
OTUS
ОНЛАЙН-ОБРАЗОВАНИЕ
Онлайн-образование

Не забыть включить запись!

Меня хорошо видно && слышно?

Ставьте + , если все хорошо
Напишите в чат, если есть проблемы

СЕТЕВАЯ ПОДСИСТЕМА ANDROID

Казанцев Анатолий

преподаватель

+7 (499) 110-61-65

Правила вебинара

Активно участвуем

Задаем вопрос в чат или голосом

Off-topic обсуждаем в Slack #general или #pentest-2019-09

Вопросы вижу в чате, могу ответить не сразу

Маршрут вебинара

Основные понятия

Устройство сетевого стека

RIL (Radio Layer Interface)

Практика

Цели вебинара

1. Рассмотреть архитектуру сетевой подсистемы ОС Linux

2. Научиться получать информацию о состоянии сетевой подсистемы

3. Провести практическую работу с ОС Android

СЕТЕВАЯ ПОДСИСТЕМА

Основные понятия

Сетевая подсистема ОС Android представляет собой надстройку над сетевым стеком Linux.

Основные понятия

Сердце сетевого взаимодействия - подсистема **RIL (Radio Interface Layer).**

Создана для того чтобы обрабатывать информацию напрямую от модулирующих чипов.

https://source.android.com/devices/tech/connect/ril

Основные понятия

RIL представляет собой абстрактный слой между сервисом телефонии (android.telephony) и оборудованием (модемом).

Основные понятия

Управляет обработкой:

- голосовых звонков;
- текстовых сообщений;
- мобильного интернета.

Основные понятия

RIL состоит из двух основных компонентов:

- RIL Daemon (/system/bin/rild);
- Vendor RIL.

RIL Daemon

RIL Daemon (/system/bin/rild)

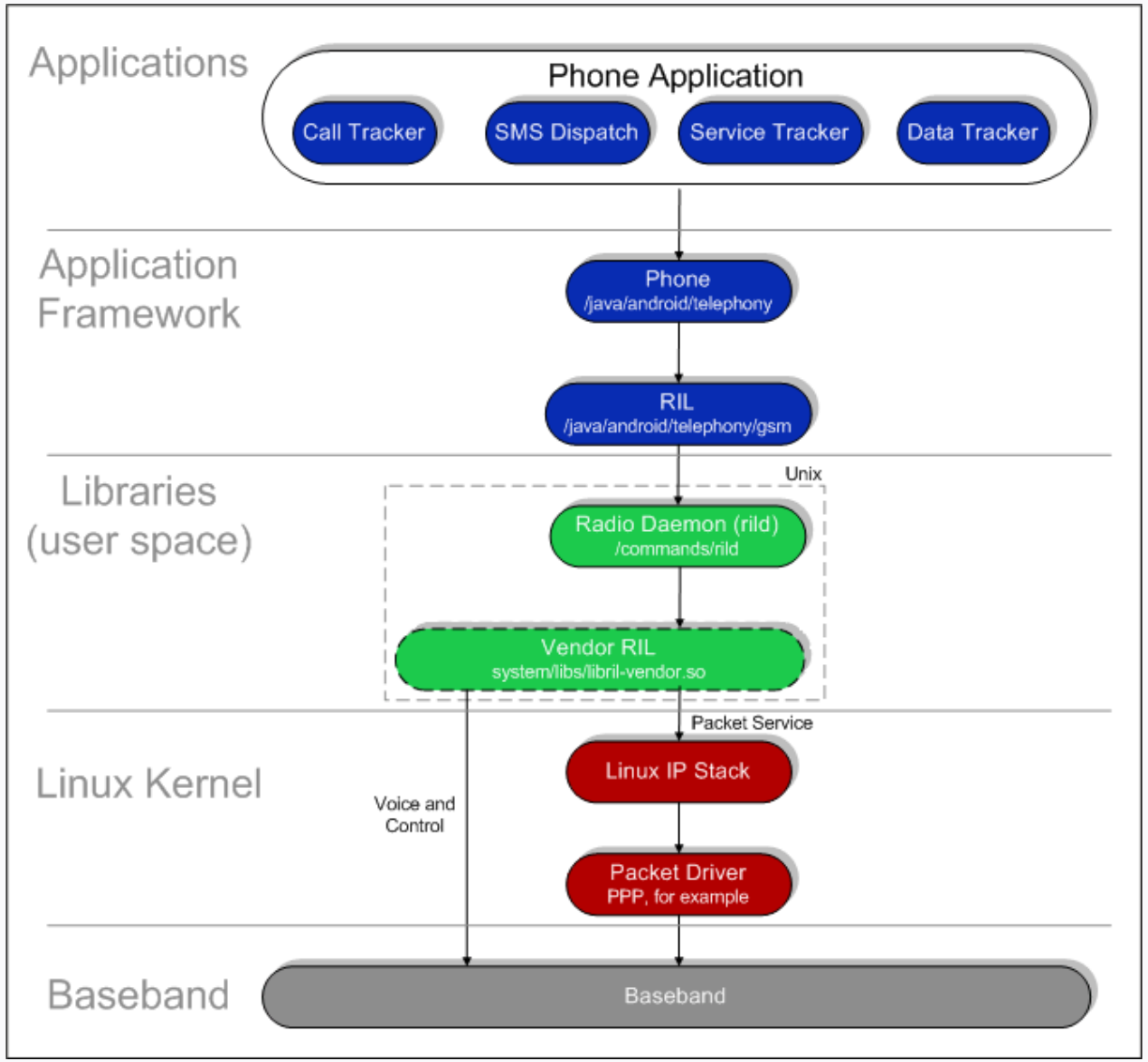
Инициализирует компонент Vendor RIL и планировщик событий, обрабатывает всю коммуникацию от сервисов телефонии Android и отправляет вызовы к Vendor RIL как запрашиваемые (solicited) команды. Исходные коды в каталоге /hardware/ril/rild/

Vendor RIL

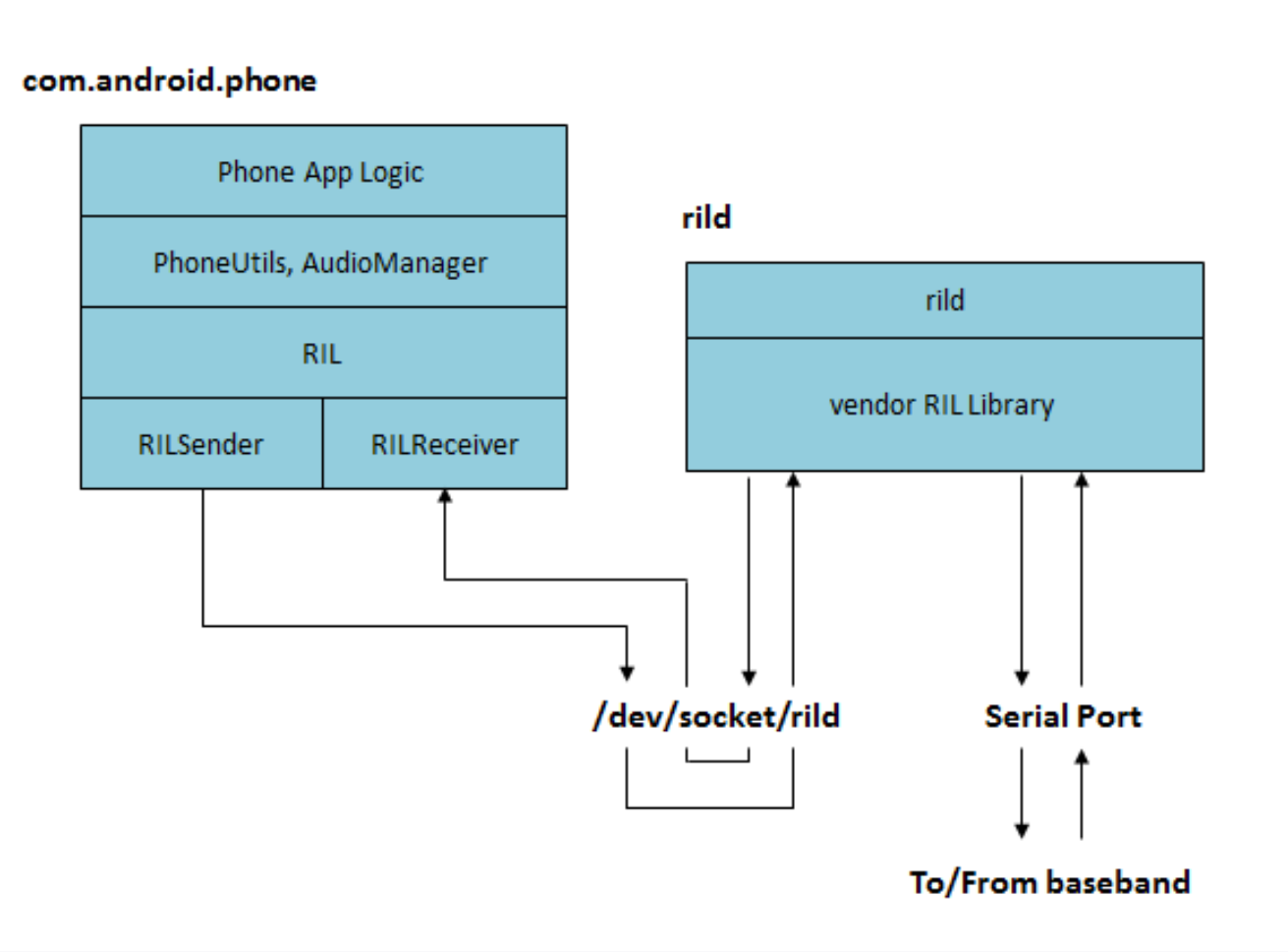
Vendor RIL

Инициализирует модем, производит взаимодействие непосредственно с модемом. RIL производителя представляет из себя динамическую библиотеку, разрабатываемую производителем модема. Шаблон для разработки располагается в каталоге /hardware/ril/reference-ril/.

Архитектура RIL



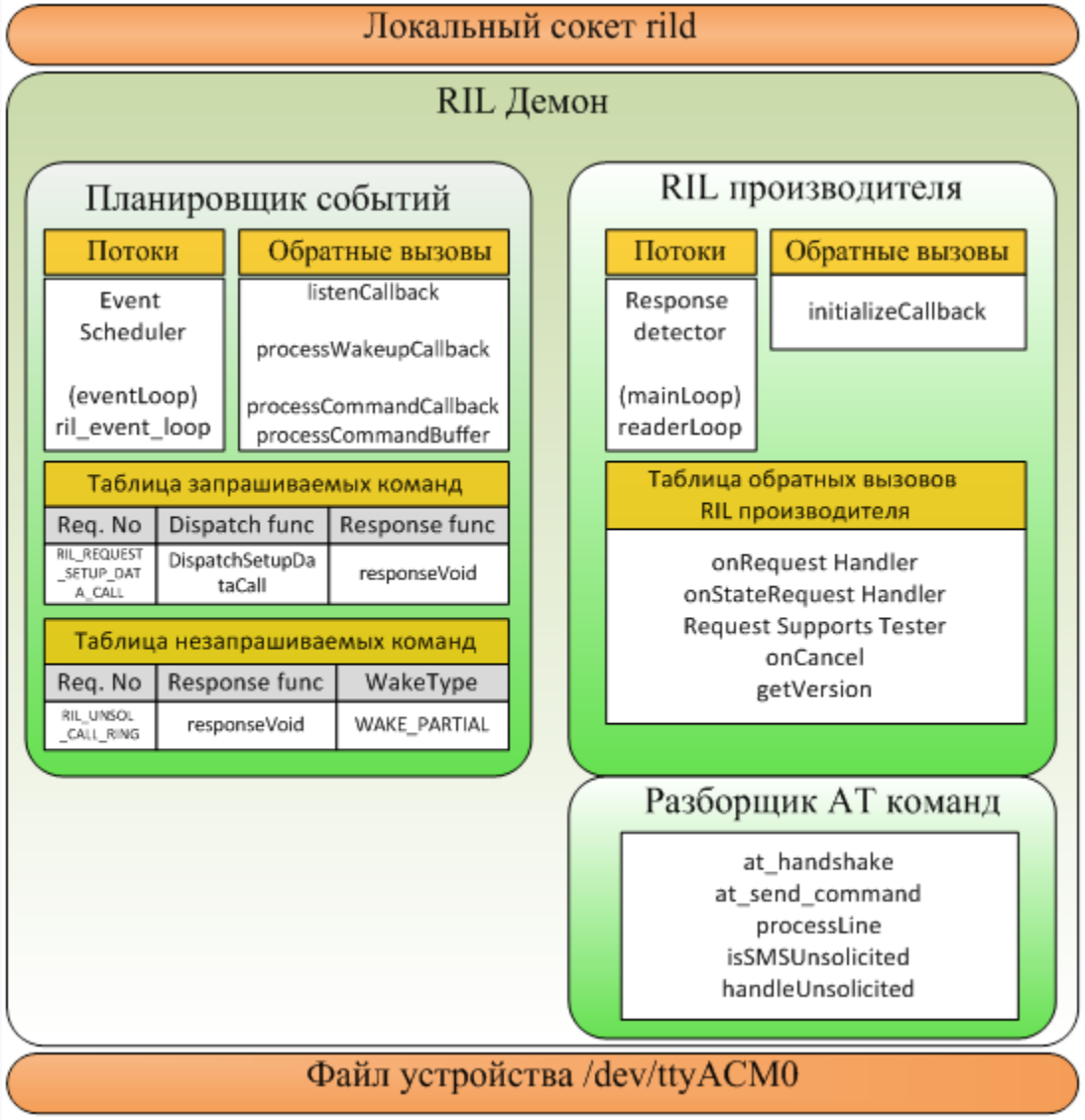
Архитектура RIL



RIL debug

Для отладочных целей демон rild также слушает сокет **/dev/socket/rild-debug**

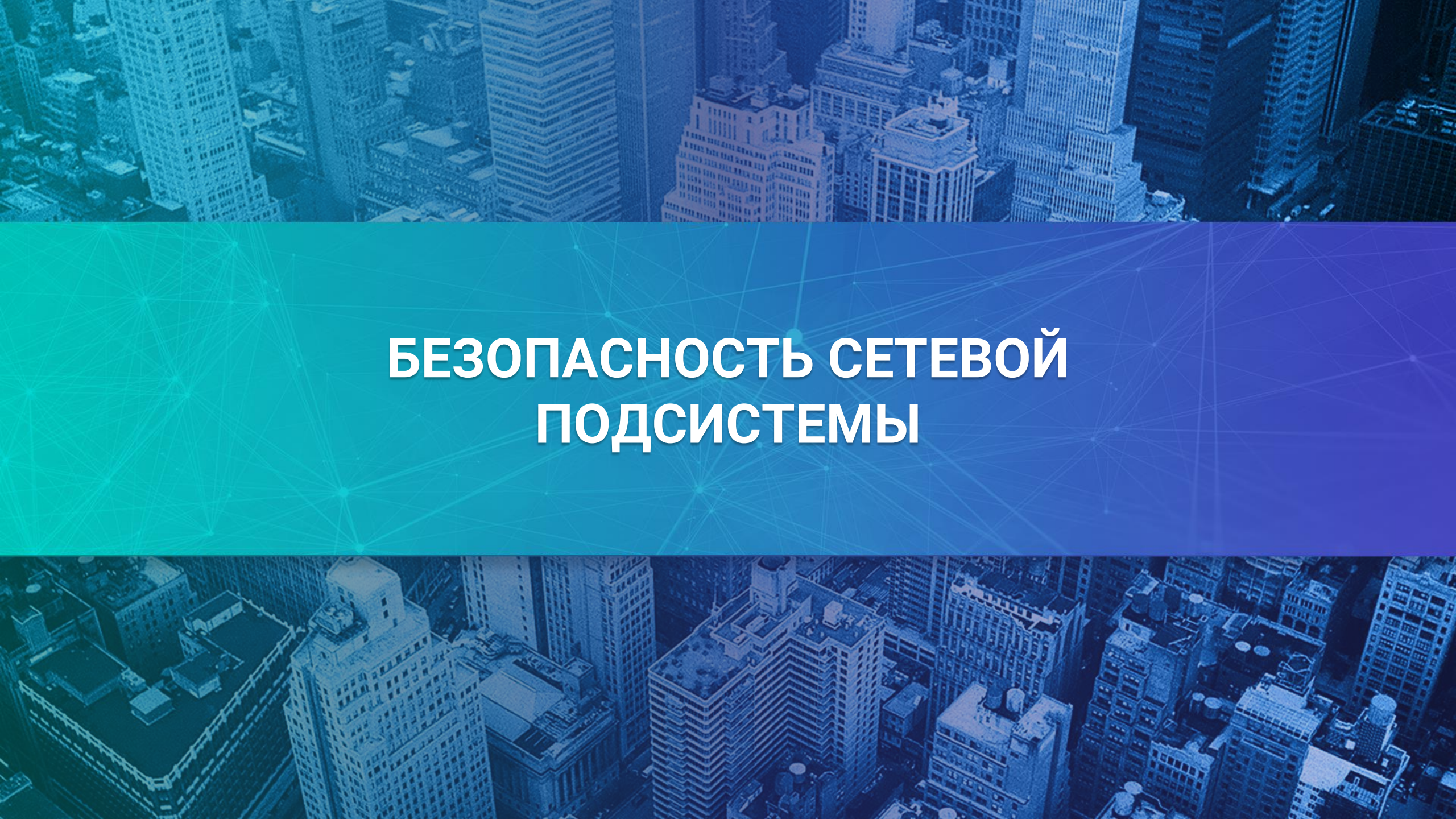
RIL


Локальный сокет rild
RIL Демон
Планировщик событий
Потоки
Обратные вызовы
Event Scheduler
(eventLoop) ril_event_loop
listenCallback
processWakeupCallback
processCommandCallback
processCommandBuffer
Таблица запрашиваемых команд
Req. No
Dispatch func
Response func
RIL_REQUEST_SETUP_DATA_CALL
DispatchSetupDataCall
responseVoid
Таблица незапрашиваемых команд
Req. No
Response func
WakeType
RIL_UNSOL_CALL_RING
responseVoid
WAKE_PARTIAL
RIL производителя
Потоки
Обратные вызовы
Response detector
(mainLoop) readerLoop
initializeCallback
Таблица обратных вызовов RIL производителя
onRequest Handler
onStateRequest Handler
Request Supports Tester
onCancel
getVersion
Разборщик AT команд
at_handshake
at_send_command
processLine
isSMSUnsolicited
handleUnsolicited
Файл устройства /dev/ttyACM0

Термины

Говоря о RIL, также следует упомянуть следующие понятия:

- **unsolicited commands**: события, генерируемые модулирующими чипами (например, входящий звонок);
- **solicited commands**: команды, которые поступают от приложений (набор номера, ответ, удержание и т.д.).

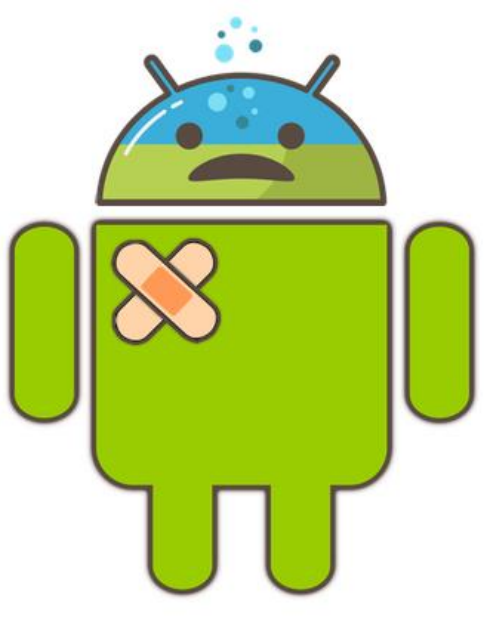


БЕЗОПАСНОСТЬ СЕТЕВОЙ ПОДСИСТЕМЫ

Безопасность сетевой подсистемы

Подсистема написана на языке программирования C/C++

- проблемы с указателями;
- переполнения;
- повреждения памяти
- и т.д.



Безопасность сетевой подсистемы

Особый механизм взаимодействия:

- RIL получает данные из сети сразу после получения данных в модеме телефона;
- есть возможность проведения фаззинга (например, SMS).

Безопасность сетевой подсистемы

В случае успешной атаки:

- можно включить подсистему дозвона и превратить телефон в жучок;
- можно подключить платные подписки;
- удаленное управление устройством.

ПОЛУЧЕНИЕ ИНФОРМАЦИИ О ДЕМОНЕ RIL

Следующий вебинар

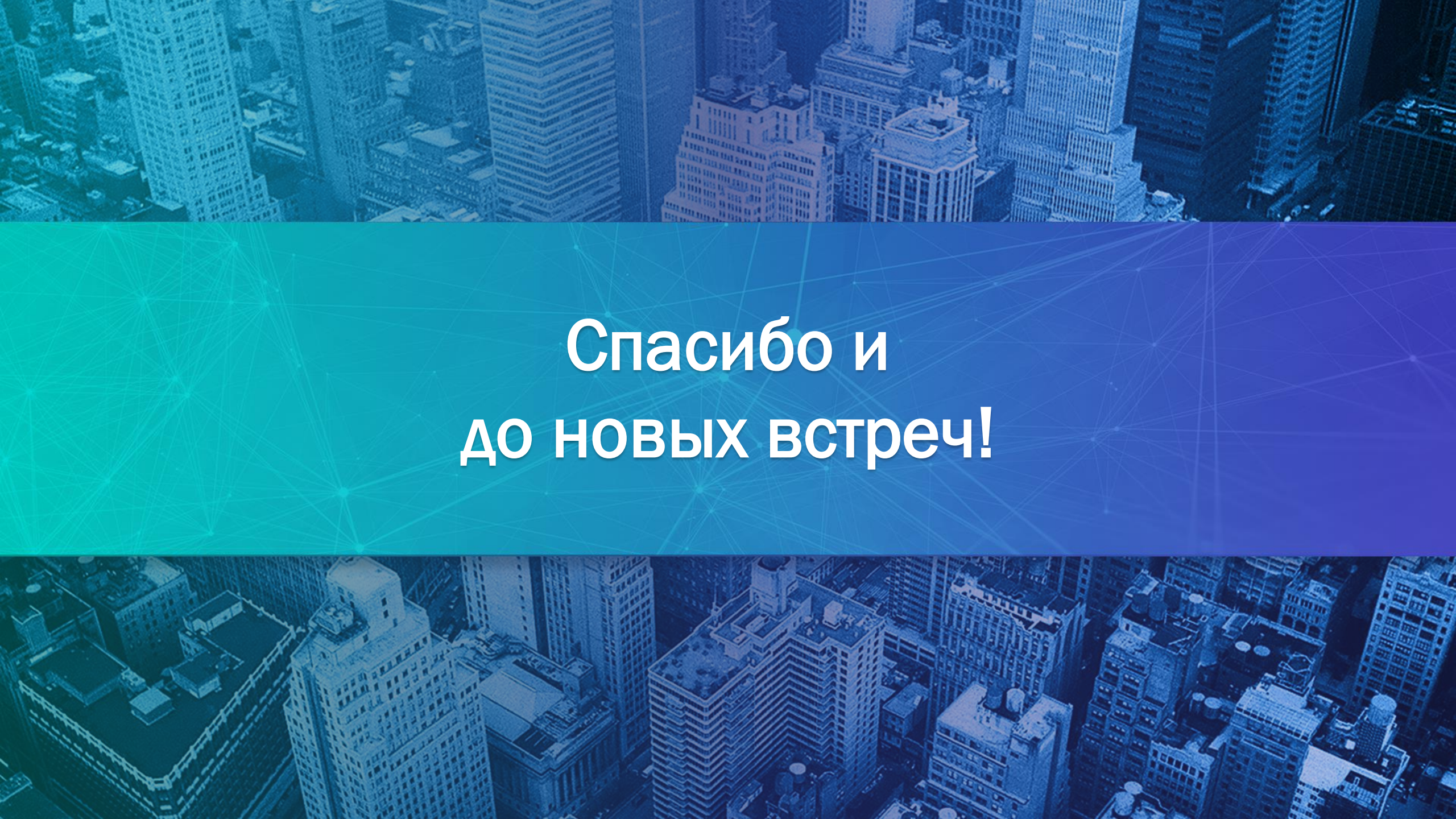
Тема: «Основные методы модификации трафика»

Вторник 19 ноября 2019 г. в 20:00

Ссылка на вебинар будет в личном кабинете за 15 минут до начала

Материалы к занятию в ЛК — можно изучать

Обязательный материал обозначен красной лентой


Спасибо и
до новых встреч!