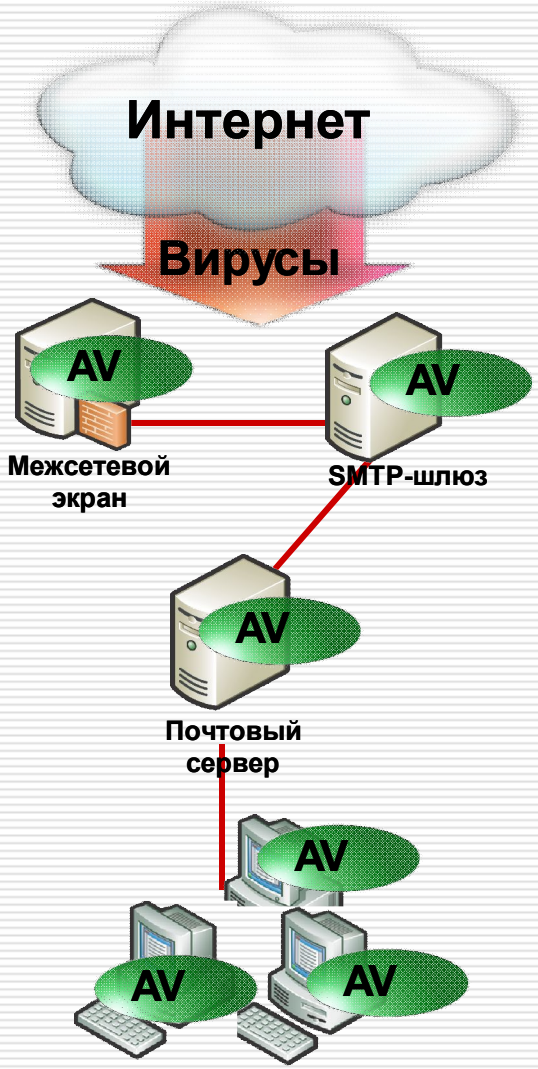
Комплексные решения в области информационной безопасности

Виктор Сердюк, к.т.н.
Генеральный директор ЗАО «ДиалогНаука»

ДиалогНаука

Решение по защите от компьютерных вирусов

Решение одного производителя

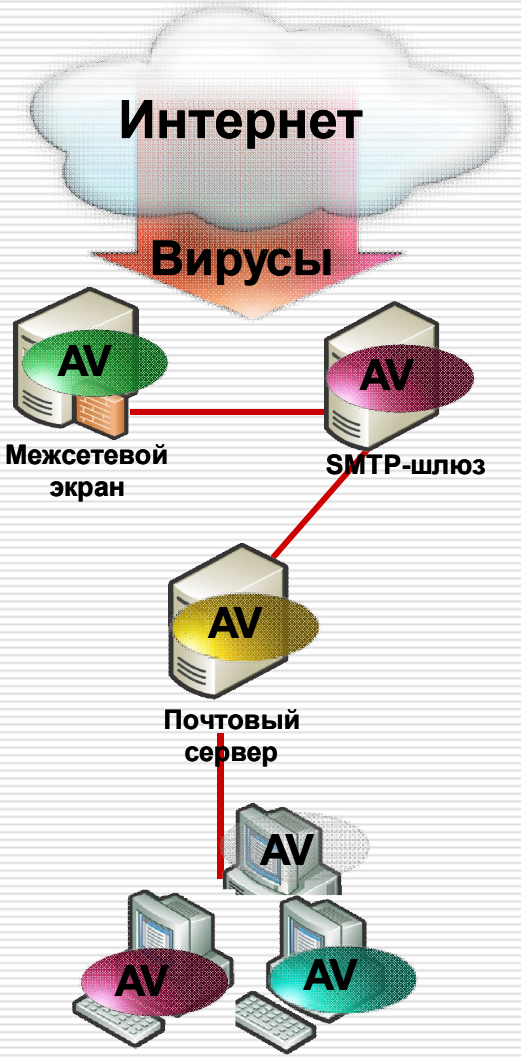


Одно и то же ядро сканирования используется на уровне шлюзов, серверов и рабочих станциях

- **Недостатки подхода:**
  - Зависимость от одной антивирусной лаборатории
  - Неизбежность очередей и задержек на серверах по время обновления баз данных сигнатур антивирусного ПО
  - Одна точка уязвимости всей системы

ДиалогНаука

Решения нескольких производителей

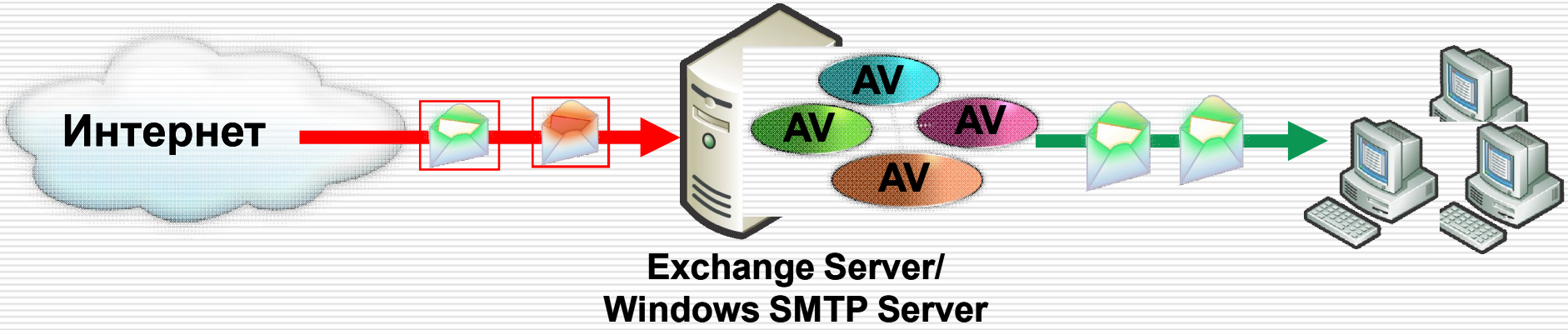


Для выявления вирусов используются различные продукты от разных производителей

ДиалогНаука

Многоядерная Антивирусная защита

Antigen



- централизованное управление несколькими серверами
- централизованное управление политиками

ДиалОгНаука

Ядра, входящие в состав Antigen

- По умолчанию в состав Antigen всегда входит 4 антивирусных ядра:
  - SOPHOS (Англия)
  - Computer Associates – Vet (Австралия)
  - Norman Data Defense (Швеция)
  - Computer Associates – Inoculate (Израиль)
- Дополнительно можно заказать еще до 4-х антивирусных ядер:
  - Лаборатория Касперского (Россия)
  - Virus Buster (Венгрия)
  - Authentium (США)
  - Ahnlab (Южная Корея)

Antigen

ДиалОгНаука

Преимущества многоядерного сканирования

Antigen

- **Высокая надёжность выявления компьютерных вирусов**
  - Antigen позволяет более эффективно обнаруживать вирусы за счёт одновременного использования нескольких антивирусных ядер
- **Защита от возможных сбоев**
  - Если нарушается работоспособность одного антивирусного ядра, то оно моментально заменяется другим
- **Защита при обновлении**
  - На тот период времени, когда одно ядро обновляет свою базу данных сигнатур, его «вахту» защиты подхватывает другое

ДиалогНаука

Решение по защите от спама

Что такое Спамооборона

Yandex
so.yandex.ru

- Решение предназначено для установки на почтовом сервере или smtp-шлюзе
- Анализируется почтовое сообщение, служебные заголовки, вложения, картинки, учитываются особенности текста и оформления
- На спам-сообщения ставится метка для возможности дальнейшей обработки (поместить в карантин, удалить, Junk E-mail)

ДиалОгНаука

Поддерживаемые платформы

Спамооборона

- **Операционные системы**
  - FreeBSD 4,5,6
  - Linux Debian 3.1
  - Linux Fedora Core 3, 4
  - Linux RedHat Enterprise Server / Advanced Server 4
  - Linux Slackware 10.2
  - Linux SuSe 10
  - ASPLinux 11
  - скоро - Sun Solaris x86/SPARC
- **Почтовые серверы**
  - SendMail 8.11 и выше
  - CommunigatePro 4.x
  - NetMail 1.0.5 или QMail 1.0.3 (+ QmailQueue)
  - PostFix 2.1 и выше
  - Exim 4 и выше

Детальное описание продукта: www.dialognauka.ru/so

ДиалОгНаука

@Спамооборона - преимущества

- Качество и полнота фильтрации: **94-97%***
- Эффективное определение **русскоязычного спама**
- **Полная автоматизация** сбора и выпуска обновлений
- Комплексный и полный анализ (около **3000** правил)
- Постоянно поддерживаемая собственная база **адресов спамеров**
- Экспертные технологии и обеспечение службами **Яндекса**
- Высокая производительность, низкие требования
- Удобный диалоговый интерфейс
- **Автоматизированные механизмы персонализации и управления пользовательскими данными**

* по результатам эксплуатации компаниями **Ай-Ти, PeterHost, КОМСТАР**

ДиалогНаука

Простота эксплуатации

Спамооборона

- ***После установки*** и интеграции продукта с почтовой системой требуется лишь ввод персональных данных:
  - Импорт списка пользователей
  - Заполнение белого списка для гарантированного предотвращения ложных срабатываний

  или просто активация опции **автозаполнения**

- ***Эксплуатация*** - исключительно как поддержка в актуальном состоянии персональных данных:
  - добавление/удаление пользователя в список пользователей (при приеме/увольнении)
  - добавление доверенного лица пользователя в белый список (по требованию)

  или просто активация опции **автозаполнения**

ДиалОгНаука

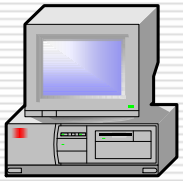
Комплексное решение по защите от утечки конфиденциальной информации

ДиалогНаука

Основные каналы утечки

несанкционированное копирование конфиденциальной информации на внешние носители

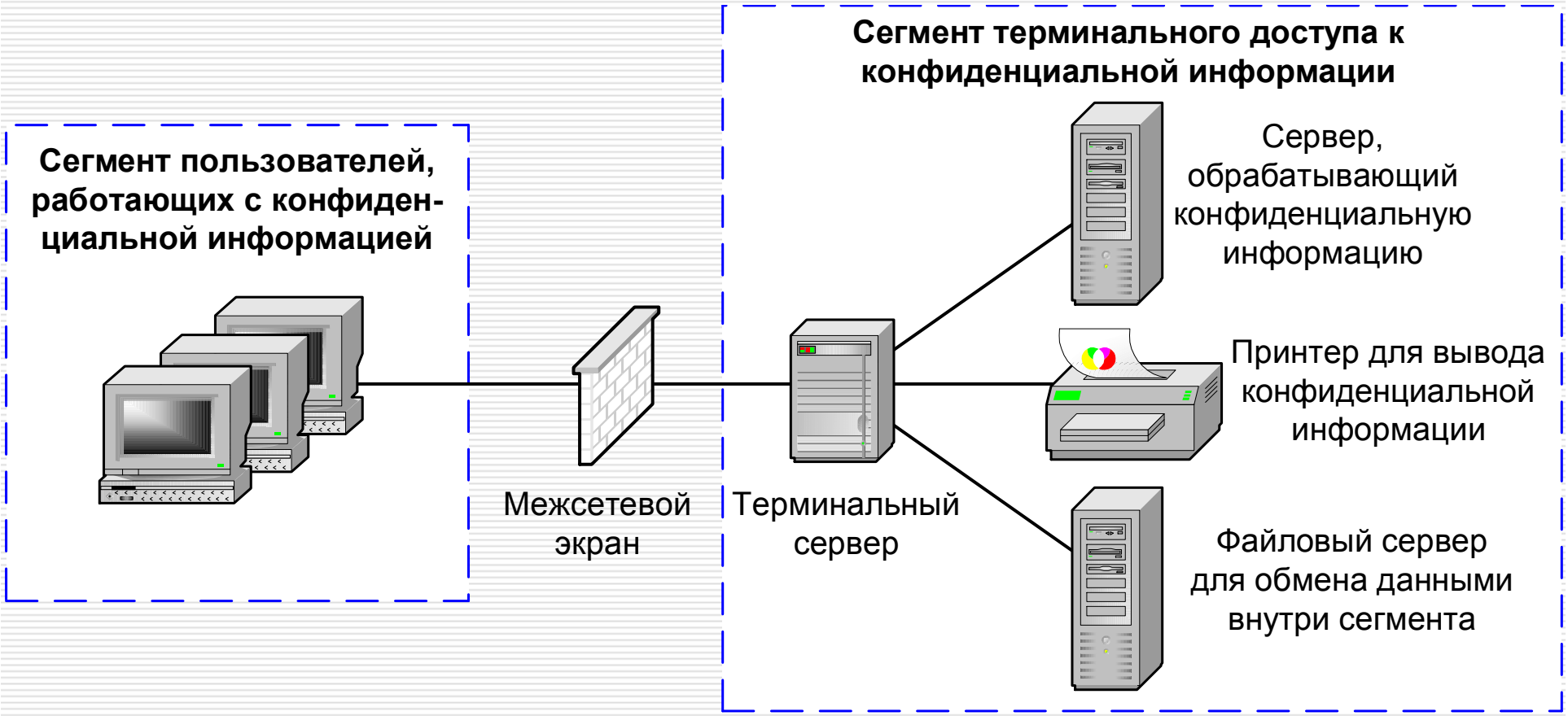
несанкционированная передача конфиденциальной информации по сети на внешние серверы



несанкционированный вывод на печать конфиденциальной информации

кража носителей, содержащих конфиденциальную информацию

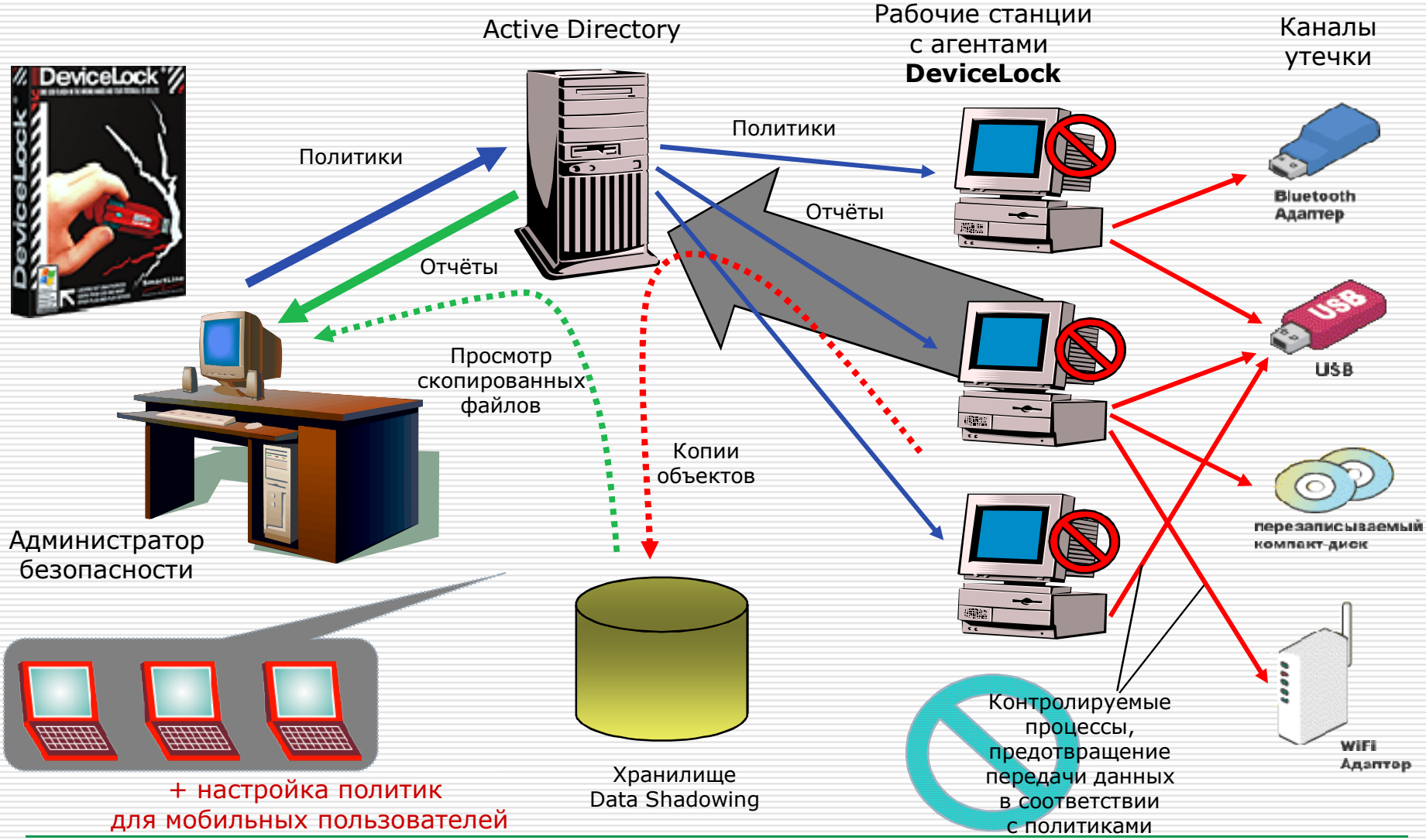
Выделенный сегмент терминального доступа



ДиалогНаука

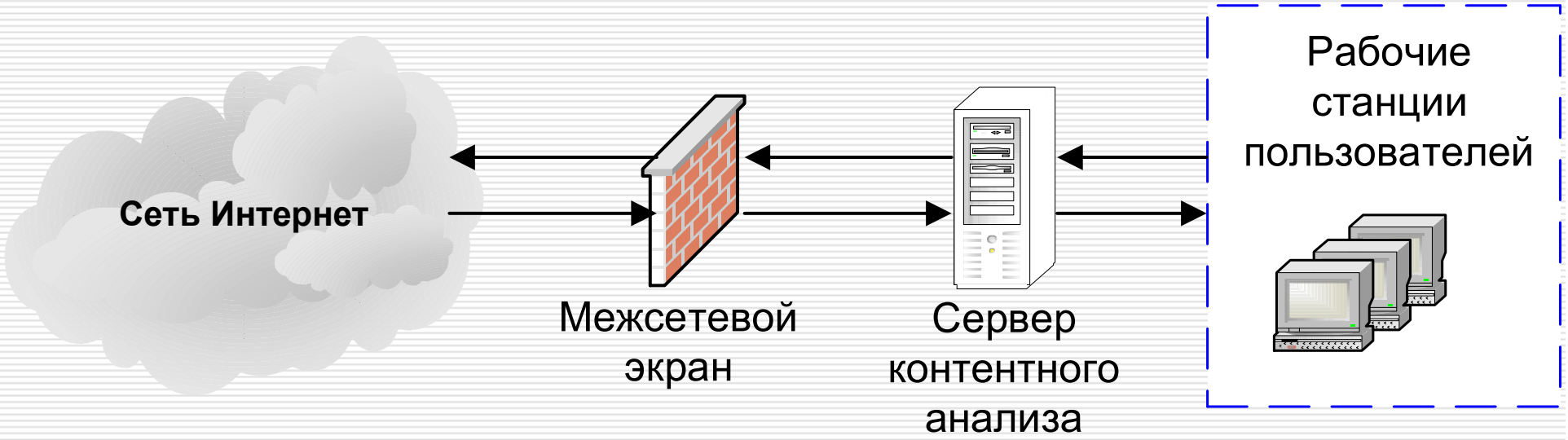
Схема функционирования

DeviceLock
контроль доступа к данным



ДиалогНаука

Мониторинг сетевого трафика



ДиалОгНаука

Нормативная основа защиты от внутренних угроз

- Политика защиты от внутренних угроз безопасности
- Регламент конфиденциального документооборота
- Регламент расследования инцидентов, связанных с утечкой конфиденциальной информации

Защита Интернет-портала

Комплексное решение по защите Интернет-портала компании

ДиалОгНаука

Угрозы информационной безопасности портала

Средства защиты, нарпавленные на выявление и устранение уязвимостей Web-портала

- Подсистема анализа защищённости

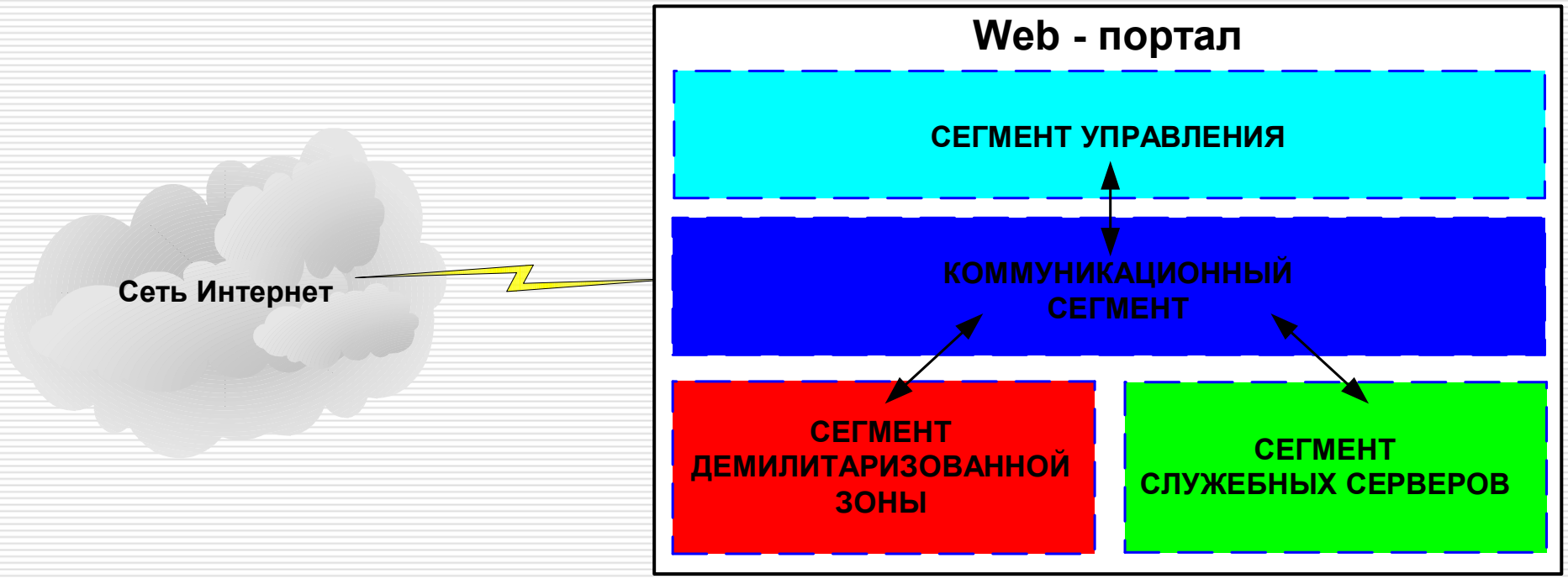
Средства, направленные на выявление и предотвращение информационных атак

- Подсистема обнаружения вторжений
- Подсистема разграничения доступа
- Подсистема криптографической защиты
- Подсистема антивирусной защиты

Средства, направленные на выявление и ликвидацию последствий информационных атак

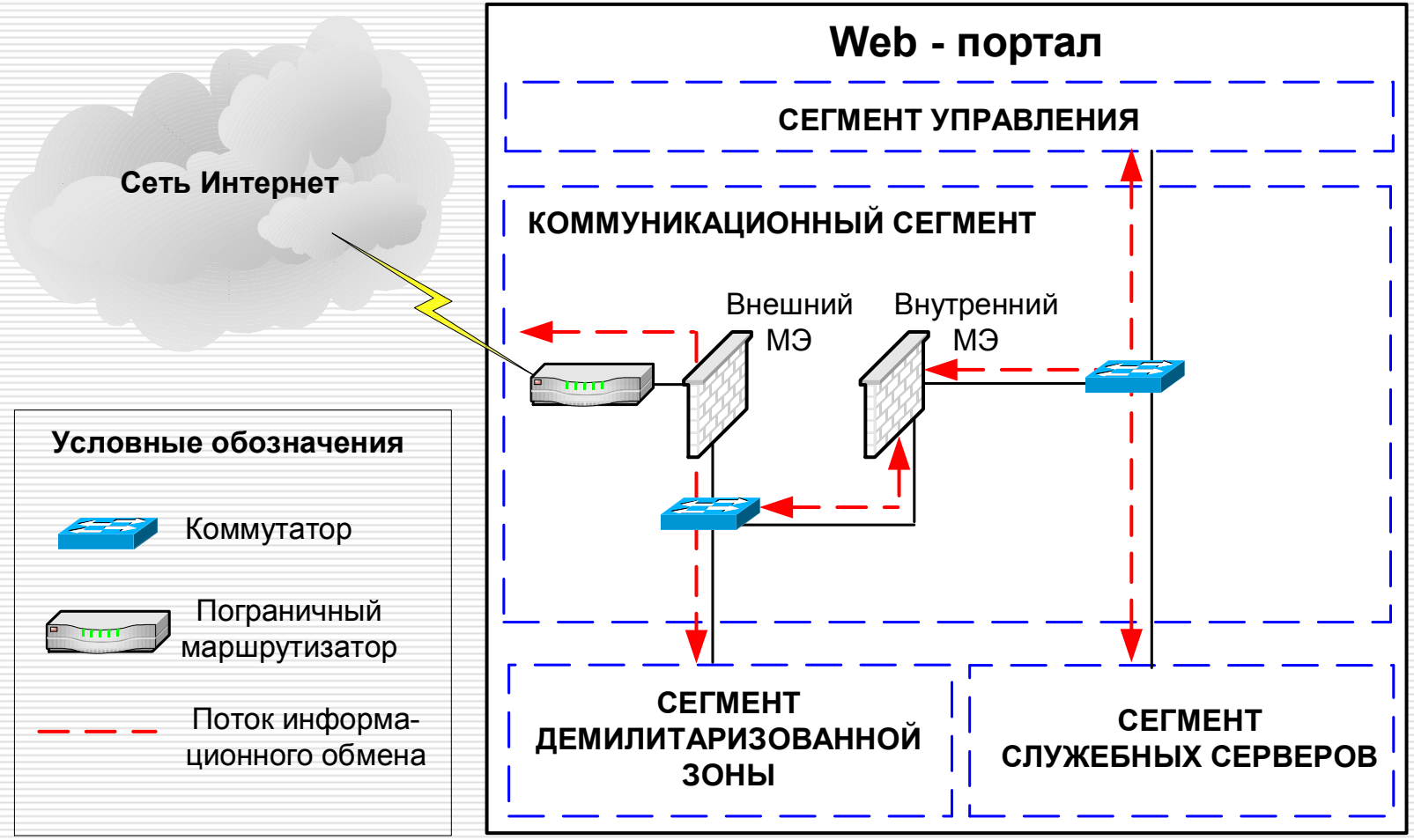
- Подсистема контроля целостности
- Подсистема резервирования ресурсов Web-портала

Структура защищённого портала



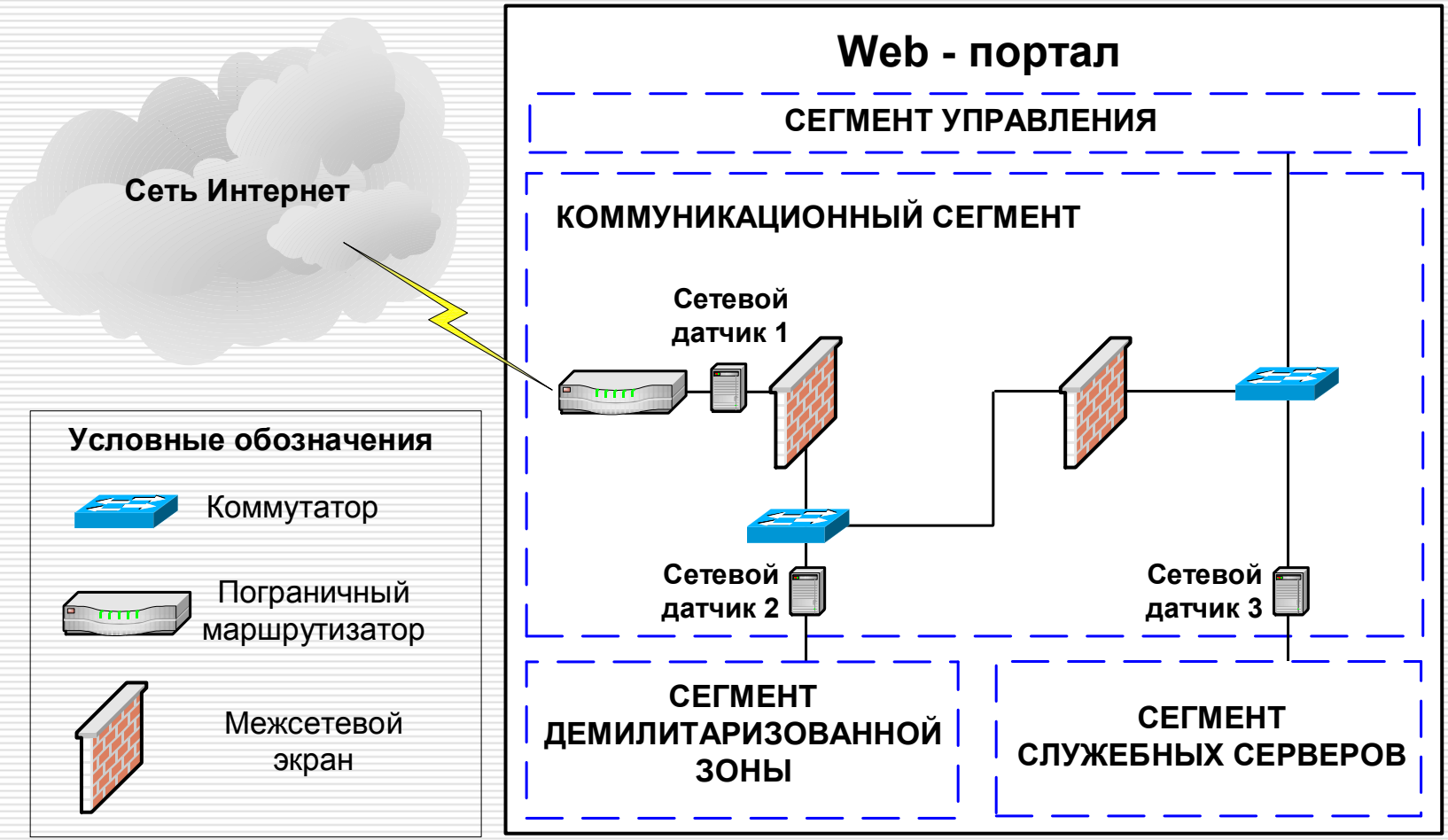
ДиалОгНаука

Схема размещения межсетевых экранов



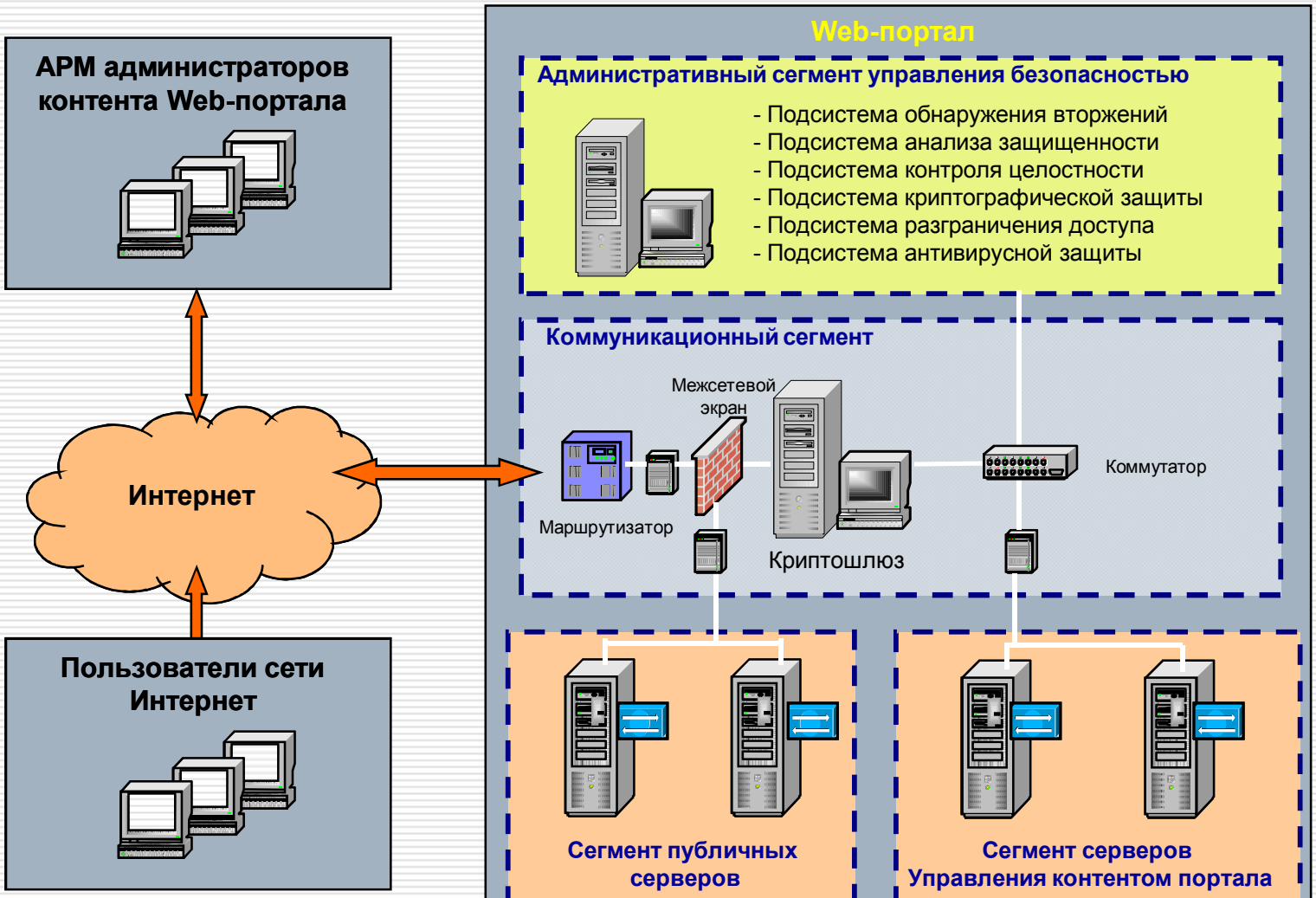
ДиалОгНаука

Схема размещения датчиков подсистемы обнаружения атак



ДиалОгНаука

Защищённый Интернет-портал

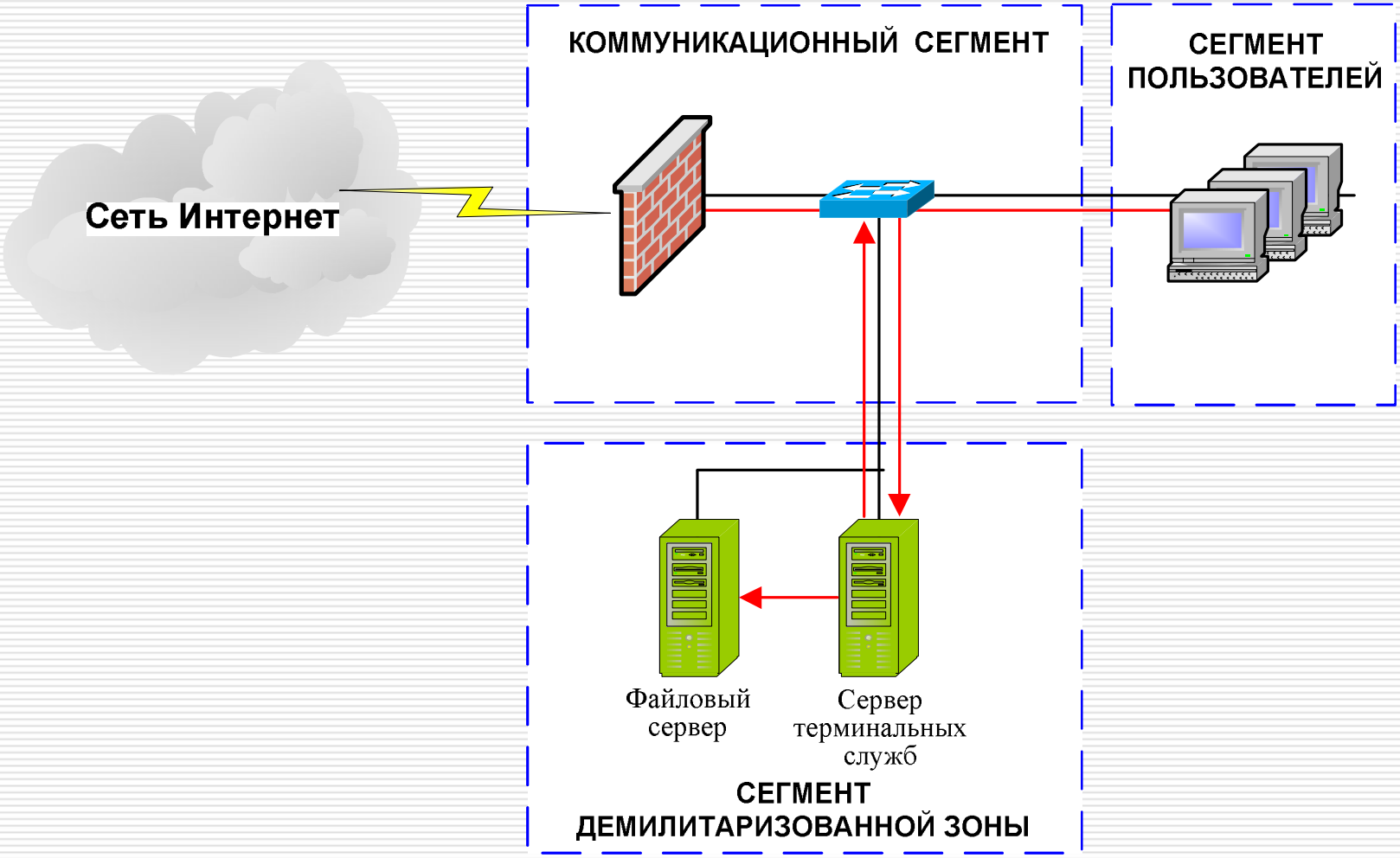


ДиалОгНаука

Защита доступа к Интернет

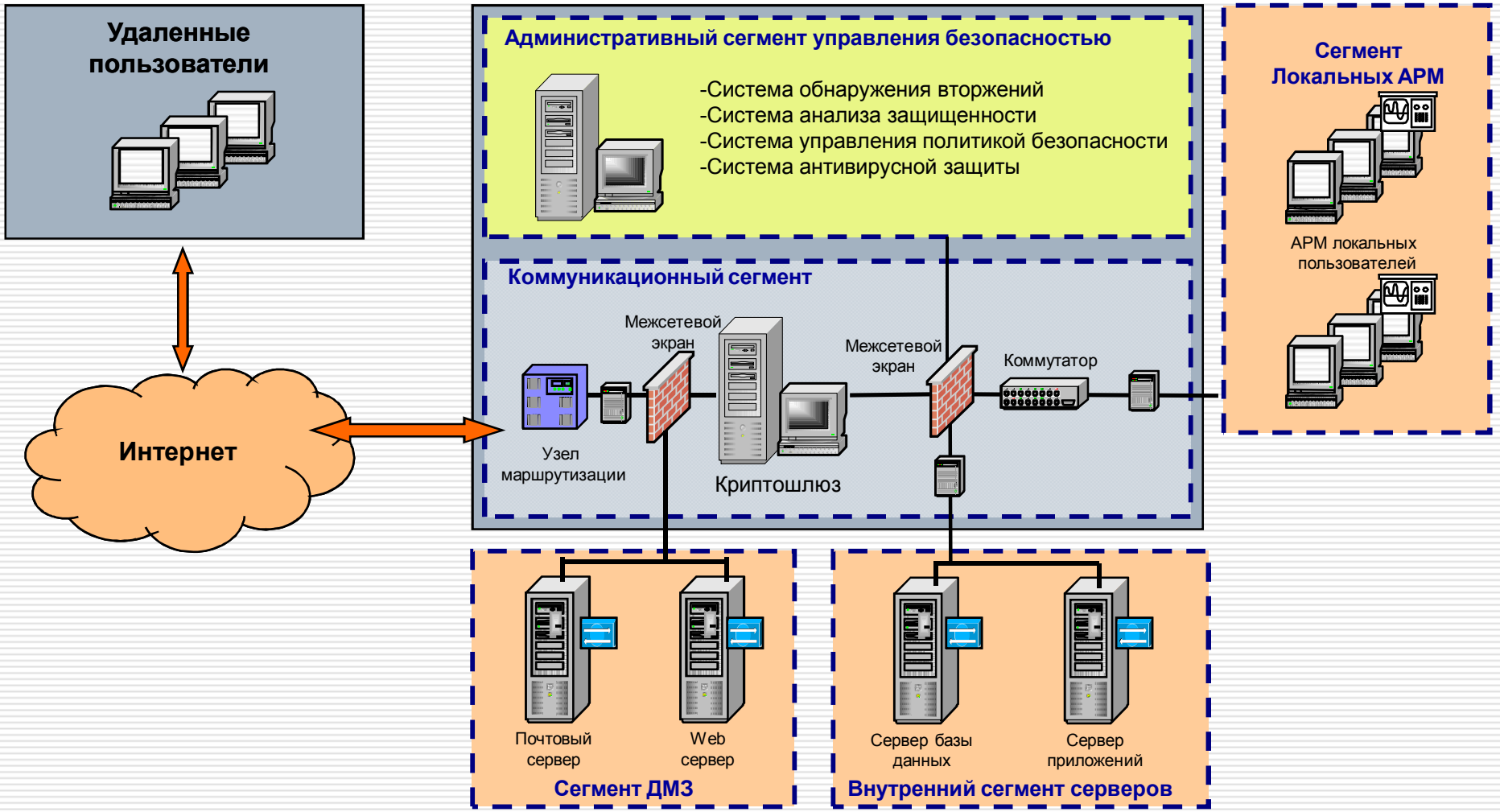
Комплексное решение по организации защищённого доступа к ресурсам сети Интернет

Защищённый доступ к Интернет на основе сервера терминальных служб



ДиалОгНаука

Защищённый доступ к Интернет на основе наложенных средств защиты



ДиалОгНаука

Решение по защите мобильных станций пользователей

ДиалОгНаука

Проблема

- Утери компьютеров с конфиденциальной информацией
- Кражи компьютерной техники с конфиденциальной информацией
- Удалённые атаки из Интернета при подключении ноутбука к сети

Решение

- Шифрование информации на жестких дисках мобильных компьютеров
- Установка систем антивирусной защиты
- Установка персональных сетевых экранов для защиты от внешних атак из сети Интернет

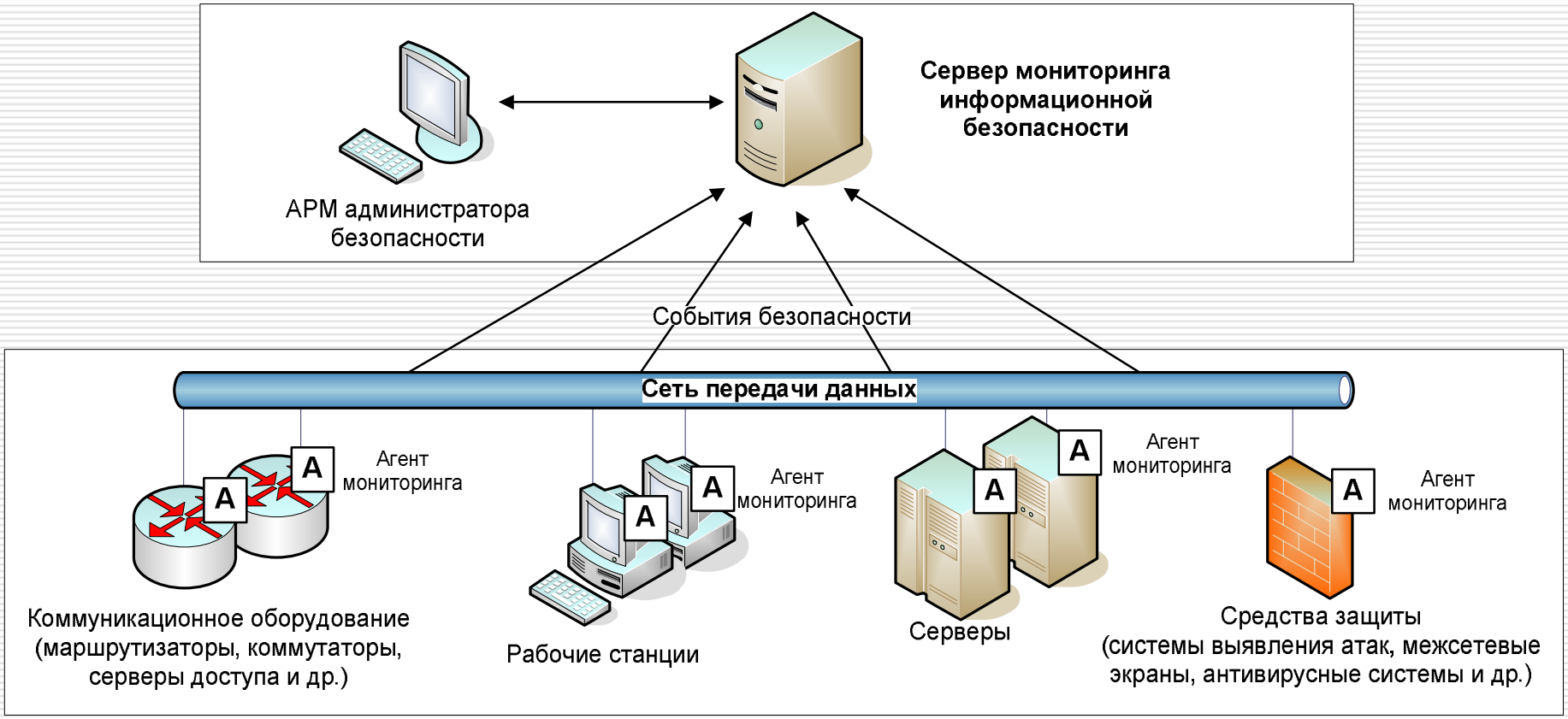
Мониторинг информационной безопасности

Комплексное решение по мониторингу информационной безопасности

Проблема

- Необходимость проведения сопоставительного анализа результатов работы различных средств защиты
- проведение сопоставительного анализа результатов работы средств защиты и параметров работы программно-аппаратного обеспечения АС
- поиск информации об одном событии в журналах аудита различных средств защиты

Решение по мониторингу информационной безопасности



ДиалогНаука

Спасибо за внимание!

Тел.: (495) 980-67-76
Факс: (495) 980-67-75

vas@DialogNauka.ru
www.DialogNauka.ru

ДиалогНаука