

Корпорация ЮНИ



Технологии обеспечения безопасности беспроводных сетей

WLAN Security

Нестеров Руслан Олегович

технический эксперт

rnesterov@uni.ru

+7 (095) 580 9555

Содержание



- Введение
- Особенности мобильных сред
- Структуры и топологии беспроводных сетей
- Проблемы защиты беспроводных сетей
- Задачи и методы защиты беспроводных сетей
- Инфраструктура решения

Протоколы мобильного доступа



Масштаб	Протокол	Скорость	Применение
WAN 	802.20 3G (UMTS) 2.5G (GPRS)	6 Mbps 384 kbps-2 Mbps 9.6 kbps-115 kbps	Глобальный транспорт + глобальный роуминг (протокол разрабатывается, внедрения ожидаются в 2005-2006 г.г.). Передача данных в сетях мобильной телефонии 3го поколения. Передача данных в современных сетях мобильной телефонии (GSM)
MAN (WiMAX) 	802.16 802.16a 802.16e	75 Mbps 134 Mbps 15 Mbps	Региональные сети («последняя миля» по радиотракту). Мобильный доступ (802.16e). Локальные радиосети
LAN (WiFi) 	802.11 802.11b 802.11a 802.11g	2 Mbps 11 Mbps 6-54 Mbps 2-54 Mbps	Локальные радиосети. Мобильный доступ в Интернет
PAN 	HomeRF BlueTooth	1 Mbps	Подключение периферийных устройств. Передача данных в малых локальных сетях

Особенности среды беспроводного доступа



- Мобильные среды удобны, обеспечивают соединение в различных местах расположения пользователей и стремительно развиваются
- Мобильные среды меняют понятие «сеть»:
 - у персонального компьютера могут появляться и исчезать динамически новые сетевые интерфейсы и соединения
 - исчезает традиционное понятие «топология»; там где в проводной сети она проста и очевидна (например, подключение компьютеров к коммутатору по схеме «звезда») – могут появляться неуправляемые и неучтенные линии связи (например, полносвязный граф соединений вместо «звезды»)
- *Мобильные протоколы используют общедоступный эфир, как среду передачи данных, где перехват информации и информационные атаки крайне трудно контролировать*
 - *возникает общая для всех мобильных сред задача защиты данных*
 - *эта задача должна решаться в условиях динамической и неопределенной топологии радиосети*

Беспроводное оборудование



Оборудование PreWiMax

Aperto

Aperto PacketWave



Airspan

AS.MAX



Infinet

SkyMAN



Alvarion

Breeze ACCESS, BreezeMax



Оборудование Wi-Fi

NETGEAR



WG302 > Wireless Access Point



DG834G > Wireless ADSL Modem Firewall Router



WG311 > Wireless PCI Adapter

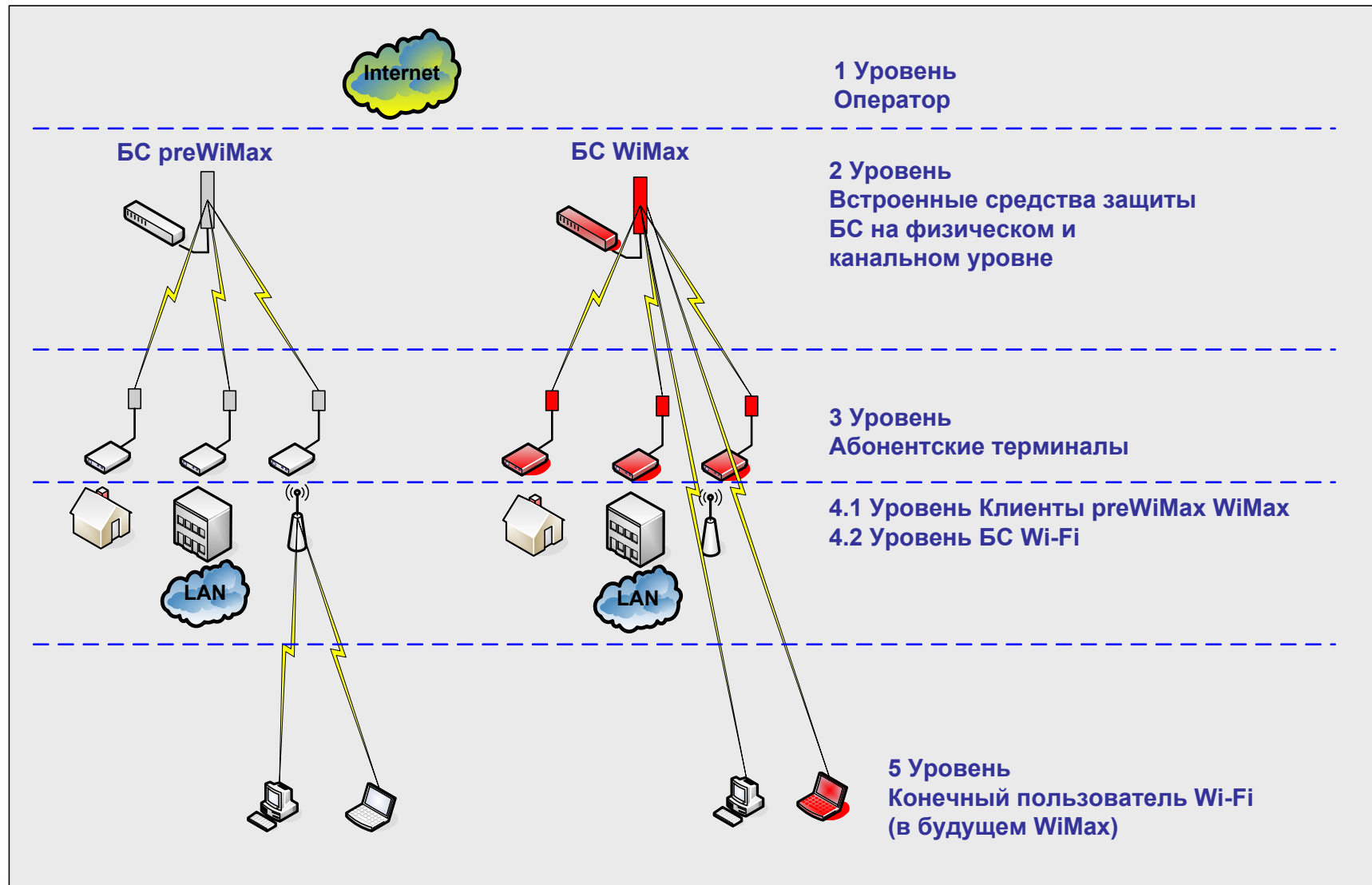
NORTEL



Security Switch 2250



Уровни защиты беспроводных сетей 802.X



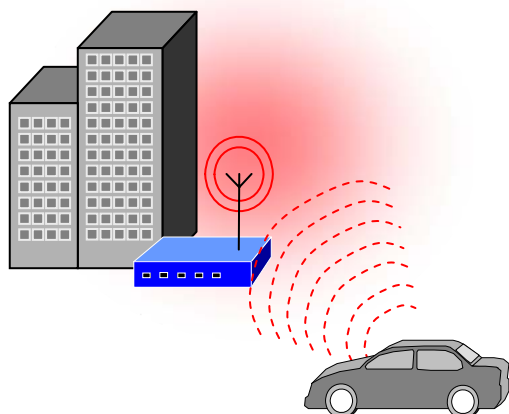
Общая схема построения системы preWiMax



Уязвимость мобильных сред



Уязвимость радиосети для профессиональной атаки



Неполный список Интернет-сайтов со средствами взлома радиосетей

<http://www.phenoelit.de/irpas/>

<http://ettercap.sourceforge.net>

<http://www.oxid.it>

<http://sourceforge.net/projects/wepattack/>

<http://asleep.sourceforge.net/>

<http://www.thc.org>

<http://naughty.monkey.org/~dugsong/dsniff>

<http://ikecrack.sourceforge.net/>

- *«Беспроводные сети очень легко устанавливаются и ими легко манипулировать, поэтому пользователи и киберпреступники будут использовать их для атаки на корпоративные сети»*

Gartner group,

Sep'03

- *«Неконтролируемые беспроводные сети составляют опасность для всей корпоративной сети, ее данных и операций»*

Forester Research,

Inc.

Технологические проблемы защиты



- Множественность протоколов (сред доступа)
- Множественность устройств
- Уязвимости конкретных протоколов
- Невозможность применить отечественные (сертифицированные средства защиты)

Проблемы безопасности WiFi



- большинство устройств поступают в продажу с установками по умолчанию, отменяющими функции безопасности в целях совместимости
- зона покрытия точки радиодоступа
- защита основанная на адресах канального уровня (MAC) недостаточна
- два режима работы сетевых адаптеров беспроводной сети:
 1. подключение только к точке доступа (infrastructure mode)
 2. режим «каждый с каждым» (ad hoc mode)

Перечень угроз



- нарушение конфиденциальности информации – Eavesdropping, посредством прослушивания злоумышленником радиоэфира;
- нарушение целостности информации передаваемой по беспроводным сетям;
- несанкционированный доступ к сети передачи данных посредством недостаточной реализации механизмов аутентификации абонентских устройств;

Перечень угроз



- нарушение подлинности получаемой информации посредством использования уязвимостей реализации протокола 802.11 в области идентификации абонентской станции/устройства;
- нарушение доступности информации посредством реализации злоумышленником атак «отказ в обслуживании»;
- возможность установки нелегальной абонентской станции вследствие выхода радио волн за границы зоны контролируемой службой безопасности;

Перечень угроз



- возможность несанкционированной установки точки доступа, подключенной к локальной вычислительной сети организации сотрудниками;
- возможность использования режима работы «точка-точка» сетевого адаптера беспроводной сети.

Задачи защиты радиосреды



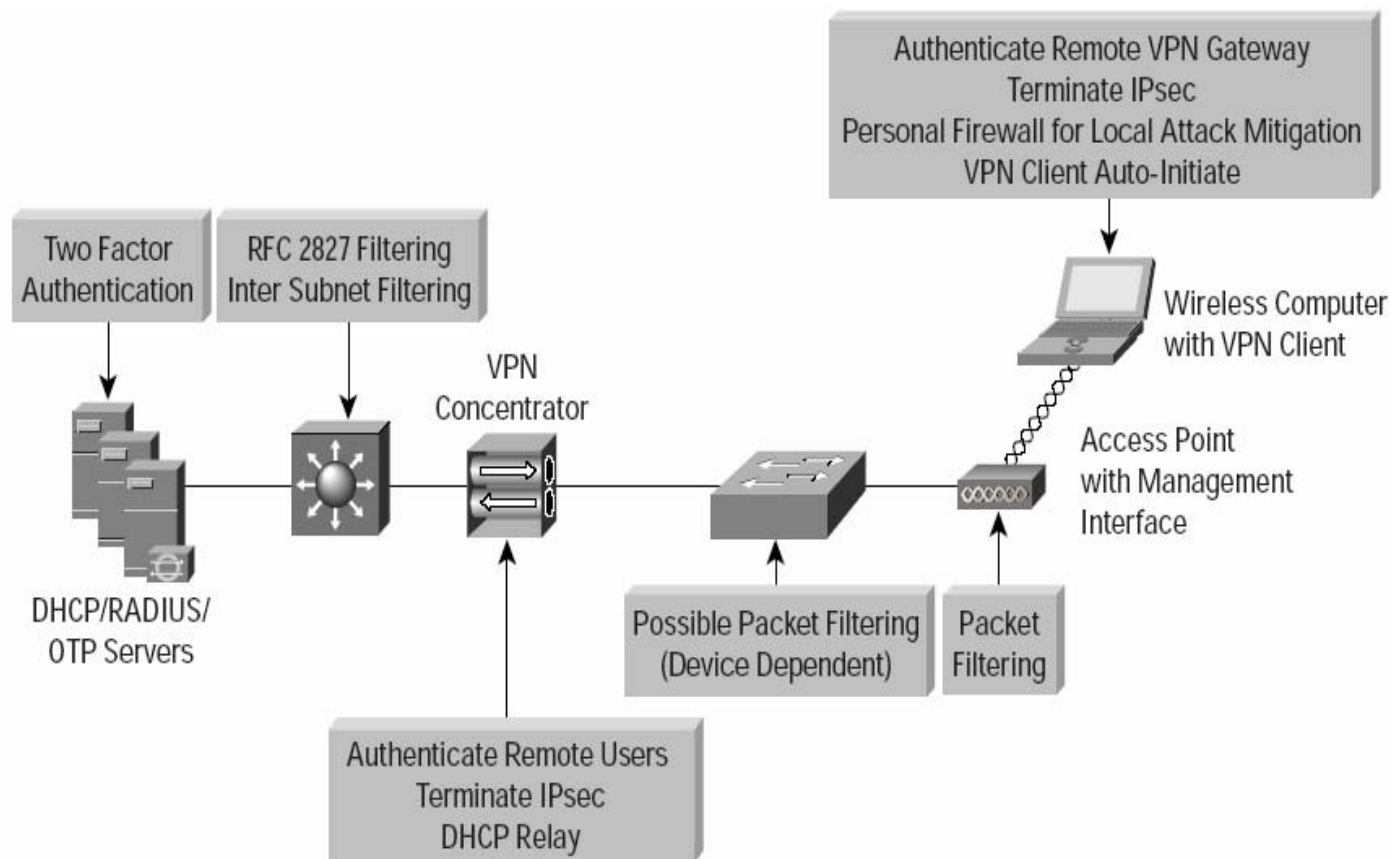
- защита *среды* передачи данных
- защита *трафика*
- защита *топологии радиосети*
- защита *проводной сетевой инфраструктуры* от несанкционированного доступа из радиосегментов

Основные рекомендации по обеспечению безопасности сетей 802.X



- для точек доступа:
 1. обеспечить аутентификацию при административном доступе
 2. использовать сильные пароли SNMP (community strings) и часто менять их
 3. если система управления позволяет – использовать SNMP Read Only
 4. запретить все неиспользуемые или уязвимые протоколы управления
 5. управление осуществлять только из заданного проводного сегмента
 6. по мере возможности – шифровать весь трафик управления
 7. по мере возможности – шифровать весь трафик в радиосегменте
- для клиентских устройств:
 1. запретить режим «каждый с каждым» (ad hoc mode)
 2. по мере возможности – шифровать весь радиотрафик
- применять надежные схемы аутентификации пользователей при подключении к точкам доступа

Методы защиты радиосетей



- защита канального уровня
- защита информационного потока
- защита топологии беспроводной сети
- защита проводной инфраструктуры

Требования к СУИБ



- обнаружение и определение базовых и абонентских станций беспроводного доступа, как санкционированных службой IT организации, так и несанкционированных;
- Определение подключения абонентских устройств как к базовым станциям – infrastructure mode, так и режим «точка – точка» - ad hoc mode;
- Обнаружение утечки сетевого трафика, передаваемого по беспроводным сетям, за пределы зоны контролируемой службой безопасности организации;

Требования к СУИБ



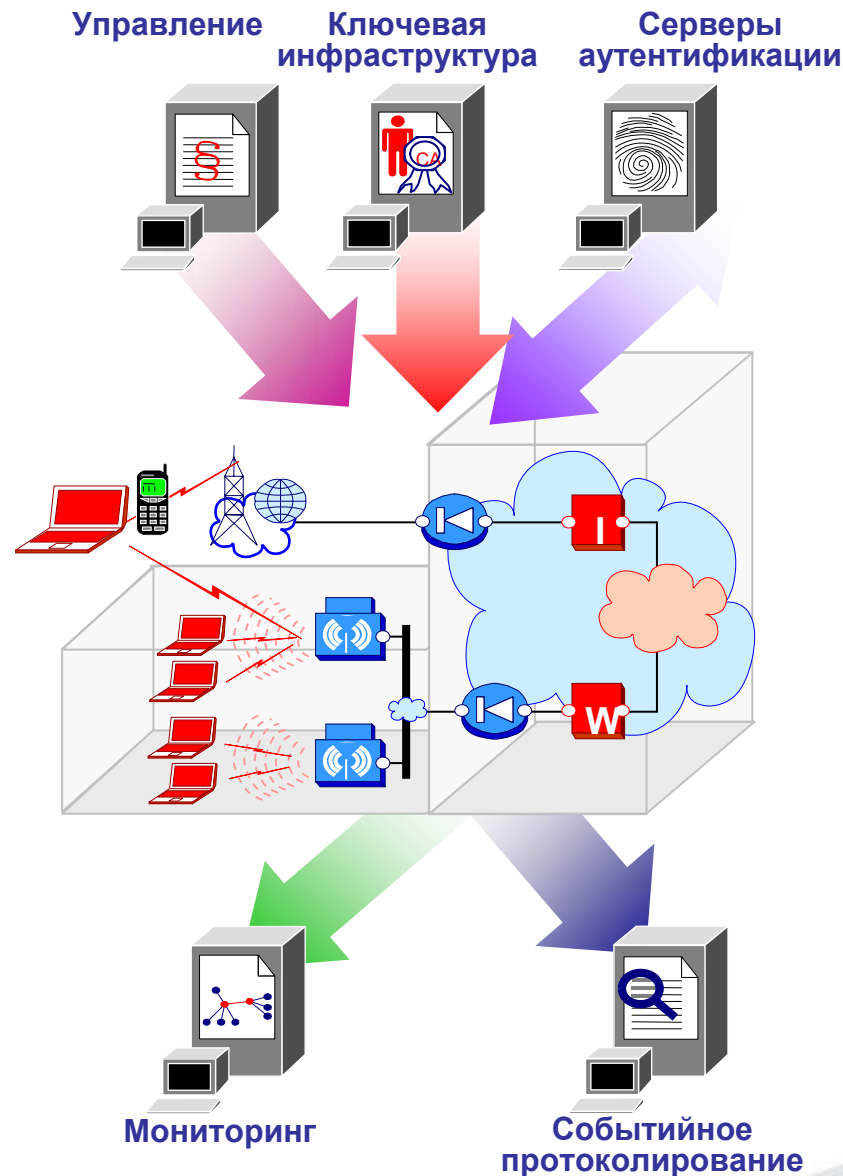
- Подсистема должна оповещать ответственного сотрудника о возникновении информационного инцидента посредством электронной почты или мобильных средств связи (отправка SMS уведомления);
- При возникновении информационного инцидента сервисами подсистемы должен быть произведен анализ и предоставлена необходимая информация для минимизации рисков информационной безопасности;
- Подсистема должна обеспечивать мониторинг радиочастот 2,4 GHz для стандарта 802.11 b/g и 5 GHz для стандарта 802.11a;

Требования к СУИБ



- Сенсоры-агенты подсистемы должны быть устойчивы к злонамеренным действиям, например атакам DoS;
- Консолидация данных и генерация отчета о состоянии беспроводной сети передачи данных должна производиться в реальном режиме времени;
- В случае необходимости подсистема должна масштабироваться в удаленные офисы организации;
- Подсистема должна управляться с единой консоли ответственного за информационную безопасность сотрудника.

Комплексная система защиты беспроводной сети



Используемые средства защиты информации

- **Подсистема управления ИБ:**
CheckPoint SmartCenter Pro
NetIQ Security Manager
- **Подсистема защиты информации:**
CheckPoint FW-1/VPN-1
CheckPoint VPN-1 Edge
CheckPoint SecureClient
S-Terra CSP Server/Client
- **Подсистема протоколирования:**
CheckPoint Eventia Reporter
- **Подсистема аутентификации:**
PassGo Defender

Система управления и мониторинга на канальном уровне



Состав системы управления и мониторинга на канальном уровне (на основе AirDefender):

- Сенсоры безопасности (Прослушивание эфира на наличие нелегального подключения)
- Система предотвращения вторжения (Анализ информационных потоков)
- Активный аудит состояния беспроводной сети 802.X
- Система управления компонентами безопасности

Корпорация ЮНИ



Вопросы ???

Спасибо за внимание.

Нестеров Руслан Олегович

технический эксперт

rnesterov@uni.ru

+7 (095) 580 9555



«Корпорация ЮНИ»

Москва, 3-ий Угрешский проезд, д.8, стр. 1

Tel. +7 (095) 580 9555

Fax +7 (095) 580-9556

www.uni.ru