# 2. ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

# 2.1 КЛАССИФИКАЦИЯ И ХАРАКТЕРИСТИКА ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

# 2.1.1. Основные объекты защиты информации

## Основные объекты защиты информации:

- информационные ресурсы;
- технические средства приема, передачи и обработки информации (ТСПИ);
- вспомогательные технические средства и системы (ВТСС).

# 2.1.2. Технические каналы утечки информации

**Технический канал утечки информации (ТКУИ)**

- совокупность объекта защиты информации, технического средства, с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал.

**Технические каналы утечки телекоммуникационной информации:**

- электромагнитные,
- электрические,
- параметрические.

## Технические каналы утечки речевой информации:

- воздушные,
- вибрационные,
- электроакустические,
- оптико-электронные,
- параметрические.

# 2.1.3. Мероприятия по защите информации от утечки по техническим каналам

**Архитектурно-строительные мероприятия по защите информации -** это мероприятия, проводимые на этапе проектирования и строительства зданий и сооружений.

**Организационные мероприятия по защите информации -** это мероприятия, проведение которых не требует применения специально разработанных технических средств.

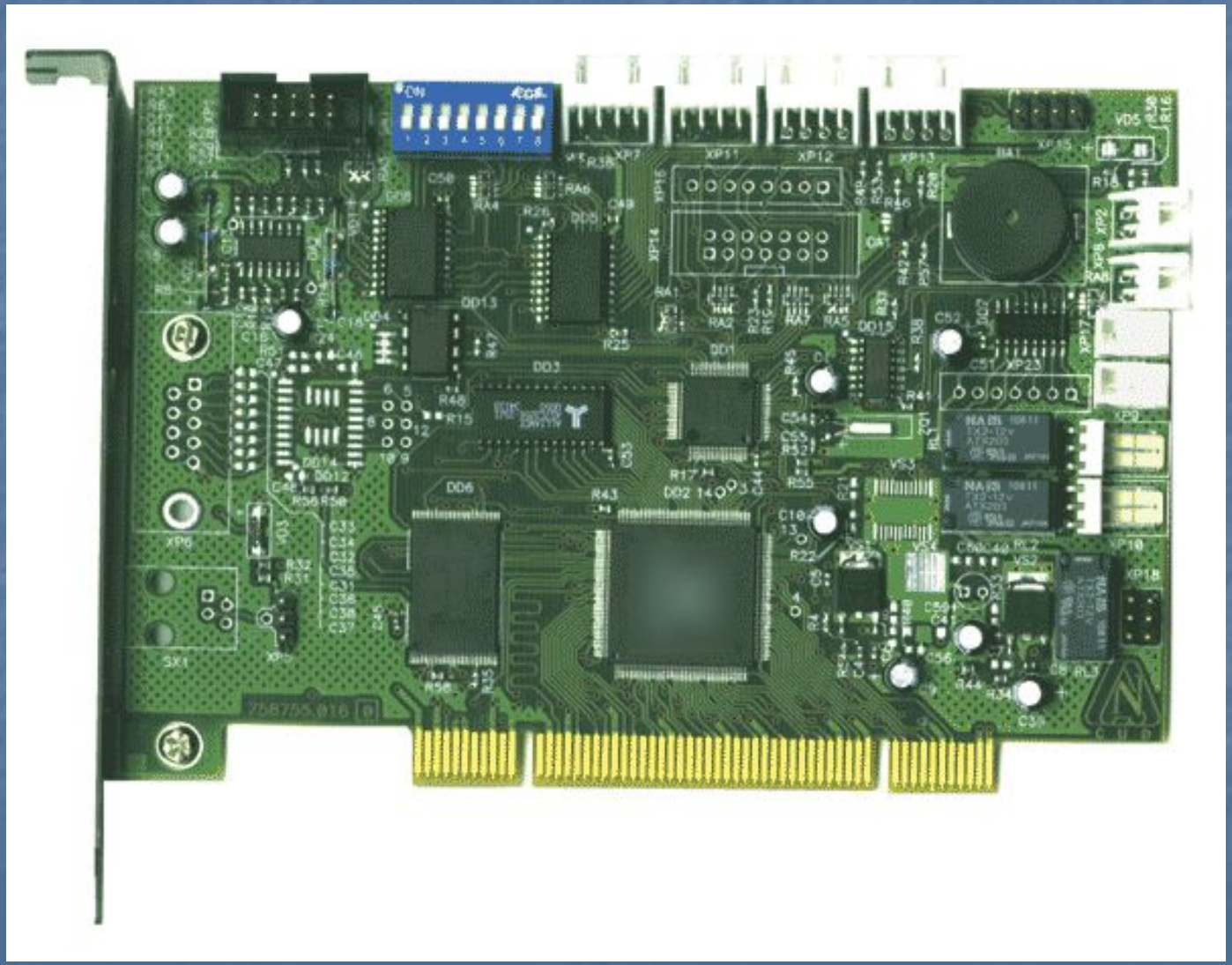
**Технические мероприятие по защите информации -** это мероприятия, предусматривающие применение специальных технических средств и реализацию технических решений.

# 5. Программно-аппаратные средства защиты компьютерных систем и систем передачи данных

# 5. Программно-аппаратные средства защиты компьютерных систем и систем передачи данных

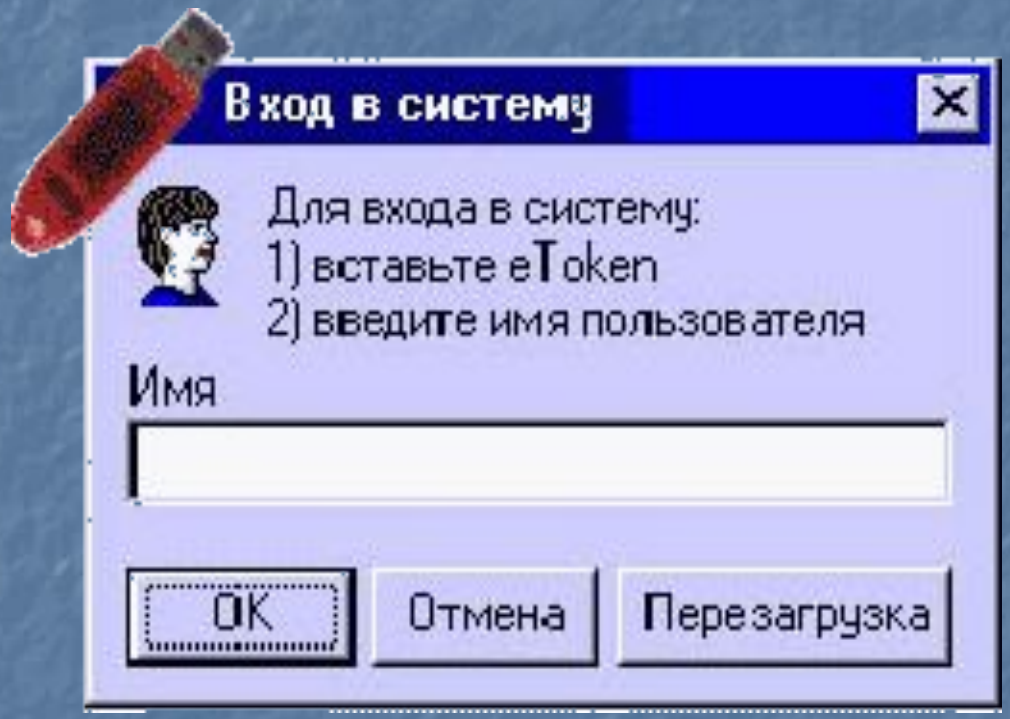
- 5.1. Системы защиты от НСД
- 5.2. Криптографическая защита программ и данных
- 5.3. Защита глобальных, корпоративных, локальных сетей от НСД

# КРИПТОН-ЗАМОК



# КРИПТОН-ЩИТ

# CRYPTON LOCK

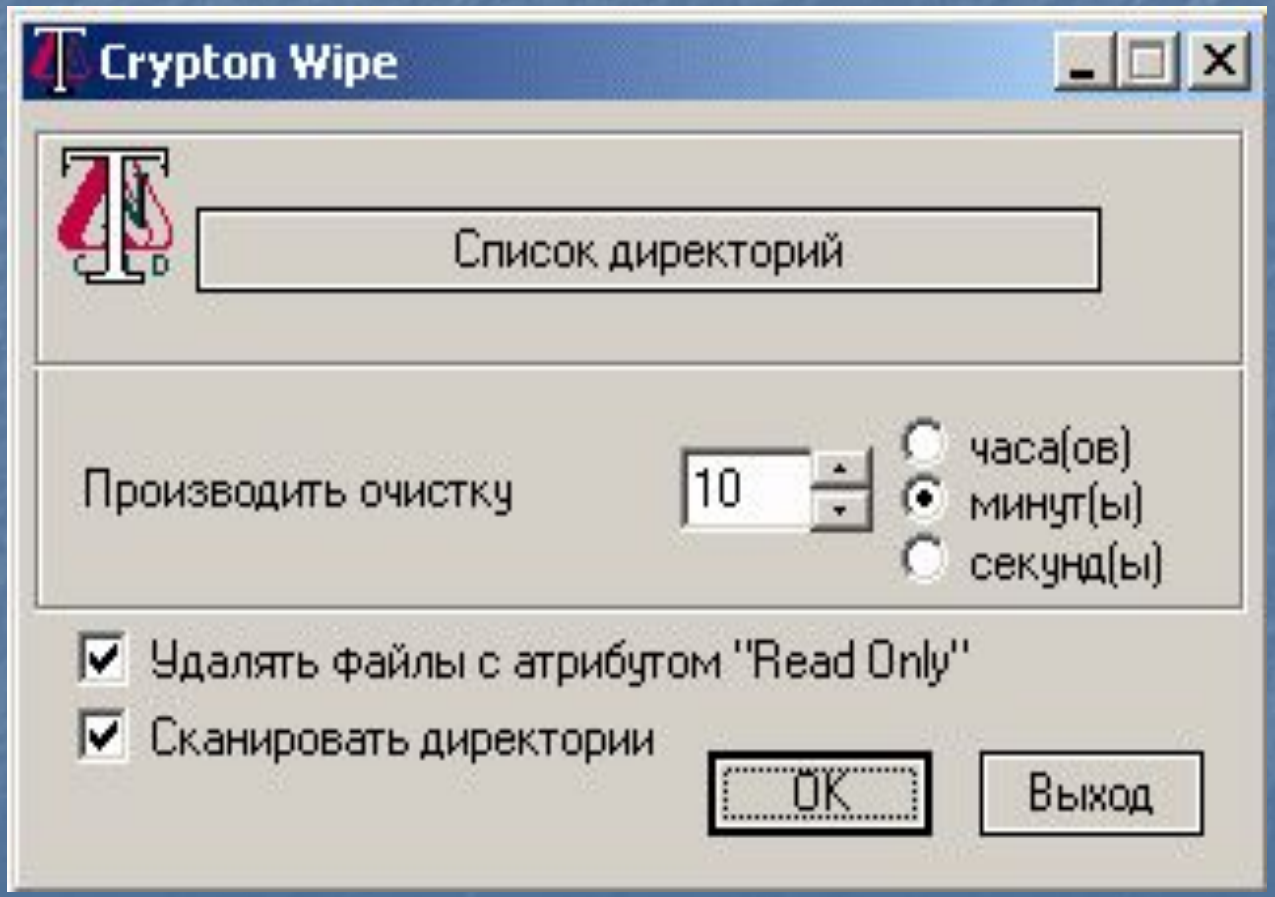


# Шифраторы жестких дисков серии КРИПТОН

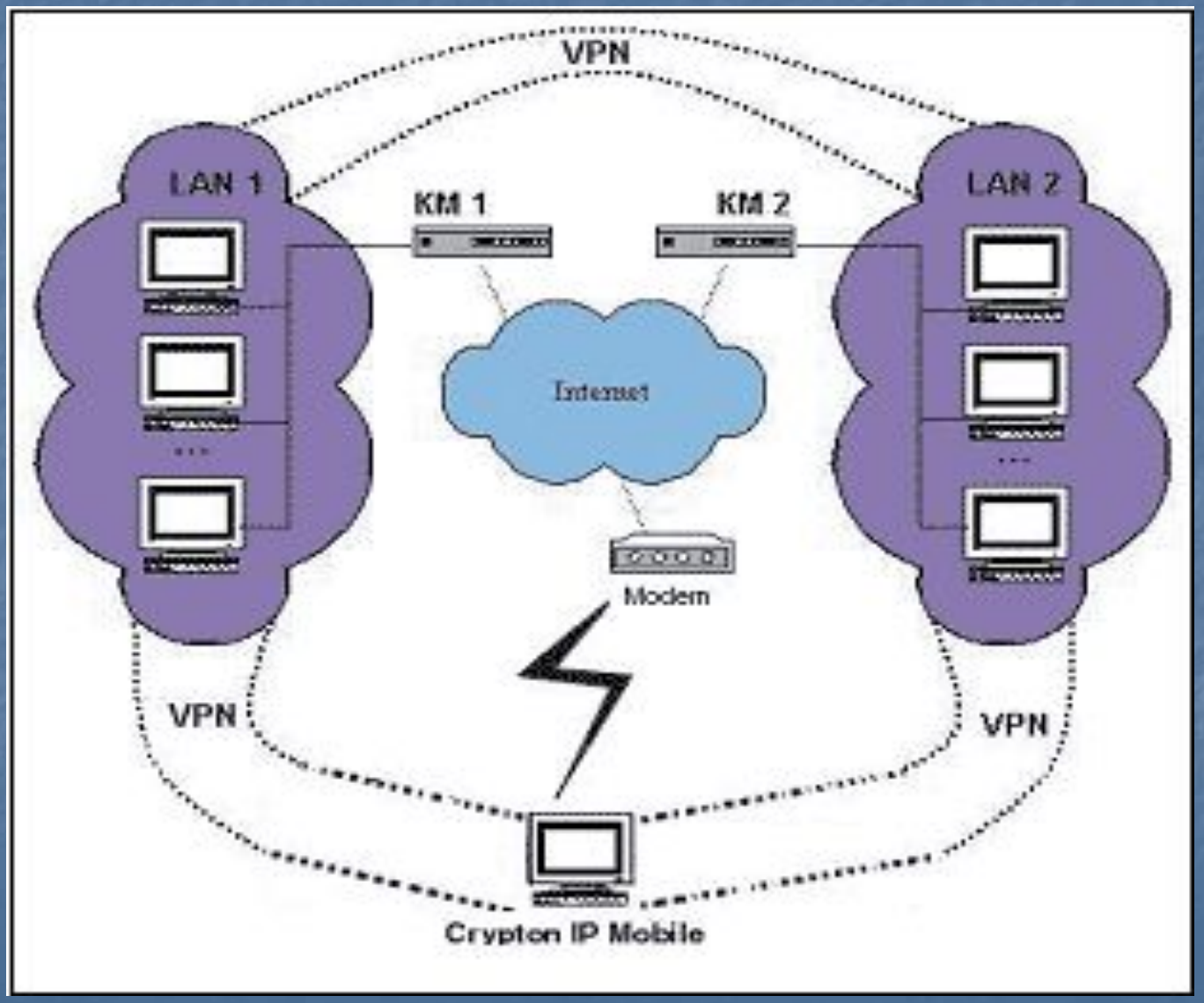
# КРИПТОН-Дозор

# Фильтр USB устройств

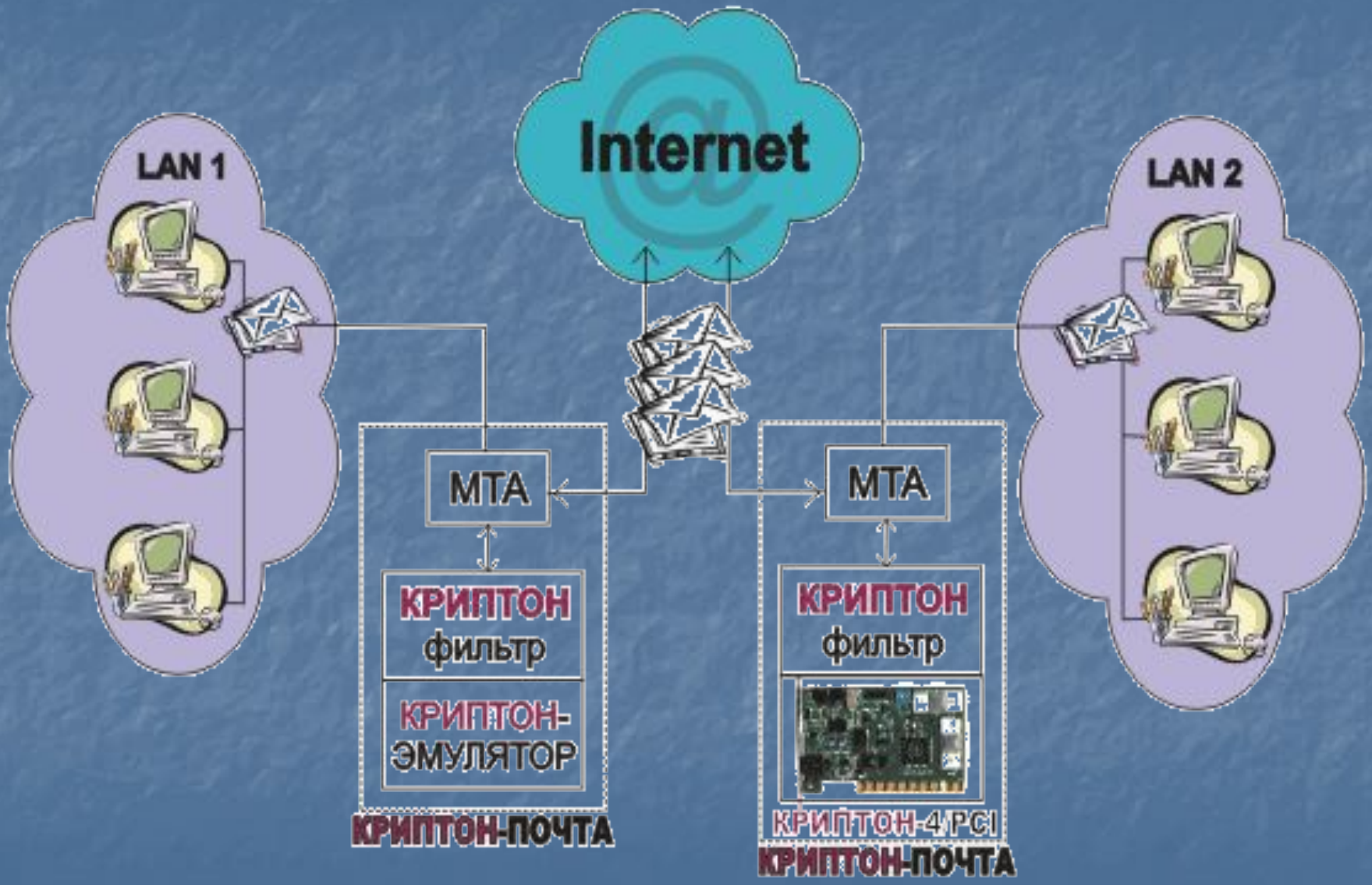
# Crypton Wipe



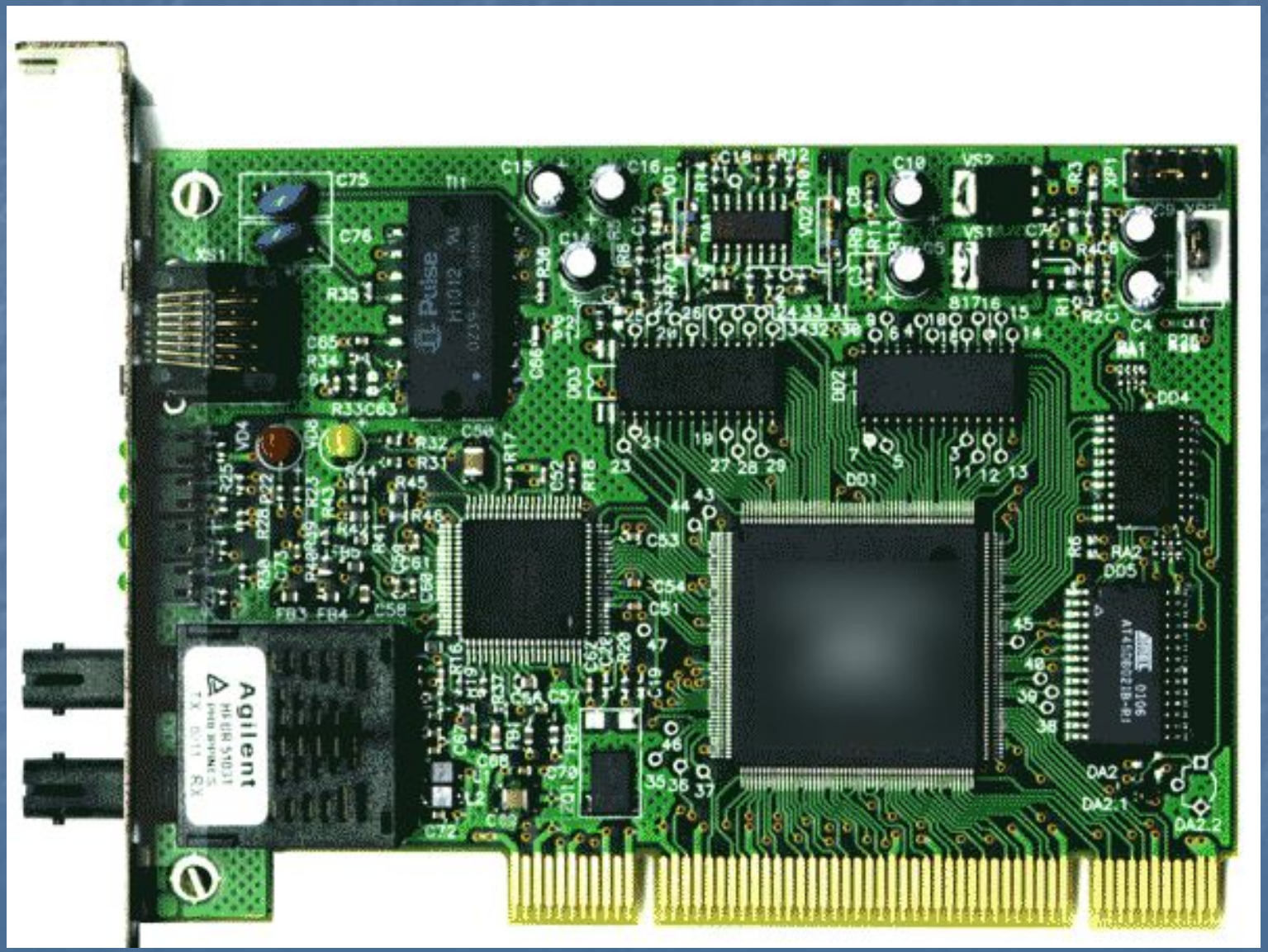
# Crypton IP Mobile 1.1



# Криптон-Почта



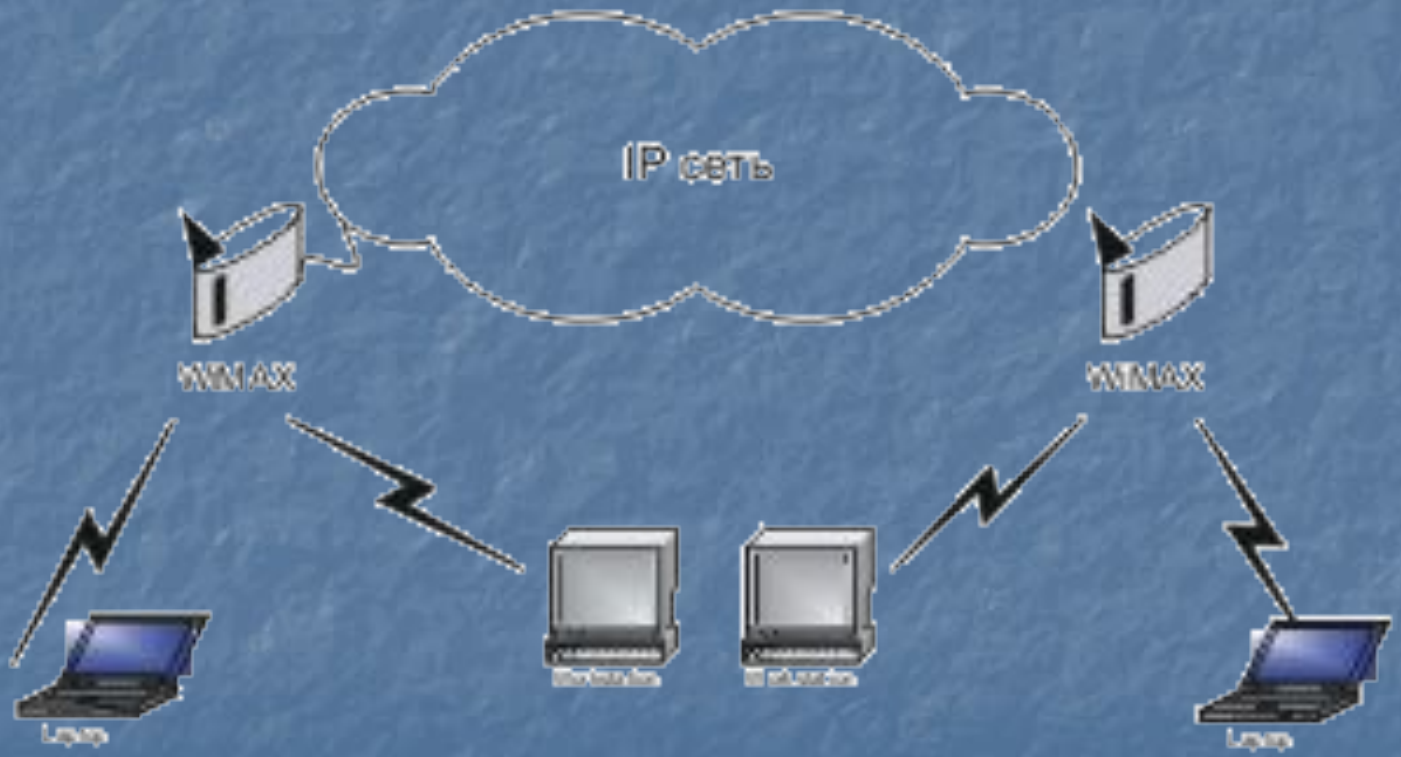
# КРИПТОН AncNet Pro



# КРИПТОН AncNet Pro x2

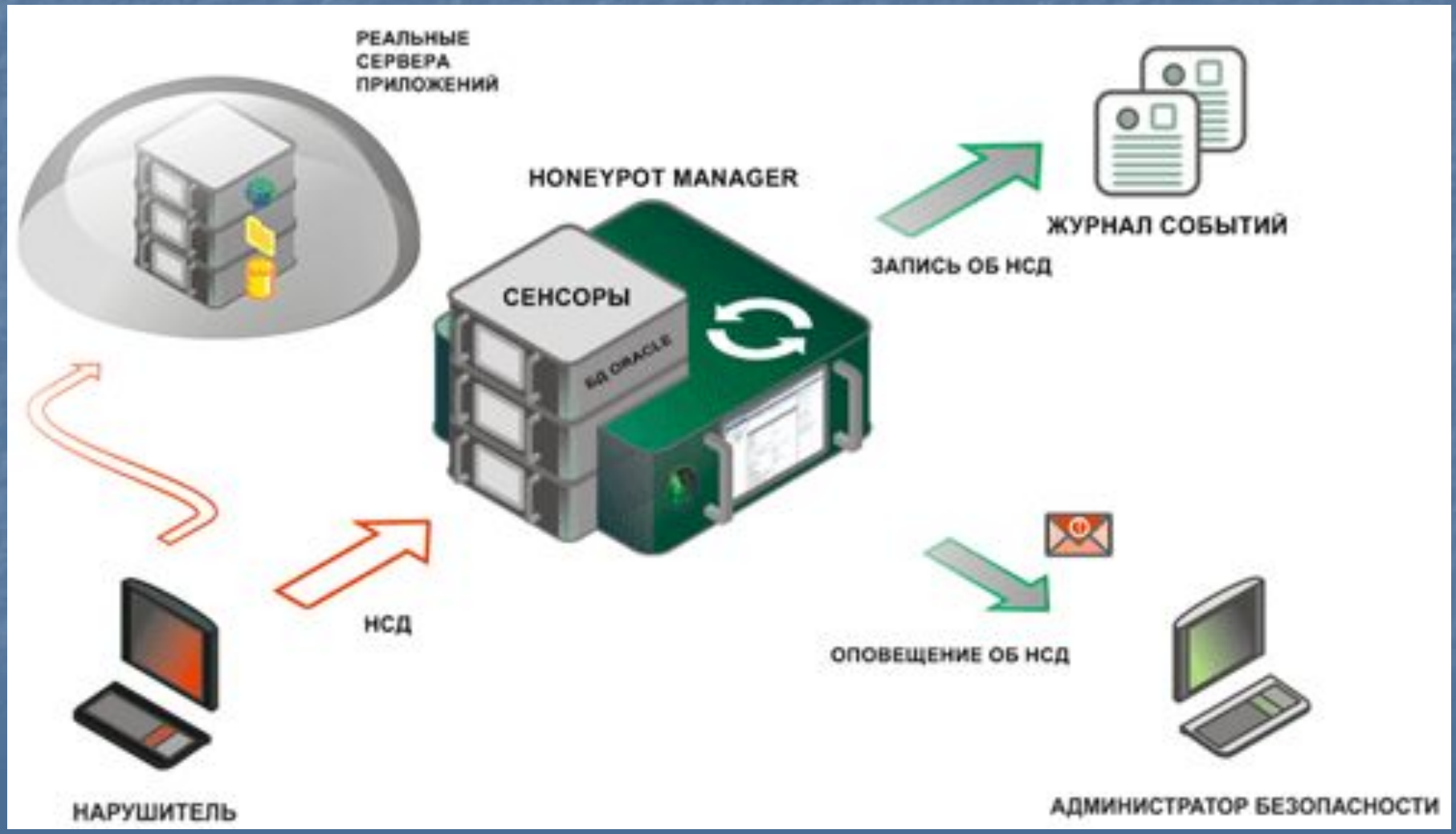
# КРИПТОН - Радио

# Защищенная точка доступа и абонентские терминалы WiMAX

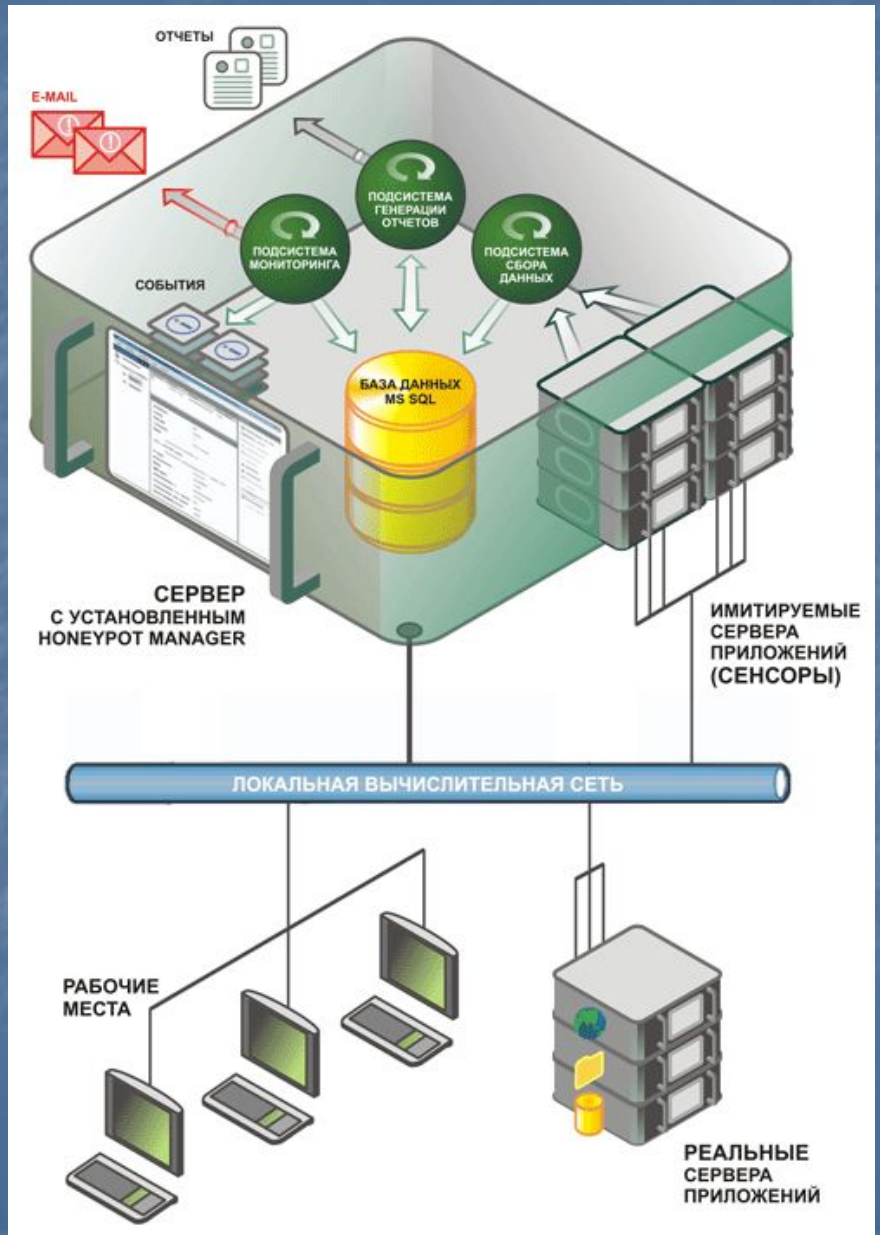


# Security Code vGate for VMware Infrastructure

# Security Studio Honeypot Manager

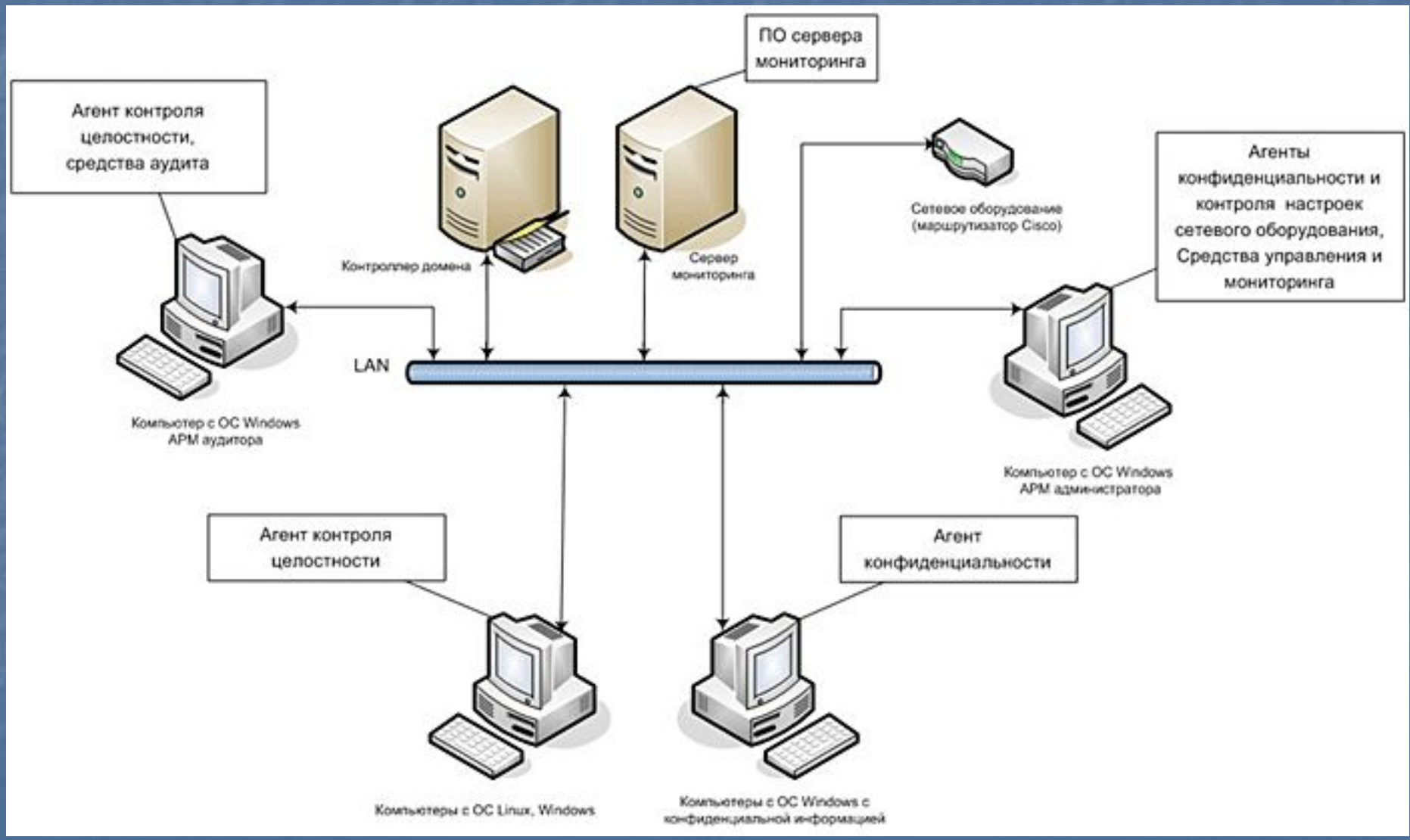


# Security Studio Honeypot Manager

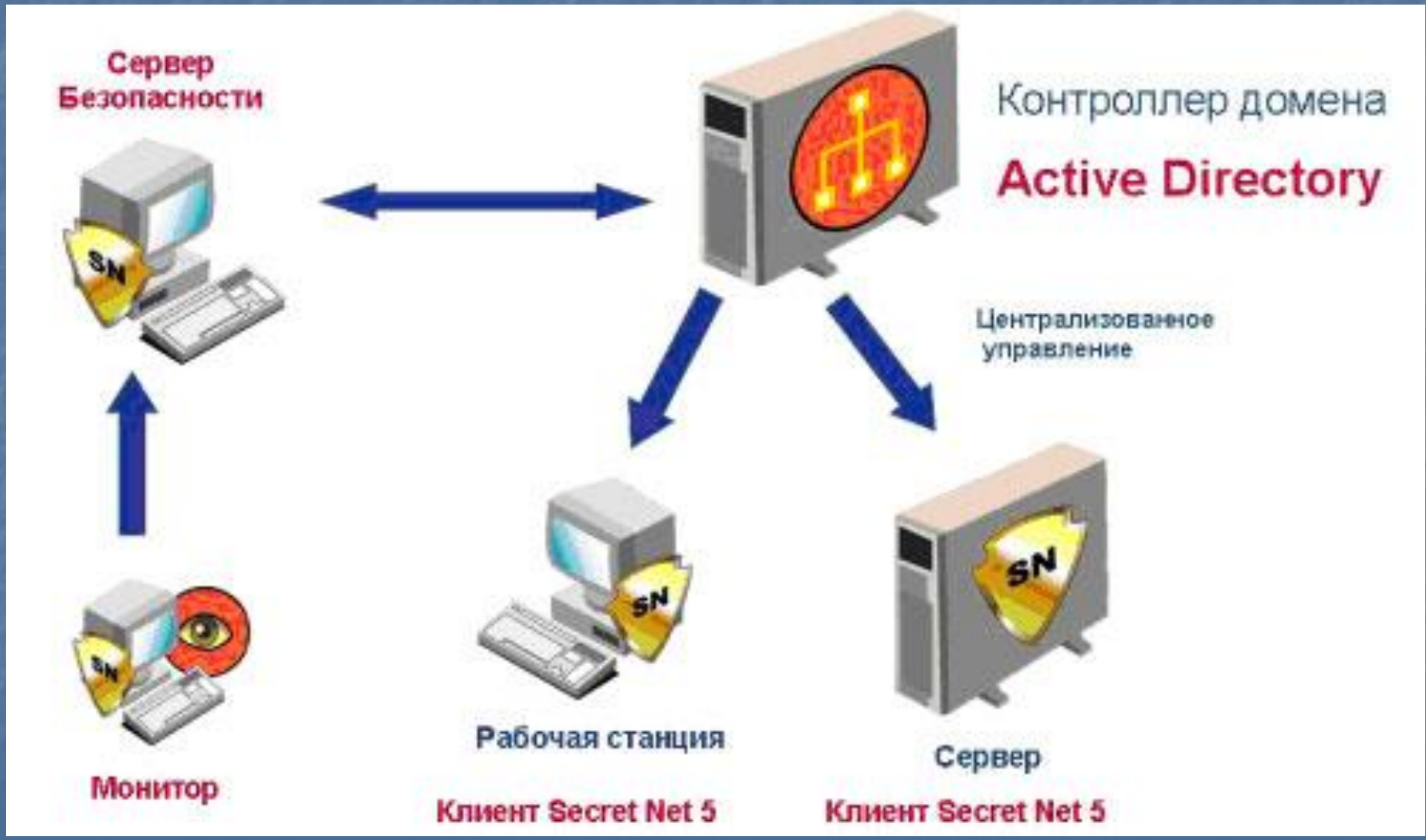


# Security Code Inventory Manager

# Security Studio

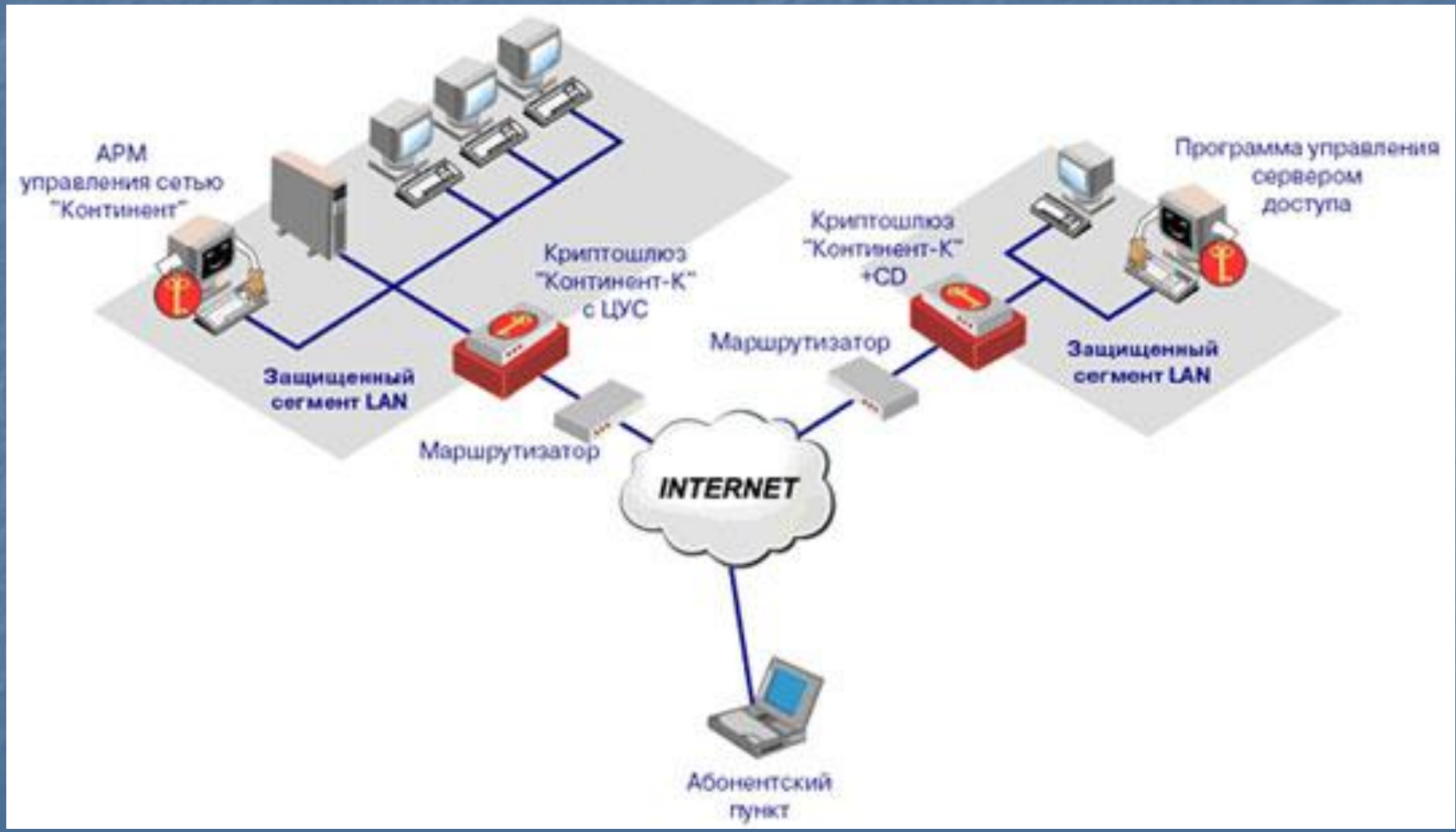


# Secret Net 5.1



# АПКШ "Континент"

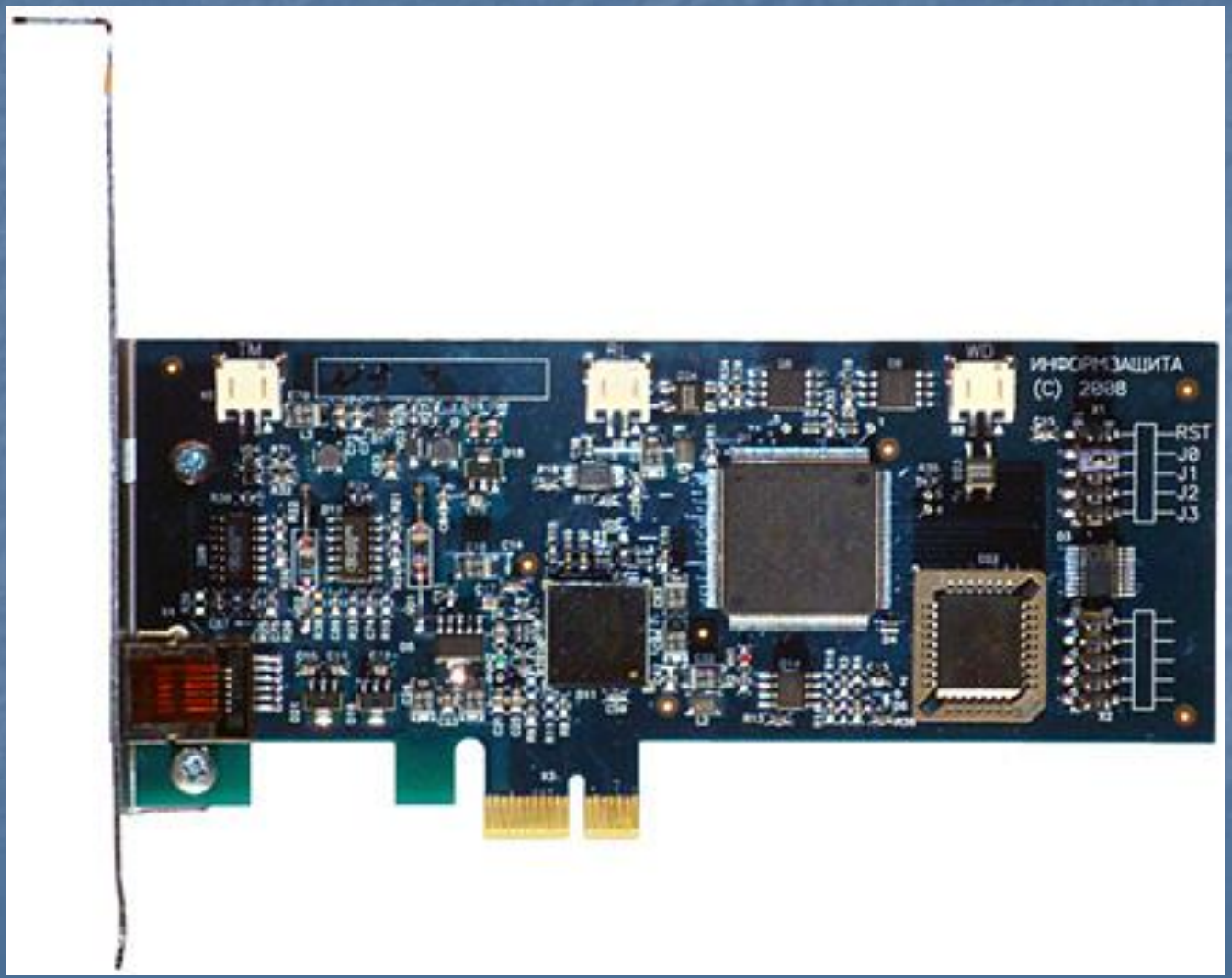
# АПКШ "Континент"



# КУБ

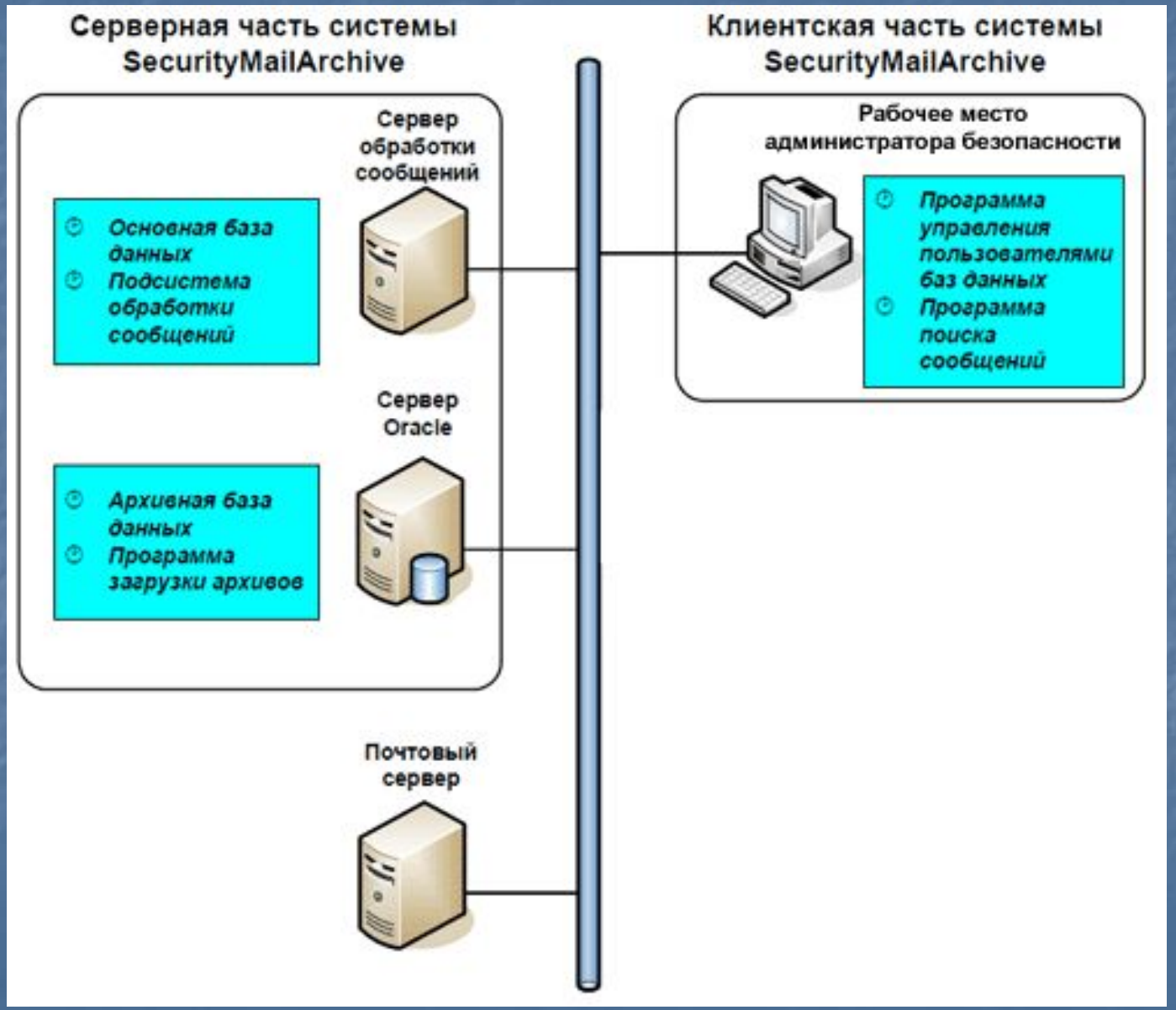

WEB-сервер
Сервер безопасности
Почтовый сервер
Агенты
Документооборот

# Электронный замок "Соболь"



# Электронный замок "Соболь“ 3.0

# SecurityMailArchive



# СКЗИ М-506А-ХР

# АРМ ЭЦП

# ПАК "Росомаха"

## Выводы:

- Разработка новых технических средств обеспечения информационной безопасности обычно сопровождается появлением новых средств несанкционированного съема информации, что в свою очередь, вновь заставляет совершенствовать систему защиты. Это очень динамичный, взаимосвязанный процесс.
- Специалистам по обеспечению информационной безопасности необходимо быть в курсе не только перспективных направлений развития техники защиты информации, но и совершенствования методов и средств ее несанкционированного съема. Только в этом заключается залог будущего успешного противодействия угрозам информационной безопасности.