среды разработки).
3) Тестирование.
4) Оценка уязвимостей (включая оценку стойкости функций безопасности).
5) Поставка и эксплуатация.
6) Управление конфигурацией.
7) Руководства (требования к эксплуатационной документации).
8) Поддержка доверия (для поддержки этапов жизненного цикла после сертификации).
9) Оценка профиля защиты.
10) Оценка задания по безопасности.

Форма представления требований доверия, та же, что и для функциональных требований (класс – семейство – компонент).

Всего в «Общих критериях» 10 классов, 44 семейства, 93 компонента требований доверия безопасности.

Применительно к требованиям доверия (для функциональных требований не предусмотрены) в «Общих критериях» введены оценочные уровни доверия (их семь), содержащие осмысленные комбинации компонентов.

Степень доверия возрастает от первого к седьмому уровню. Так, оценочный уровень доверия 1 (начальный) применяется, когда угрозы не рассматриваются как серьезные, а оценочный уровень 7 применяется к ситуациям чрезвычайно высокого риска.

РАЗДЕЛ 7. СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РФ

Сервисы безопасности в вычислительных сетях

Рекомендации X.800 выделяют следующие сервисы (функции) безопасности и исполняемые ими роли:

1) Аутентификация. Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. Аутентификация партнеров по общению используется при установлении соединения и периодически во время сеанса. Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).
2) Управление доступом обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.

Рекомендации X.800 выделяют следующие сервисы (функции) безопасности и исполняемые ими роли:

3) Конфиденциальность данных обеспечивает защиту от несанкционированного получения информации. Отдельно выделяется конфиденциальность трафика – это защита информации, которую можно получить, анализируя сетевые потоки данных.
4) Целостность данных подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры – с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.
5) Неотказуемость (невозможность отказаться от совершенных действий) обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки.

Механизмы безопасности

В X.800 определены следующие сетевые механизмы безопасности:

- шифрование;
- электронная цифровая подпись;
- механизм управления доступом;
- механизм контроля целостности данных;
- механизм аутентификации;
- механизм дополнения трафика;
- механизм управления маршрутизацией;
- механизм нотаризации (заверения).

Взаимосвязь функций и механизмов безопасности

Функции	Механизмы							
	Шифрование	Электронная подпись	Управление доступом	Целостность	Аутентификация	Дополнение трафика	Управление маршрутизацией	Нотаризация
Аутентификация партнеров	+	+	-	-	+	-	-	-
Аутентификация источника	+	+	-	-	-	-	-	-
Управление доступом	-	-	+	-	-	-	-	-
Конфиденциальность	+	-	+	-	-	-	+	-
Избирательная конфиденциальность	+	-	-	-	-	-	-	-
Конфиденциальность трафика	+	-	-	-	-	+	+	-
Целостность соединения	+	-	-	+	-	-	-	-
Целостность вне соединения	+	+	-	+	-	-	-	-
Неотказуемость	-	+	-	+	-	-	-	+

Согласно рекомендациям X.800, усилия администратора средств безопасности должны распределяться по трем направлениям:

- администрирование информационной системы в целом;
- администрирование сервисов безопасности;
- администрирование механизмов безопасности.

Администрирование информационной системы в целом включает обеспечение актуальности политики безопасности, взаимодействие с другими административными службами, реагирование на происходящие события, аудит и безопасное восстановление.

Администрирование сервисов безопасности включает в себя определение защищаемых объектов, выработку правил подбора механизмов безопасности (при наличии альтернатив), комбинирование механизмов для реализации сервисов, взаимодействие с другими администраторами для обеспечения согласованной работы.

Администрирование механизмов безопасности включает:

- управление криптографическими ключами (генерация и распределение);
- управление шифрованием (установка и синхронизация криптографических параметров);
- администрирование управления доступом (распределение информации, необходимой для управления – паролей, списков доступа и т. п.);
- управление аутентификацией (распределение информации, необходимой для аутентификации – паролей, ключей и т. п.);
- управление дополнением трафика (выработка и поддержание правил, задающих характеристики дополняющих сообщений – частоту отправки, размер и т. п.);
- управление маршрутизацией (выделение доверенных путей);
- управление нотаризацией (распространение информации о нотариальных службах, администрирование этих служб).

Для обеспечения непрерывности функционирования могут применяться следующие защитные меры:

- внесение в конфигурацию той или иной формы избыточности (резервное оборудование, запасные каналы связи и т. п.);
- наличие средств реконфигурирования для изоляции и/или замены узлов или коммуникационных каналов, отказавших или подвергшихся атаке на доступность;
- рассредоточенность сетевого управления, отсутствие единой точки отказа;
- наличие средств нейтрализации отказов (обнаружение отказавших компонентов, оценка последствий, восстановление после отказов);
- выделение подсетей и изоляция групп пользователей друг от друга.

РАЗДЕЛ 8.

ВИРУСЫ

КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Современный компьютерный вирус – это практически незаметный для обычного пользователя «враг», который постоянно совершенствуется, находя все новые и более изощренные способы проникновения на компьютеры пользователей.

Необходимость борьбы с компьютерными вирусами обусловлена возможностью нарушения ими всех составляющих информационной безопасности.

Характерные черты компьютерных вирусов

Приведем одно из общепринятых определений вируса, содержащееся в ГОСТе Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

Программный вирус – это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах.

Исходя из этого, необходимо понимать, что нет достаточных программных и аппаратных средств защиты от вирусов, а надежная защита от вирусов может быть обеспечена комплексным применением этих средств и, что немаловажно, соблюдением элементарной «компьютерной гигиены».

Классификация компьютерных вирусов

1) По среде «обитания» вирусы делятся на файловые, загрузочные, макровирусы, сетевые.

- Файловые вирусы внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы.
- Загрузочные вирусы записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик жесткого диска.
- Макровирусы заражают файлы-документы и электронные таблицы офисных приложений.
- Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Классификация компьютерных вирусов

2) По особенностям алгоритма работы вирусы делятся на резидентные, стелс-вирусы, полиморфик-вирусы и вирусы, использующие нестандартные приемы.

- Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них.
- Стелс-вирусы скрывают свое присутствие в «среде обитания».
- Самошифрование и полиморфичность используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования (обнаружения) вируса.
- Различные нестандартные приемы часто используются в вирусах для того, чтобы как можно глубже спрятать себя в ядре операционной системы, защитить от обнаружения свою резидентную копию, затруднить лечение от вируса (например, поместив свою копию в Flash-BIOS) и т. д.

Классификация компьютерных вирусов

3) По деструктивным возможностям вирусы можно разделить на безвредные, неопасные, опасные и очень опасные вирусы.

- безвредные, т. е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
- неопасные, влияние которых ограничивается уменьшением свободной памяти на диске;
- опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;
- очень опасные, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже повредить аппаратные средства компьютера.

Характеристика «вирусоподобных» программ

Вирусоподобная» программа – это программа, которая сама по себе не является вирусом, она может использоваться для внедрения, скрытия или создания вируса.

К «вирусоподобным программам» относятся:

- «троянские программы» (логические бомбы);
- утилиты скрытого администрирования удаленных компьютеров;
- «intended»-вирусы;
- конструкторы вирусов;
- полиморфик-генераторы.

Характеристика «вирусоподобных» программ

- К «троянским» программам относятся программы, наносящие какие-либо разрушительные действия в зависимости от каких-либо условий.
- Утилиты скрытого администрирования являются разновидностью «логических бомб» («троянских программ»), которые используются злоумышленниками для удаленного администрирования компьютеров в сети.
- Внедренные в операционную систему утилиты скрытого управления позволяют делать с компьютером все, что в них заложил их автор: принимать/отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т. д.
- Конструкторы вирусов предназначены для создания новых компьютерных вирусов.
- Полиморфик-генераторы, как и конструкторы вирусов, не являются вирусами, поскольку в их алгоритм не закладываются функции размножения; главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика.

Антивирусные программы

Антивирусная программа – программа, предназначенная для поиска, обнаружения, классификации и удаления компьютерного вируса и вирусоподобных программ.

Профилактика компьютерных вирусов

Основные пути проникновения вирусов в компьютеры пользователей:

1) Глобальные сети – электронная почта.
2) Электронные конференции, файл-серверы ftp.
3) Пиратское программное обеспечение.
4) Локальные сети.
5) Персональные компьютеры «общего пользования».
6) Сервисные службы.

Правила защиты от компьютерных вирусов

1. Внимательно относитесь к программам и документам, которые получаете из глобальных сетей.
2. Перед тем, как запустить файл на выполнение или открыть документ/таблицу, обязательно проверьте его на наличие вирусов.
3. Используйте специализированные антивирусы – для проверки «на лету» всех файлов, приходящих по электронной почте (и из Интернета в целом). Постоянно обновляйте вирусные базы используемого антивируса.
4. Регулярно проверяйте сервер обычными антивирусными программами, для удобства и системности используйте планировщики заданий.
5. Для уменьшения риска заразить файл на сервере администраторам сетей следует активно использовать стандартные возможности защиты сети.
6. Целесообразно запустить новое программное обеспечение на тестовом компьютере, не подключенном к общей сети.
7. Используйте лицензионное программное обеспечение, приобретенное у официальных продавцов.
8. Дистрибутивы копий программного обеспечения (в том числе копий операционной системы) необходимо хранить на защищенных от записи дисках.
9. Пользуйтесь только хорошо зарекомендовавшими себя источниками программ и прочих файлов.
10. Старайтесь не запускать непроверенные файлы, в том числе полученные из компьютерной сети. Перед запуском новых программ обязательно проверьте их одним или несколькими антивирусами.
11. Ограничьте (по возможности) круг лиц допущенных к работе на конкретном компьютере.
12. Пользуйтесь утилитами проверки целостности информации. Такие утилиты сохраняют в специальных базах данных информацию о системных областях дисков (или целиком системные области) и информацию о файлах (контрольные суммы, размеры, атрибуты, даты последней модификации файлов и т. д.).
13. Периодически сохраняйте на внешнем носителе файлы, с которыми ведется работа.

Общий алгоритм обнаружения вируса

При анализе алгоритма вируса необходимо выяснить:

- способ(ы) размножения вируса;
- характер возможных повреждений, которые вирус нанес информации, хранящейся на дисках;
- метод лечения оперативной памяти и зараженных файлов (секторов).

РАЗДЕЛ 9.

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Цели сетевой безопасности могут меняться в зависимости от ситуации, но основные цели обычно связаны с обеспечением составляющих «информационной безопасности»:

целостности данных;

конфиденциальности данных;

доступности данных.

Удаленная угроза – потенциально возможное информационное разрушающее воздействие на распределенную вычислительную сеть, осуществляемая программно по каналам связи. Это определение охватывает обе особенности сетевых систем – распределенность компьютеров и распределенность информации. Поэтому при рассмотрении вопросов информационной безопасности вычислительных сетей рассматриваются два подвида удаленных угроз – это удаленные угрозы на инфраструктуру и протоколы сети и удаленные угрозы на телекоммуникационные службы. Первые используют уязвимости в сетевых протоколах и инфраструктуре сети, а вторые – уязвимости в телекоммуникационных службах.

При рассмотрении вопросов, связанных с информационной безопасностью, в современных вычислительных сетях необходимо учитывать следующие факторы:

- глобальную связанность;
- разнородность корпоративных информационных систем;
- распространение технологии «клиент/сервер».

Специфика средств защиты в компьютерных сетях

Особенности вычислительных сетей и, в первую очередь, глобальных, предопределяют необходимость использования специфических методов и средств защиты, например:

- защита подключений к внешним сетям;
- защита корпоративных потоков данных, передаваемых по открытым сетям;
- защита потоков данных между клиентами и серверами;
- обеспечение безопасности распределенной программной среды;
- защита важнейших сервисов (в первую очередь – Web-сервиса);
- аутентификация в открытых сетях.

Существуют два принципа организации обмена данными в вычислительных сетях:

1) Установление виртуального соединения с подтверждением приема каждого пакета.

2) Передача датаграмм.

Общая характеристика типовых удаленных атак

Типовая удаленная атака	Характер воздействия		Цель воздействия			Условие начала			Наличие обратной связи		Расположение субъекта атаки		Уровень модели OSI						
Класс воздействия	1.1	1.2	2.1	2.2	2.3	3.1	3.2	3.3	4.1	4.2	5.1	5.2	6.1	6.2	6.3	6.4	6.5	6.6	6.7
Анализ сетевого трафика	+	-	+	-	-	-	-	+	-	+	+	-	-	+	-	-	-	-	-
Подмена доверенного объекта сети	-	+	+	+	-	-	+	-	+	+	+	+	-	-	+	+	-	-	-
Внедрение ложного объекта	-	+	+	+	+	-	-	+	+	+	+	+	-	-	+	-	-	-	-
Отказ в обслуживании	-	+	-	-	+	-	-	+	-	+	+	+	-	+	+	+	+	+	+

РАЗДЕЛ 10.

МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Идентификация – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Аутентификация (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

В целом аутентификация по уровню информационной безопасности делится на три категории:

1) Статическая аутентификация.

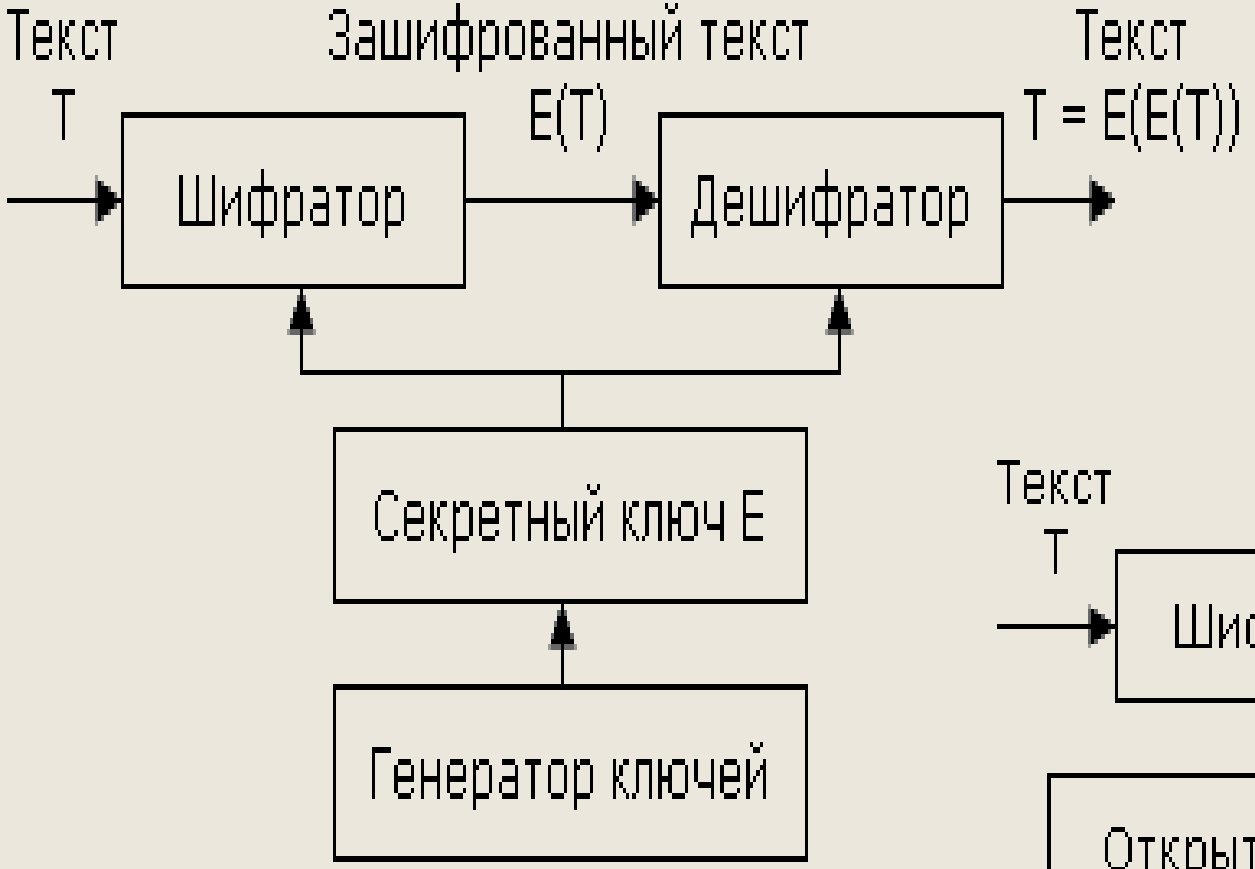
2) Устойчивая аутентификация.

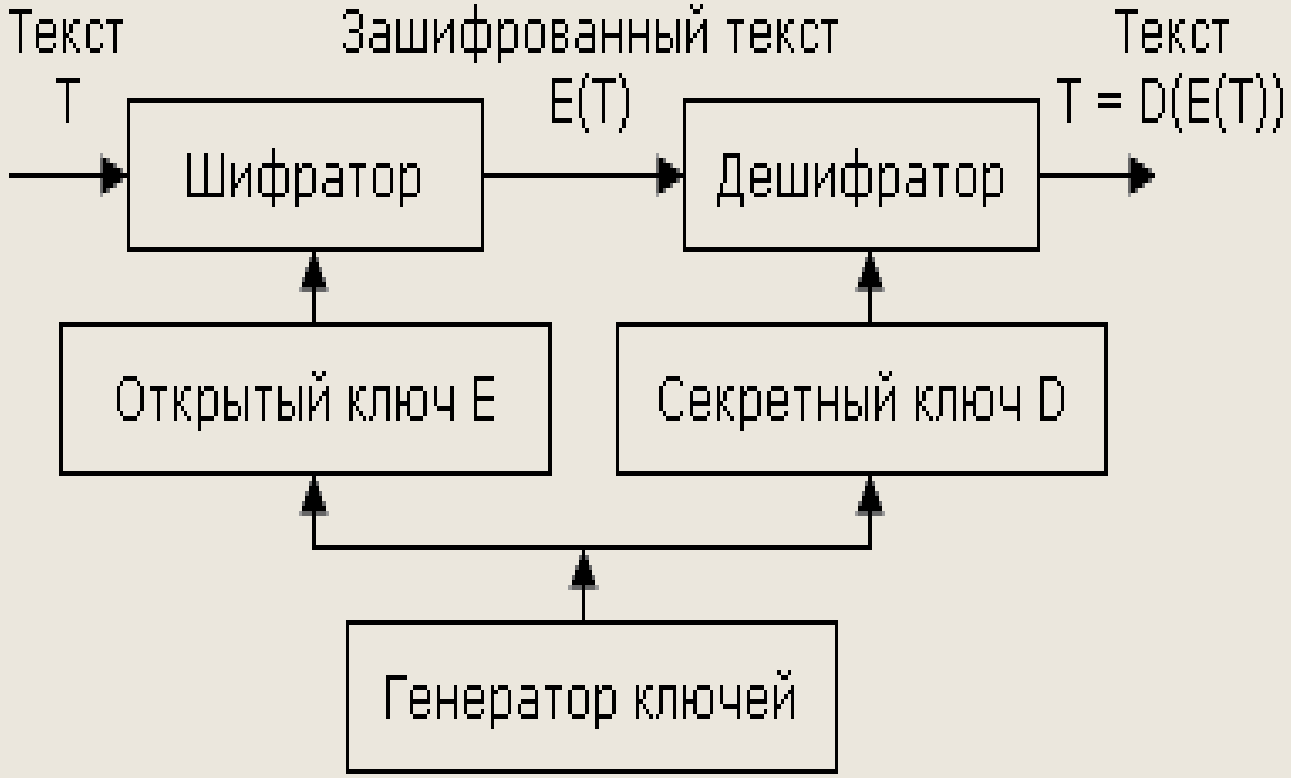
3) Постоянная аутентификация.

Самый надежный технический метод защиты информации основан на использовании криптосистем. Криптосистема включает:

- алгоритм шифрования;
- набор ключей (последовательность двоичных чисел), используемых для шифрования;
- систему управления ключами.

Симметричные и асимметричные методы шифрования





Методы разграничение доступа

1) Разграничение доступа по спискам.

2) Использование матрицы установления полномочий.

3) Разграничение доступа по уровням секретности и категориям.

4) Парольное разграничение доступа.

Мандатное и дискретное управление доступом

В ГОСТе Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации» и в документах ФСТЭК РФ определены два вида (принципа) разграничения доступа:

1) Дискретное управление доступом представляет собой разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту. Данный вид организуется на базе методов разграничения по спискам или с помощью матрицы.
2) Мандатное управление доступом основано на сопоставлении меток конфиденциальности информации, содержащейся в объектах (файлы, папки, рисунки) и официального разрешения (допуска) субъекта к информации соответствующего уровня конфиденциальности.

При внимательном рассмотрении можно заметить, что дискретное управление доступом есть ничто иное, как произвольное управление доступом (по «Оранжевой книге США»), а мандатное управление реализует принудительное управление доступом.

Определение и содержание регистрации и аудита информационных систем

Регистрация является еще одним механизмом обеспечения защищенности информационной системы. Этот механизм основан на подотчетности системы обеспечения безопасности, фиксирует все события, касающиеся безопасности, такие как:

- вход и выход субъектов доступа;
- запуск и завершение программ;
- выдача печатных документов;
- попытки доступа к защищаемым ресурсам;
- изменение полномочий субъектов доступа;
- изменение статуса объектов доступа и т. д.

Аудит ИС – это анализ накопленной информации, проводимый оперативно в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Реализация механизмов регистрации и аудита позволяет решать следующие задачи обеспечения информационной безопасности:

- обеспечение подотчетности пользователей и администраторов;
- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления и анализа проблем.

Практическими средствами регистрации и аудита являются:

- различные системные утилиты и прикладные программы;
- регистрационный (системный или контрольный) журнал.

Фрагмент журнала безопасности подсистемы регистрации и аудита

Безопасность 13 событий

Тип	Дата	Время	Источник	Категория	Событие	Пользователь	Компьютер
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	562	admin	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	562	admin	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Учетные записи	643	admin	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	560	admin	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	560	admin	GHJ
Аудит успехов	26.04.2004	5:34:49	Security	Доступ к объектам	562	admin	GHJ

Регистрационный журнал – это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата.

Организация регистрации событий, связанных с безопасностью информационной системы включает как минимум три этапа:

1) Сбор и хранение информации о событиях.

2) Защита содержимого журнала регистрации.

3) Анализ содержимого журнала регистрации.

Межсетевое экранирование

Типы межсетевых экранов и уровни модели ISO OSI

	Уровень модели OSI	Протокол	Тип межсетевого экрана
1	Прикладной	Telnet, FTP, DNS, NFS, SMTP, HTTP	– шлюз прикладного уровня; – межсетевой экран экспертного уровня.
2	Представления данных		
3	Сеансовый	TCP, UDP	– шлюз сеансового уровня.
4	Транспортный	TCP, UDP	
5	Сетевой	IP, ICMP	– межсетевой экран с фильтрацией пакетов.
6	Канальный	ARP, RAP	
7	Физический	Ethernet	

Межсетевое экранирование

1) Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды, тем самым, обеспечивая все составляющие информационной безопасности. Кроме функций разграничения доступа экранирование обеспечивает регистрацию информационных обменов.
2) Функции экранирования выполняет межсетевой экран или брандмауэр (firewall), под которым понимают программную или программно-аппаратную систему, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации.

Межсетевое экранирование

3) Межсетевые экраны классифицируются по следующим признакам: по месту расположения в сети и по уровню фильтрации, соответствующему эталонной модели OSI/ISO.
4) Внешние межсетевые экраны обычно работают только с протоколом TCP/IP глобальной сети Интернет. Внутренние сетевые экраны могут поддерживать несколько протоколов.
5) Межсетевые экраны разделяют на четыре типа:
   - межсетевые экраны с фильтрацией пакетов;
   - шлюзы сеансового уровня;
   - шлюзы прикладного уровня;
   - межсетевые экраны экспертного уровня.

Межсетевое экранирование

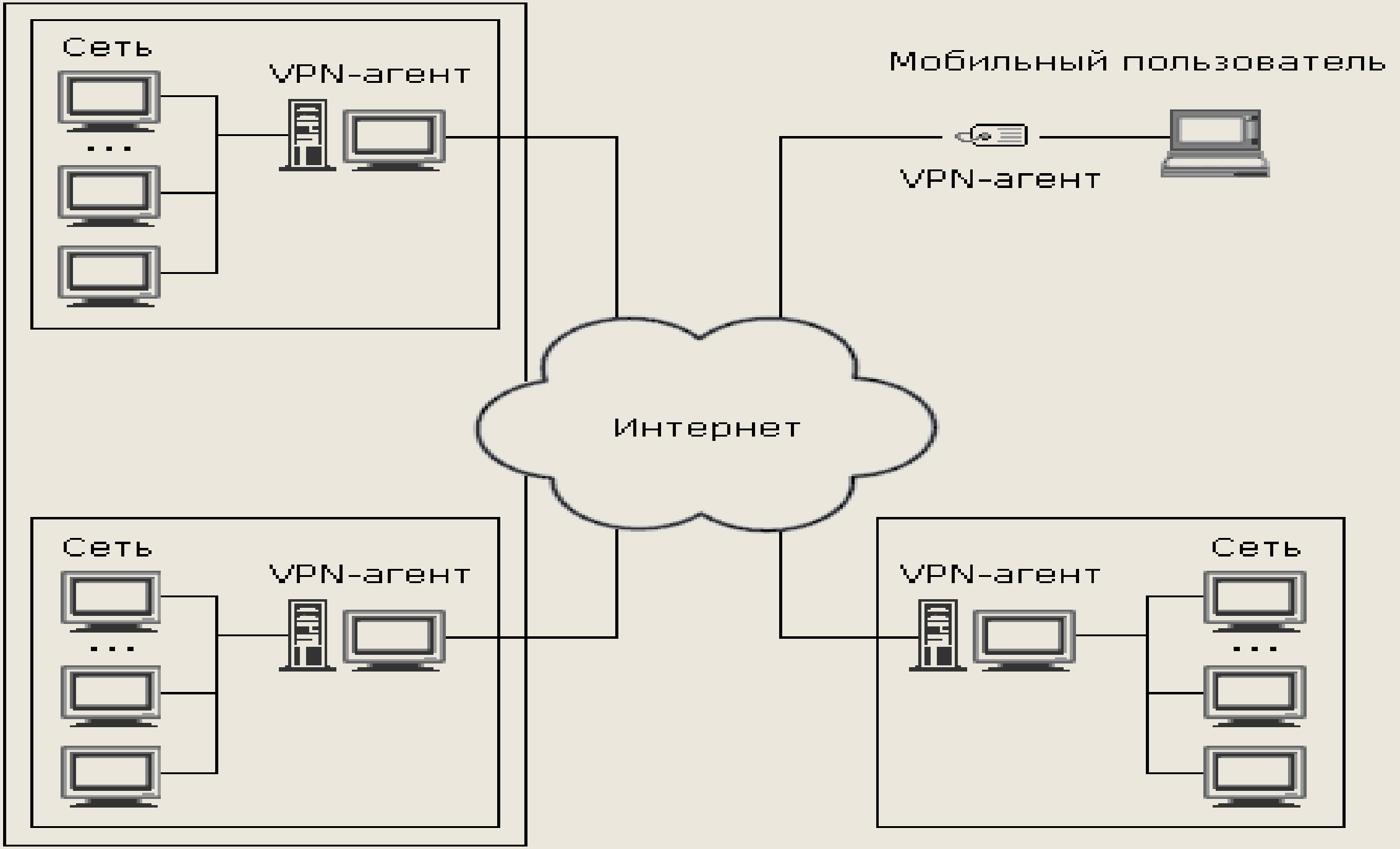
6) Наиболее комплексно задачу экранирования решают межсетевые экраны экспертного уровня, которые сочетают в себе элементы всех типов межсетевых экранов.

Технология виртуальных частных сетей (VPN)

Технология виртуальных частных сетей (VPN – Virtual Private Network) является одним из эффективных механизмов обеспечения информационной безопасности при передаче данных в распределенных вычислительных сетях.

Виртуальные частные сети являются комбинацией нескольких самостоятельных сервисов (механизмов) безопасности:

- шифрования (с использование инфраструктуры криптосистем) на выделенных шлюзах (шлюз обеспечивает обмен данными между вычислительными сетями, функционирующими по разным протоколам);
- экранирования (с использованием межсетевых экранов);
- туннелирования.


Сеть
VPN-агент
Мобильный пользователь
VPN-агент
Интернет
Сеть
VPN-агент
VPN-агент
Сеть