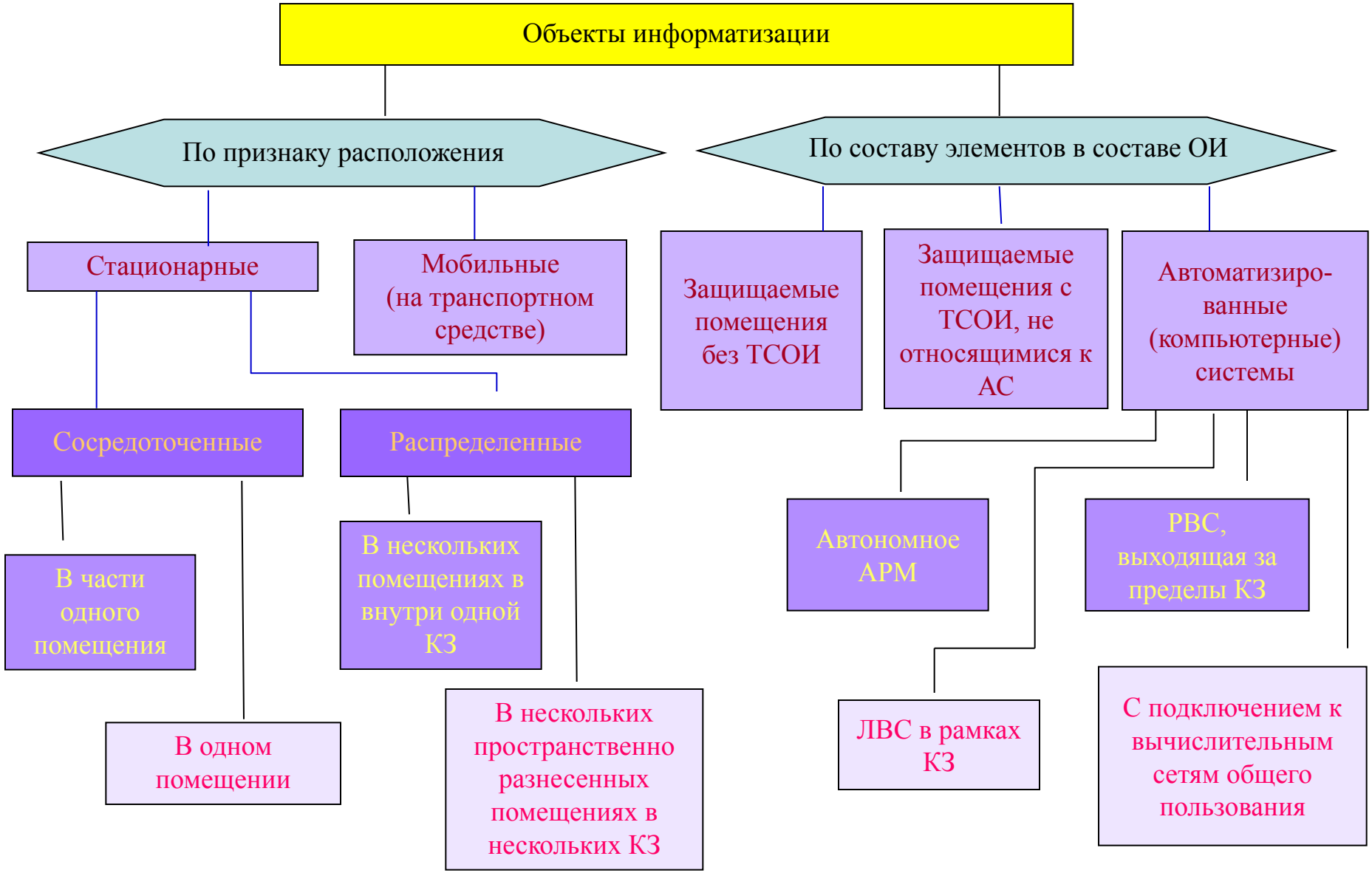
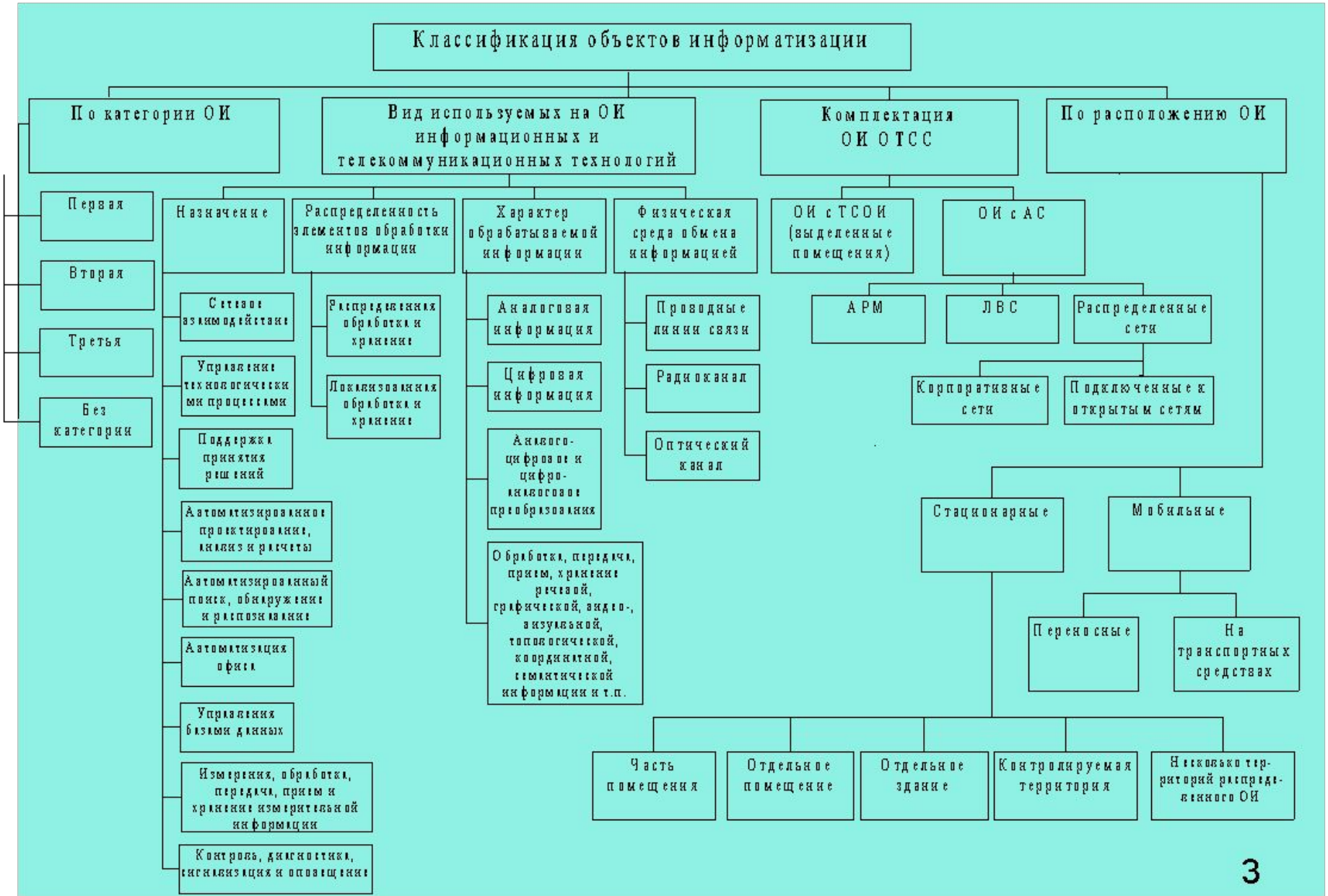
Аттестация объектов информатизации по требованиям безопасности информации. Защита от утечки по техническим каналам

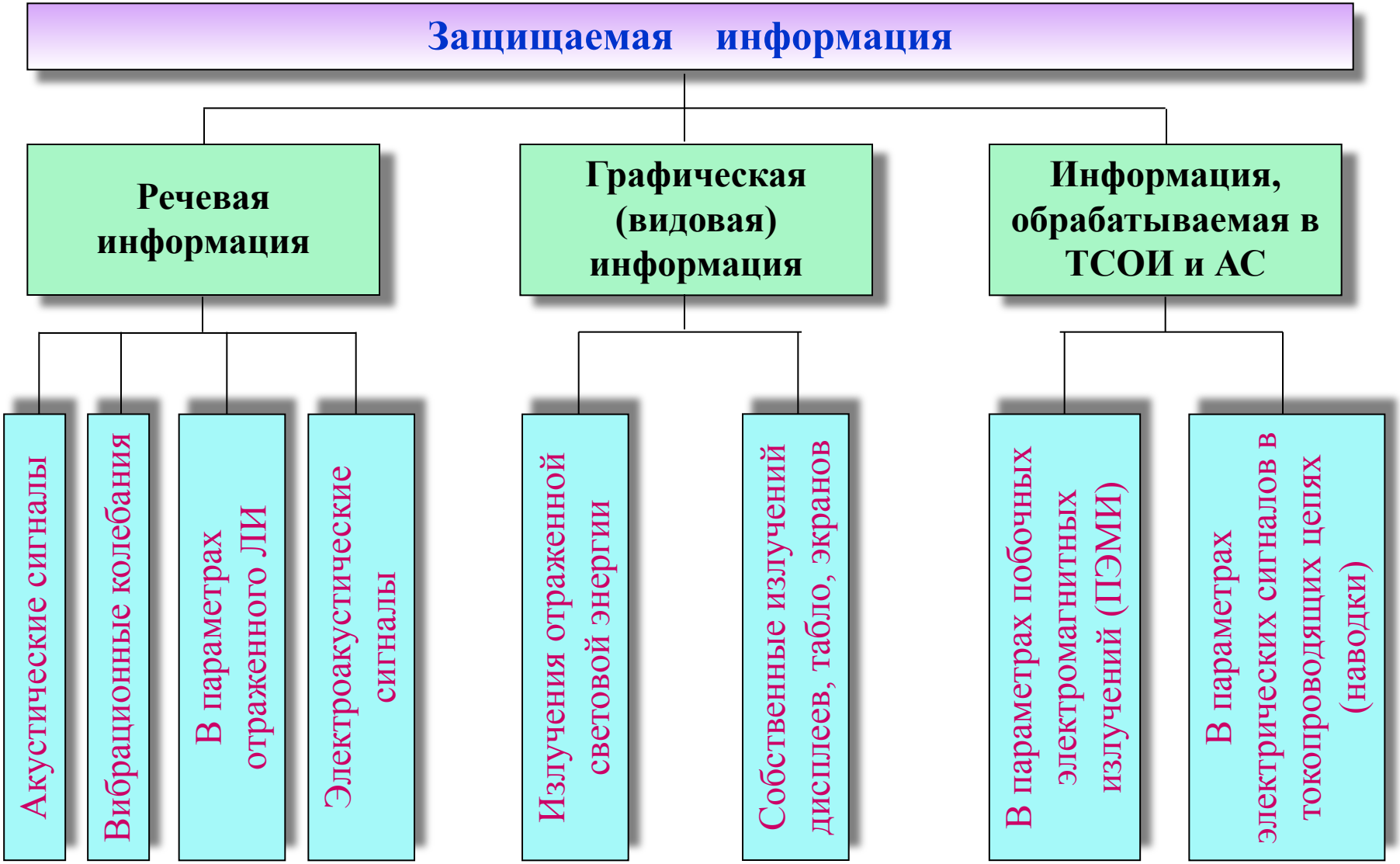


Классификационная схема объектов информатизации
по наиболее существенным классификационным признакам

• Классификация объектов информатизации



Основные формы представления защищаемой конфиденциальной информации



Основные формы представления защищаемой информации на ОИ

Защищаемая информация

В **параметрах акустических колебаний** (речевая информация) в воздушной среде (в помещениях ОИ)

В параметрах **вибрационных колебаний** (речевая информация) **в твердых телах** (в ограждающих конструкциях помещений ОИ, в инженерных коммуникациях, в оконных стеклах и др.)

В **алфавитно-цифровой (символьной) форме** (в виде текста и формул) на различных носителях (на бумажных, на экранах мониторов, табло, демонстрационных экранах и др.)

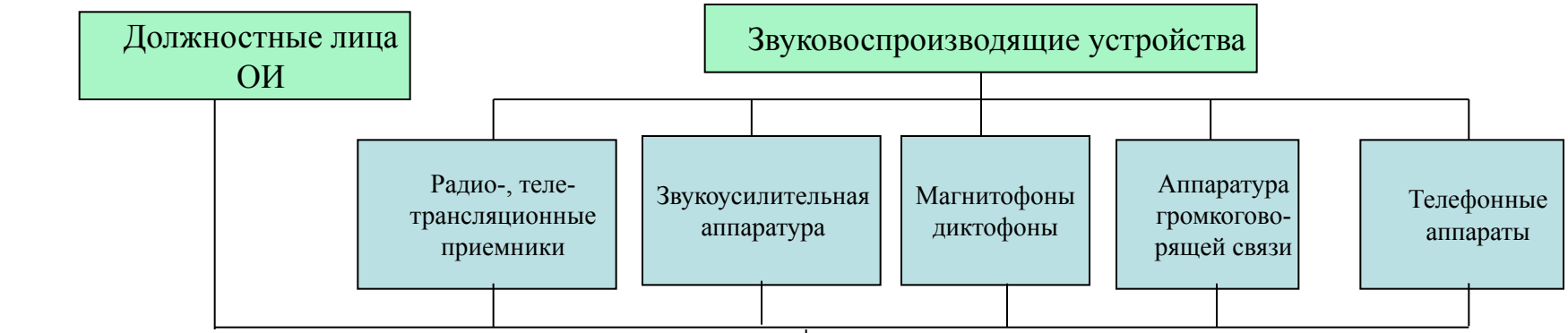
В **графической форме** (в виде графиков, рисунков, схем, фотографий, видеоизображений на экранах, плакатах, в документах и др.) на различных носителях (на бумажных, на экранах мониторов, табло, демонстрационных экранах и др.)

В **параметрах промодулированного речевым сигналом лазерного излучения** (внешнего, облучающего оконные стекла помещений ОИ, излучения в ВОЛС, проходящих через помещения ОИ)

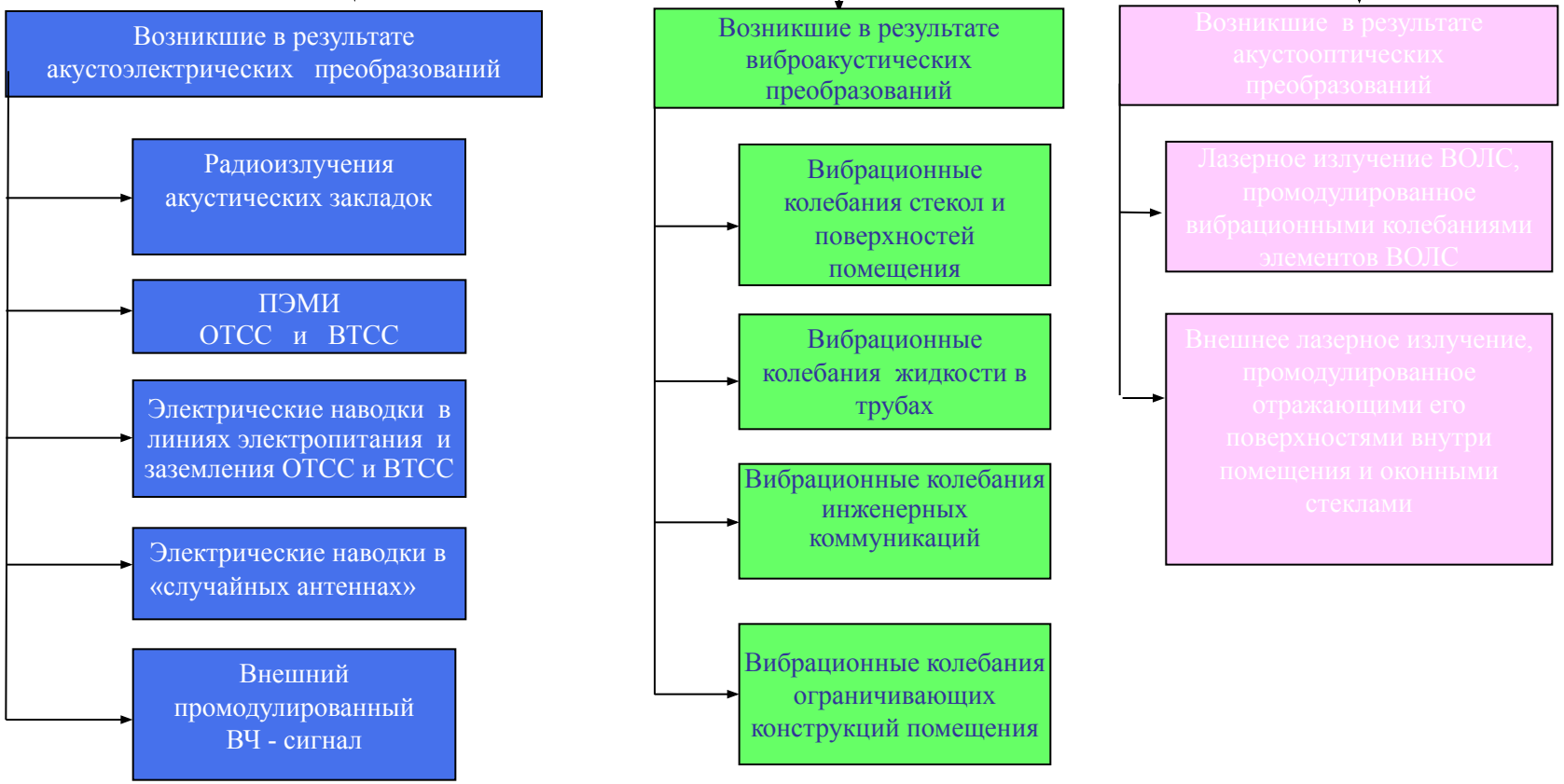
В **параметрах промодулированных информативным сигналом электрических сигналов** в звуковоспроизводящих устройствах, кабелях связи, проводниках электропитания и заземления, пожарно-охранной сигнализации и др.

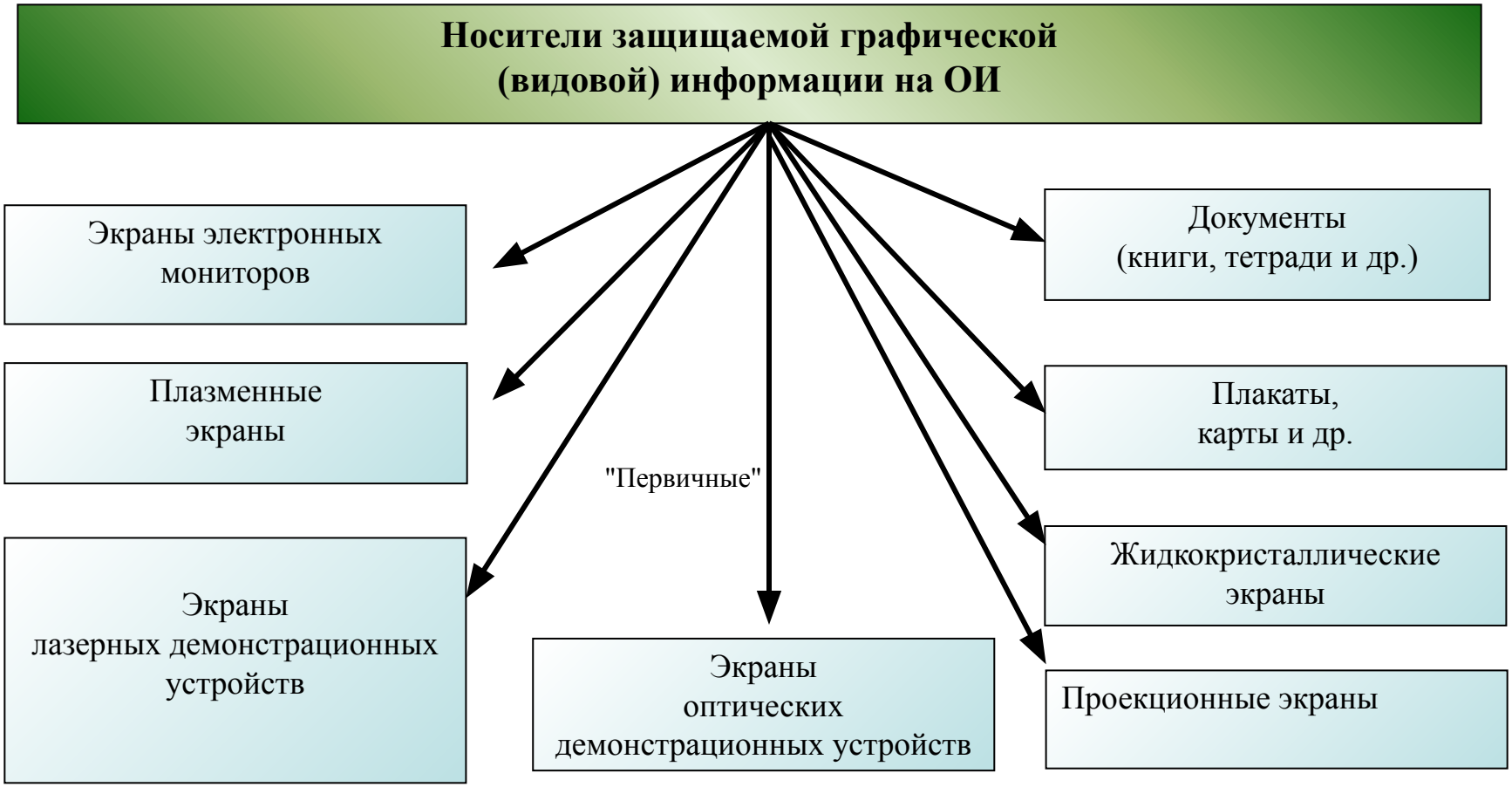
В **параметрах промодулированных информативным сигналом электромагнитных излучений** (побочных, паразитных, отраженных внешних высокочастотных излучений, радиоизлучении радиозакладок)

«Первичные» носители защищаемой речевой информации



«Вторичные» носители защищаемой речевой информации



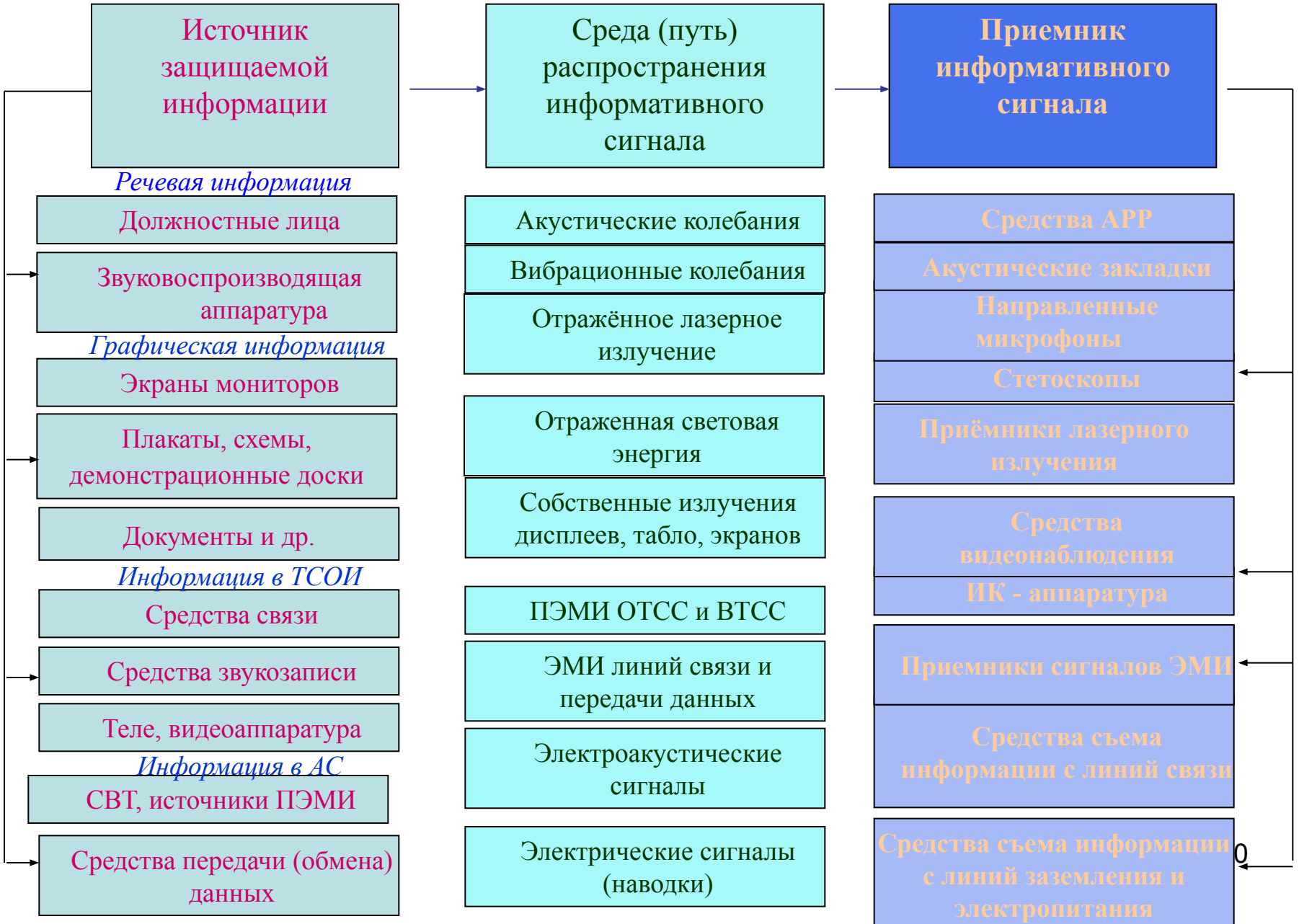

Носители защищаемой графической (видовой) информации на ОИ
Экраны электронных мониторов
Плазменные экраны
Экраны лазерных демонстрационных устройств
"Первичные"
Экраны оптических демонстрационных устройств
Документы (книги, тетради и др.)
Плакаты, карты и др.
Жидкокристаллические экраны
Проекционные экраны

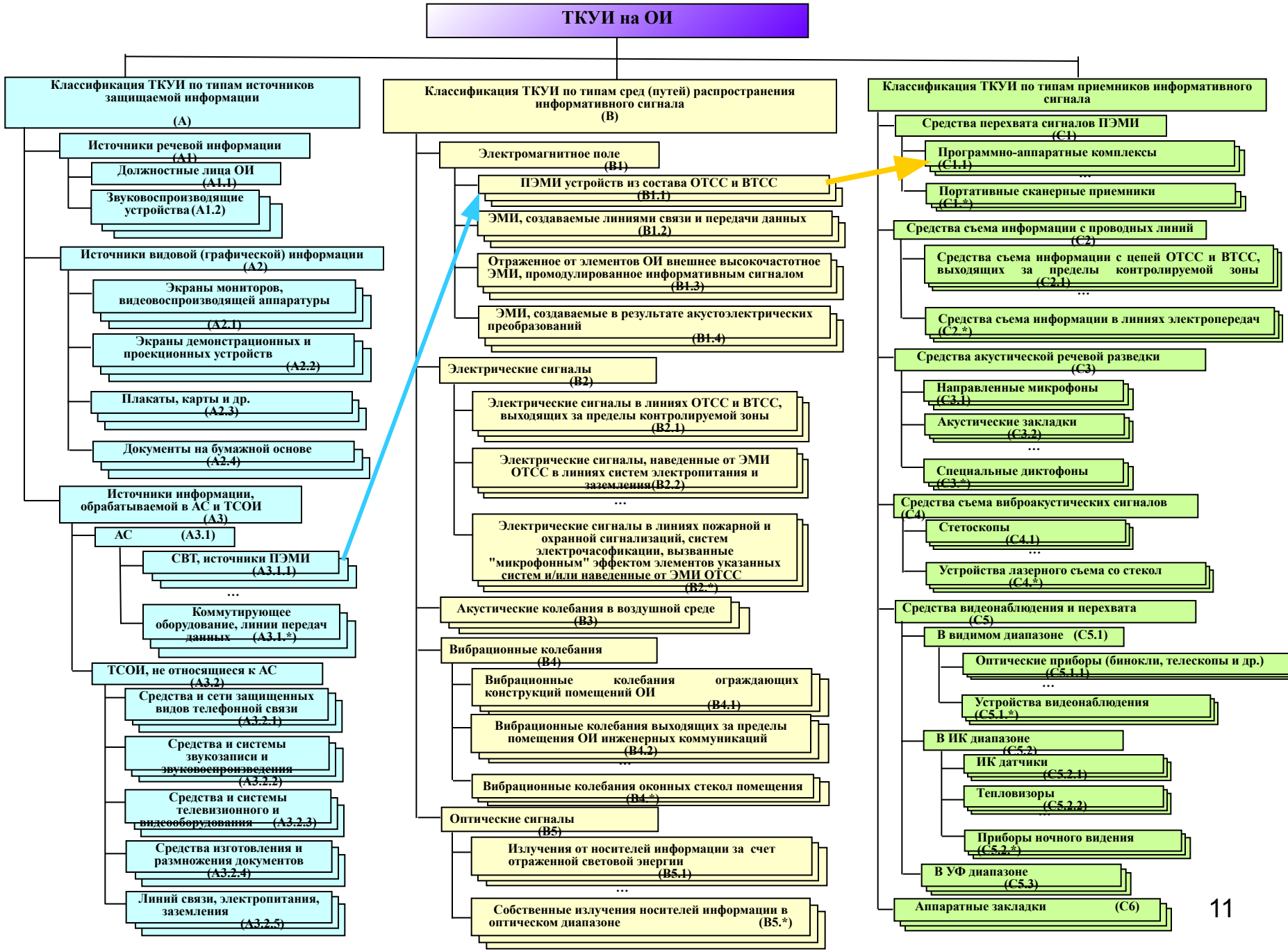
Основные виды носителей защищаемой информации, циркулирующей и хранящейся в АС

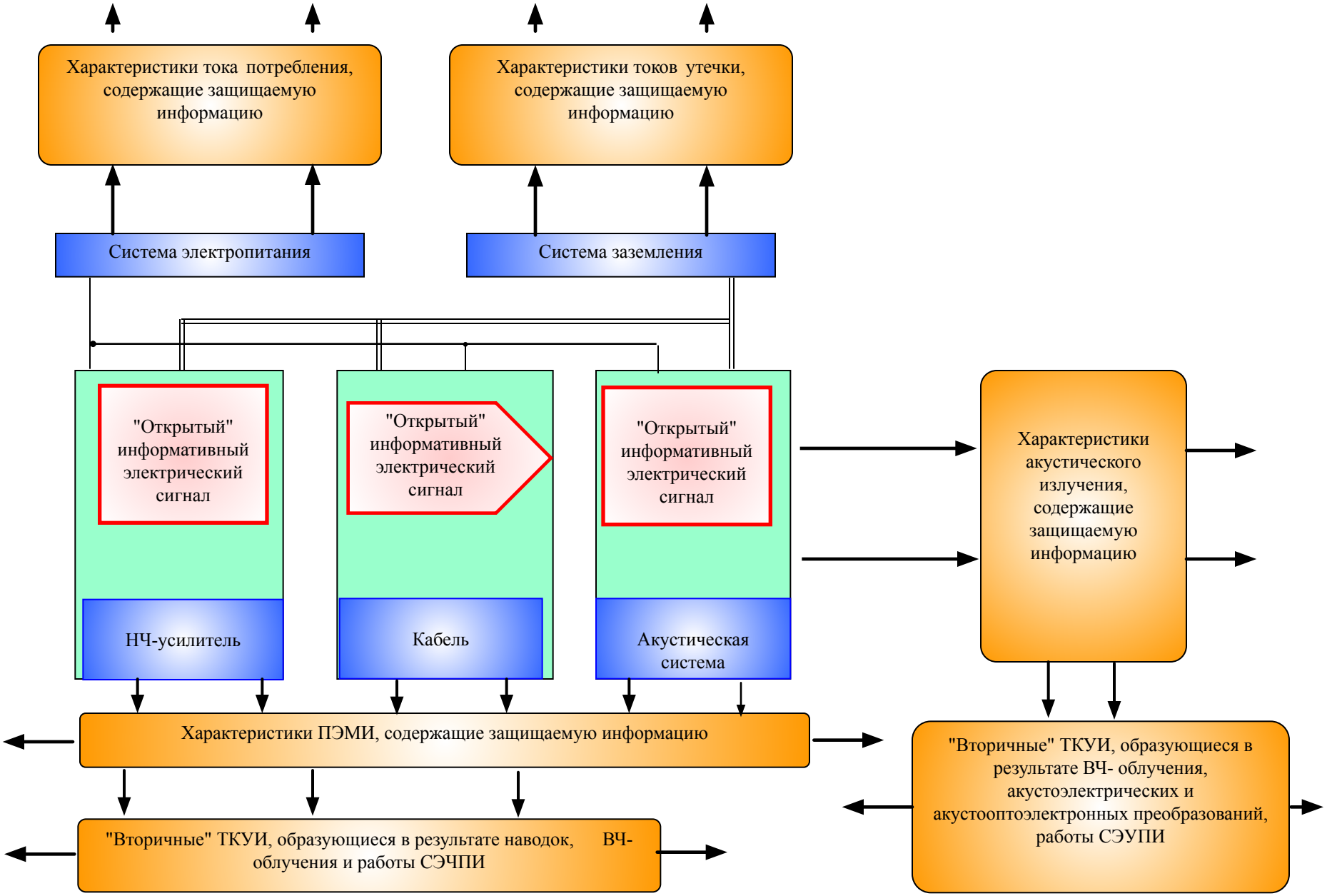
Основные (наиболее характерные) типы объектов информатизации

Основные (наиболее характерные) типы объектов информатизации	Защищаемая информация Основные элементы ОИ, содержащие защищаемую информацию			
	Акустическая речевая	Графическая (видовая)	Обрабатываемая в ТСОИ, не относящихся к АС	Обрабатываемая в АС
Защищаемые помещения для совещаний по конфиденциальным вопросам	ЕСТЬ -должностные лица ОИ	НЕТ	ЕСТЬ - средства размножения документов; - средства звукозаписи и звуковоспроизводства	НЕТ
Зщащищаемые помещения для совещаний и демонстрации кино- и видео материалов по конфиденциальным вопросам	ЕСТЬ -должностные лица ОИ	ЕСТЬ - плакаты; - экраны; - дисплеи	ЕСТЬ - средства связи - звуковоспроизводящие средства; - кино-, видеооборудование	НЕТ
Помещения, содержащие автоматизированные системы (ПЭВМ, ЛВС, РВС, РВС с подключением к компьютерным сетям общего пользования)	НЕТ	ЕСТЬ - дисплеи; - принтеры	НЕТ	ЕСТЬ - ПЭВМ; -сети ЭВМ; -периферия
Защищаемые помещения для совещаний по конфиденциальным вопросам, содержащие АС и ТСОИ, не относящиеся к АС	ЕСТЬ -должностные лица ОИ	ЕСТЬ - дисплеи; - принтеры	ЕСТЬ - средства связи	ЕСТЬ - ПЭВМ; -сети ЭВМ; -периферия

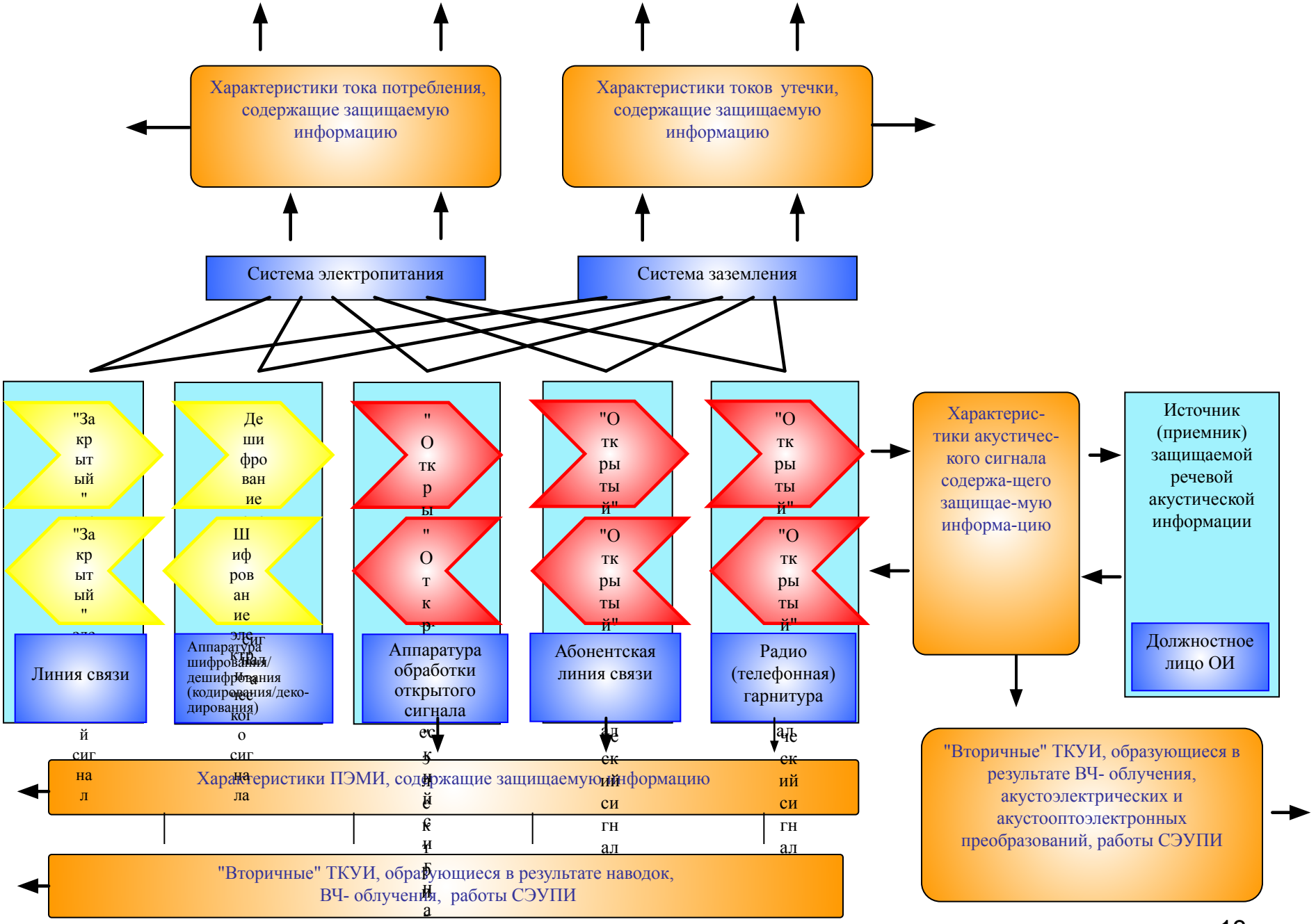
Краткая характеристика ТКУИ



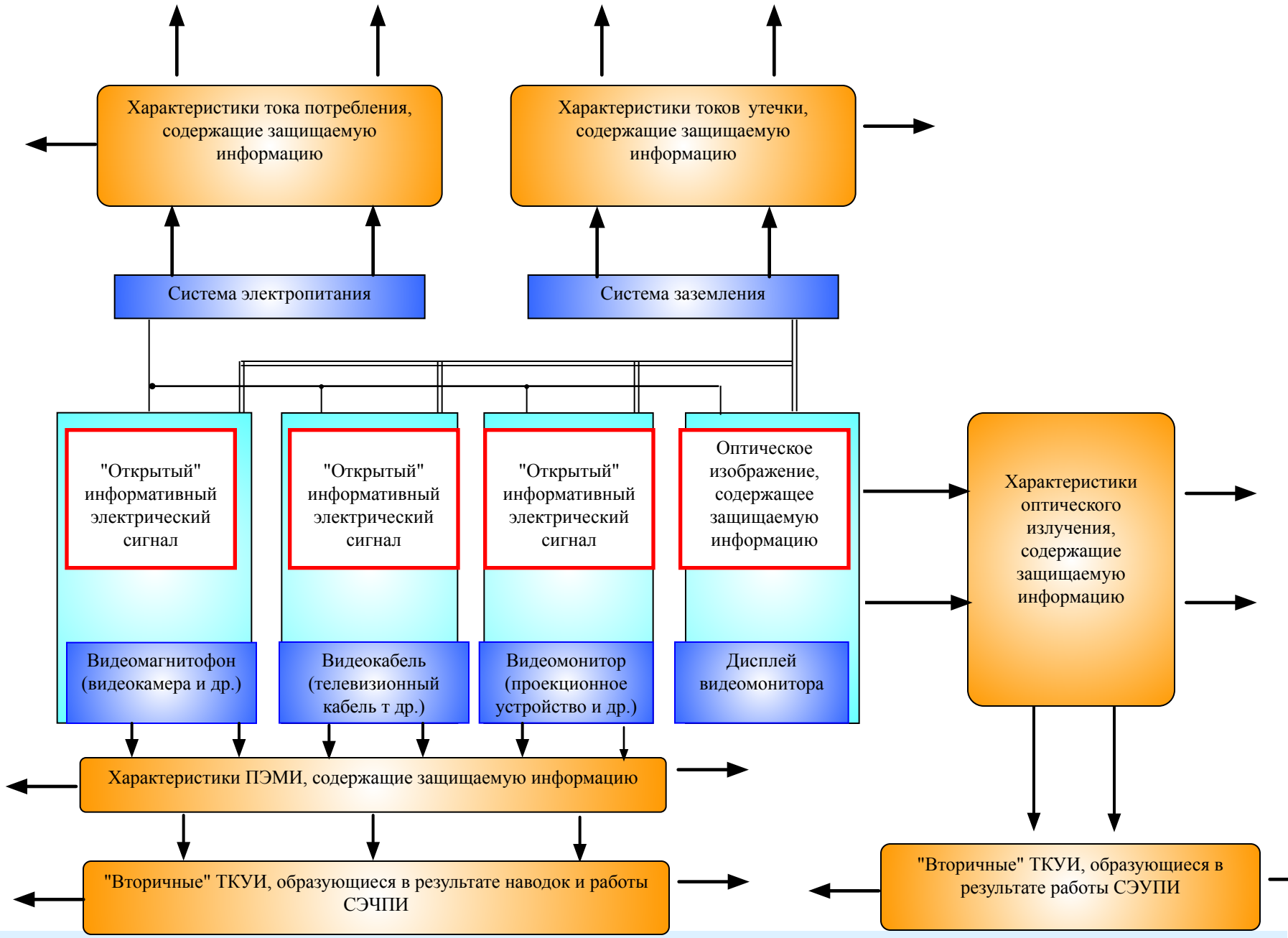

ТКУИ на ОИ
Классификация ТКУИ по типам источников защищаемой информации (А)
Источники речевой информации (А1)
Должностные лица ОИ (А1.1)
Звуковоспроизводящие устройства (А1.2)
Источники видовой (графической) информации (А2)
Экраны мониторов, видеовоспроизводящей аппаратуры (А2.1)
Экраны демонстрационных и проекционных устройств (А2.2)
Плакаты, карты и др. (А2.3)
Документы на бумажной основе (А2.4)
Источники информации, обрабатываемой в АС и ТСОИ (А3)
АС (А3.1)
СВТ, источники ПЭМИ (А3.1.1)
…
Коммутирующее оборудование, линии передач данных (А3.1.*)
ТСОИ, не относящиеся к АС (А3.2)
Средства и сети защищенных видов телефонной связи (А3.2.1)
Средства и системы звукозаписи и звуковоспроизведения (А3.2.2)
Средства и системы телевизионного и видеооборудования (А3.2.3)
Средства изготовления и размножения документов (А3.2.4)
Линий связи, электропитания, заземления (А3.2.5)
Классификация ТКУИ по типам сред (путей) распространения информативного сигнала (В)
Электромагнитное поле (В1)
ПЭМИ устройств из состава ОТСС и ВТСС (В1.1)
ЭМИ, создаваемые линиями связи и передачи данных (В1.2)
Отраженное от элементов ОИ внешнее высокочастотное ЭМИ, промодулированное информативным сигналом (В1.3)
ЭМИ, создаваемые в результате акустоэлектрических преобразований (В1.4)
Электрические сигналы (В2)
Электрические сигналы в линиях ОТСС и ВТСС, выходящих за пределы контролируемой зоны (В2.1)
Электрические сигналы, наведенные от ЭМИ ОТСС в линиях систем электропитания и заземления (В2.2)
…
Электрические сигналы в линиях пожарной и охранной сигнализаций, систем электрочасофикации, вызванные "микрофонным" эффектом элементов указанных систем и/или наведенные от ЭМИ ОТСС (В2.*)
Акустические колебания в воздушной среде (В3)
Вибрационные колебания (В4)
Вибрационные колебания ограждающих конструкций помещений ОИ (В4.1)
Вибрационные колебания выходящих за пределы помещения ОИ инженерных коммуникаций (В4.2)
…
Вибрационные колебания оконных стекол помещения (В4.*)
Оптические сигналы (В5)
Излучения от носителей информации за счет отраженной световой энергии (В5.1)
…
Собственные излучения носителей информации в оптическом диапазоне (В5.*)
Классификация ТКУИ по типам приемников информативного сигнала
Средства перехвата сигналов ПЭМИ (С1)
Программно-аппаратные комплексы (С1.1)
…
Портативные сканерные приемники (С1.*)
Средства съема информации с проводных линий (С2)
Средства съема информации с цепей ОТСС и ВТСС, выходящих за пределы контролируемой зоны (С2.1)
…
Средства съема информации в линиях электропередач (С2.*)
Средства акустической речевой разведки (С3)
Направленные микрофоны (С3.1)
Акустические закладки (С3.2)
…
Специальные диктофоны (С3.*)
Средства съема виброакустических сигналов (С4)
Стетоскопы (С4.1)
…
Устройства лазерного съема со стекол (С4.*)
Средства видеонаблюдения и перехвата (С5)
В видимом диапазоне (С5.1)
Оптические приборы (бинокли, телескопы и др.) (С5.1.1)
…
Устройства видеонаблюдения (С5.1.*)
В ИК диапазоне (С5.2)
ИК датчики (С5.2.1)
Тепловизоры (С5.2.2)
…
Приборы ночного видения (С5.2.*)
В УФ диапазоне (С5.3)
Аппаратные закладки (С6)



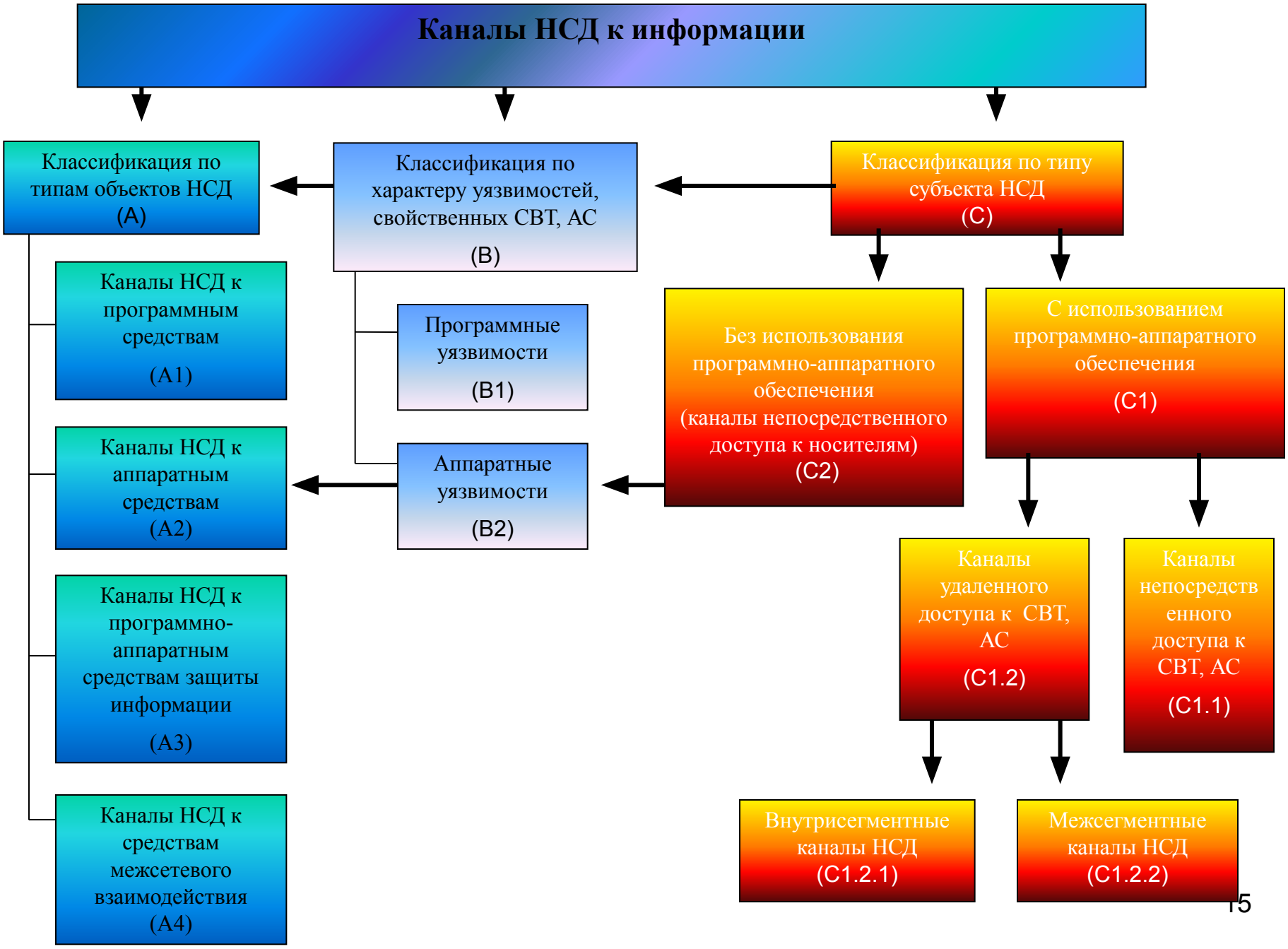
Обобщенная схема образования технических каналов утечки защищаемой речевой акустической информации в средствах и системах звуковоспроизведения

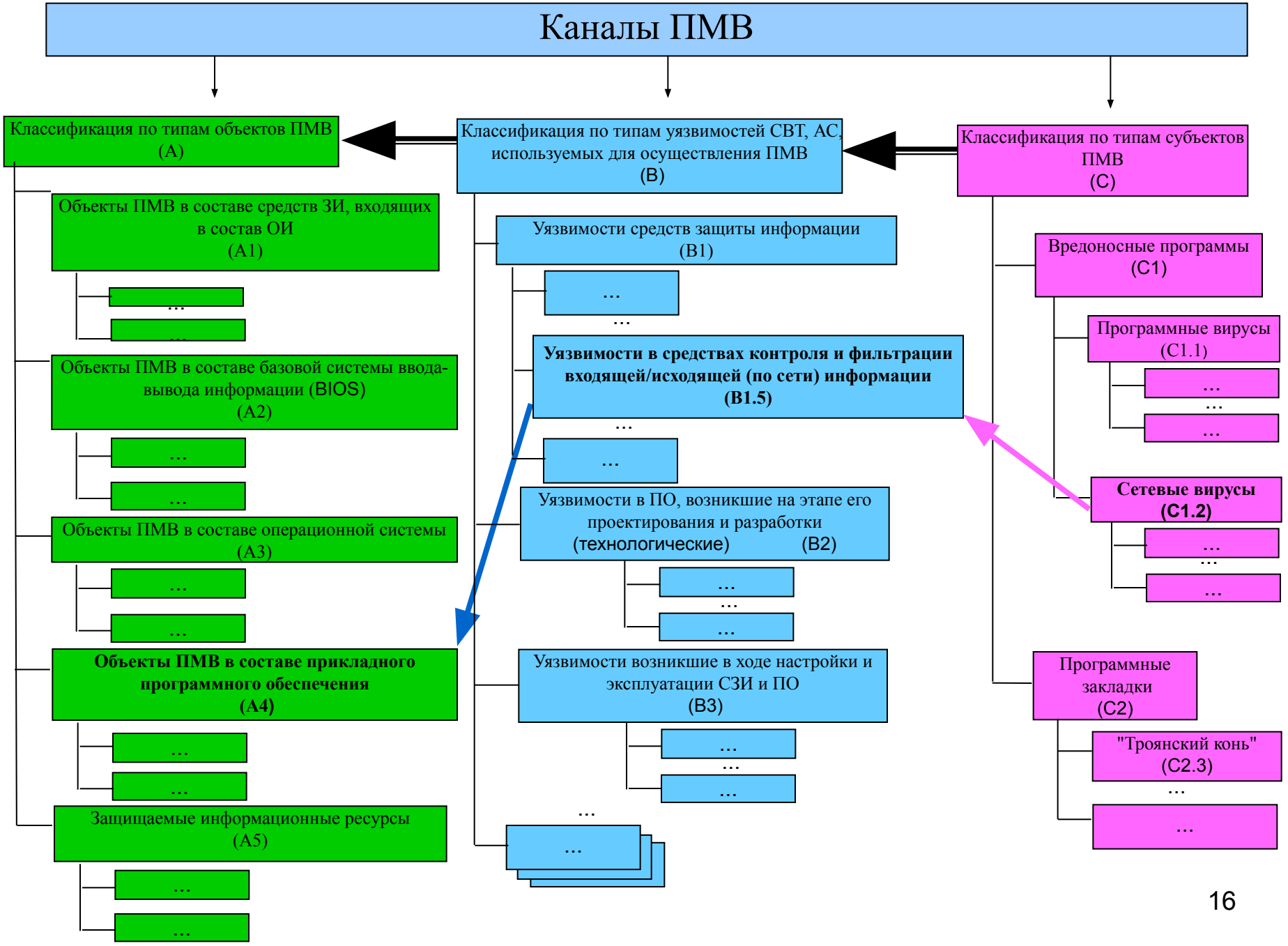


Обобщенная схема образования технических каналов утечки защищаемой речевой акустической информации в защищенных средствах и системах связи



Обобщенная схема образования технических каналов утечки защищаемой видовой (графической) информации в средствах и системах телевизионного видео оборудования


Каналы НСД к информации
Классификация по типам объектов НСД (А)
Классификация по характеру уязвимостей, свойственных СВТ, АС (В)
Классификация по типу субъекта НСД (С)
Каналы НСД к программным средствам (А1)
Каналы НСД к аппаратным средствам (А2)
Каналы НСД к программно-аппаратным средствам защиты информации (А3)
Каналы НСД к средствам межсетевого взаимодействия (А4)
Программные уязвимости (В1)
Аппаратные уязвимости (В2)
Без использования программно-аппаратного обеспечения (каналы непосредственного доступа к носителям) (С2)
С использованием программно-аппаратного обеспечения (С1)
Каналы удаленного доступа к СВТ, АС (С1.2)
Каналы непосредственного доступа к СВТ, АС (С1.1)
Внутрисегментные каналы НСД (С1.2.1)
Межсегментные каналы НСД (С1.2.2)


Каналы ПМВ
Классификация по типам объектов ПМВ (А)
Классификация по типам уязвимостей СВТ, АС, используемых для осуществления ПМВ (В)
Классификация по типам субъектов ПМВ (С)
Объекты ПМВ в составе средств ЗИ, входящих в состав ОИ (А1)
Объекты ПМВ в составе базовой системы ввода-вывода информации (BIOS) (А2)
Объекты ПМВ в составе операционной системы (А3)
Объекты ПМВ в составе прикладного программного обеспечения (А4)
Защищаемые информационные ресурсы (А5)
Уязвимости средств защиты информации (В1)
Уязвимости в средствах контроля и фильтрации входящей/исходящей (по сети) информации (В1.5)
Уязвимости в ПО, возникшие на этапе его проектирования и разработки (технологические) (В2)
Уязвимости возникшие в ходе настройки и эксплуатации СЗИ и ПО (В3)
Вредоносные программы (С1)
Программные вирусы (С1.1)
Сетевые вирусы (С1.2)
Программные закладки (С2)
"Троянский конь" (С2.3)

Основные типы ОИ

ОИ типа 1
выделенное помещение без ОТСС

ОИ типа 2
выделенное помещение с ТСОИ

ОИ типа 3
АС на базе автономного АРМ

ОИ типа 4
АС на базе ЛВС

ОИ типа 5
АС на базе РВС

ОИ типа 6
выделенное помещение с АС

Характеристика ОИ типа 3

Наименование:	Помещение с автономным АРМ, не предназначенное для проведения закрытых совещаний
Защищаемая информация:	графическая (видовая) информация; информация, обрабатываемая в АС и ТСОИ

Носители графической (видовой) информации

Первичные	Вторичные
экраны мониторов АС, телевизионной и видеоаппаратуры ОИ, воспроизводящие защищаемую информацию; **документы на бумажной основе** – книги, тетради, плакаты, карты, чертежи и др.	**электрические сигналы** в сканирующих электронных устройствах (телевизионных камерах, мониторах) и **их излучение**, модулированное информативным видеосигналом; **ПЭМИ** телевизионных камер электронных мониторов, **содержащие информативный сигнал**; **электромагнитное излучение внедрённых** на ОИ специальных электронных **устройств** перехвата графической (видео) информации ("видеозакладок")

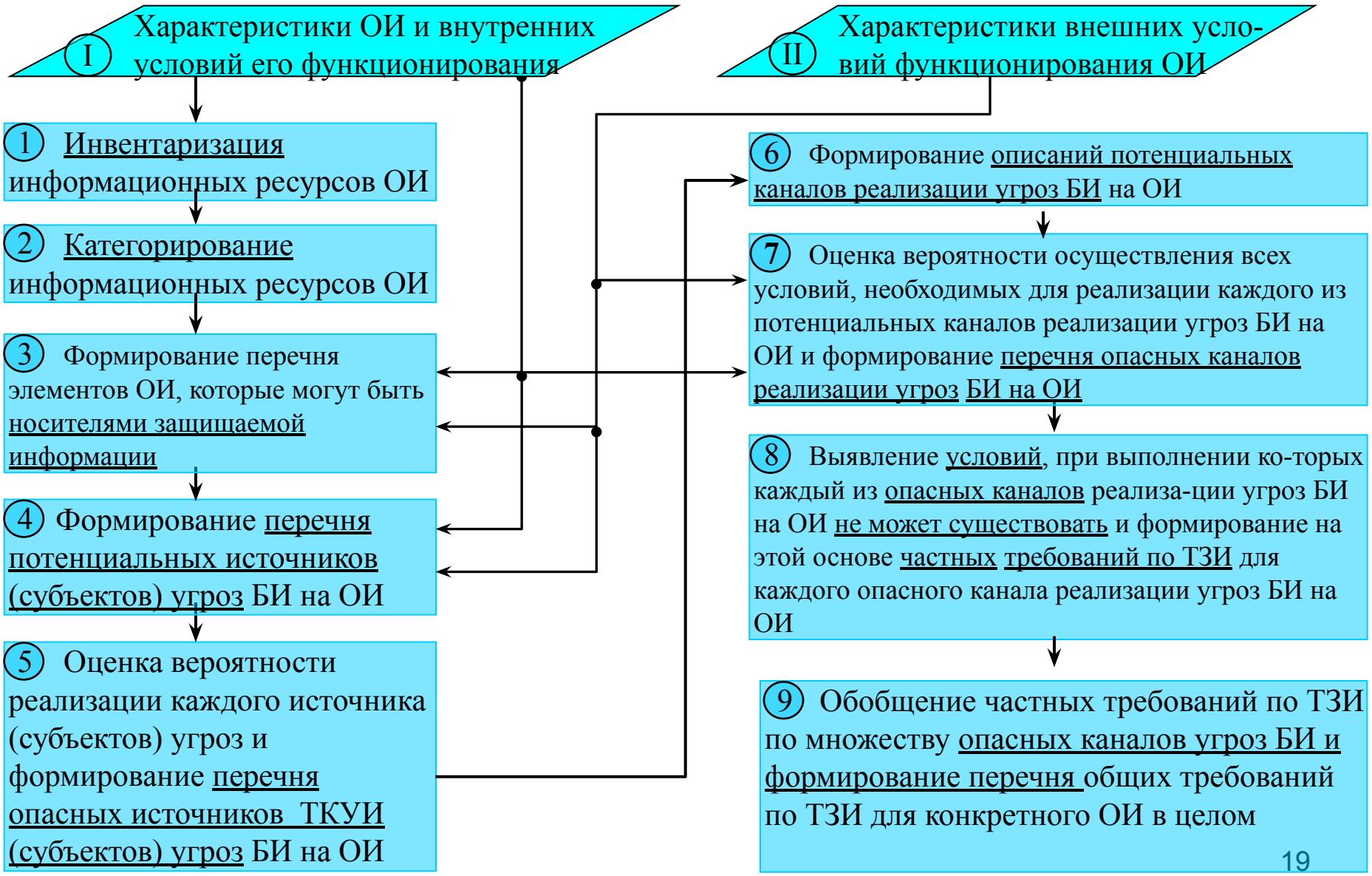
Носители информации, обрабатываемой в АС и ТСОИ

Первичные	Вторичные
источники ПЭМИ в АС; источники ПЭМИ в ТСОИ; носители защищаемой информации	**электрические сигналы** (наводки) в токопроводящих цепях ОТСС и (или) ВТСС, **наведённые ПЭМИ ОТСС**; **ПЭМИ ВТСС**, модулированные информативными сигналами; отражённые от элементов ОТСС **электромагнитные излучения внешнего облучающего источника**, модулированные информативными сигналами ОТСС

Объекты НСД (ПМВ)

- Пользовательская информация.
- Общесистемное ПО (ОС, драйверы (микропрограммы) устройств, и др.).
- Прикладное ПО общего назначения (редакторы, СУБД).
- Специальное ПО (пользовательское).
- ПО средств ЗИ.

Обобщённый алгоритм формирования требований по ТЗИ для конкретного объекта информатизации



Группы основных требований по ТЗИ к защищаемым помещениям

Требования к размещению ЗП

- в пределах КЗ;
- отсутствие смежных помещений других организаций;
- не ниже 2- го этажа;
- ...

Требования к ограждающим конструкциям (ОК)

- звукоизоляция ОК должна исключать прослушивание АРИ из- за пределов ЗП;
- исключить возможность установки посторонних предметов на внешних поверхностях ОК;
- исключить размещение СЭУПИ;
- ...

Требования к оснащению ОТСС и ВТСС

- использование сертифицированных ОТСС и ВТСС;
- использование для линий связи экранирующих кабелей или ВОЛС;
- использование дополнительных экранированных отдельных элементов ОТСС, ВТСС;
- …

Требования к средствам обеспечения функционирования ОИ

- требования к системам электропитания;
- требования к системам заземления;
- требования к охранной сигнализации;
- …

Требования к средствам ЗИ

- использование только сертифицированных средств ЗИ;
- обеспечение требуемой эффективности ТЗИ;
- отсутствие помех функционированию ОИ;
- …

Требования к документальному оформлению мер ТЗИ

- для этапа разработки ЗП;
- …
- для этапа проектирования и создания ЗП;
- …
- для этапа ввода в строй ЗП;
- …

Требования к порядку ввода ЗП в строй

- обеспечение опытной эксплуатации ЗП;
- проведение приемо-сдаточных испытаний;
- проведение аттестации ОИ по требованиям БИ;
- ...

Требования к порядку эксплуатации ЗП

- эксплуатация только в соответствии с утвержденной организационно-распорядительной и эксплуатационной документацией;
- реализация разрешительной системы допуска в ЗП;
- проверка наличия СЭУПИ в ЗП перед мероприятиями;
- ...

Требования к порядку ремонта, модернизации

- проведение работ под контролем подразделения по ЗИ;
- установка нового оборудования после проверки на отсутствие закладных устройств;
- …

Основные группы требований по ТЗИ обрабатываемой в технических средствах, не относящихся к АС

Требования к ТСОИ

-применение только сертифицированных по БИ;
-применение экранирующих кабелей или ВОЛС размещаемых в пределах КЗ;
-отсутствие самовозбуждения элементов ТСОИ;
- …

Требования к порядку эксплуатации ТСОИ

- эксплуатация только в соответствии с утвержденной организационно- распорядительной и эксплуатационной документацией;
-исключение физического НСД к ТСОИ;
-отсутствие посторонних (нештатных) элементов оборудования и предметов
- …

Требования к размещению

-выполнение нормативов удалению от посторонних проводников;
-исключение внешнего ВЧ-облучения;
-исключение несанкционированного наблюдения дисплеев, экранов , табло, …
-…

Требования к порядку ремонта, модернизации

-только организаций имеющий лицензию на осуществление работ по ЗИ;
-обязательное тестирование;
-документальное оформление фактов ремонта, модернизации

Требования к средствам обеспечения функционирования ТСОИ

-требования к системам электропитания
- …
-требования к системам заземления
- …
-требования к системам ограничения НСД к ТСОИ
- …

Требования к средствам ЗИ

-использование только сертифицированных средств ЗИ;
-выполнение нормативов по уровню информативного сигнала в ПЭМИН на границе КЗ;
- …

Основные требования по ЗИ в АС

Определение и присвоение АС **класса защищённости**

Организация системы ЗИ в АС в соответствии с официально установленным **классом защищённости** АС

Наличие и функционирование:

- **разрешительной системы доступа** пользователей и обслуживающего персонала к элементам АС и ЗИ;
- **системы учёта**, **хранения**, **выдачи** и **уничтожения** носителей защищаемой информации

Запрет использования:

- **посторонних носителей информации**;
- **внесения в АС посторонних программных средств** без санкции администратора БИ и соответствующей проверки;
- **незащищённых каналов передачи данных**, выходящих за пределы КЗ

Наличие и применение средств:

- **идентификации и аутентификации** пользователей АС;
- **разграничения доступа** пользователей к программам и информации;
- **изоляции программ** разных пользователей;
- **стирания остаточной информации** на несъёмных носителях

Основные требования по защите конфиденциальной информации в ЛВС

ЛВС должна располагаться **в пределах контролируемой зоны** (КЗ)

Подключение ЛВС к другим АС – только **через межсетевой экран** (МЭ) по правилу:
- АС класса 1Г – МЭ класса 4 и выше (3, 2, 1);
- АС класса 1Д, 2Б, 3Б – МЭ класса 5 и выше (4, 3, 2, 1)

Подключение ЛВС к АС, находящимся **за пределами КЗ** только:
- по защищённым каналам связи;
- по открытым каналам связи с применением сертифицированных криптографических средств ЗИ

Применение **сертифицированных** средств ЗИ от НСД **на всех** узлах ЛВС

Постоянный **контроль настроек** средств ЗИ от НСД

Установление и изменение **состава** пользователей и **прав** их доступа – только на основании письменного распоряжения **руководства** ОИ и только **администратором** БИ

Обязательное применение **уникальных** идентификаторов и паролей **всеми** пользователями и администраторами ЛВС

Требования к подсистемам защиты информации от НСД (ПМВ) для отдельного АРМ

1 Подсистема управления доступом

- 1.1 Идентификация и проверка подлинности субъектов доступа при входе в систему (по идентификатору (коду) и паролю)
- 1.2 Идентификация ЭВМ, внешних устройств, программ, файлов (по логическим именам)
- 1.3 Контроль доступа субъектов к защищаемым ресурсам
- 1.4 Управление потоками информации с помощью меток конфиденциальности

2 Подсистема регистрации и учета

- 2.1 Регистрация входа (выхода) субъектов доступа в систему (из системы), регистрация загрузки и инициализации ОС
- 2.2 Регистрация запуска/завершения программ и процессов обработки защищаемых ИР
- 2.3 Регистрация доступа программ субъектов доступа к защищаемым файлам (создание и удаление, передачу по линиям и каналам связи)
- 2.4 Регистрация попыток доступа ПС к дополнит. защищаемым объектам (внешним устройствам)
- 2.5 Регистрация изменения полномочий субъектов доступа
- 2.6 Учет защищаемых носителей информации
- 2.7 Очистка освобождаемых областей оперативной памяти ЭВМ и внешних накопителей
- 2.8 Сигнализация попыток нарушения защиты

3 Криптографическая подсистема

- 3.1 Шифрование всей конфиденциальной информации, записываемой на носители данных
- 3.2 Контроль доступа субъектов к операциям шифрования и к соответствующим криптографическим ключам
- 3.3 Использование разных криптографических ключей для шифрования информации, принадлежащей различным субъектам доступа

4 Подсистема обеспечения целостности

- 4.1 Проверка целостности программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды
- 4.2 Физическая охрана средств вычислительной техники и носителей информации
- 4.3 Периодическое тестирование СЗИ от НСД
- 4.5 Наличие средств восстановления СЗИ от НСД

5 Подсистема антивирусной защиты

- 5.1 Блокирование вирусных воздействий на системные области, общесистемное программное обеспечение (ПО), на прикладное ПО и данные пользователя
- 5.2 Контроль целостности файловой системы, системных областей, позволяющий обнаруживать неизвестные вирусы
- 5.3 Обнаружение вирусов в архивах, а также в объектах, загружаемых на АРМ из съемных носителей
- 5.4 Удаление обнаруженных вирусов
- 5.5 Самоконтроль целостности (неинфицированности) средства защиты от вирусов при его запуске

Требования к подсистемам защиты информации от НСД (ПМВ) для ЛВС

1 Подсистема управления доступом	2 Подсистема регистрации и учета	3 Криптографическая подсистема	4 Подсистема обеспечения целостности	5 Подсистема антивирусной защиты
Требования по ЗИ от НСД для отдельного АРМ				
+	+	+	+	+
1.5 Идентификация администратором защиты каналов связи ЛВС (по логическим именам)	2.9 Регистрация администратором защиты доступа к узлам ЛВС, каналам связи, периферийным устройствам ЛВС	3.4 Шифрование всей конфиденциальной информации, передаваемой по линиям передачи данных в ЛВС	4.7 Проверка администратором защиты ЛВС неизменности программной среды сети	5.6 Контроль антивирусной защиты серверных станций
1.6 Контроль администратором защиты доступа субъектов к файл-серверам ЛВС	2.10 Регистрация администратором защиты изменения полномочий субъектов ЛВС		4.8 Расположение всех узлов ЛВС в пределах контролируемой зоны	5.7 Обнаружение вирусов в в объектах, загружаемых на рабочие станции ЛВС по сети
1.7 Контроль администратором защиты процесса управления потоками информации на рабочих станциях ЛВС	2.11 Контроль администратором защиты попыток нарушения системы защиты информации в ЛВС			5.8 Регистрация событий в системном журнале администратора защиты ЛВС и централизованное управление средствами антивирусной защиты

6 Подсистема аудита и адаптивной безопасности

6.1 Контроль и оповещение администратора о несанкционированных действиях пользователей

6.2 Установление средств ЗИ на всех рабочих станциях и серверах ЛВС

6.3 Централизованное управление и настройка СЗИ в ЛВС

Требования к подсистемам защиты информации от НСД для распределенных вычислительных сетей (РВС)

1 Подсистема управления доступом	2 Подсистема регистрации и учета	3 Криптографическая подсистема	4 Подсистема обеспечения целостности	5 Подсистема антивирусной защиты
Требования по ЗИ от НСД для ЛВС				
+	+	+	+	+
1.8 Контроль администратором защиты субъектов удаленного доступа к файл-серверам, почтовым серверам и др. элементам РВС	2.12 Регистрация администратором защиты удаленного доступа к узлам РВС	3.6 Шифрование всей информации, передаваемой по сети	4.9 Расположение всех коммутационных узлов РВС в пределах контролируемой зоны	5.9 Антивирусный контроль информации, получаемой при межсетевом взаимодействии
	2.13 Анализ сетевого трафика			5.10 Антивирусная защита почтовых систем РВС

6 Подсистема аудита и адаптивной безопасности	7 Подсистема межсетевого взаимодействия (передачи данных)
Требования по ЗИ от НСД для ЛВС	
+	+
6.3 Выявление уязвимостей в РВС путем тестирования (всестороннего, выборочного) средствами анализа защищенности	7.1 Межсетевое экранирование при подключении отдельных узлов сети
6.4 Распознавание сетевой атаки и оперативное оповещение об этом администратора защиты средствами обнаружения вторжений	7.2 Использование для передачи данных по сети защищенных каналов связи (доверенные каналы) и защищенных линий связи (ВОЛС)

Требования к АС при подключении к открытым сетям типа **Internet**

1. Межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры

2. Контроль и обнаружение сетевых вторжений (сетевых атак), нарушающих или создающих предпосылки к нарушению
установленных в АС требований по защите информации

3. Анализ и контроль защищенности сети с помощью сканеров безопасности

4. Шифрование информации при ее передаче по открытым сетям, а также использование электронно-цифровой подписи для контроля целостности и подтверждения подлинности отправителя и/или получателя информации

5. Использование электронных замков и других защищенных носителей информации для надежной идентификации и аутентификации пользователей

6. Использование средств антивирусного контроля информации, получаемой из открытой сети

7. Централизованное управление системой защиты информации в АС

Рис. 1. Классификация беспроводных технологий коммуникаций

Обобщенный алгоритм формирования рекомендаций по ТЗИ (мер и средств ТЗИ) на конкретном ОИ

Основные требования к организации комплексной ЗИ на ОИ

Комплексная ЗИ:

- мероприятия по ЗИ осуществляются от всех опасных угроз БИ на всех стадиях (этапах) жизненного цикла ОИ;
- эффективность мероприятий ЗИ по всем направления защиты соответствует требуемому уровню

При организации комплексной ЗИ должны быть обеспечены:

1. Соответствие состава и эффективности мероприятий по ЗИ составу и уровню угроз БИ.

2. Непротиворечивость и согласованность мер ЗИ.

3. Преемственность мероприятий по ЗИ по стадиям и этапам жизненного цикла ОИ.

4. Непрерывность процесса защиты (в том числе отслеживание и учёт изменений в составе и возможностях реализации угроз БИ).

Классификация работ по ТЗИ

1 УРОВЕНЬ – по виду нарушения безопасности информации, относительно которых решается задача ТЗИ

- Предотвращение нарушения конфиденциальности (утечки) информации
- Предотвращение нарушения целостности информации
- Предотвращение нарушения доступности (блокирования) информации

2 УРОВЕНЬ – по этапам возникновения и реализации угроз

- Предупреждение условий, благоприятных для возникновения угроз
- Предупреждение появления угроз
- Поиск, обнаружение и устранение источников угроз
- Нейтрализация воздействия угроз
- Обнаружение воздействия угроз
- Локализация воздействия угроз
- Восст. информации после воздействия угроз

3 УРОВЕНЬ - по видам защищаемой информации

- Защита речевой информации
- Защита графической (видовой) информации
- ЗИ в ТСОИ и АС от утечки по каналам ПЭМИН
- Защита СВТ, АС от НСД и ПМВ

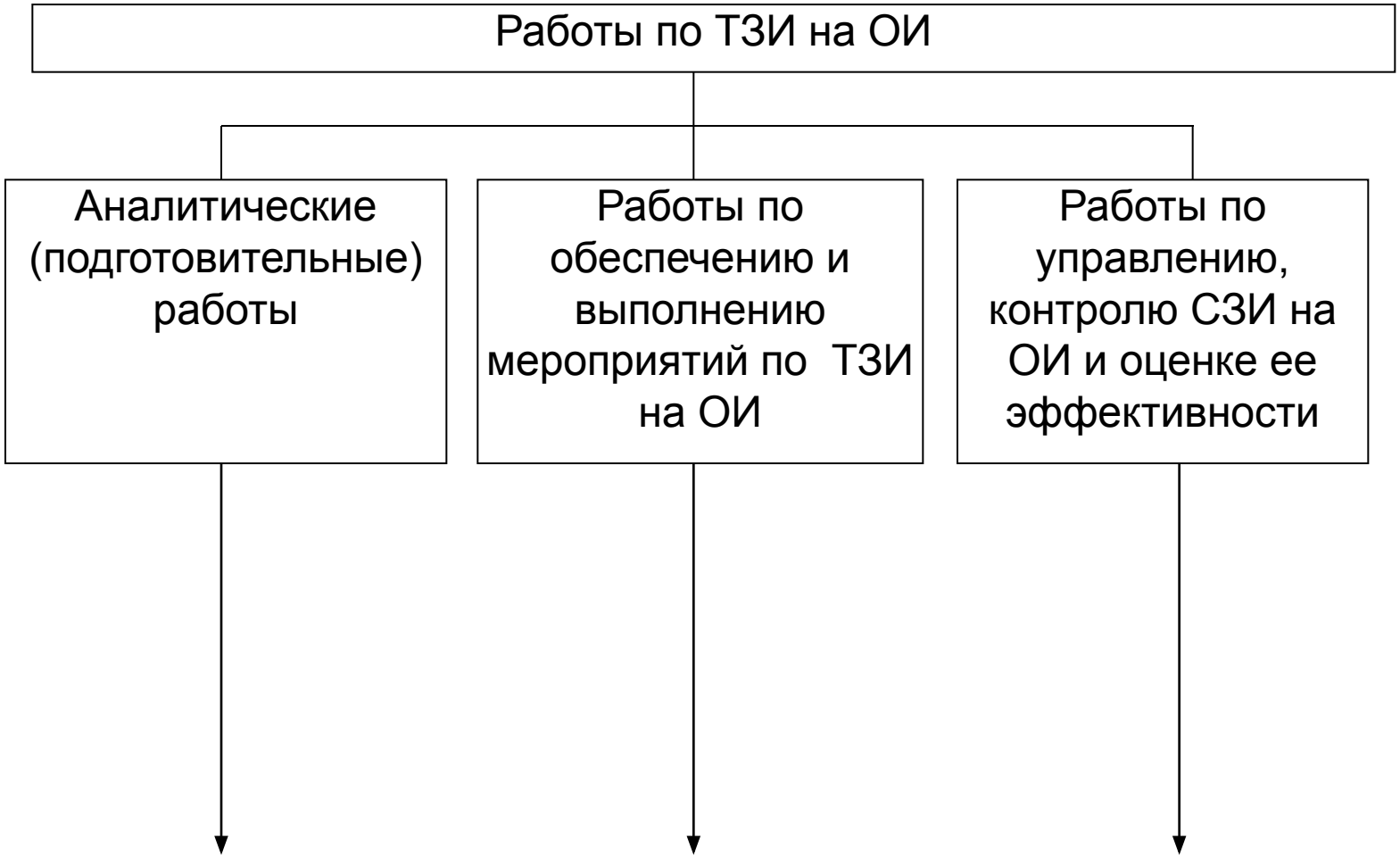
4 УРОВЕНЬ – по типам защищаемых элементов ОИ на различных стадиях их жизненного цикла

- Защита ВП, элементов их конструкций и средств обеспечения
- Защита ТСОИ
- Защита СВТ и АС
  - технических средств
  - программных средств

Работы по ЗИ:

- на предпроектной стадии
- на стадии проектирования
- на стадии ввода в эксплуатацию
- на стадии эксплуатации
- на стадии ремонта (модернизации)

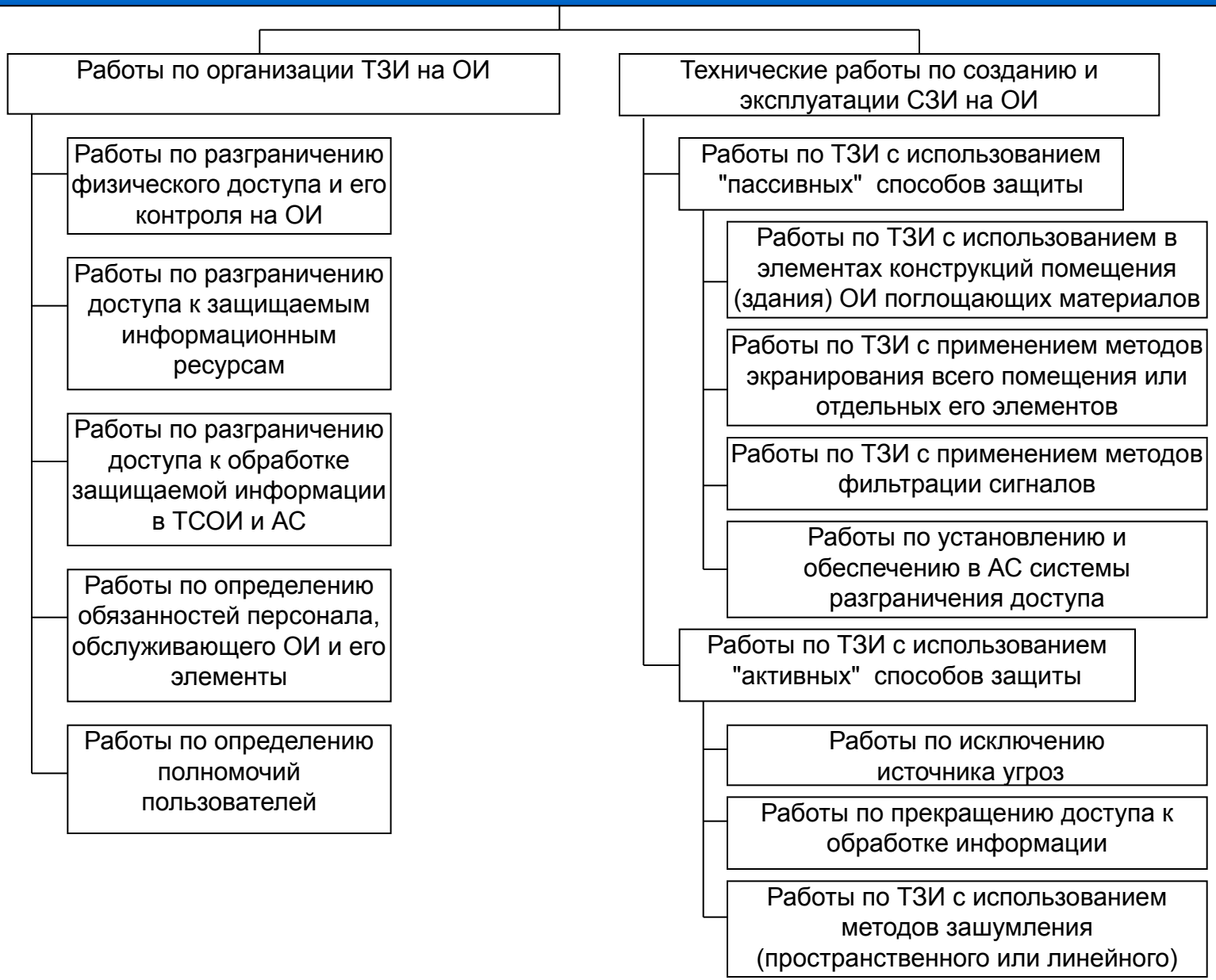
Направленность типовых работ по ТЗИ на ОИ



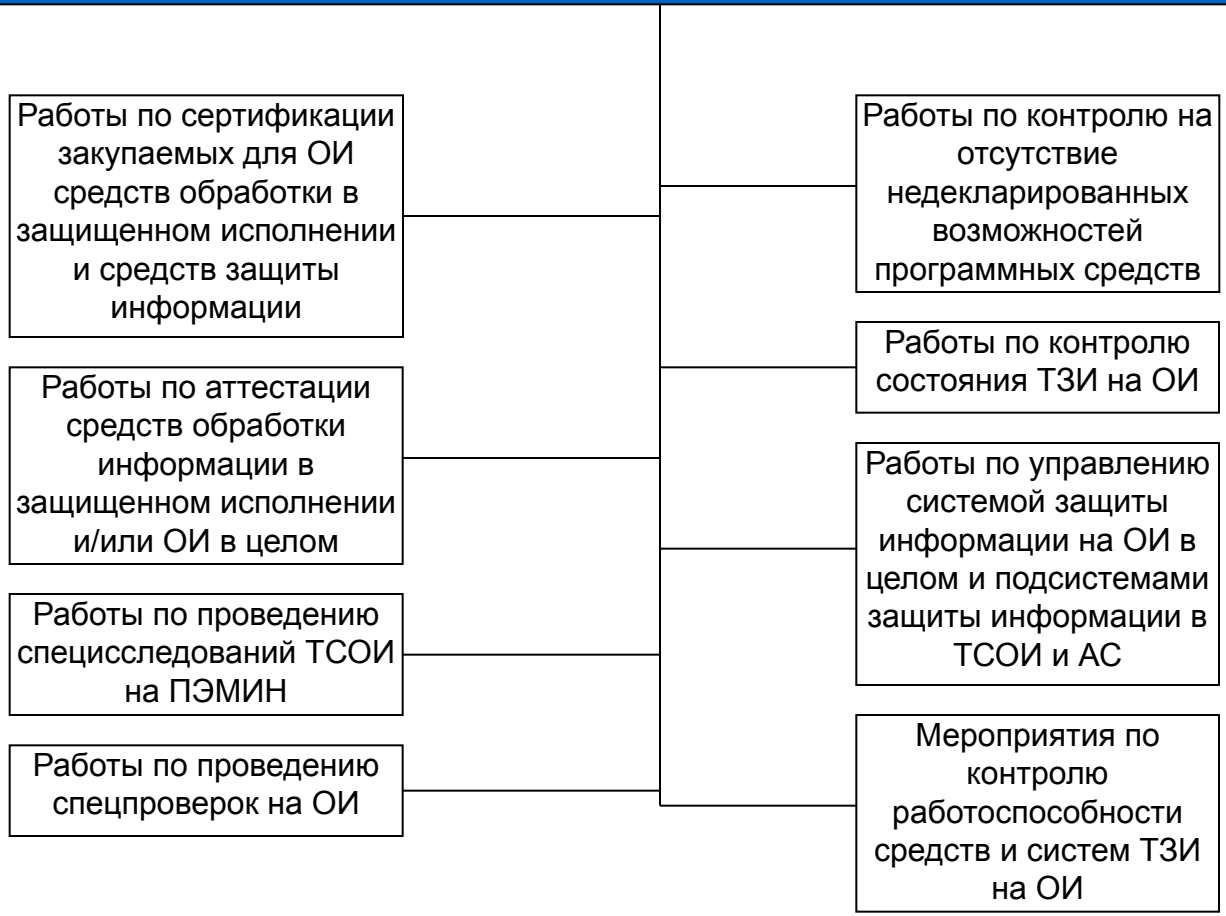
Аналитические (подготовительные) работы

- Работы по анализу исходных данных об ОИ
  - Работы по анализу процессов обработки защищаемой информации
  - Работы по анализу условий расположения ОИ и особенностей его эксплуатации
  - Работы по анализу угроз, реализация которых приводит к нарушениям БИ
- Работы по формированию требований к СЗИ на ОИ
  - Работы по определению перечня ТКУИ, каналов НСД к информации и ПМВ на информацию
  - Работы по определению требований по предотвращению утечки информации (воздействия на нее)
- Работы по определению направленности и содержания работ по ТЗИ на ОИ
  - Работы по формированию технического облика СЗИ на ОИ
  - Работы по определению состава и содержания организационных мероприятий по ТЗИ
  - Работы по определению состава и содержания технических мероприятий по ТЗИ

Работы по обеспечению и выполнению мероприятий по ТЗИ на ОИ



Работы по управлению, контролю ТЗИ на ОИ и оценке её эффективности



Общие требования по ТЗИ для ЗП по стадиям ЖЦ

Стадия ЖЦ ЗП	Требования по ТЗИ
Предпроектная	1 Исключить разглашение и утечку по ТКУИ сведений о назначении, характеристиках ЗП. 2 Исключить разглашение и утечку по ТКУИ сведений о результатах обследования зданий, помещений, в которых предполагается создание ЗП
Проектирование	1 Исключить разглашение и утечку по ТКУИ сведений о конструктивных решениях по созданию З 2 Исключить разглашение и утечку по ТКУИ сведений по характеристикам системы ЗИ, организационным и техническим мерам по обеспечению ТЗИ на разрабатываемом ВП. 3 Исключить разглашение и утечку по ТКУИ сведений по составу ОТСС и ВТСС, которые предполагается устанавливать в ЗП
Строительство	1 Исключить возможность установки закладных устройств (СЭУПИ) в ограждающих конструкциях ЗП (в элементах фундамента, стен, перекрытий). 2 Обеспечить требуемую эффективность звукоизоляции ограждающих конструкций ЗП, средств и систем вентиляции и отопления. 3 Обеспечить требуемую степень изоляции ("развязки") системы электропитания ОИ от внешних сетей электропитания. 4 Обеспечить требуемую эффективность защитного заземления оборудования ЗП. 5 Обеспечить применение сертифицированных ОТСС и ВТСС, которые планируется установить в ЗП. 6 Проведение спецпроверок и специсследований несертbфицированных программных, программно-аппаратных средств для ОТСС и разработка предписаний на их эксплуатацию. 7 Исключить несанкционированный физический доступ посторонних лиц в ЗП
Эксплуатация	1 Исключить эксплуатации ЗП без проведения аттестационных испытаний ЗП по требованиям БИ. 2 Периодическое проведение (перед проведением каждого режимного мероприятия) специальных проверок ЗП. 3 Обеспечить необходимую виброакустическую защиту ЗП. 4 Исключить доступ посторонних лиц в пределы КЗ и в ЗП
Реконструкция	1 Обеспечить постоянный контроль за осуществлением реконструкции (ремонта) ЗП. 2 Исключить (существенно затруднить) возможность установки злоумышленниками закладных устройств (СЭУПИ) в ЗП в ходе реконструкции (ремонта). 3 Исключить неконтролируемый доступ посторонних лиц в пределы КЗ и в ЗП в ходе реконструкции. 4 Исключить возможность эксплуатации ЗП после реконструкции без проведения аттестационных испытаний ЗП по требованиям БИ

Общие требования по ТЗИ для ТСОИ по стадиям ЖЦ

Стадия ЖЦ ТСОИ	Требования по ТЗИ
Обоснование разработки (НИР)	1 Исключить разглашение и утечку по ТКУИ сведений о теоретических и экспериментальных исследованиях по созданию ТСОИ
Разработка (ОКР)	1 Исключить возможность проектирования ТСОИ без аттестации рабочих мест проектировщиков по требованиям БИ. 2 Обеспечить контроль качества сборки образца в защищенном исполнении. 3 Исключить возможность производства ТСОИ без проведения приемочных испытаний опытного образца
Производство	1 Исключить возможность производства образца без аттестации рабочих мест, производственных помещений и рабочего персонала, задействованного в производстве. 2 Исключить разглашение и утечку по ТКУИ сведений о программе, методике квалификационных испытаний и технологий производства образца. 3 Обеспечить контроль технологии производства образца. 4 Исключить (существенно затруднить) возможность установки злоумышленниками закладных устройств (СЭУПИ) в образцах. 5 Обеспечить требуемую эффективность защитного заземления ТСОИ. 6 Исключить возможность эксплуатации образца ТСОИ без сертификационных испытаний, контроля качества монтажных работ, опытной эксплуатации
Эксплуатация	1 Обеспечить проведение аттестационных испытаний ТСОИ в составе ОИ по требованиям БИ. 2 Для линий передачи данных ОТСС обеспечить соответствующее удаление от границ КЗ. 3 Обеспечить периодический контроль состояния и эффективности защиты ТСОИ
Капитальный ремонт	1 Исключить (существенно затруднить) возможность установки злоумышленниками закладных устройств (СЭУПИ) в ТСОИ после ремонта. 2 Обеспечить проведение аттестационных испытаний по требованиям БИ ТСОИ после его доработки

Общие требования по ТЗИ для АС по стадиям ЖЦ

Стадия ЖЦ АС	Требования по ТЗИ
Формирование требований к АС	Исключить разглашение и утечку по ТКУИ сведений о проводимых работах на ОИ по обработке информации различной степени конфиденциальности, а также результатов оценки целесообразности создания АС
Разработка концепции АС	Исключить разглашение и утечку по ТКУИ сведений о выбранной концепции (разработанном замысле) СЗИ в АС
Разработка ТТЗ	Исключить разглашение и утечку по ТКУИ тактико-технического задания (или его части) на создание АС
Разработка эскизного проекта на АС и её СЗИ	Исключить разглашение и утечку по ТКУИ сведений об эскизном проекте на АС и ее СЗИ
Технический проект на АС и ее СЗИ	1 Исключить разглашение и утечку по ТКУИ сведений о техническом проекте на АС и ее СЗИ. 2 Обеспечить экспертизу отчетной научно-технической документации на создание АС и ее СЗИ на соответствие требованиям ТТЗ. 3 Исключить разглашение и утечку по ТКУИ сведений о проектировании помещений для АС
Разработка РКД и производство	1 Исключить разглашение и утечку по ТКУИ сведений о РКД на АС и ее СЗИ. 2 Обеспечить сертификацию и аттестацию СЗИ на соответствие требованиям по БИ. 3 Обеспечить отсутствие НДВ и СЭУПИ
Ввод в действие	1 Исключить разглашение и утечку по ТКУИ сведений об организационных мерах ТЗИ в АС. 2 Обеспечить проведение проверки квалификации специалистов подразделения по ЗИ. 3 Исключить поставку несертифицированных по требованиям БИ комплектующих изделий для СЗИ. 4 Обеспечить участие специалистов по ЗИ в ходе комплексной наладки всех средств АС. 5 Обеспечить проведение специсследований и аттестации АС
Сопровождение АС и ее СЗИ	1 Обеспечить периодический контроль за стабильностью характеристик и общего состояния АС. 2 Исключить разглашение и утечку по ТКУИ сведений об АС и мерах ТЗИ. 3 Проводить периодические спецпроверки программных и технических средств на отсутствие недекларированных возможностей и СЭУПИ