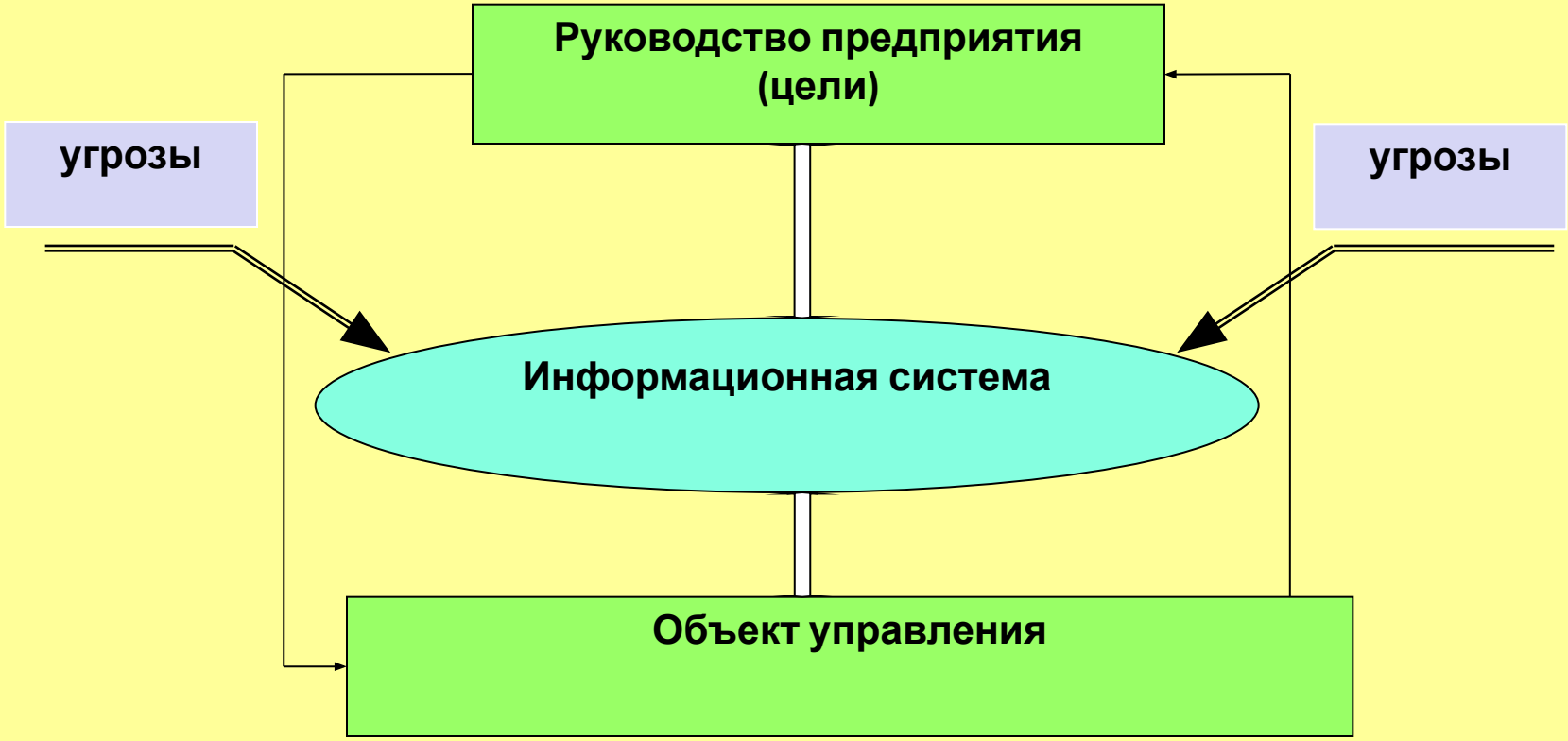
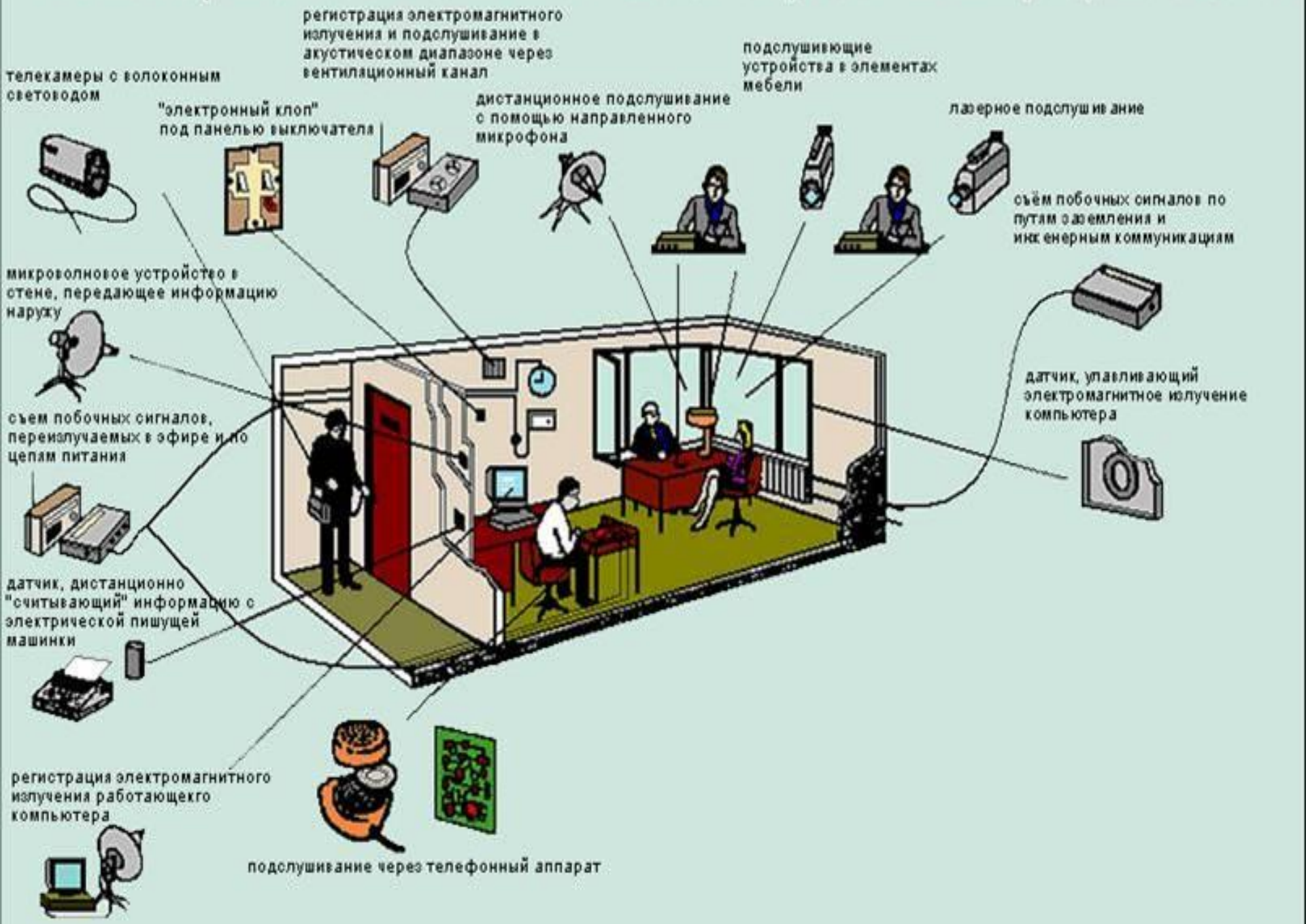
Информационная система как объект воздействия злоумышленников



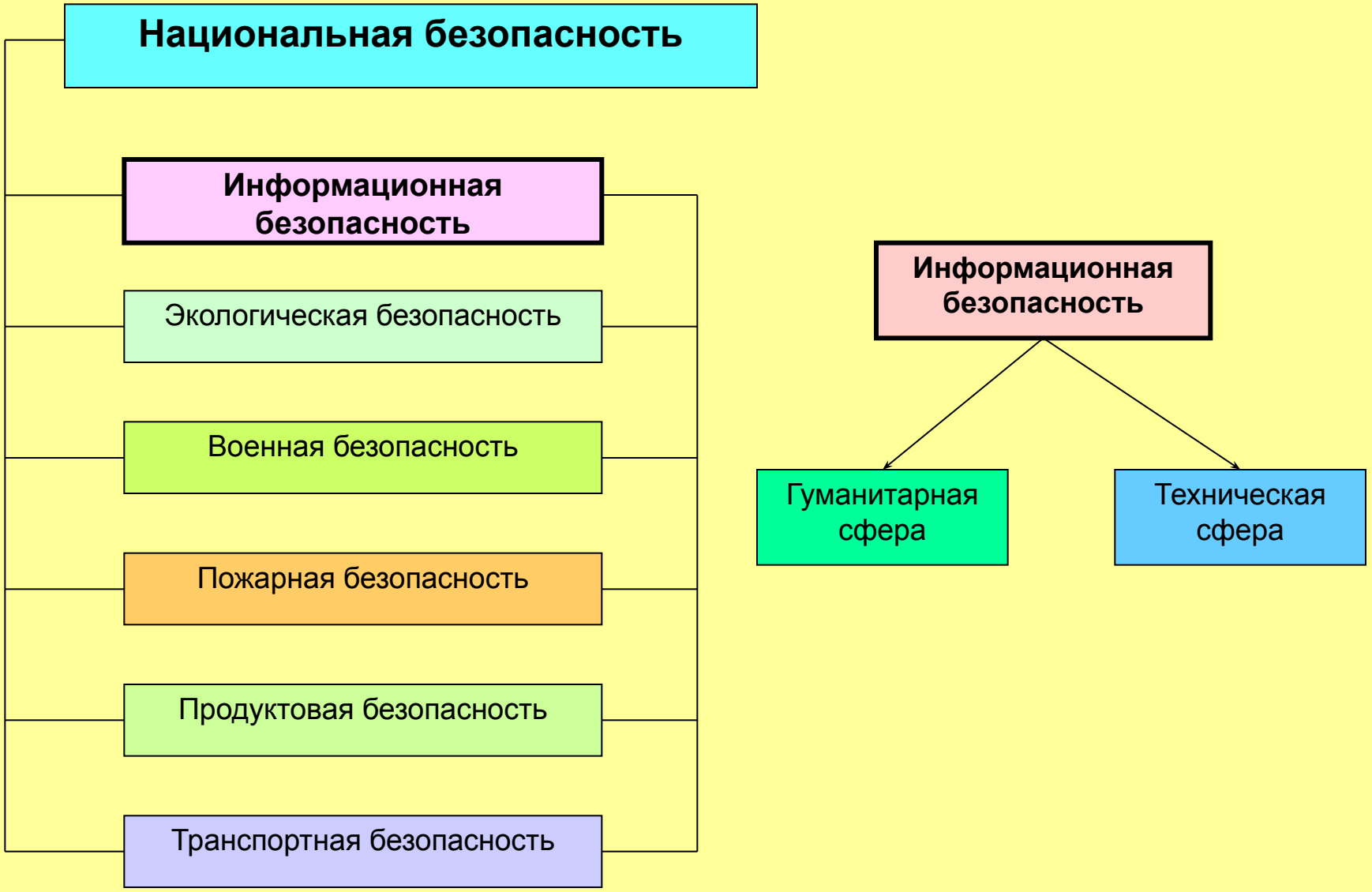
Некоторые возможные каналы утечки информации



Факторы, обуславливающие решение проблем информационной безопасности

- **высокие темпы роста парка персональных компьютеров**
- **увеличение объёмов информации**
- **интенсивное развитие АПС и технологий, не соответствующих современным требованиям безопасности**
- **слабое регулирование государством процессов функционирования и развития рынка средств информатизации, информационных услуг**
- **несоответствие стремительного развития СОИ и основ теории ИБ международным стандартам и правовым нормам**
- **широкое использование не защищенных от утечки информации и несертифицированных импортных АПС и технологий для хранения, обработки и передачи информации**
- **повсеместное распространение сетевых технологий, создание единого информационно-коммуникационного пространства на базе сети Internet**
- **обострение криминогенной обстановки, рост числа компьютерных преступлений**

Место информационной безопасности в обеспечении национальной безопасности



Информационная безопасность

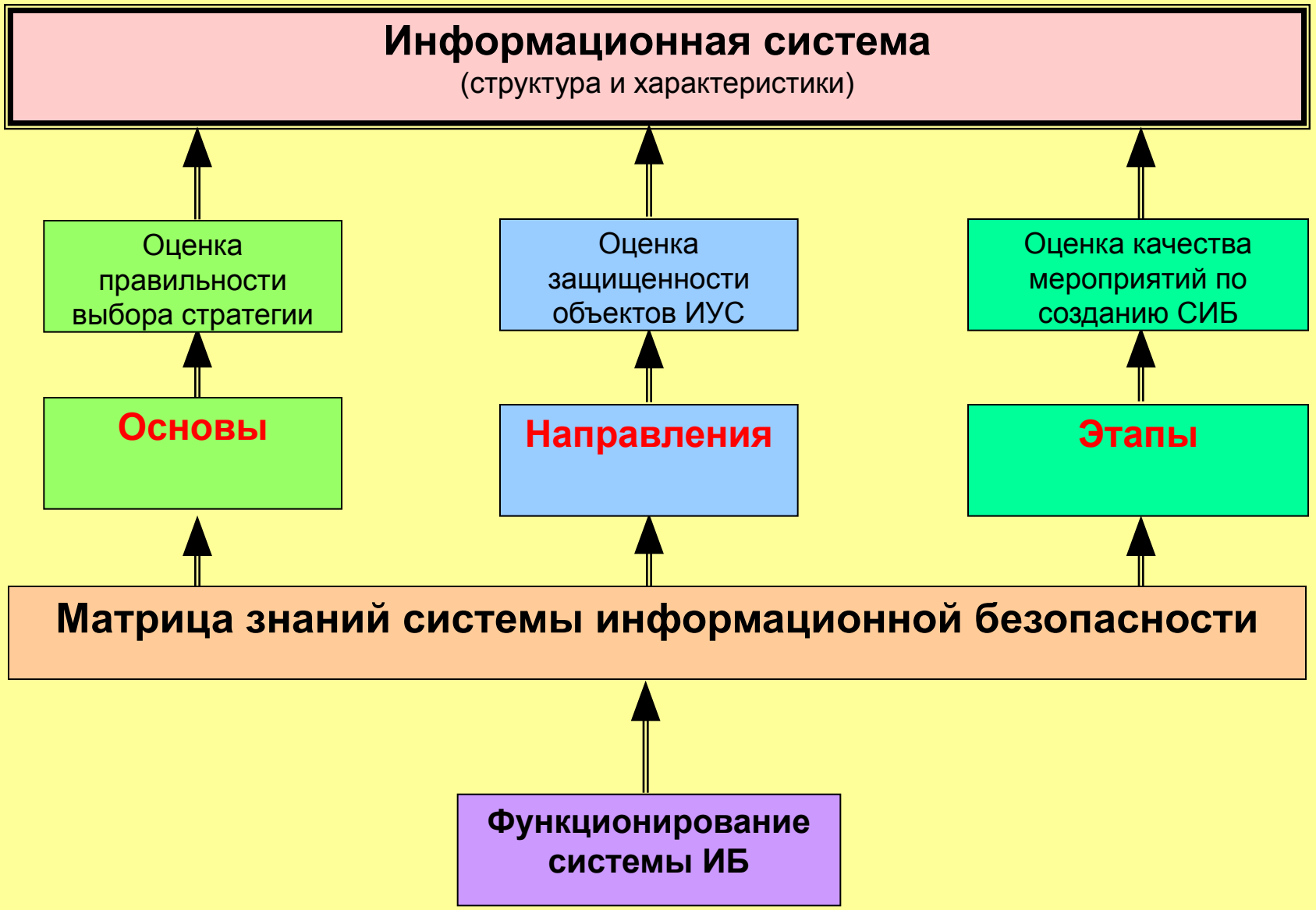
Безопасность [Safety (security)] - свойство системы противостоять внешним или внутренним дестабилизирующим факторам, следствием воздействия которых могут быть нежелательные её состояния или поведение.

Безопасность информации [Information security] - состояние защищенности информации от различных угроз, обеспечивающее сохранение таких качественных характеристик (свойств) информации как секретность /конфиденциальность/, целостность и доступность.

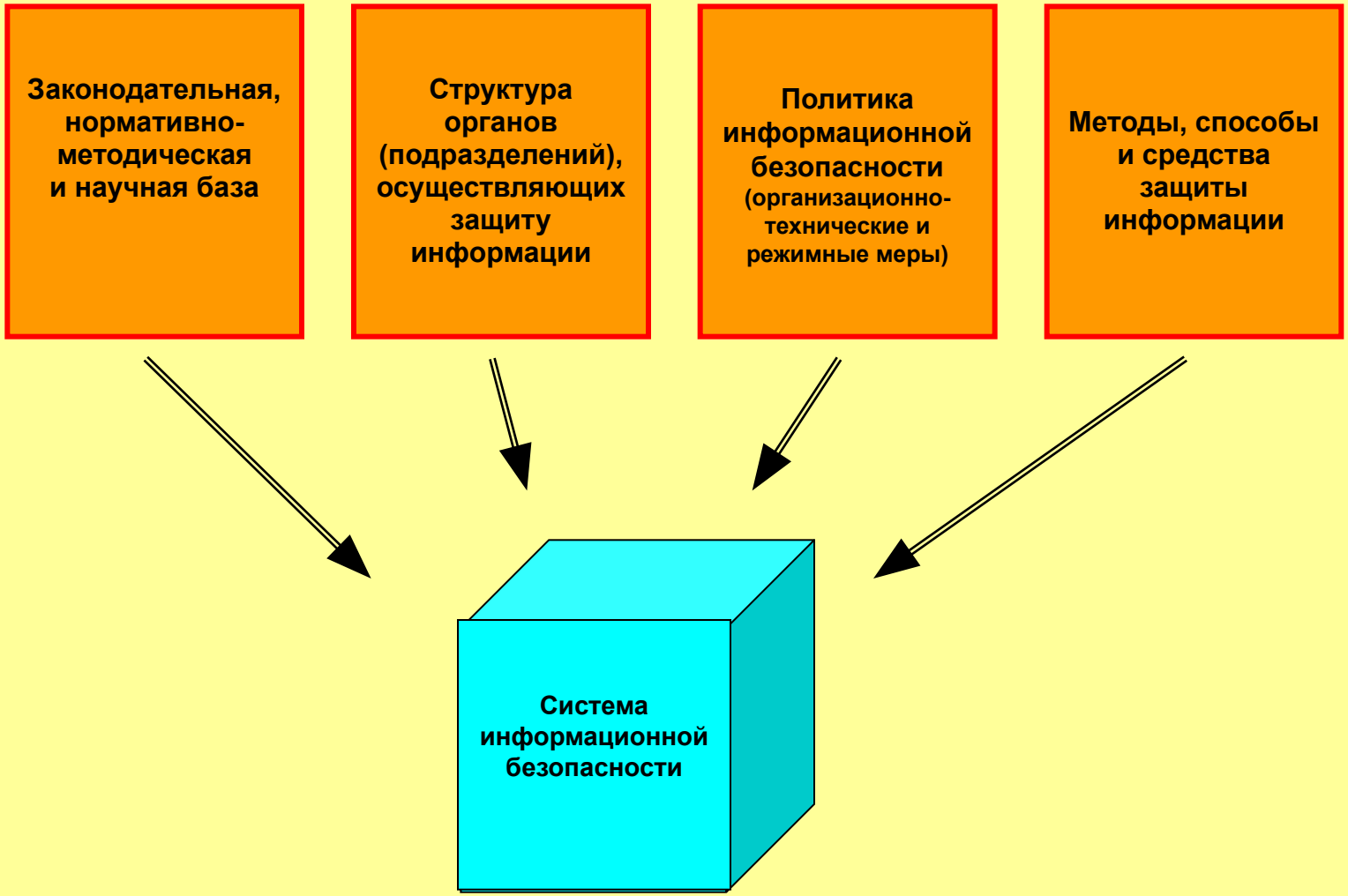
Безопасность информации в ИС - защищённость информации и оборудования ИС от факторов, представляющих угрозу для: конфиденциальности (обеспечение санкционированного доступа); целостности; доступности.

Информационная безопасность - способность ИС противостоять случайным или преднамеренным, внутренним или внешним информационным воздействиям, следствием которых могут быть её нежелательное состояние или поведение.

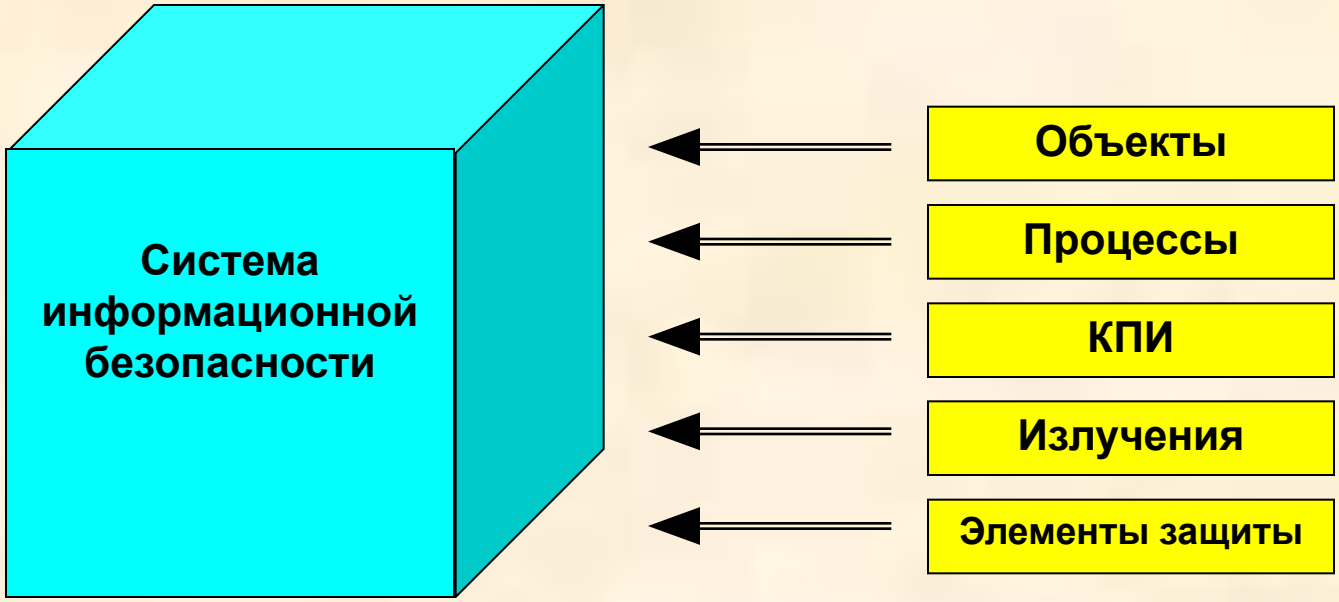
Информационная безопасность - это защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.


Информационная система
(структура и характеристики)
Оценка правильности выбора стратегии
Оценка защищенности объектов ИУС
Оценка качества мероприятий по созданию СИБ
Основы
Направления
Этапы
Матрица знаний системы информационной безопасности
Функционирование системы ИБ

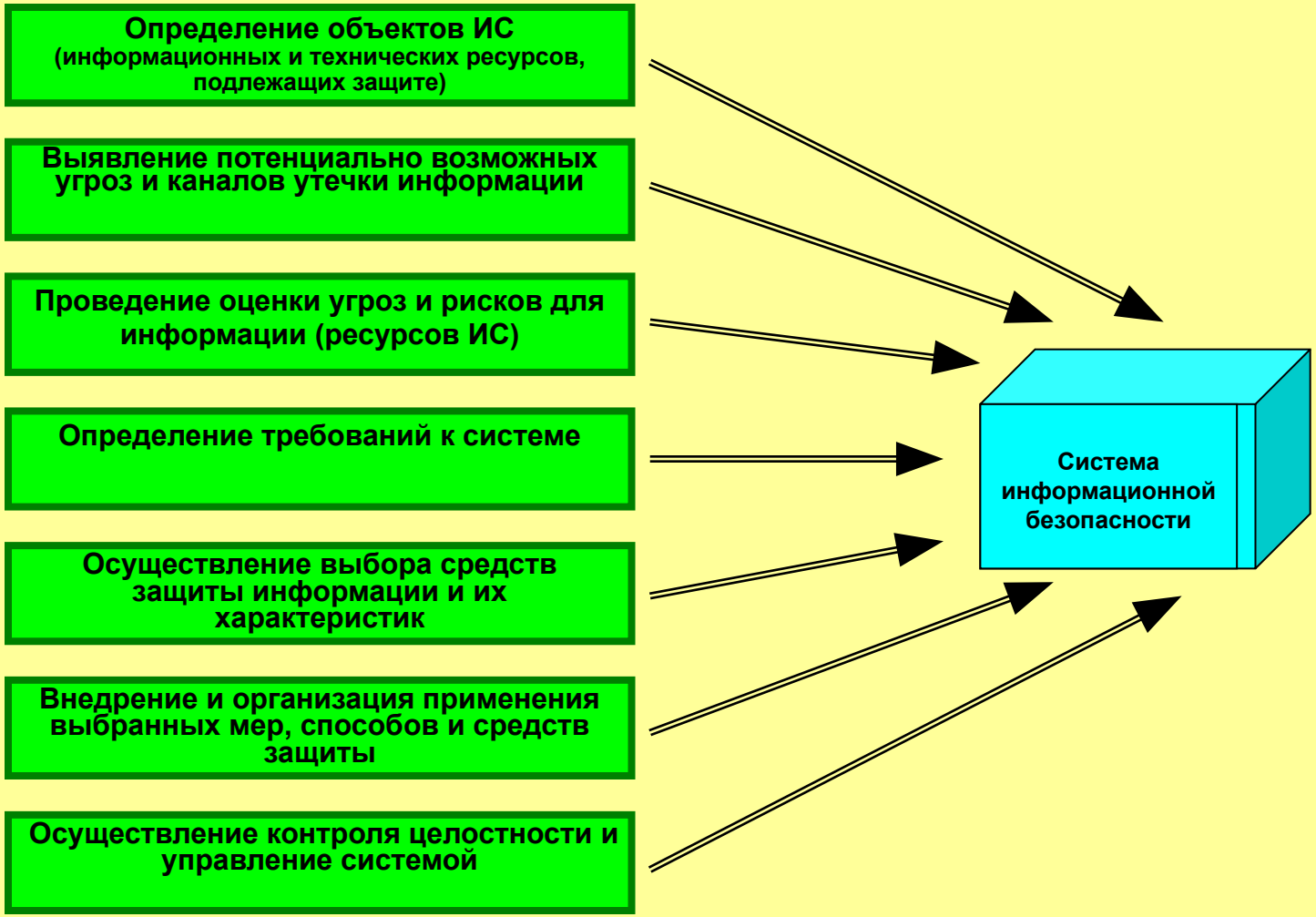
Основы информационной безопасности



Направления информационной безопасности



Этапы формирования информационной безопасности



Компьютерная система - *человеко-машинная система, представляющая совокупность электронно-программируемых технических средств обработки, хранения и представления данных, программного обеспечения (ПО), реализующего информационные технологии осуществления каких-либо функций, и информации (данных).*

Состав:

- средства вычислительной техники;
- программное обеспечение;
- каналы связи;
- информация на различных носителях;
- персонал и пользователи системы.

***под конфиденциальностью информации** понимается специфическое свойство отдельных категорий (видов) информации, которое субъективно устанавливается ее обладателем, когда ему может быть причинен ущерб от ознакомления с информацией неуполномоченных на то лиц, при условии того, что обладатель принимает меры по организации доступа к информации только уполномоченных лиц*

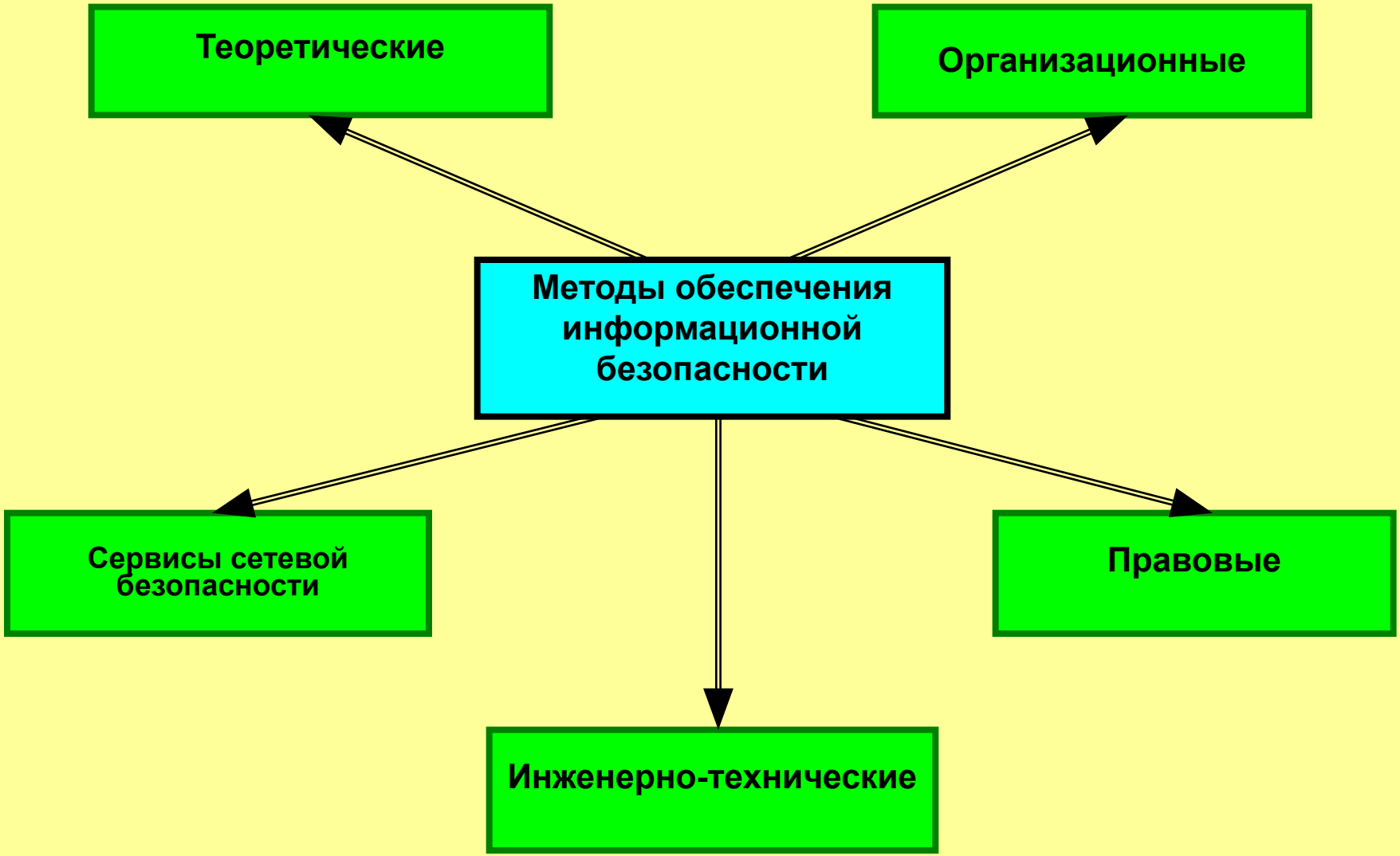
***под целостностью информации (данных)** понимается неискаженность, достоверность, полнота, адекватность и т.д. информации, т.е. такое ее свойство, при котором содержание и структура данных определены и изменяются только уполномоченными лицами и процессами*

***под [правомерной] доступностью информации (данных)** понимается такое свойство информации, при котором отсутствуют препятствия доступа к информации и закономерному ее использованию обладателем или уполномоченными лицами*

Общая характеристика принципов обеспечения компьютерной безопасности

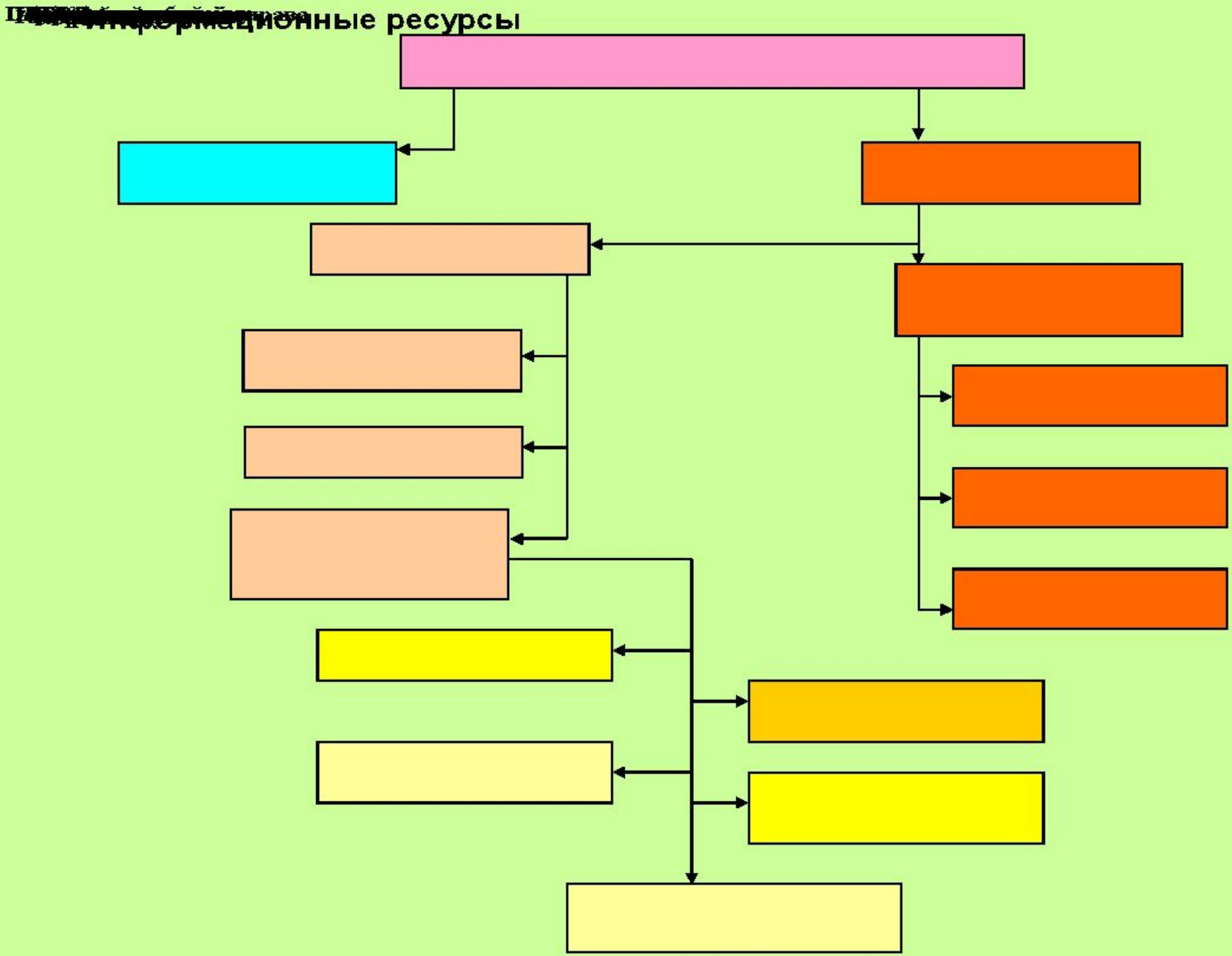
- разумной достаточности
- целенаправленности
- системности
- комплексности
- непрерывности
- управляемости
- сочетания унификации и оригинальности

Основные методы обеспечения информационной безопасности




Систематика методов и механизмов обеспечения КБ
Основного характера (прямого действия)
Обеспечивающего (профилактирующего) характера
Общесистемного характера
Непосредственного действия
Инфраструктурного характера
Общеархитектурного характера
Управление (контроль) конфигурацией
Управление сеансами
Управление удаленным доступом с раб. станций
Управление сетевым соединениями
Идентификация/аутентификация пользователей, устройств, данных
Управление памятью, потоками, изоляция процессов
Управление транзакциями
Управление инфраструктурой сертификатов криптоключей
Разграничение доступа к данным
Контроль, управление информационной структурой данных
Контроль ограничений целостности данных
Шифрование данных
ЭЦП данных
Защита/удаление остаточной информации на носителях данных и в освобождаемых областях оперативной памяти
конфиденциальность
целостность
доступность
Протоколирование, аудит событий
Резервирование данных, журнализация процессов изменения данных
Профилактика носителей данных
Учет/контроль носителей данных
Нормативно-организационная регламентация использования КС
Обучение. нормативно-административное побуждение и принуждение пользователей по вопросам ИБ

Структура информационных ресурсов




Нормативная правовая база
Международные правовые акты
Нормативные правовые акты федерального уровня
Конституция
Концептуальные документы
Кодексы
Федеральные законы
Указы Президента Российской Федерации
Постановления правительств
Государственные стандарты
Акты федеральных органов исполнительной власти
Межведомственные акты
Ведомственные акты
Отраслевые стандарты
Нормативные акты субъектов РФ
Нормативные акты органов местного самоуправления
Нормативные документы уровня предприятий

Понятие стандарта информационной безопасности

Стандарт - документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнение работ или оказание услуг.

Главная задача стандартов информационной безопасности:

создать основы взаимодействия между производителями, потребителями и экспертами по квалификации продуктов информационных технологий

Требования по безопасности должны быть предельно конкретными, и должны регламентировать необходимость использования тех или иных средств, механизмов или алгоритмов. Эти требования также не должны вступать в противоречие с существующими алгоритмами

Общепринятая классификация стандартов в области информационной безопасности

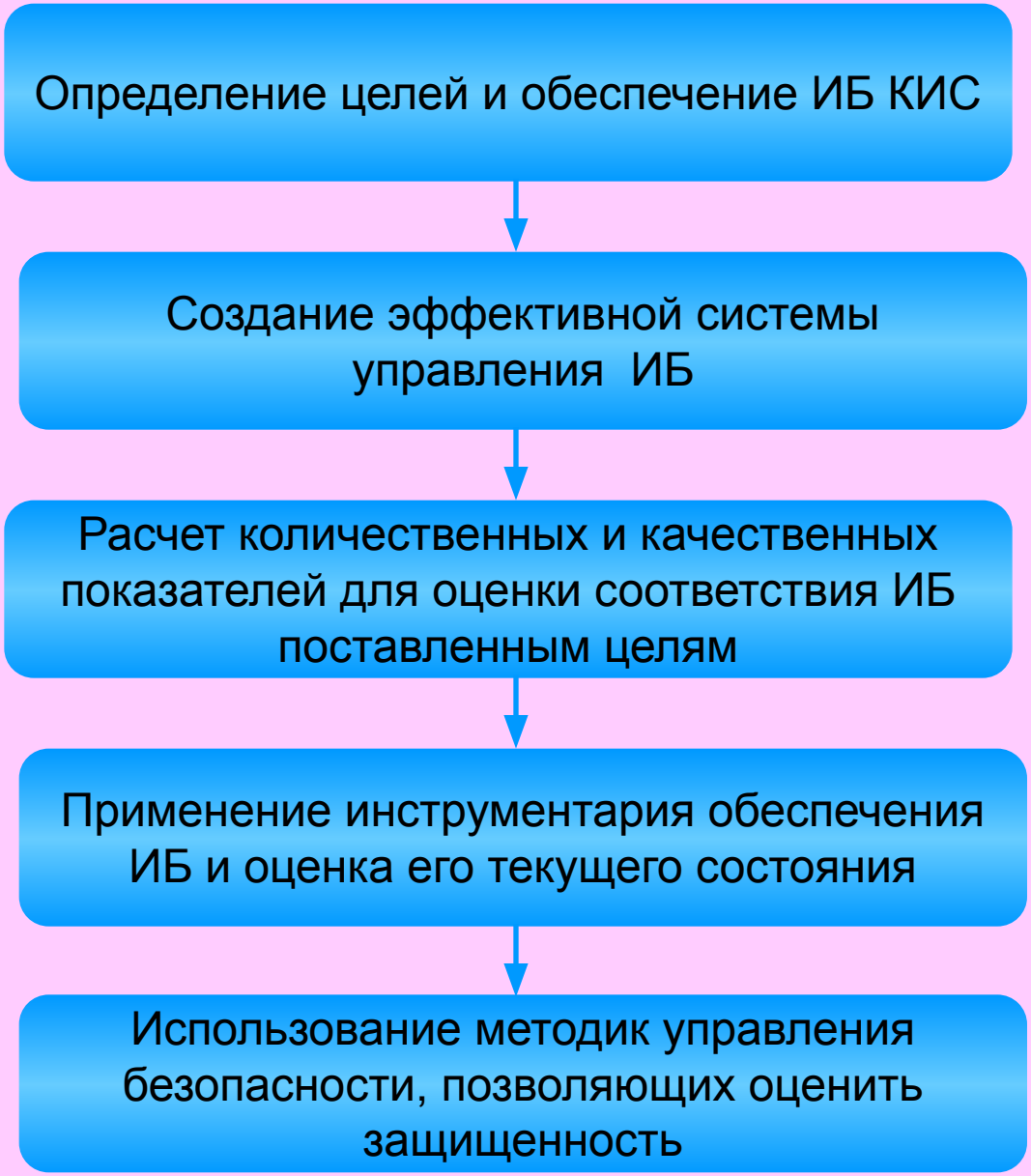
Оценочные стандарты

- Оранжевая книга
- Общие критерии ISO/IEC 15408-1999
- РД ФСТЭК РФ

Спецификации

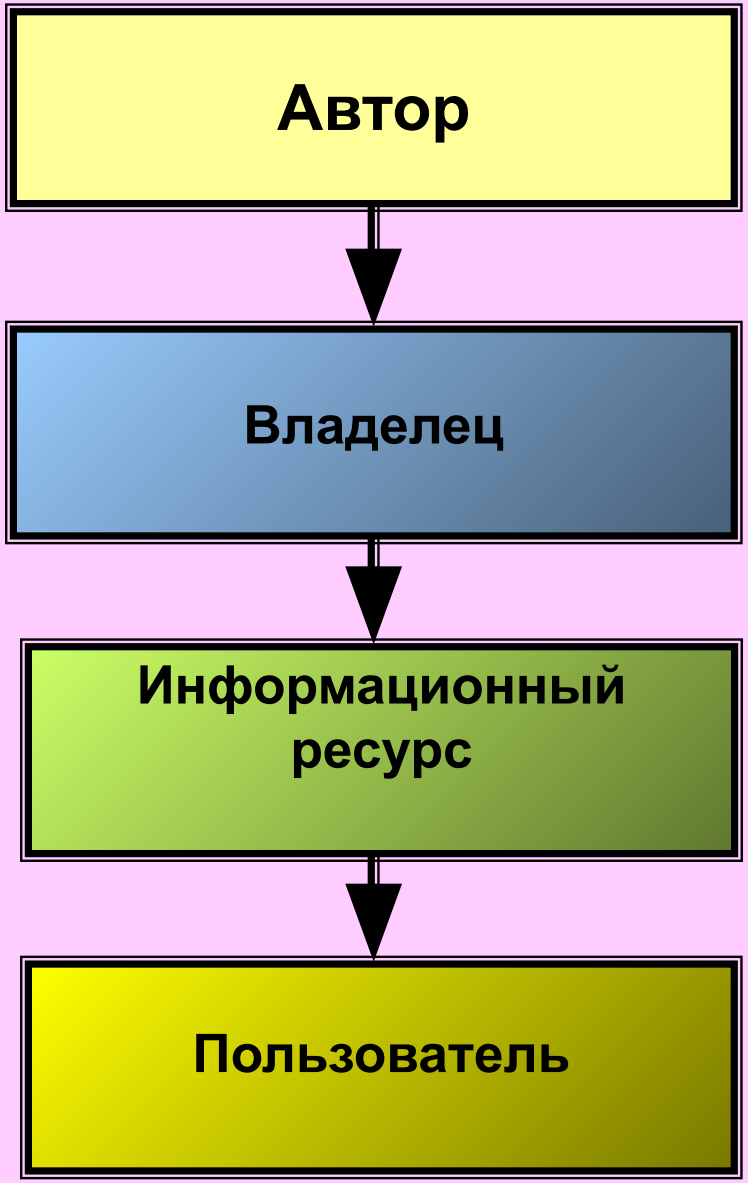
- Инфраструктура открытых ключей X.509
- Криптографический алгоритм СКА ГОСТ 28147-89
- Управленческий стандарт ISO 17799
- Управленческий стандарт ISO 27001
- ГОСТ 3410-2001
- ГОСТ 28147-89
- ГОСТ 4311-94

В соответствии со стандартами обеспечение ИБ в организации предполагает

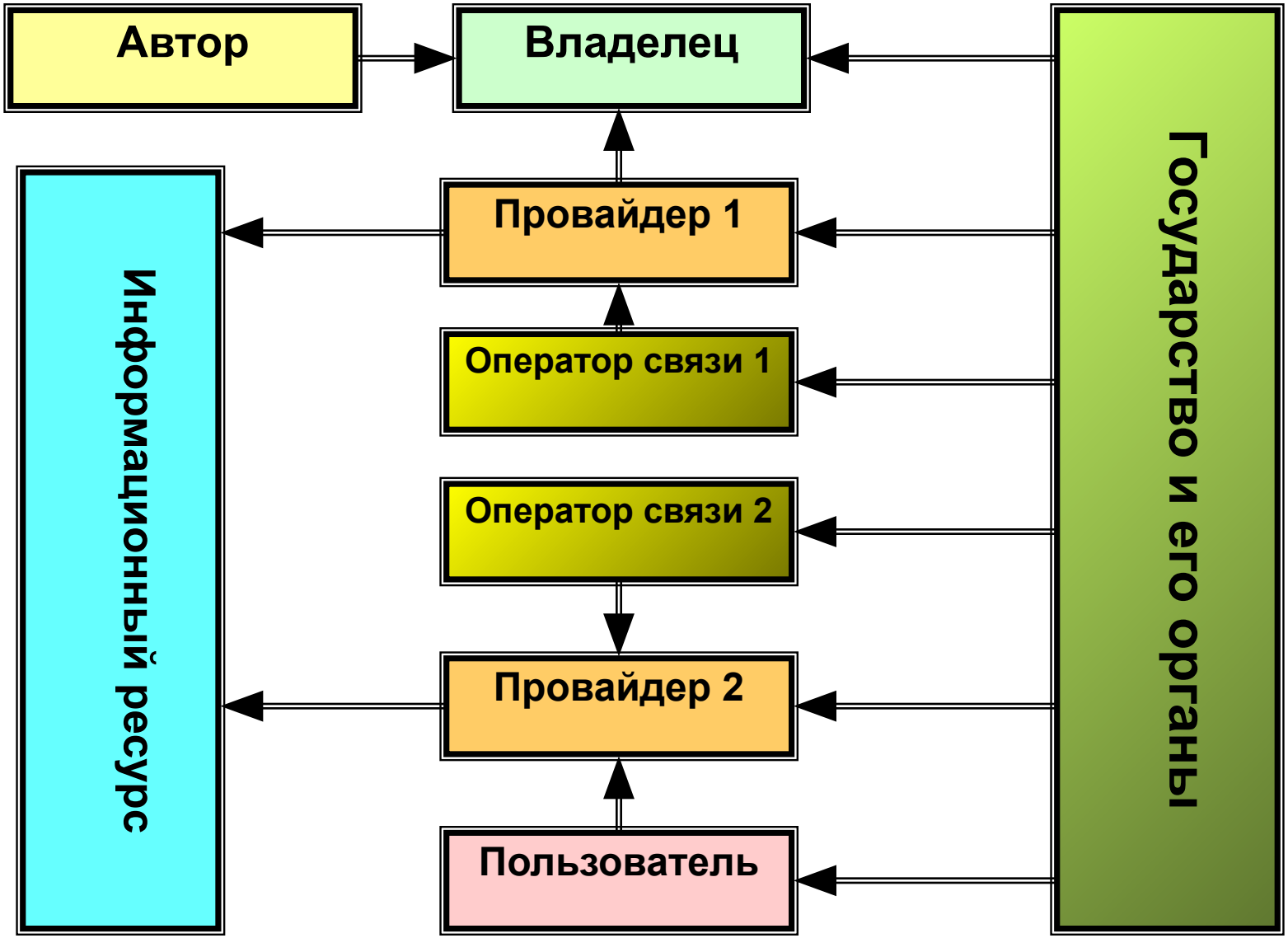


Модель информационной безопасности

Отношения субъектов информационного обмена в сети Internet



Отношения субъектов информационных процессов в сети Internet



Нормативно-правовые акты, регламентирующие использование сети Интернет

Указ президента 2004г. № 611 «О мерах по обеспечению ИБ РФ в сфере международного информационного обмена.

Постановление правительства № 564 от 1998г. «Об утверждении положения о лицензировании деятельности по международному информационному обмену»

Постановление правительства № 538 от 2005г.«Об утверждении правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность»

Постановление правительства №32 от 2006г. «Об утверждении правил оказания услуг связи по передаче данных»

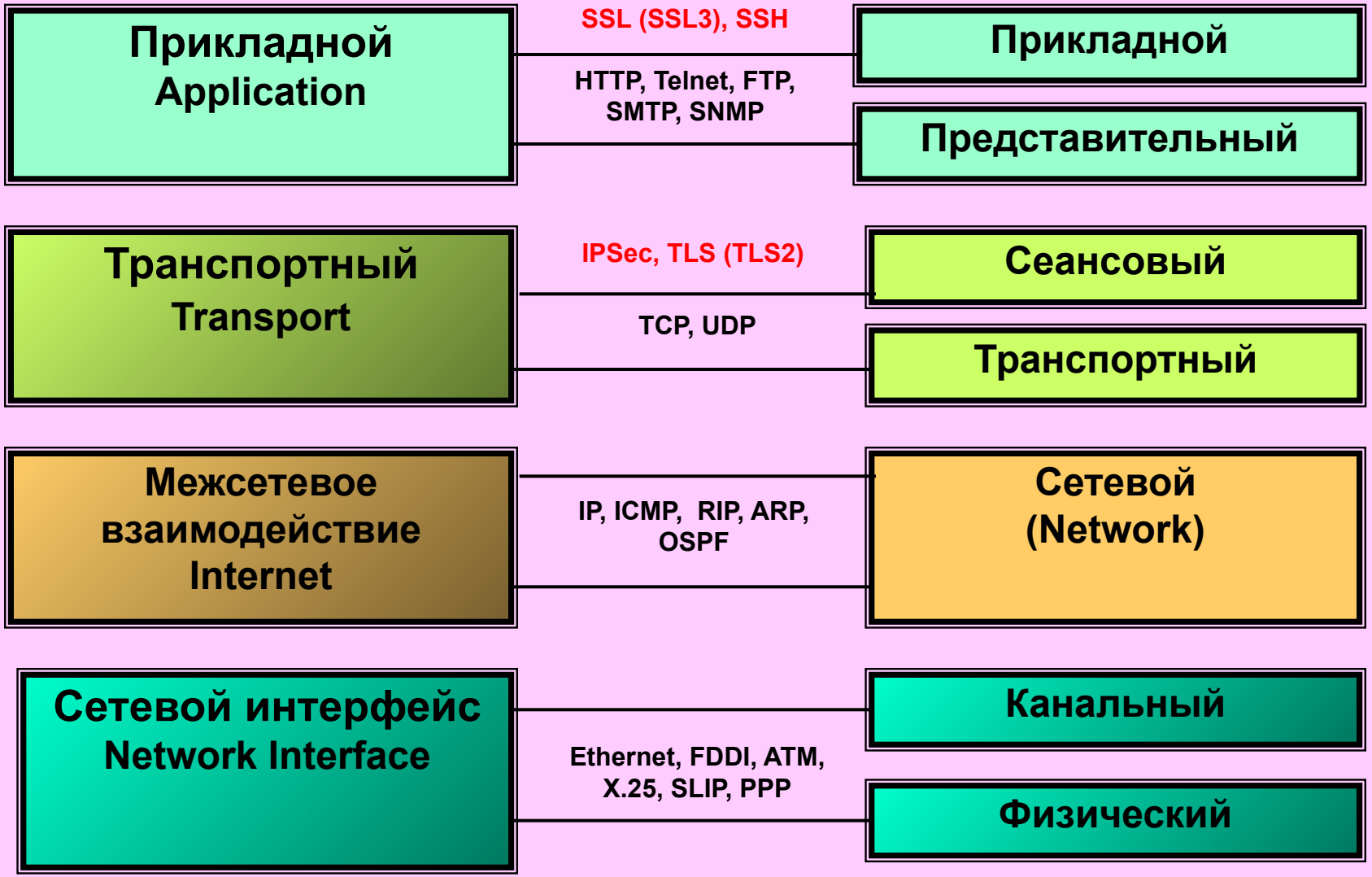
Постановление правительства № 147 от 2007г. «Об утверждении положения о о пользовании официальными сайтами в сети Интернет для размещения информации о заказах на поставку товаров, выполнении работ, оказании услуг для государственных и муниципальных нужд и о требованиях к технологическим программам, лингвистическим, правовым и организационным средствам обеспечения пользования указанными сайтами».

Принятая в 2007г. Советом безопасности «Стратегия развития информационного общества в России».

Стандартная модель взаимодействия открытых систем OSI (Open System Interconnection)

Тип данных	Уровень	Функции
Данные	прикладной	Доступ к сетевым службам
	представительный	Представление и кодирование данных
	сеансовый	Управление сеансом связи
Блоки	транспортный	Прямая связь между конечными пунктами и надежность
Пакеты	сетевой	Определение маршрута и логическая адресация
Кадр	канальный	Физическая адресация
Биты	физический	Работа со средой передачи, сигналами и двоичными кодами

Уровни стека протоколов TCP/IP



Уровни стека TCP/IP

Уровни модели OSI

Логические и физические соединения между уровнями стека TCP/IP

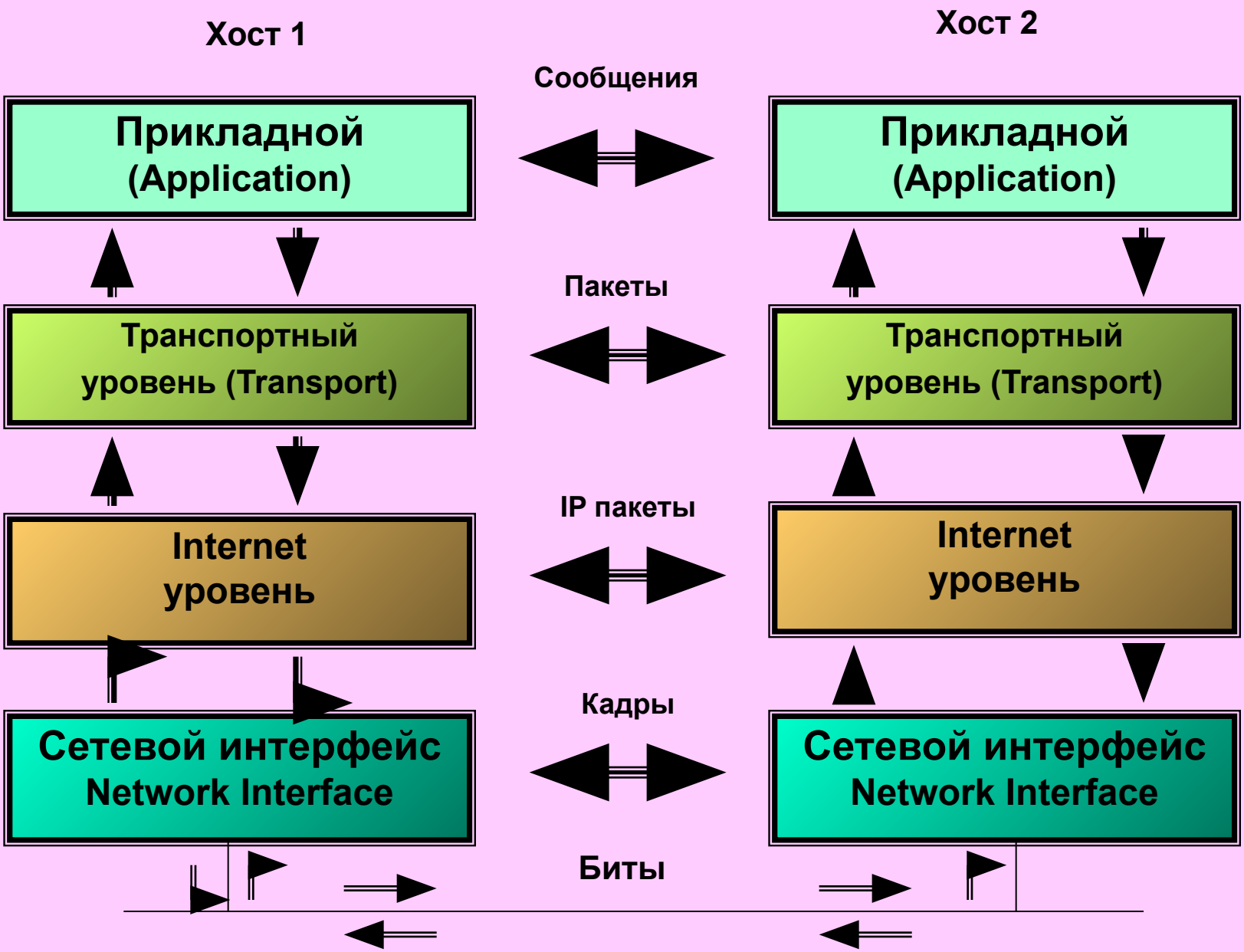
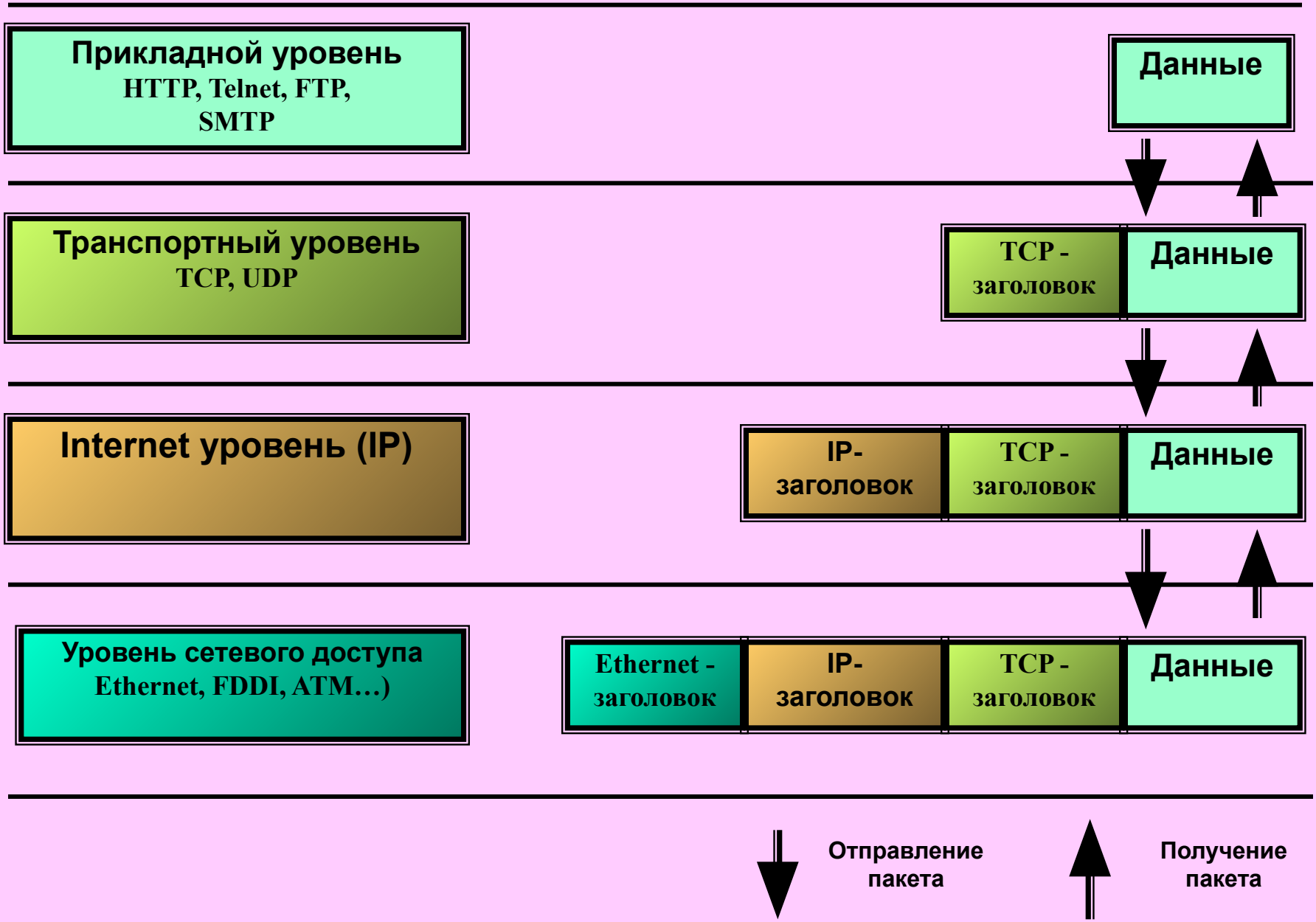


Схема инкапсуляции данных в стеке протоколов TCP/IP



Некоторые зарезервированные порты

Порт	Протокол	Использование
21	FTP	Передача файлов
23	Telnet	Дистанционный вход в систему
25	SMTP	Электронная почта
69	TFTP	Простейший протокол передачи файлов
79	Finger	Поиск информации о пользователе
80	HTTP	Мировая Паутина
110	POP-3	Удаленный доступ к электронной почте
119	NNTP	Группы новостей