Обнаружение нарушений политик безопасности при работе в сетях WiFi для помещений с ограниченным доступом

Бусленко С.Е.
Макаренков С.А.
Старичков В.В.

УМО ИБ, г. Москва

конференция
РусКрипто'2013

Постановка задачи

Преимущества сетей БСПД:

- *простота развёртывания*
- *мобильность инфраструктурных сетевых средств*
- *возможность использования абонентских устройств*

Следствие:

- *использование технологии WiFi в качестве сегмента корпоративных сетей*

Проблемы:

- *утечка информации по радиоканалу*
- *атаки на корпоративную БСПД*

Утечка информации БСПД

Типовые ситуации, приводящие к утечке информации по каналам связи Wi-Fi

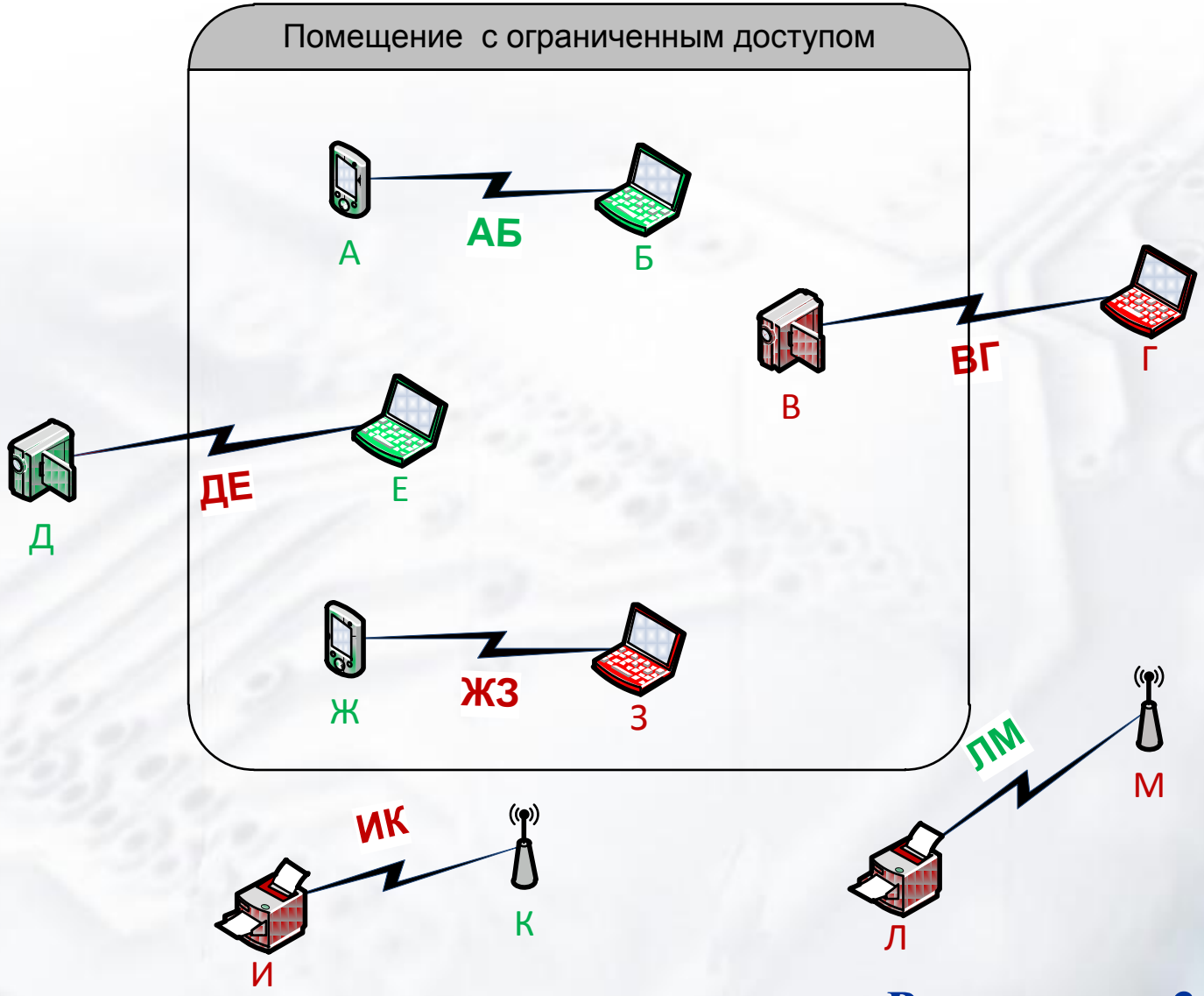
- *несанкционированное подключение нарушителя к точке доступа организации*
- *подключение сотрудника организации из режимного помещения к точке доступа внешней сети*

Типовые источники угроз

Сотрудники организации	Злоумышленники
Обладают служебными или личными ПЭВМ, КПК, коммуникаторами со средствами доступа к БСПД	Обладают WiFi-средствами. Пытаются получить доступ к служебной сети или передать информацию по БСПД
Как правило, используют заводской аппаратный адрес, на служебную сеть вредоносного влияния не оказывают	Могут атаковать служебную сеть. Подменяют сегменты служебной сети, компрометируют адресную информацию

Защита от НПИ

Содержание политик безопасности



Рускрипто 2013

Требования к средствам интеллектуального блокирования

- Поиск сигналов БСПД стандартов IEEE 802.11a/b/g
- Обнаружение и блокирование «двойников» WiFi устройств
- Классификация устройств WiFi по принципу «свой-чужой»
- Обеспечение беспрепятственной работы «своих» WiFi устройств
- Предотвращение информационного взаимодействия с «чужими» WiFi устройствами
- Определение местоположения WiFi устройств
- Конфигурирование и контроль состояния автономных портативных датчиков
- Передача в реальном времени принятой датчиками информации в систему анализа (IDS, DLP)

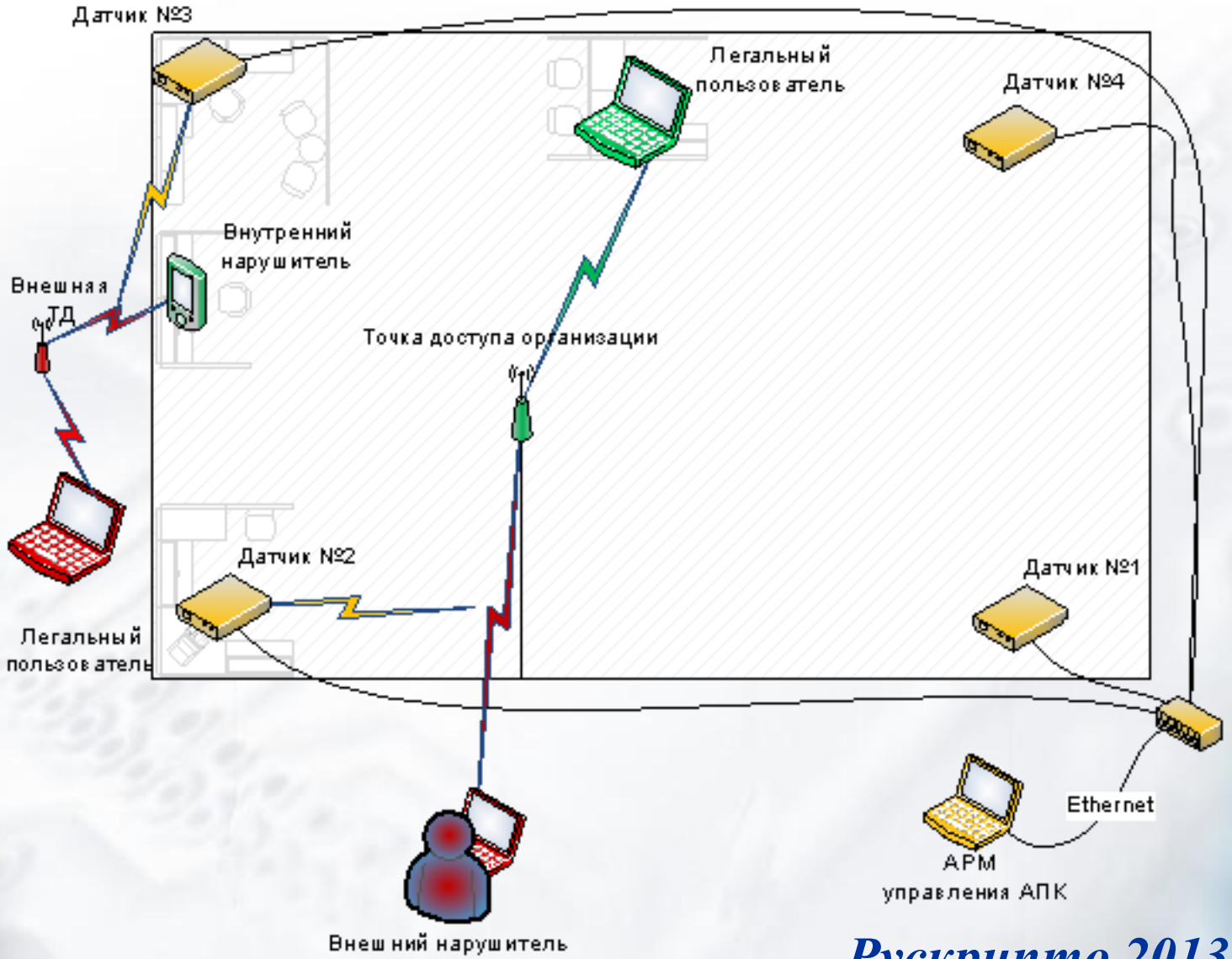
Способы интеллектуального блокирования

- Метод помеховых кадров
  - использует особенности CSMA/CA
- Метод «деаутентификации»
  - «мягкое» блокирование соединения с точкой доступа
- Использование особенностей реализации стека 802.11 в различных ОС
  - «жесткое» блокирование для Windows XP
- Использование процедуры обмена RTS/CTS кадрами
  - отправка CTS кадра о занятости среды передачи

Способы оценки местоположения абонента

- модель центра масс
- модель равновесия
- модель Фрииса (Friis)

Типовая схема размещения средств интеллектуального блокирования



Спасибо за внимание!

Вопросы?

Старичков Владимир Викторович

контакты: +7 916 934-42-54

v.starichkov@mail.ru