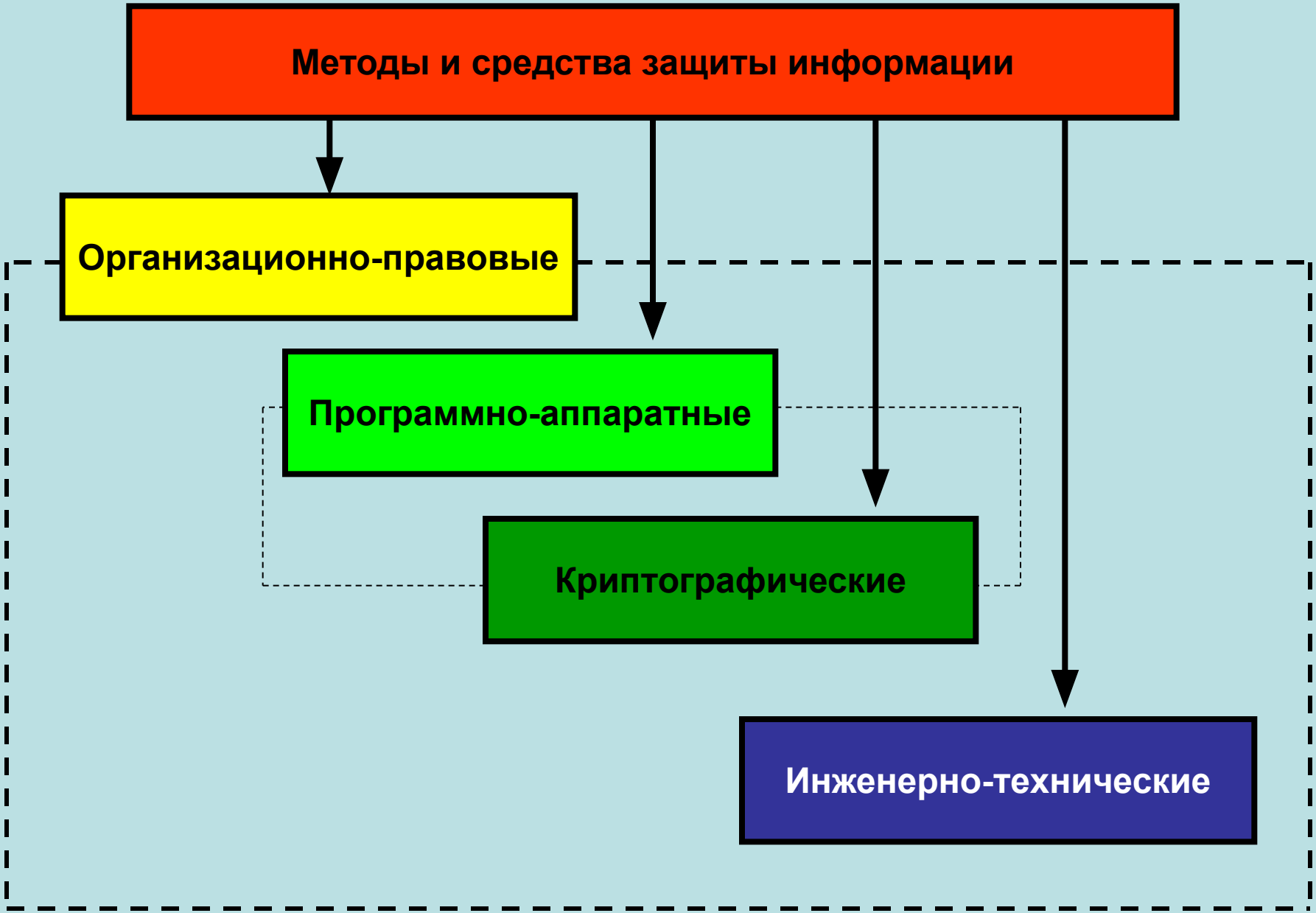
Методы и средства защиты информации


Методы и средства защиты информации
Организационно-правовые
Программно-аппаратные
Криптографические
Инженерно-технические

Программно-аппаратные и криптографические способы и средства защиты информации

Компьютерная система (КС) – это комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации/информационных ресурсов.

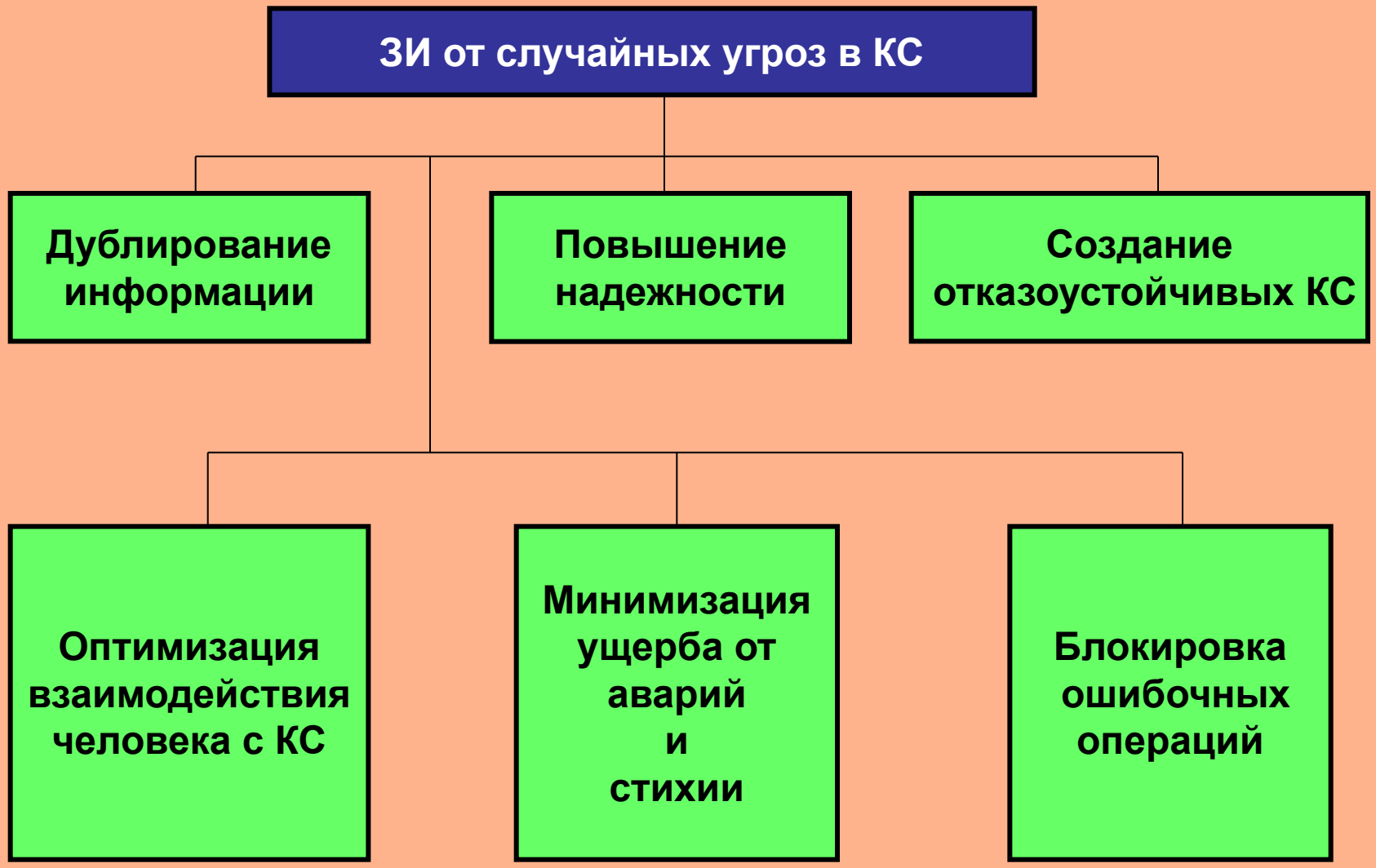
Информационные ресурсы – отдельные документы и массивы документов в информационных системах (библиотеках, архивах, банках данных).

Безопасность информации в КС – это такое состояние всех компонентов КС, при котором обеспечивается защита информации от возможных угроз на требуемом уровне.

Под системой защиты информации в КС понимается единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающих защищенность информации в КС.

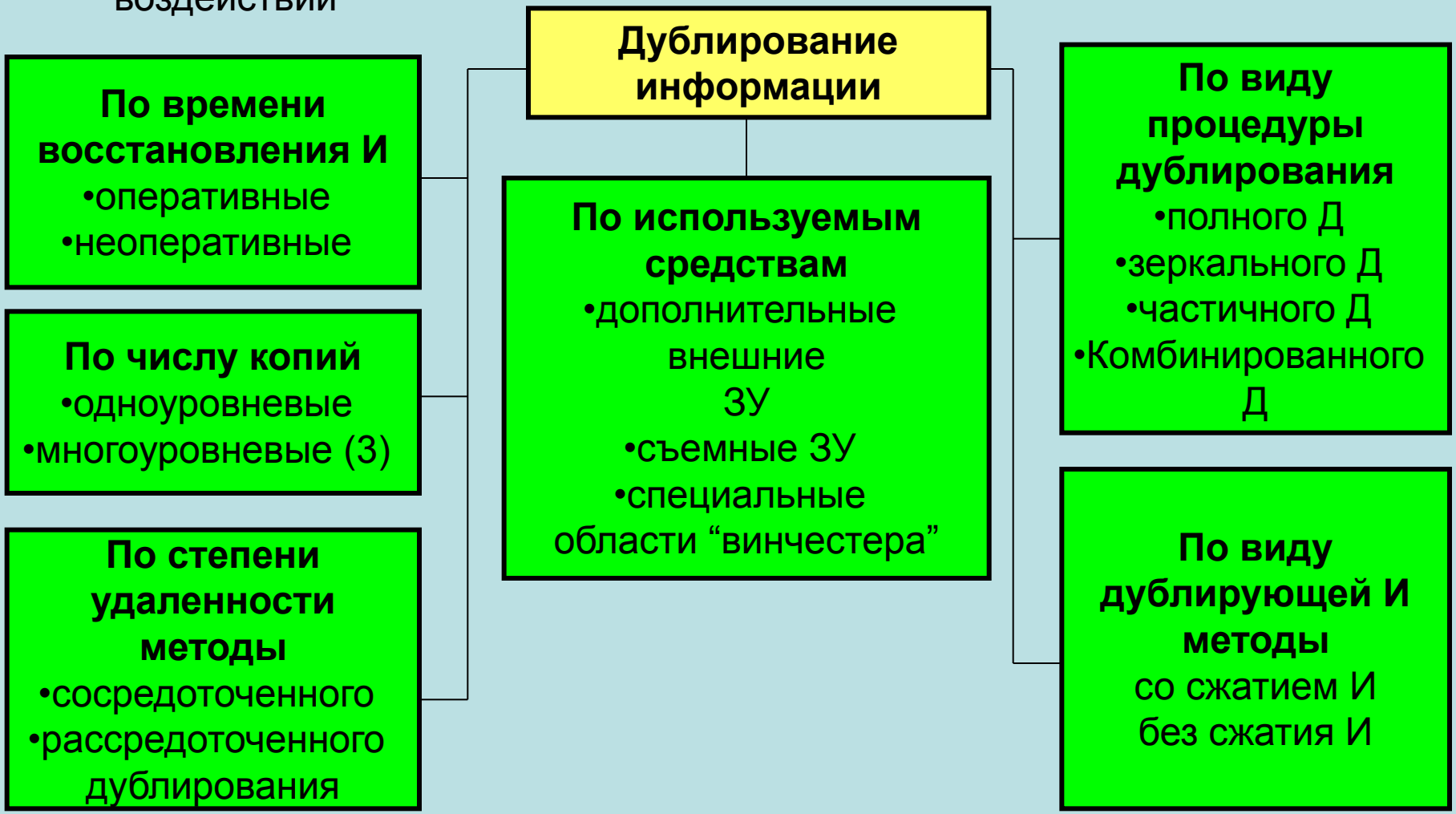
Угрозы безопасности информации в КС

Задачи защиты информации в КС от случайных угроз



Дублирование информации

Дублирование информации является одними из самых эффективных способов защиты информации от случайных угроз и преднамеренных воздействий

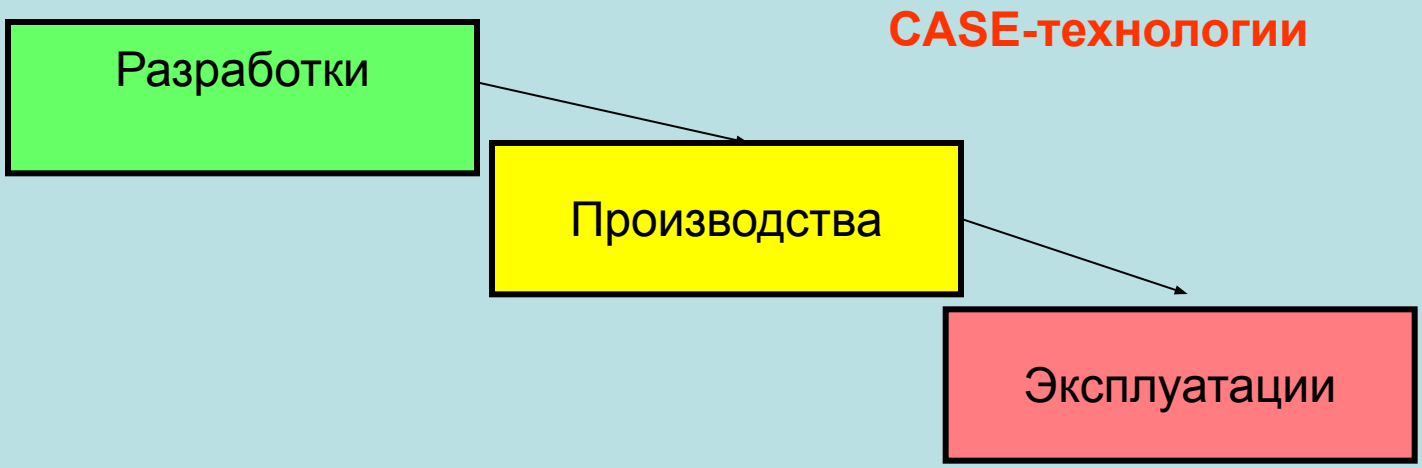


Повышение надежности КС

Под ***надежностью*** понимается свойство системы выполнять возложенные на нее задачи в определенных условиях эксплуатации.

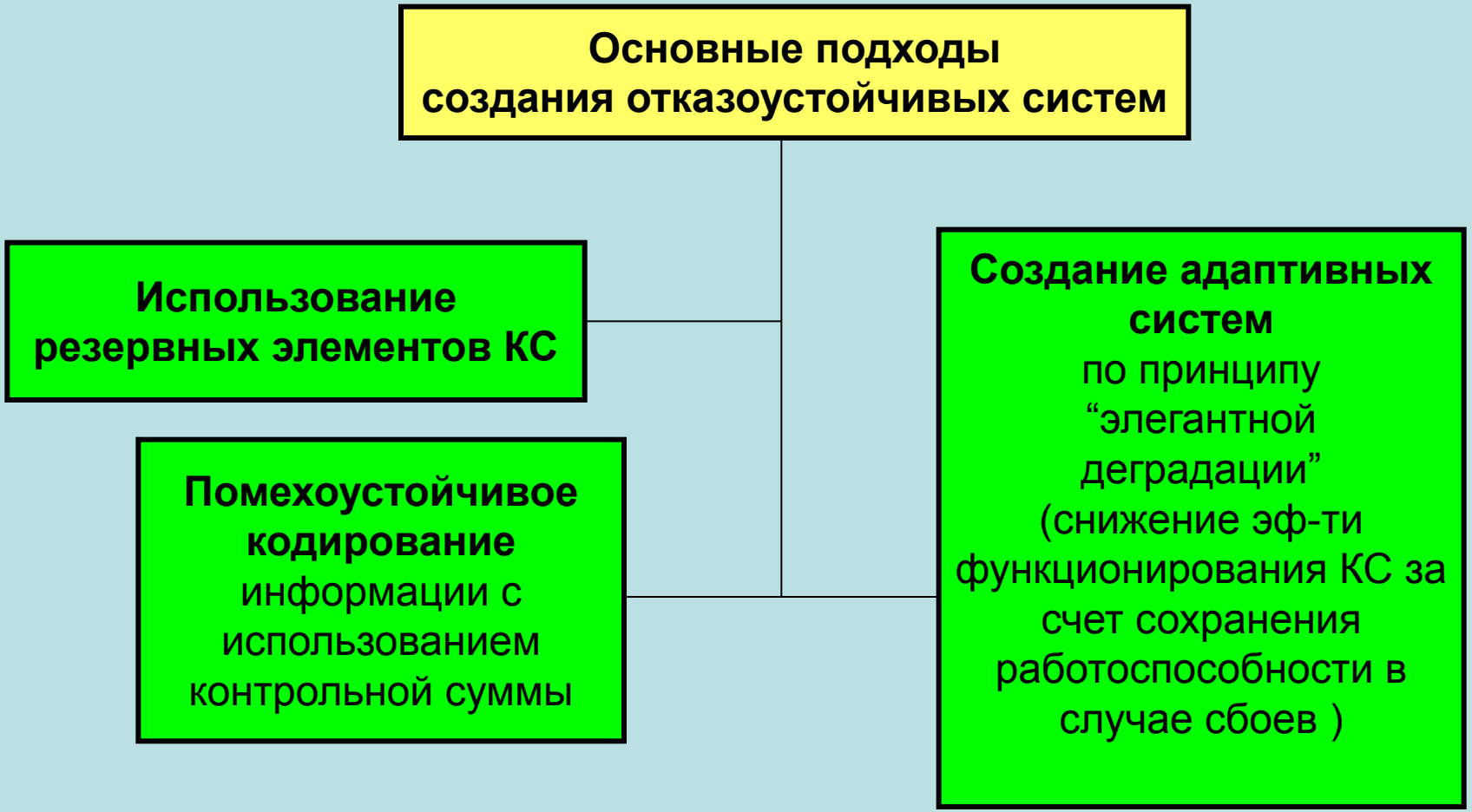
С точки зрения ЗИ необходимо обеспечивать надежность и работоспособность КС.

Надежность КС обеспечивается надежностью программных и аппаратных средств на этапах:

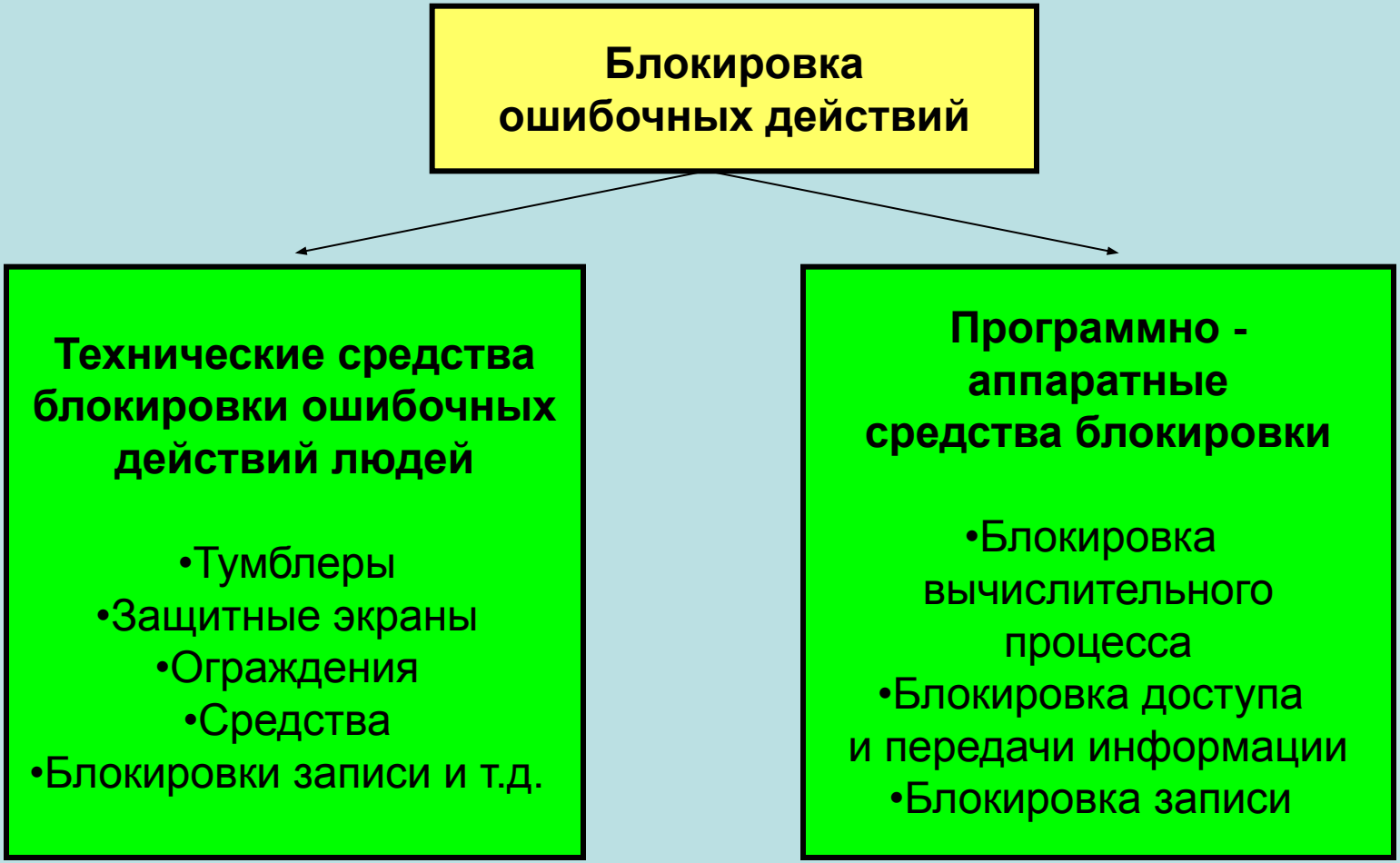


Создание отказоустойчивых КС

Отказоустойчивость – свойство КС сохранять работоспособность при отказах отдельных устройств, блоков и алгоритмов.



Блокировка ошибочных операций



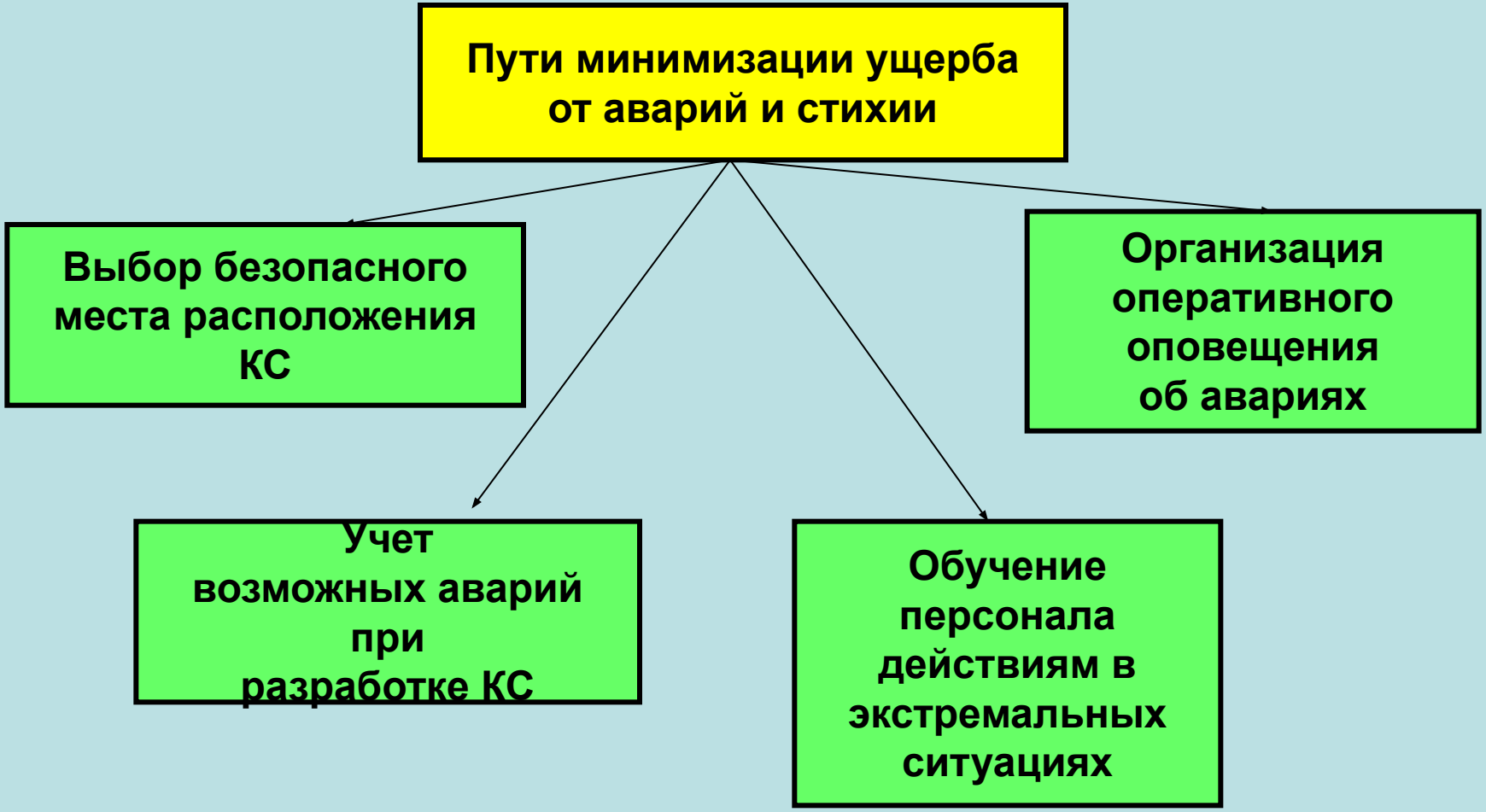
Оптимизация взаимодействия пользователей и КС

Основной задачей ЗИ в КС является защита от преднамеренных угроз и ошибок обслуживающего персонала.

Для достижения этих целей необходимы:

- Стимулирование труда и заинтересованность;
- Воспитание и обучение персонала;
- Анализ и совершенствование процессов взаимодействия человека с КС;
- Оборудование рабочих мест;
- Оптимальный режим труда и отдыха.

Минимизация ущерба от аварий и стихийных бедствий



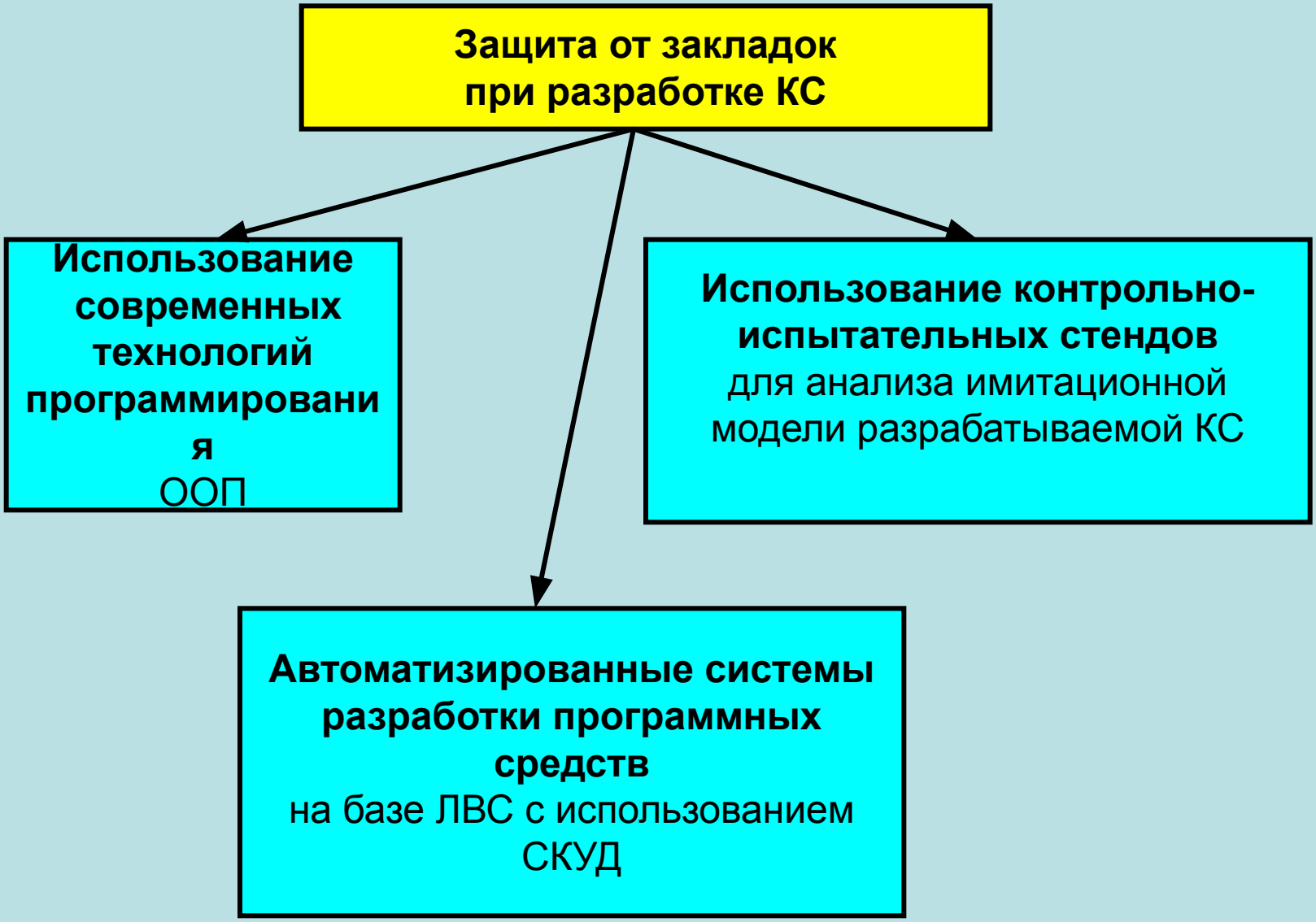
Задачи защиты информации в КС от преднамеренных угроз

Методы защиты от несанкционированного изменения структур (НИС) КС

Несанкционированному изменению могут быть подвергнуты алгоритмическая, программная и техническая структуры КС на этапах разработки и эксплуатации.

Особенностью НИС является универсальность методов, позволяющая наряду с умышленными воздействиями выявлять и блокировать непреднамеренные ошибки персонала.

НИК КС, выполненные на этапе разработки и при модернизации называются закладками.


Защита от закладок
при разработке КС
Использование современных технологий программирования
ООП
Использование контрольно-испытательных стендов
для анализа имитационной модели разрабатываемой КС
Автоматизированные системы разработки программных средств
на базе ЛВС с использованием СКУД

Защита от закладок
В процессе эксплуатации КС

Охрана помещений КС

Разграничение доступа к оборудованию КС

•идентификация и
•аутентификация
•блокирование
•журнализация
•действий

Противодействие несанкционированному подключению Устройств

идентификаторы
устройств с использованием
кода - идентификатора

Защита от монтажа, замены и переключения элементов КС

Блокировка доступа
Автоматизированный контроль
вскрытия аппаратуры

Защита информации в КС от НСД

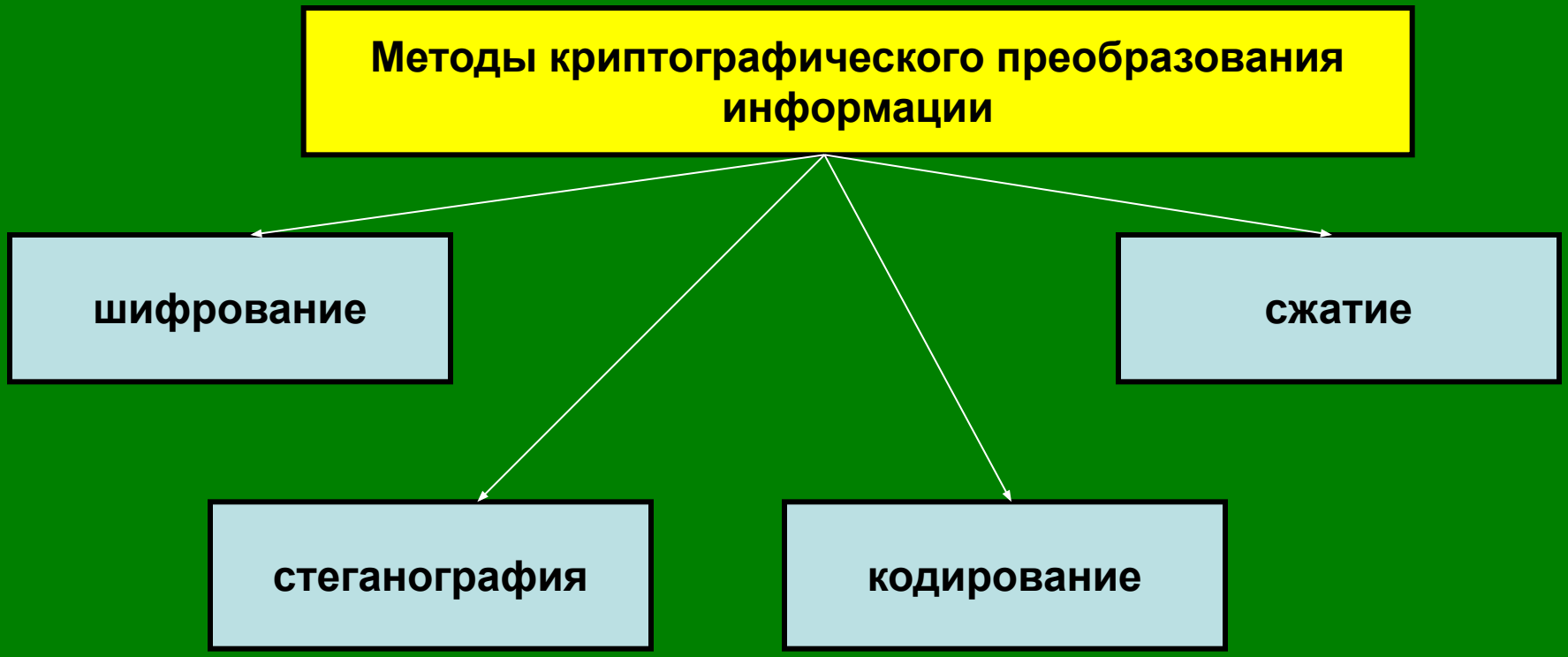
Для защиты информации в КС от НСД применяют отечественные **программные системы** защиты ПЭВМ “Снег - 1”, “Кобра”, “Страж” и др, и **программно - аппаратные средства** защиты “Аккорд”, “SecretNET”, “VipNET”, “Редут”, “ДИЗ - 1” и др.

Данные средства реализуют максимальное число защитных механизмов:

- Идентификация и аутентификация пользователей
- Разграничение доступа к файлам, каталогам, дискам
- Шифрование информации
- Защита процесса загрузки ОС путем блокирования устройств в/вывода и каналов связи
- Блокировка КС на время отсутствия персонала
- Регистрация событий
- Защита информации от копирования
- Очистка памяти

Криптографические методы защиты информации

Под криптографической защитой понимают такое преобразование информации, в результате которого она становится недоступной для преобразования и использования лицами, не имеющими на то прав.



Шифрование

Процесс **шифрования** заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информации представляет собой хаотический набор букв, цифр, других символов и двоичных кодов.

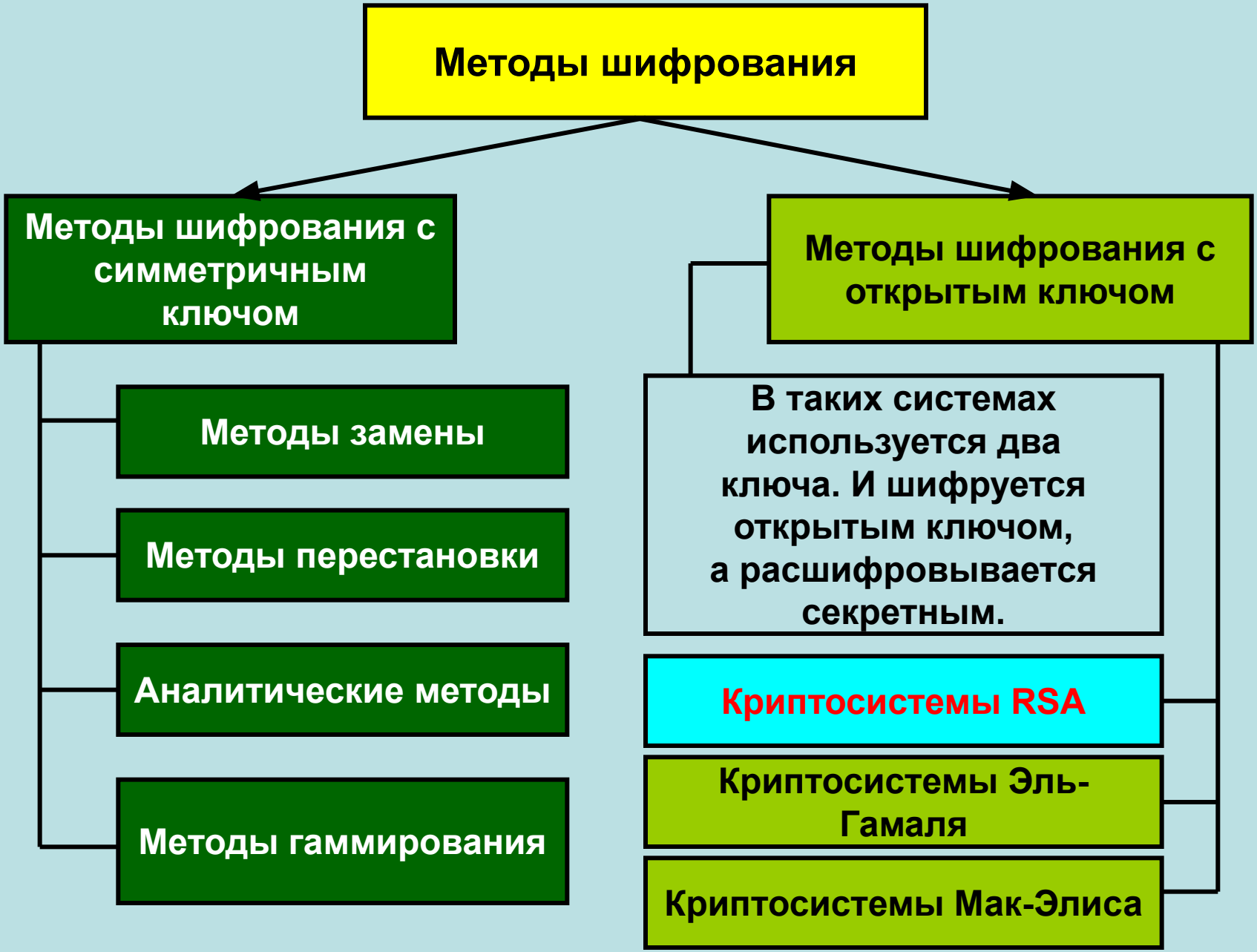
Для шифрования информации используются **алгоритм преобразования информации** и **ключ**. Алгоритм для определенного метода шифрования является неизменным. Ключ содержит управляющую информацию, который определяет выбор преобразования на определенных шагах алгоритма шифрования.

Методом шифрования или **шифром** называется совокупность обратимых преобразований открытой информации в закрытую в соответствии с алгоритмом шифрования.

Атака на шифр или **криптоанализ** – это процесс расшифрования закрытой информации без знания ключа и при отсутствии сведений об алгоритме шифрования.

Современные методы шифрования должны отвечать следующим **требованиям**:

- Криптостойкость должна быть такой, чтобы вскрытие шифра могло быть осуществлено только путем полного перебора;
- Криптостойкость обеспечивается не секретностью алгоритма шифрования, а секретностью ключа;
- Шифротекст не должен существенно превосходить по объему исходную информацию;
- Время и стоимость шифрования не должны быть большими.


Методы шифрования
Методы шифрования с симметричным ключом
Методы замены
Методы перестановки
Аналитические методы
Методы гаммирования
Методы шифрования с открытым ключом
В таких системах используется два ключа. И шифруется открытым ключом, а расшифровывается секретным.
Криптосистемы RSA
Криптосистемы Эль-Гамаля
Криптосистемы Мак-Элиса

Методы стеганографии позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения и передачи информации.

Кодирование информации – замена смысловых конструкций исходной информации кодами, в качестве которых могут использоваться сочетания букв и цифр.

Сжатие информации относится к криптографии с ограничениями: при сжатии сокращается объем информации, но при этом сжатая информация может быть использована без обратного преобразования. Поэтому вместе с методами сжатия применяют методы шифрования.

Конфиденциальность и безопасность при работе с электронной почтой

Методы обеспечения информационной безопасности при работе с электронной почтой

Анонимность

- Использование бесплатных анонимных Web почтовых ящиков *www.rambler.ru* *www.narod.ru*
- Системы переадресовки (*www.iname.com*)

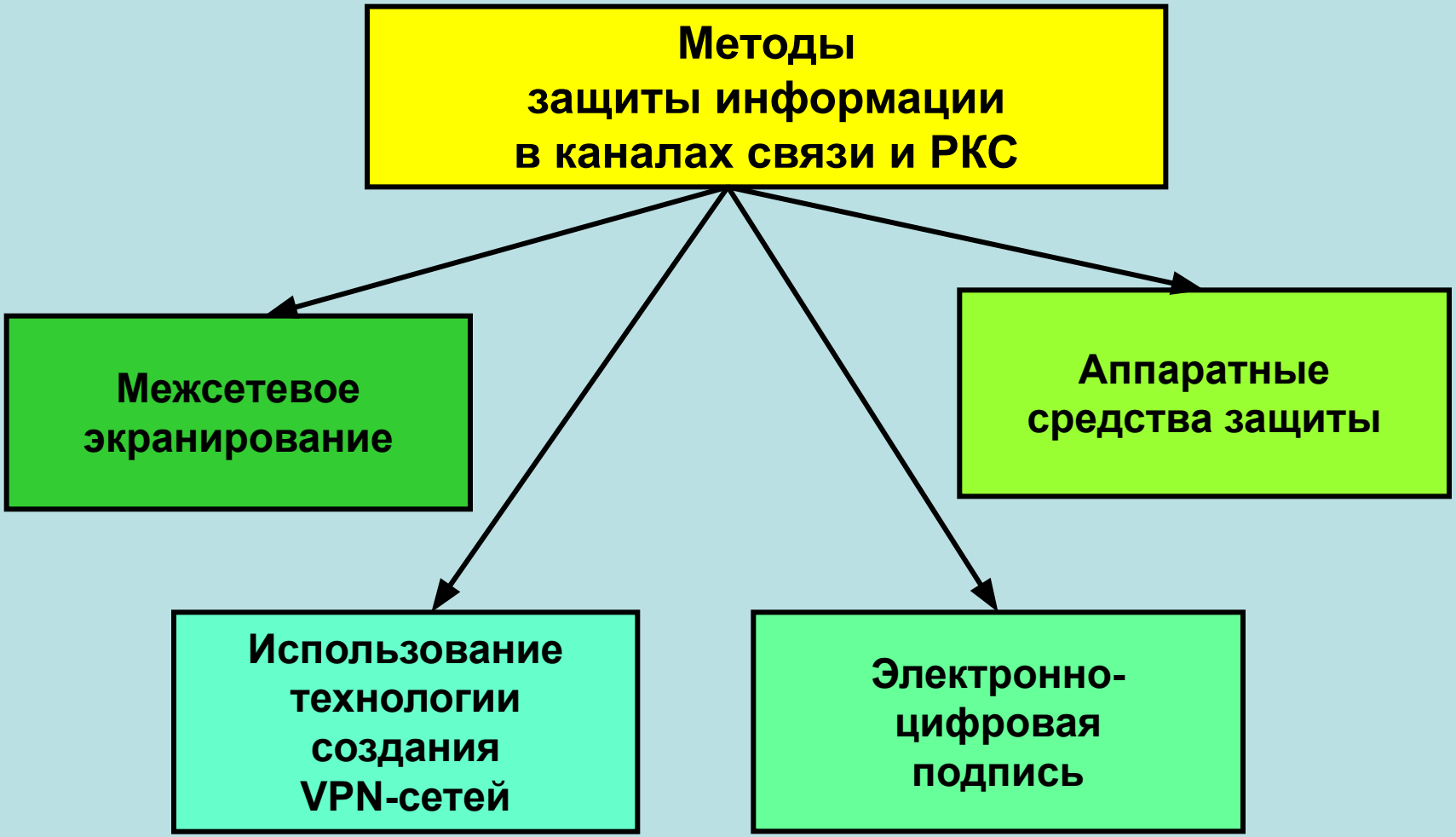
Шифрование

- Настройка стандартных почтовых программ(*The Bat, Outlook Express*)
- ЭЦП (*www.pgpi.com*)
- Спецпрограммы для шифрования информации типа SaveDisk
- ЭЦП

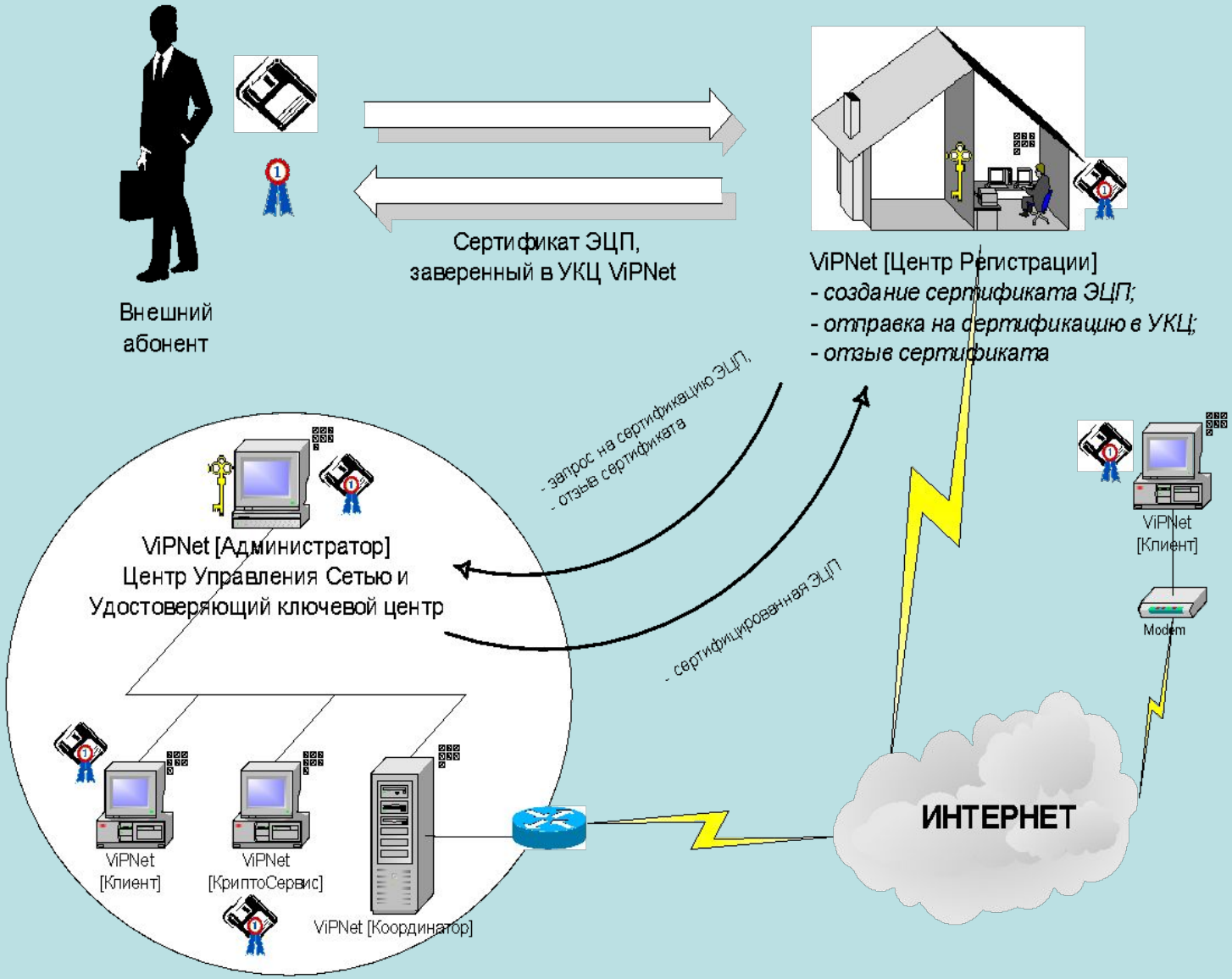
Антивирусная защита

- Межсетевые экраны *ZoneAlarm* *www. zonelabs.com* *Outpost* *www.outpost.agnitum.com*
- Антивирусные программы
- Утилиты

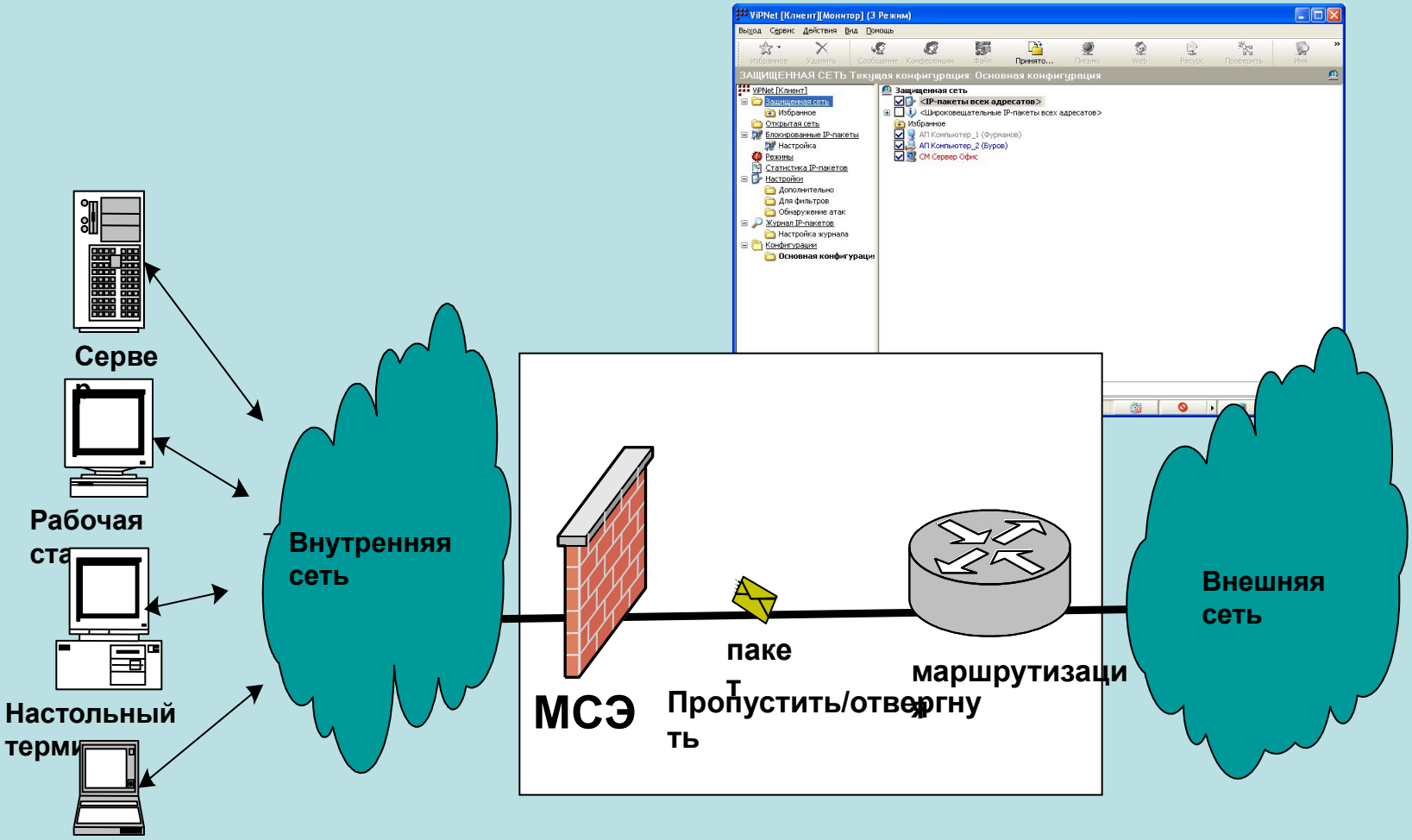
Защита информации в каналах связи и РКС



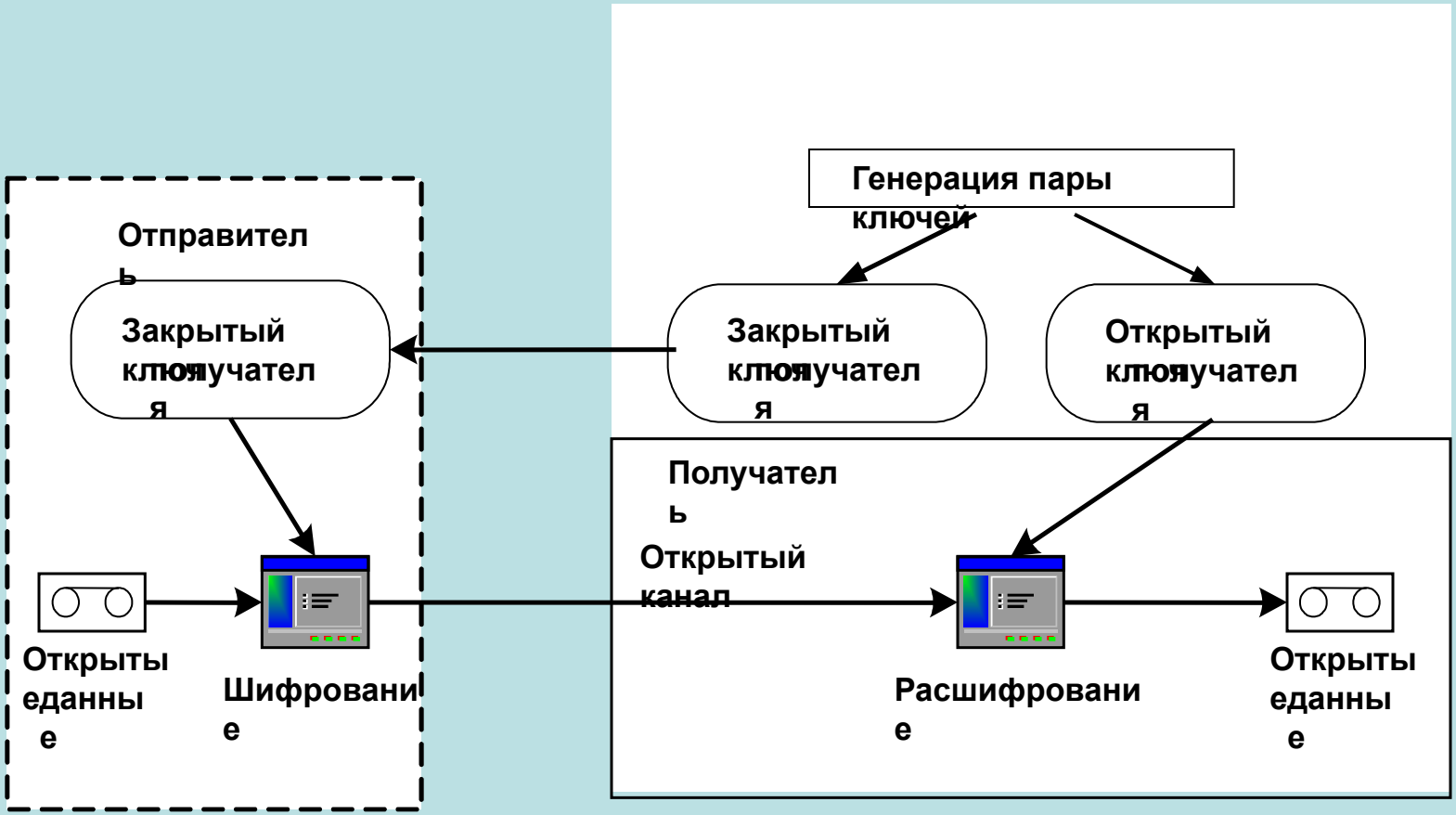
Структура VPN -сети



Межсетевое экранирование



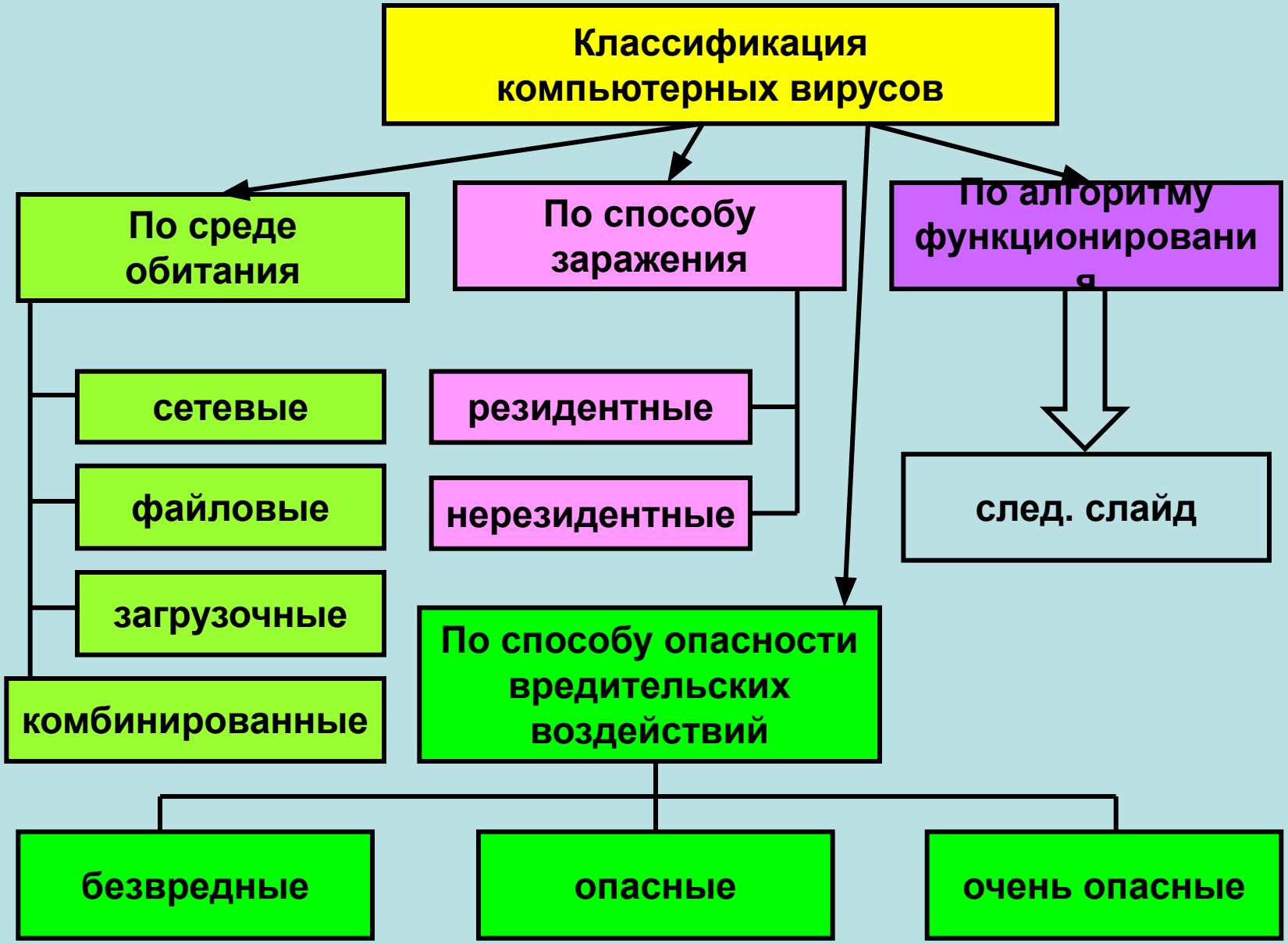
Технология применения ЭЦП

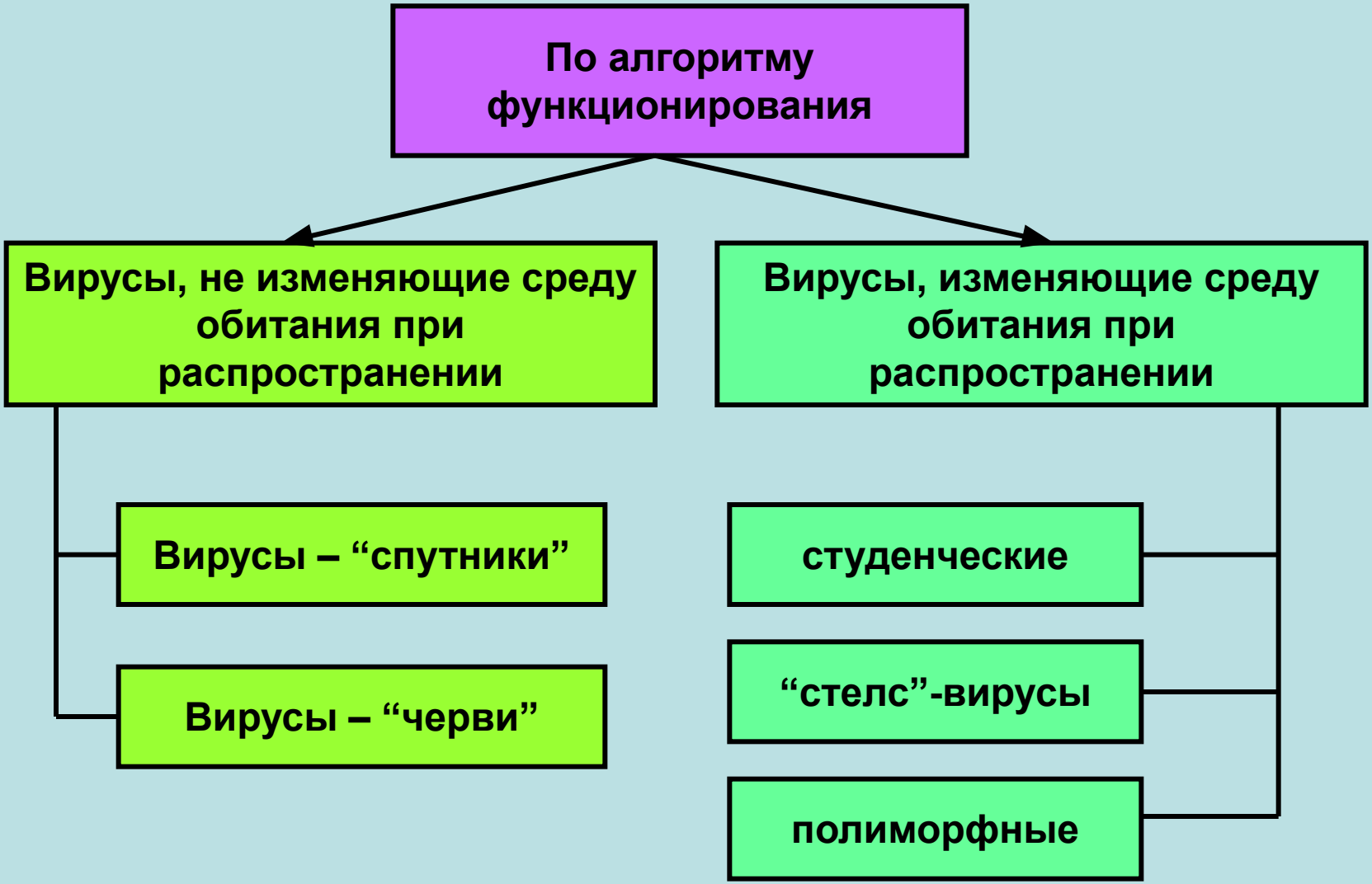


Антивирусная борьба

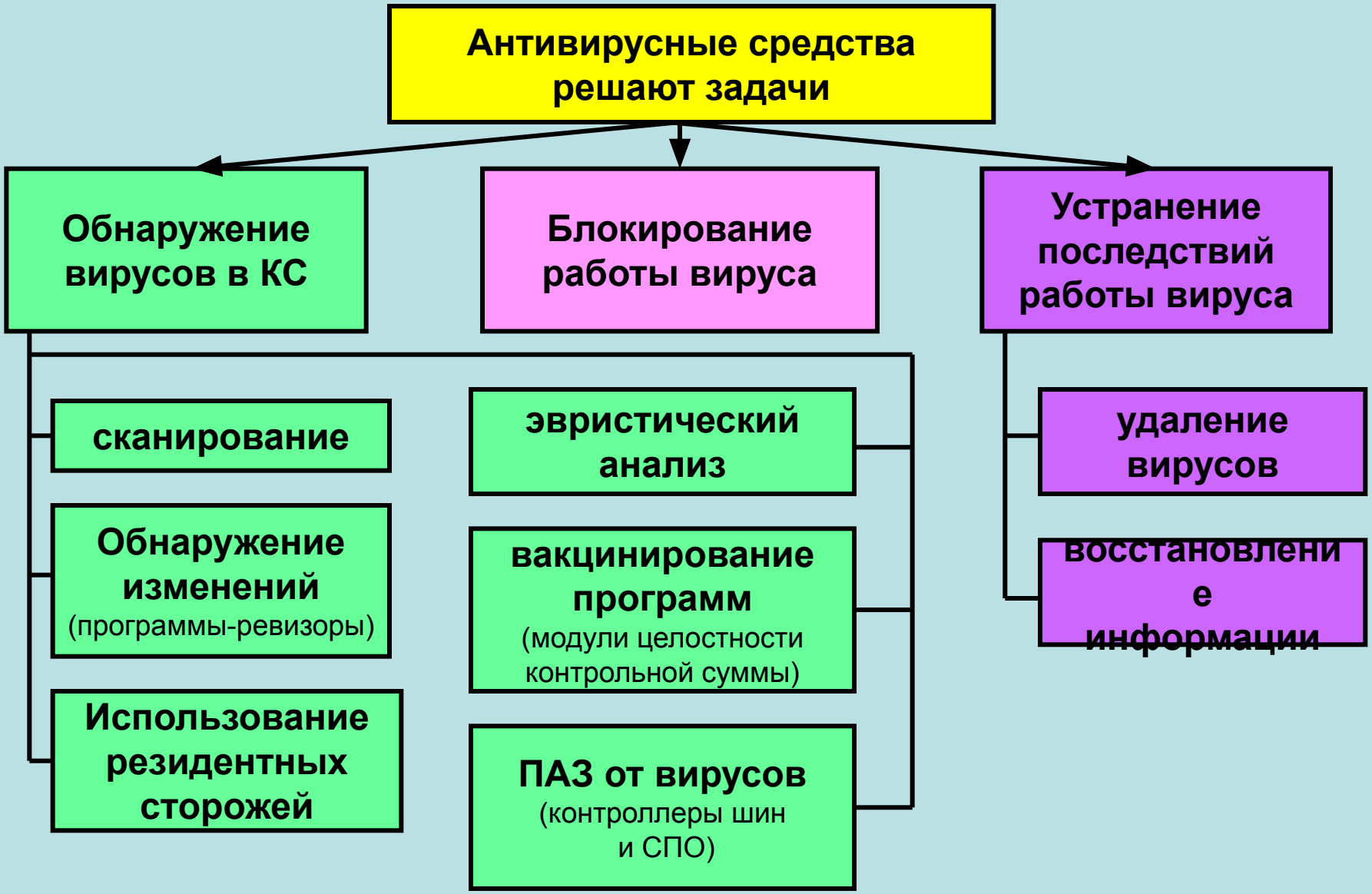
Компьютерные вирусы – это небольшие исполняемые программы, обладающие свойством распространения и самовоспроизведения в КС.

Вирусы могут выполнять изменение или уничтожение ПО или данных, хранящихся в КС.


Классификация компьютерных вирусов
По среде обитания
По способу заражения
По алгоритму функционировани я
сетевые
файловые
загрузочные
комбинированные
резидентные
нерезидентные
след. слайд
По способу опасности вредительских воздействий
безвредные
опасные
очень опасные


По алгоритму функционирования
Вирусы, не изменяющие среду обитания при распространении
Вирусы, изменяющие среду обитания при распространении
Вирусы – “спутники”
Вирусы – “черви”
студенческие
“стелс”-вирусы
полиморфные

Методы и средства борьбы с вирусами



Профилактика заражения вирусами КС

1. Использование лицензированного ПО
2. Дублирование информации
3. Регулярное использование антивирусных программ.
4. Обновление баз и версий антивирусных программ
5. Проведение антивирусной проверки внешних носителей информации при их использовании в КС
6. При работе в РКС обязательное использование межсетевых экранов и аппаратных средств защиты
7. Периодические проверки КС специалистами на предмет заражения вирусами.

Порядок действий при заражении ЭВМ вирусами

1. Выключить ЭВМ для уничтожения резидентных вирусов
2. Загрузить эталонную ОС с резервного носителя
3. Сохранить важную информацию на съемных носителях
4. Использовать антивирусные средства для удаления вирусов и восстановления информации. Если работоспособность ЭВМ восстановлена, то следует перейти к пункту 8
5. Осуществить форматирование и новую разметку жесткого диска ЭВМ
6. Восстановить ОС и необходимое ПО на ЭВМ
7. Тщательно проверить информацию, сохраненную после заражения вирусами ЭВМ
8. Завершить восстановление информации проверкой ЭВМ с помощью имеющихся антивирусных программ