



**УНИВЕРСАЛЬНАЯ ОТЕЧЕСТВЕННАЯ  
ПЛАТФОРМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ  
РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННО-  
ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ**

***Коноплев А.С.***

# Распределенные ИТКС



Системы передачи мультимедиа и телеметрической информации (VoIP-системы)

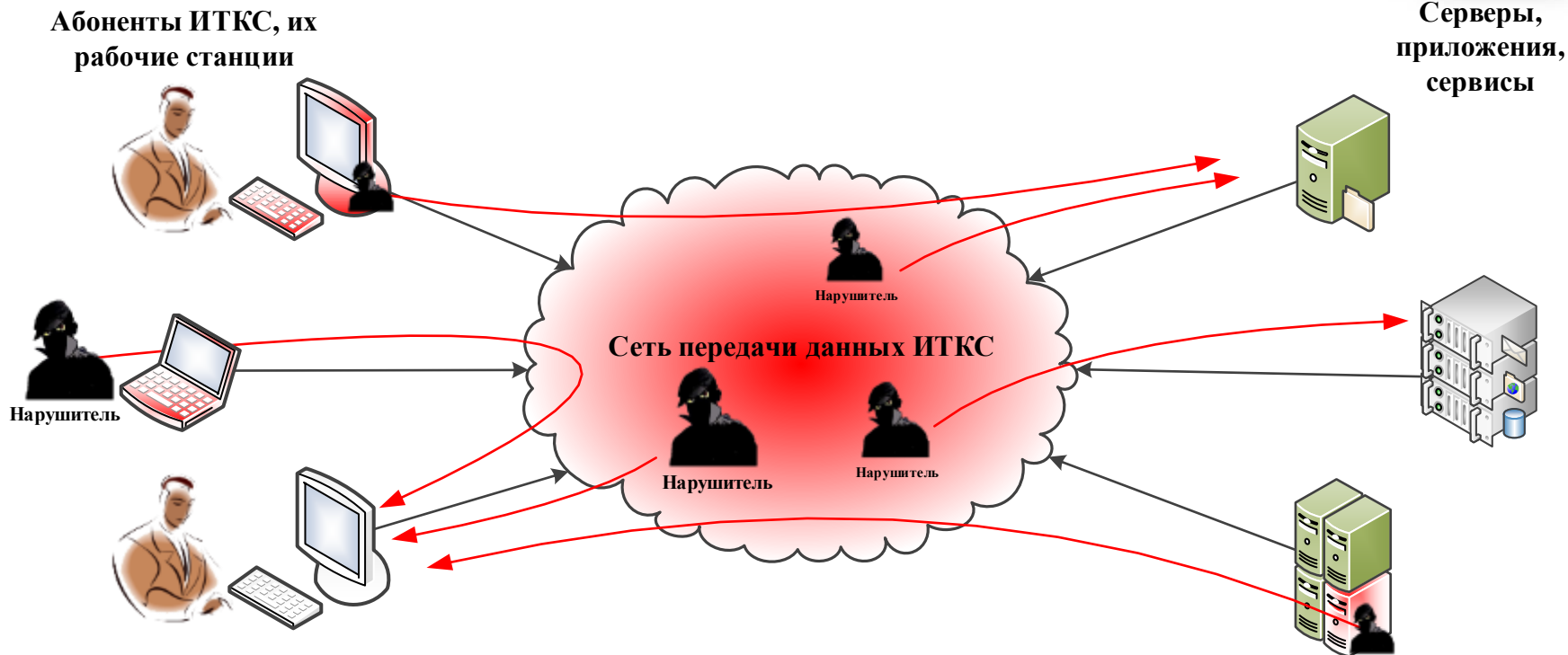


Распределенные системы обработки данных



Распределенные информационные системы: SOAP, SQL, RPC и др.

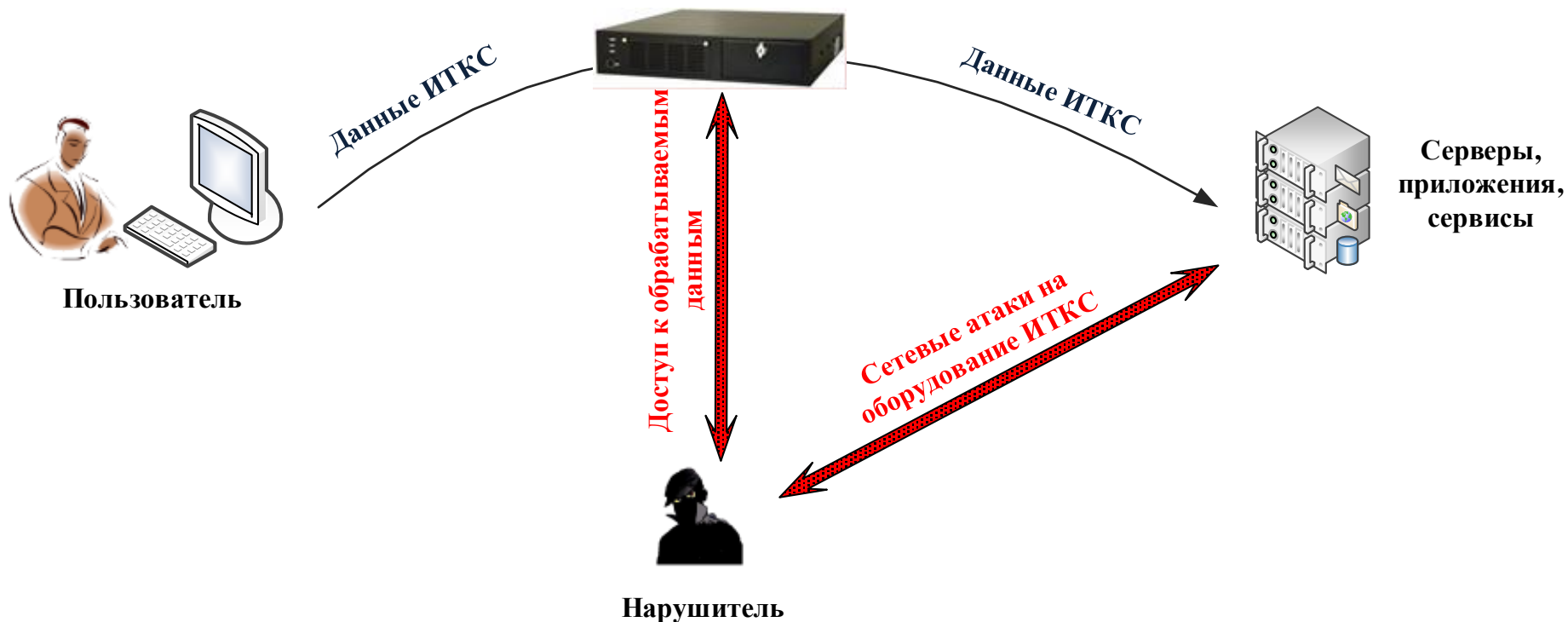
# Угрозы информационной безопасности в распределенных ИТКС



Источниками угроз в распределенной ИТКС являются:

- внешние нарушители;
- внутренние нарушители;
- программные закладки в оборудовании.

# Угрозы безопасности со стороны внешних нарушителей



- Прослушивание канала связи
- Внедрение вредоносного ПО
- Изменение потока сообщений
- Блокирование работы устройств

# Угрозы безопасности со стороны внутренних нарушителей

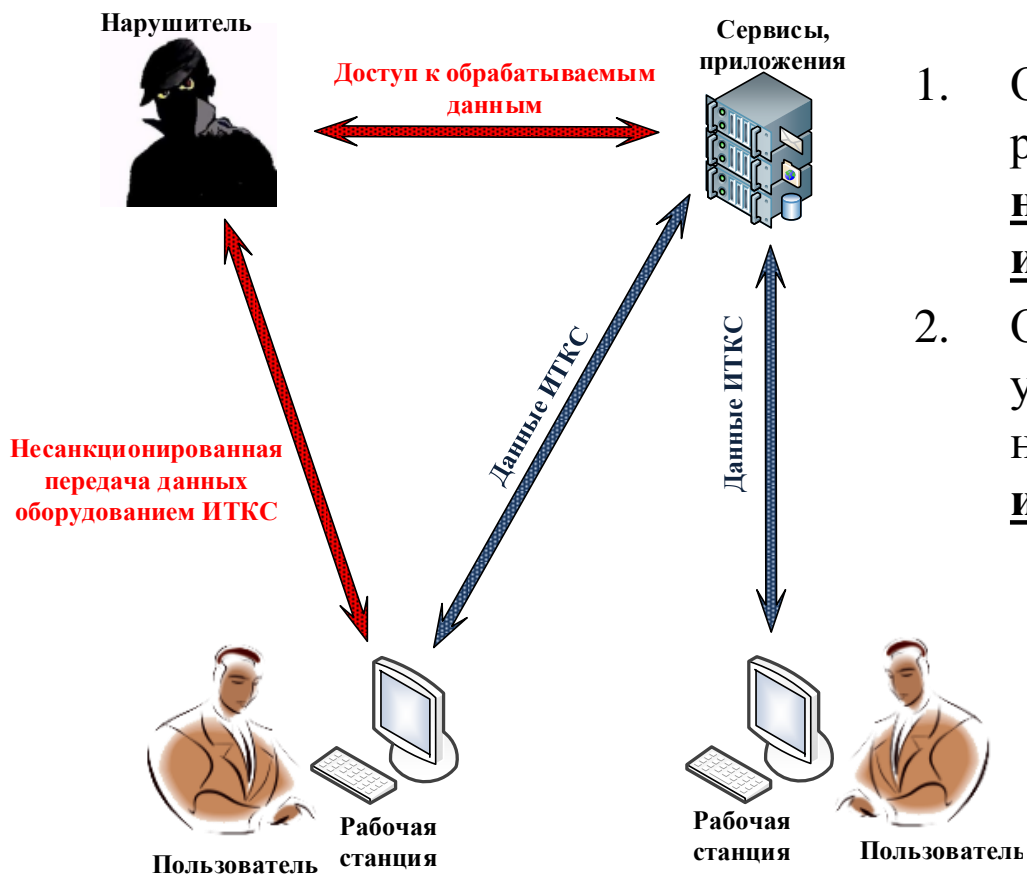


- Несанкционированное установление сеансов связи
- Утечка данных при обработке разнокатегорийной информации

# Угрозы безопасности со стороны оборудования ИТКС



Существует ряд угроз информационной безопасности, являющихся следствием использования недовверенного оборудования:



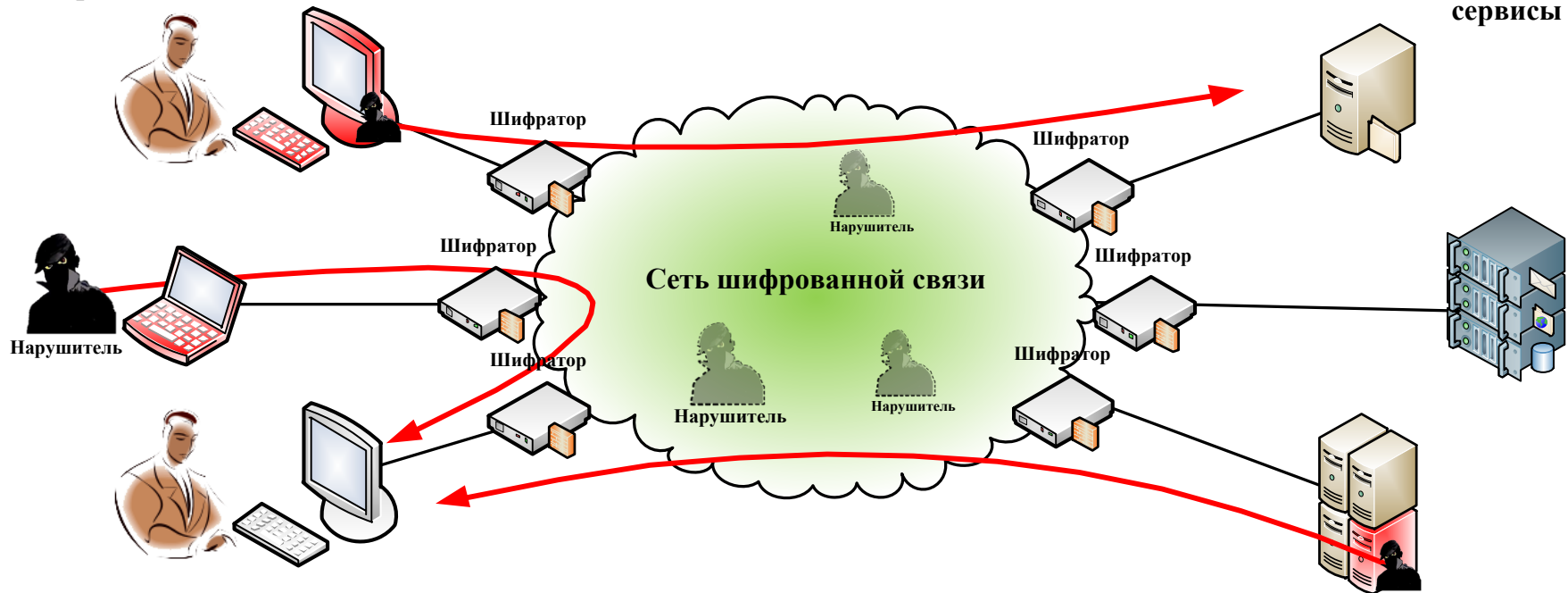
1. Оборудование ИТКС может выступать в роли нарушителя и осуществлять **несанкционированную передачу информации**.
2. Оборудование ИТКС может содержать уязвимости, используя которые, нарушитель может **получить доступ к информации**.

# Защита от внешнего и внутреннего нарушителя в распределенных ИТКС



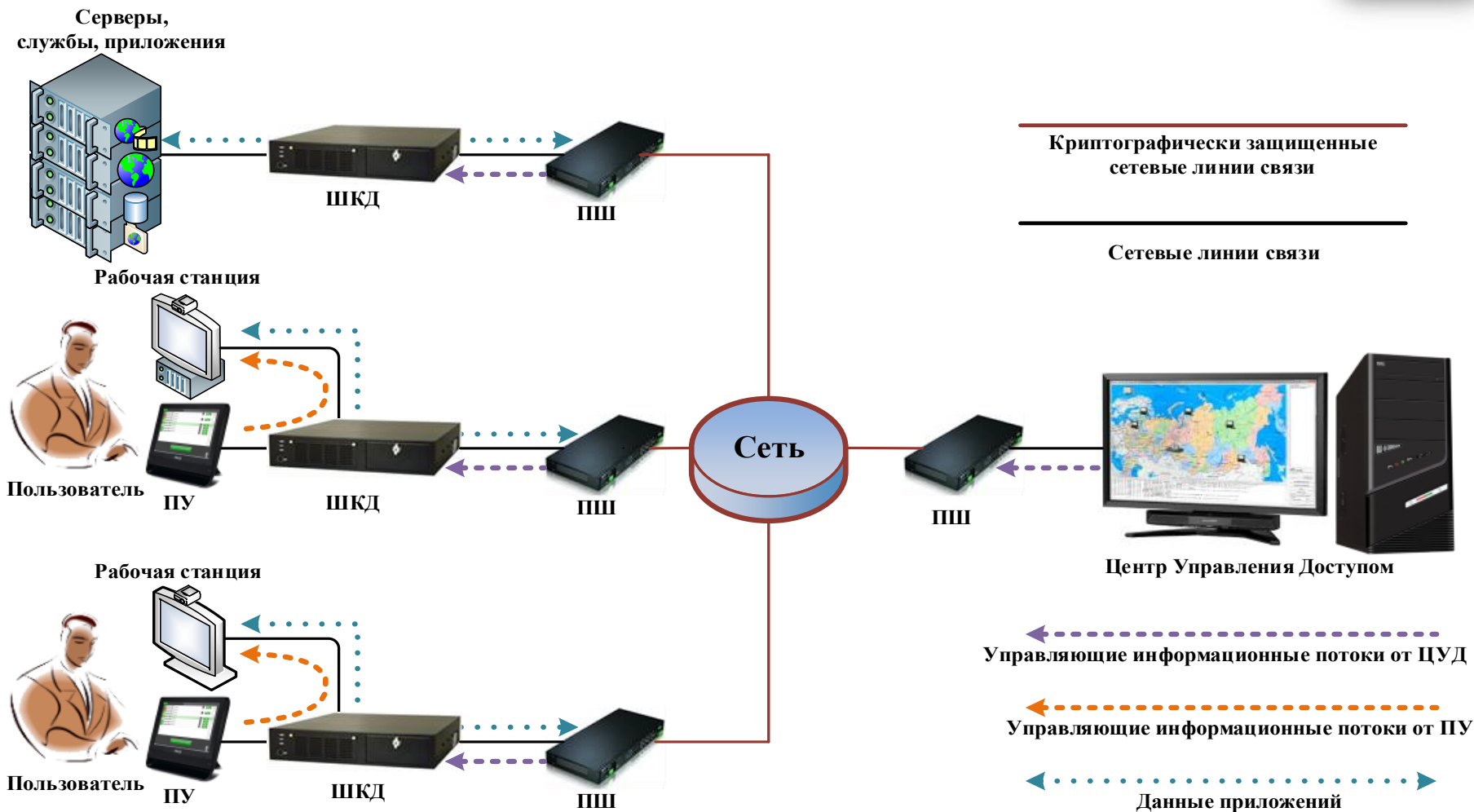
Абоненты ИТКС, их рабочие станции

Серверы, приложения, сервисы



- Использование сетей шифрованной связи в современных ИТКС позволяет надежно защититься от внешнего нарушителя.
- На сегодняшний день не существует такого же простого способа защиты от внутреннего нарушителя.

# Архитектура платформы обеспечения безопасности распределенных ИТКС





# Реализация защиты в распределенных ИТКС



## Шлюз контроля доступа (ШКД)



- средство разграничения и контроля доступа;
- обеспечивает выполнение правил политики безопасности;
- защищает от угроз со стороны внутреннего нарушителя

## Потоковый Шифратор (ПШ)



- средство криптографической защиты;
- защищает от угроз со стороны внешнего нарушителя.

## Пульт управления (ПУ)



- средство идентификации операций доступа;
- защищает от угроз со стороны недоверенного оборудования ИТКС.

## Центр управления доступом (ЦУД)

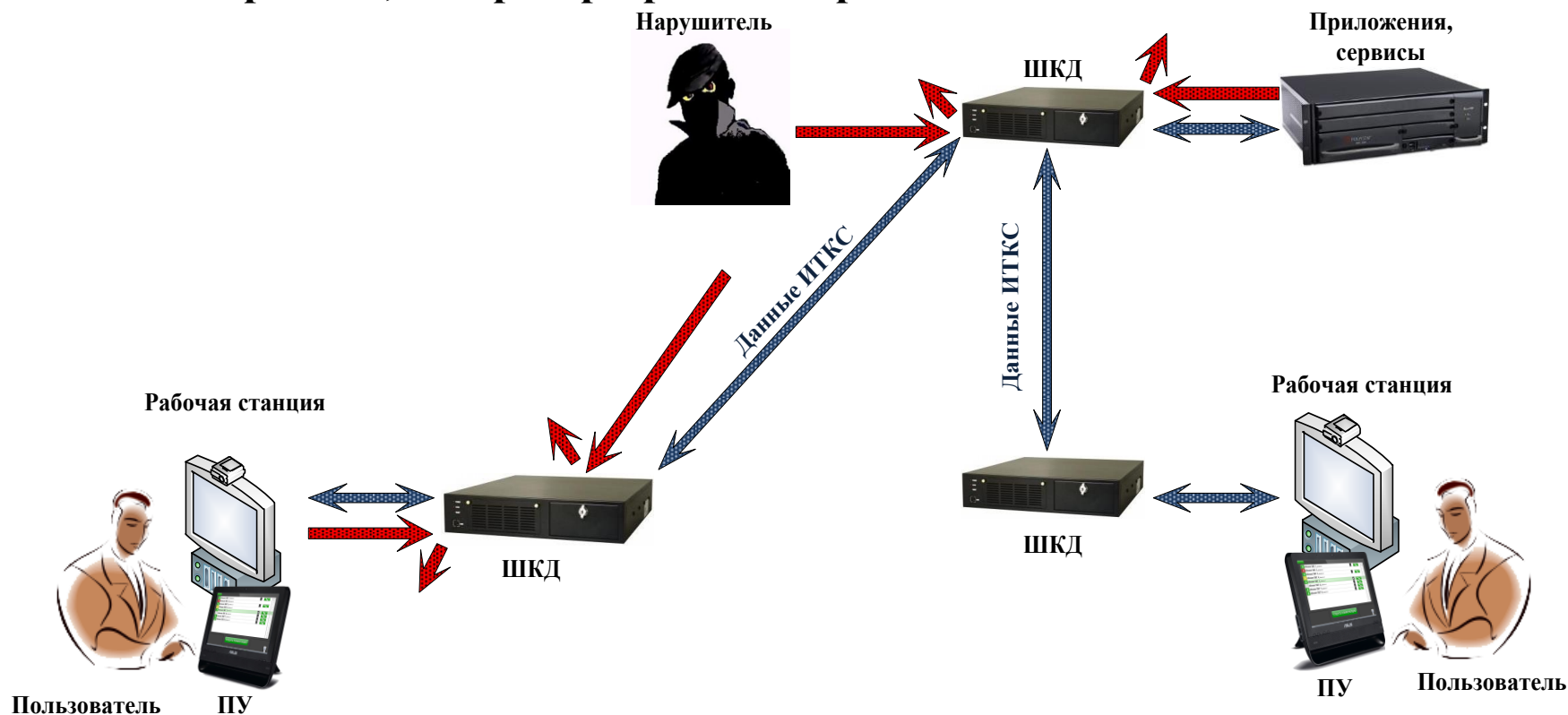


- средство мониторинга и управления;
- используется как АРМ администратора ИТКС;
- позволяет осуществлять надзор за функционированием системы.

# Защита от угроз безопасности со стороны оборудования ИТКС



**1. ШКД разрешает передачу данных только между теми узлами и только в те моменты времени, которые разрешены правилами политики безопасности**



**2. Несанкционированная отсылка данных, а также попытки использования уязвимостей в оборудовании ИТКС будут предотвращены ШКД**



## **НАЗНАЧЕНИЕ:**

Управление потоками данных в защищенных распределенных информационных системах, построенных с использованием IP-сетей шифрованной связи.



## **ЦЕЛЬ:**

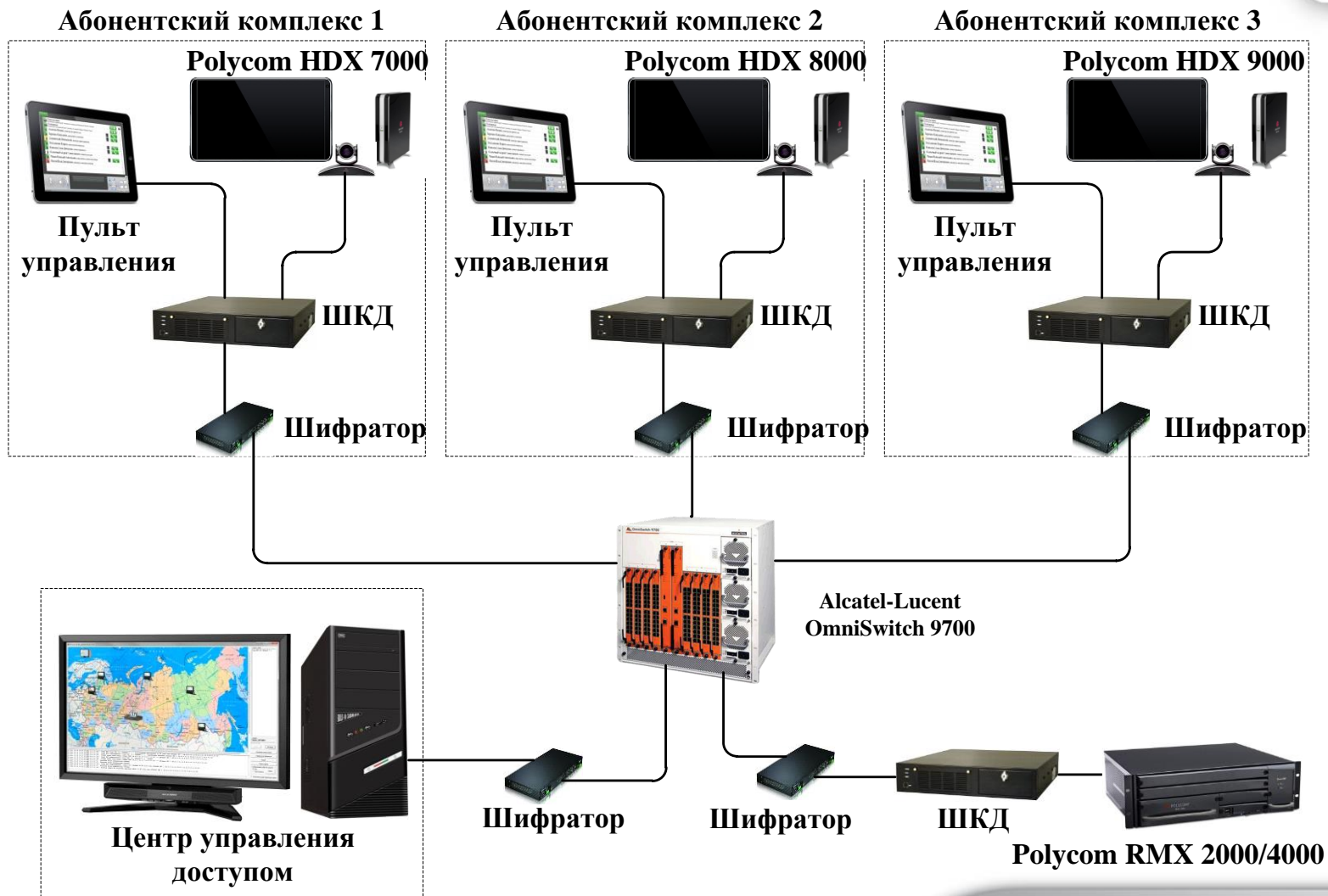
Предотвращение несанкционированного доступа пользователей к сетевым информационным ресурсам и сервисам.



## **ОСНОВНАЯ ФУНКЦИОНАЛЬНОСТЬ:**

Распределенный контроль устанавливаемых сетевых соединений в соответствии с заданной политикой безопасности.

# Использование ПАК «Купидон» в системах видеоконференцсвязи



# Центр Управления Доступом



Мониторинг сети и текущих сеансов связи

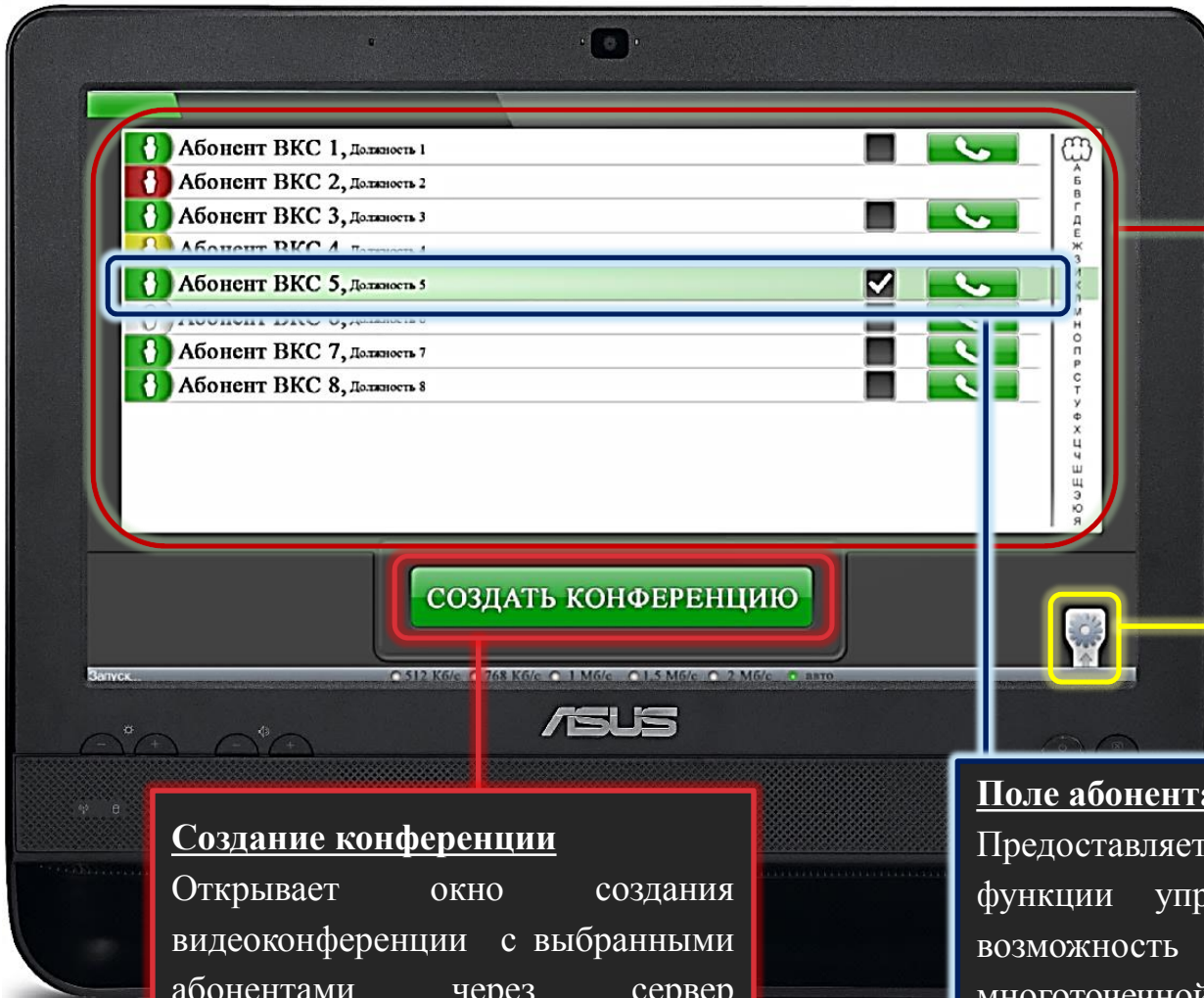
Управление текущими сеансами связи



Отображение аудита системных событий

Настройки и управление системой

# Пульт Управления сеансами связи VoIP



**Адресная книга**  
Поля адресной книги отображают:

- список абонентов сети и их статусы
- список текущих конференций

**Управление оборудованием**  
Открывает панель управления видеооборудованием, которое закреплено за данным Пультom Управления

**Создание конференции**  
Открывает окно создания видеоконференции с выбранными абонентами через сервер многоточечной видеосвязи

**Поле абонента**  
Предоставляет основную информацию об абоненте, функции управления сеансом связи, а также возможность выбора абонента для участия в многоточечной конференции

# Поддержка VoIP оборудования



- ✓ CISCO EX 90
- ✓ CISCO Quick Set C20



- ✓ Tandberg Edge 85 MXP
- ✓ Tandberg Edge 95 MXP
- ✓ Tandberg Codian MCU



- ✓ Polycom HDX 4000
- ✓ Polycom HDX 7000
- ✓ Polycom HDX 8000
- ✓ Polycom HDX 9000
- ✓ Polycom RMX 2000
- ✓ Polycom RMX 4000

