Личная безопасность и защита беспроводных сетей

Лекция 23

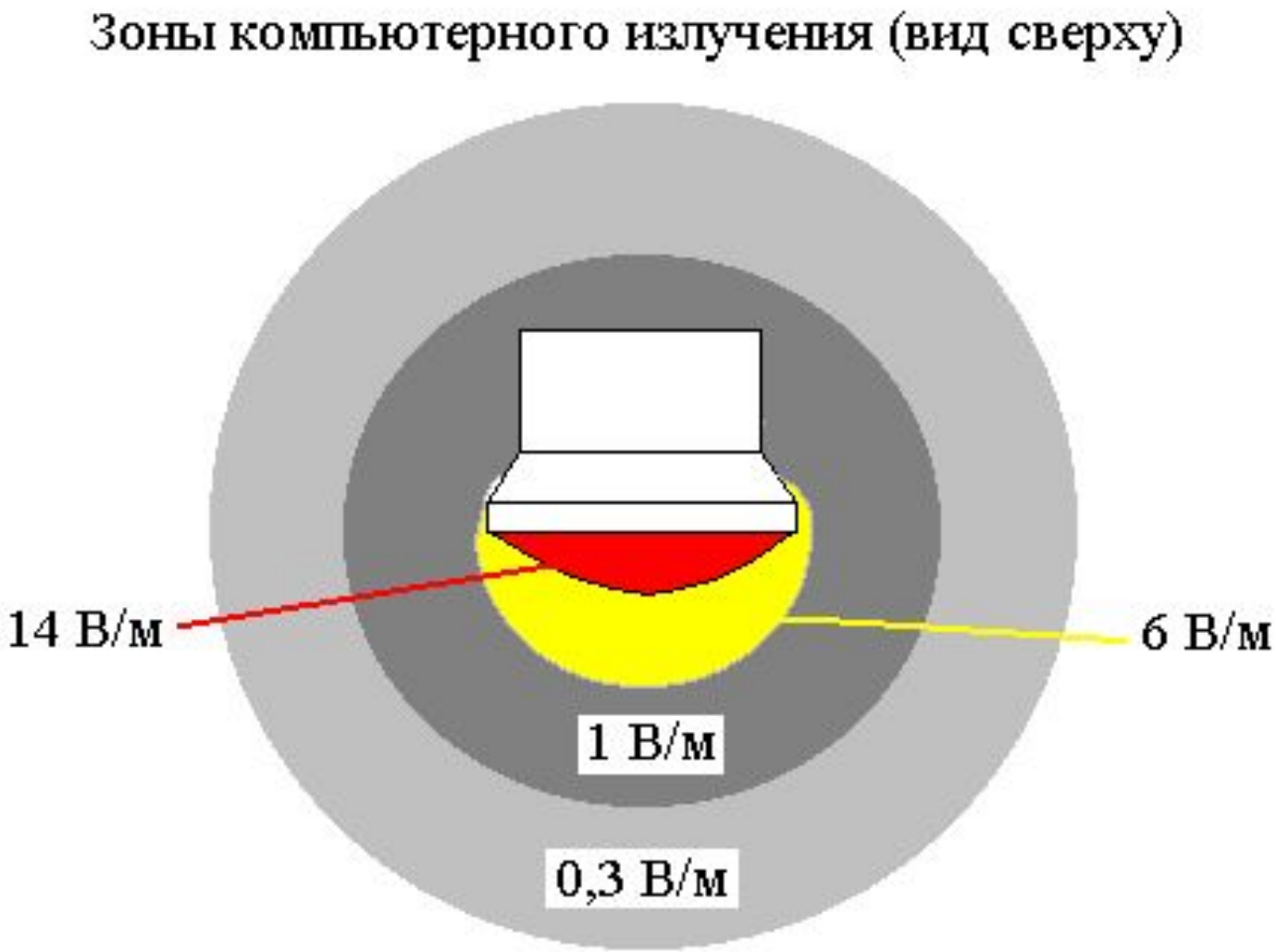
Объекты изучения безопасности

- Имущество
- Угрозы
- Риски
- Уязвимость
- Реакция
- Меры защиты

Допустимые уровни ЭМ полей

Частота, ГГц	Длина, дм	Допустимый уровень
0,03-0,3	100-10	3 В/м
0,3-3	10-1	10 мкВт/см^2
3-30	1-0,1	10 мкВт/см^2

Излучает монитор



Параметры мышечной ткани

Частота, МГц	Отн. диэлект. проница-емость	Проводи-мость, См/м	Глубина проникновения, см
1	411	0,59	70
100	79	0,81	7,7
1 000	60	1,33	3,4
10 000	42	13,3	0,27
100 000	8	60	0,03

Резонансная частота человека 100 МГц

- Удельная скорость поглощения (*SAR – specific absorption rate*) является важным количественным дозиметрическим фактором в диапазоне частот 100 кГц - 10 ГГц, и для внутренних электрических полей

$$SAR = (\sigma|E|^2)/\rho, \text{ Вт/кг},$$

где σ - проводимость ткани; ρ - плотность массы, кг/м^3; E - среднеквадратичное значение электрического поля, В/м

Предел для сотовых

- Для сотовых телефонов стандарт безопасности США предусматривает ограничение на пиковое, усредненное по пространству значение *SAR* – не более 1,6 Вт/кг, усредненное по любому образцу 1г ткани в форме куба
- В Европе предел установлен в 2 Вт/кг, усредненных по 10 г непрерывного образца ткани

Наши нормы

- Для частот 30-300 МГц предельная напряженность электрического поля 80 В/м
- Для частот свыше 300 МГц предельно допустимая мощность излучения 10 мкВт/см^2

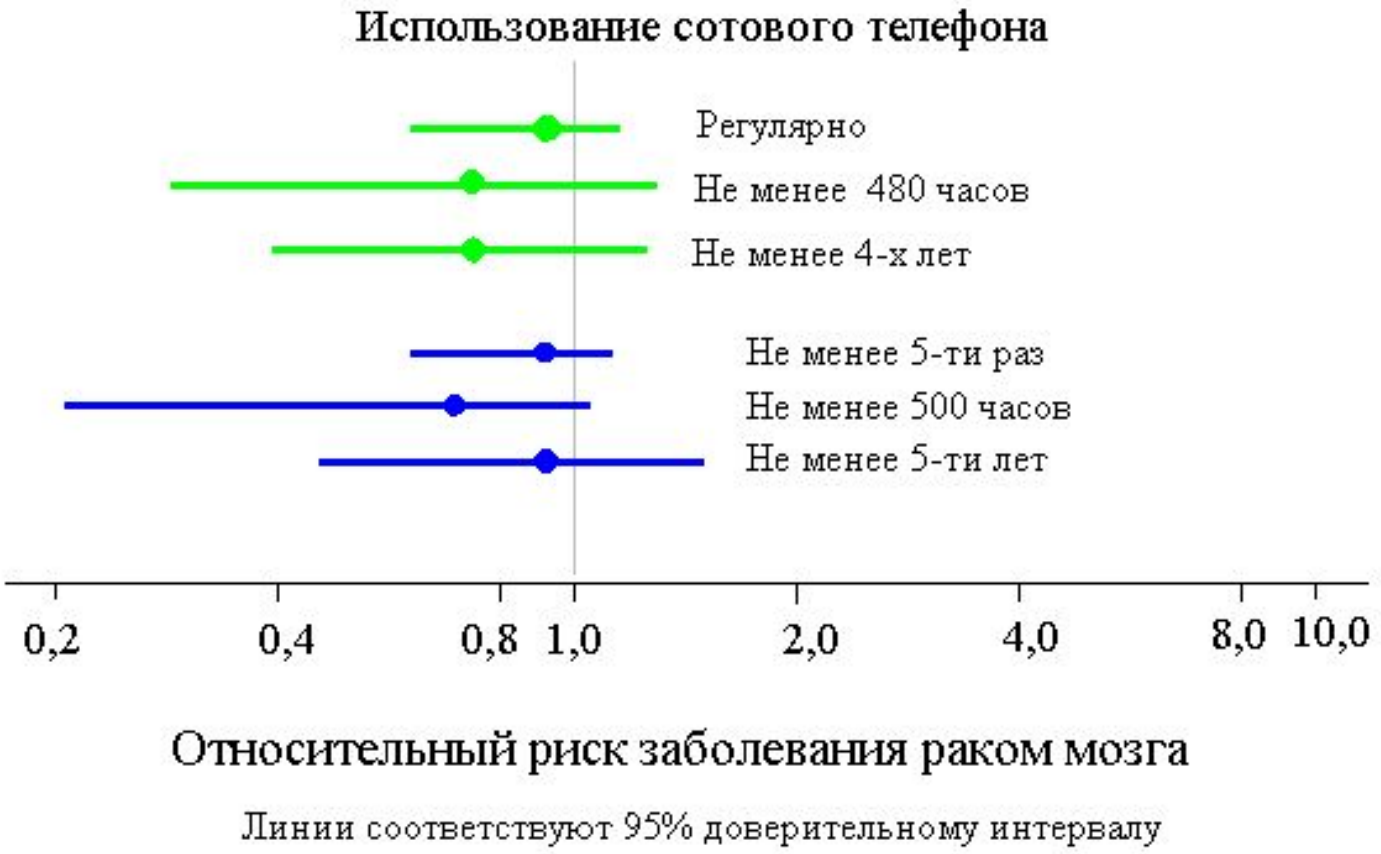
Простейшие оценки показывают

- Телефон (900 МГц) с мощностью излучения около 1 Вт способен создать в области височной кости плотность мощности в 10-100 раз большую, чем предельно допустимые значения

Исследования по *GSM*

- 20 добровольцев 6 дней в неделю по 2 часа в день использовали стандартный сотовый телефон
- Результат – снижение *тиреотропного* гормона, отвечающего за работу щитовидной железы
- Возможные последствия – прорежение волос; сухая, одуловатая кожа; хриплый голос

Экспериментальные данные



Сравнение сотовых аппаратов по *SAR*

Модель	Излучение, мВт/г
*Motorola T*2288	0,54
Nokia 6150	0,71
Nokia 3210	0,81
*Siemens S*35*i*	0,99
Nokia 6210	1,19
*Ericsson T*28*s*	1,27

Механизмы контроля доступа

- Авторизация ресурсов
- Идентификация пользователей
- Аутентификация пользователя
- Контроль регистрации
- Контроль использования ресурсов
- Управление парольной информацией
- Протоколирование и аудит
- Контроль целостности ПО и данных

По словарю

- Идентификация – отождествление, установление совпадения чего-либо с чем-либо
- Аутентификация – установление подлинности, опознавание, отождествление; проверка прав доступа

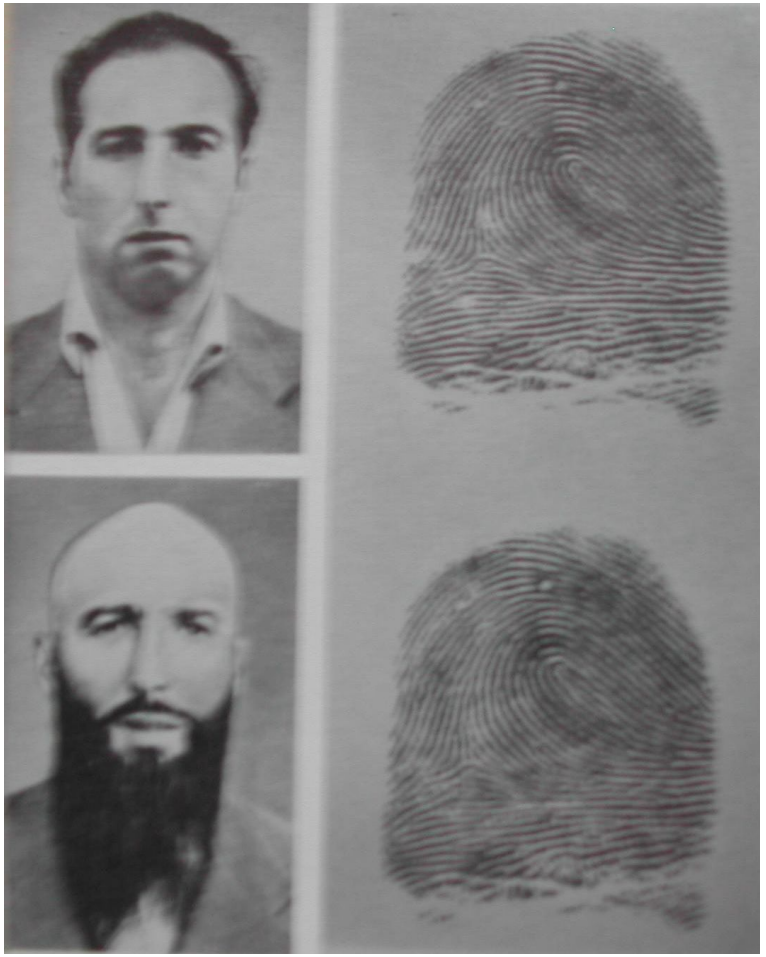
Дактилоскопия

- В 1892 году Фрэнсис Гальтон опубликовал книгу «Отпечатки пальцев»
- Им выделялись 4 основные группы рисунков отпечатков пальцев (без треугольников, треугольник слева, треугольник справа и несколько элементов – дуги и завихрения)

Отпечатки пальцев помогают

Здесь изображен один и тот же человек, но возраст, прическа и борода создают впечатление, что это два разных лица

Их идентичность выдают отпечатки пальца



Глаз - идентификатор

- Первый подход основан на идентификации рисунка радужной оболочки глаз
- Вторая технология использует метод сканирования глазного дна – сетчатки глаза, и базируется на уникальности углового распределения кровеносных сосудов для каждого человека

Преимущества идентификации по оболочке

- Радужная оболочка – это тонкая мембрана внутри глазного яблока, имеет чрезвычайно сложный и уникальный для каждого человека рисунок
- Рисунок радужной оболочки при идентификации различен даже у близнецов

Методы идентификации -1

Метод распознавания	Идентификатор	Вероятность ошибки	Надежность	Применение
Радужная оболочка глаз	Узор радужной оболочки	1/ 1 200 000	Высокая	Высокосекретные объекты
Отпечатки пальцев	Дактилоскопический узор кожи пальцев	1/1 000	Средняя	Повсеместно
По ладони руки	Форма и размеры ладони руки	1/700	Низкая	Малосекретные объекты

Методы идентификации -2

Метод распознавания	Идентификатор	Вероятность	Надежность	Применение
По особенностям лица	Форма, очертания, расположение глаз, носа и др.	1/100	Низкая	Малосекретные
По особенностям почерка	Форма букв, порядок написания, давление на бумагу	1/100	Низкая	Малосекретные
По особенностям голоса	Характеристики голоса	1/30	Низкая	Телефонные службы

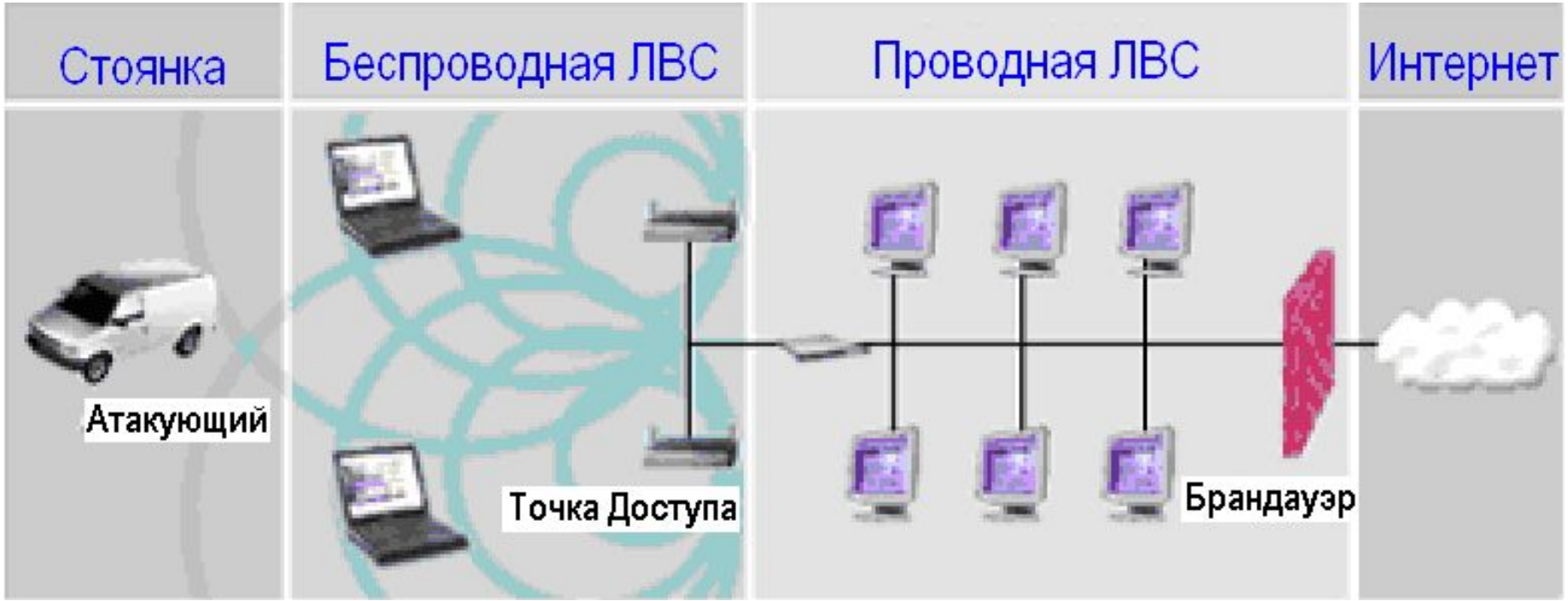
Угрозы на информационном уровне – перехват информации

Угроза	Условия реализации угрозы	Уязвимый элемент	Средства нейтрализации угрозы
Выявление канала передачи для перехвата	Наличие в передаваемых данных отличительных признаков, работа на одном канале	Системы шифрования и управления каналами	Исключение отличительных признаков данных, изменение номера канала в течение сеанса связи
Определение формата данных	Использование стандартных форматов без дополнительной коррекции	Системы кодирования и шифрования	Использование оригинальных форматов, проведение коррекции передаваемых данных
Восстановление пакетов (кадров)	Отсутствие маскировки синхронизации и маркеров доступа	Система управления обменом	Применение адаптивного кодирования

Угрозы на информационном уровне – искажение данных

Угроза	Условия реализации угрозы	Уязвимый элемент	Средства нейтрализации угрозы
Передача ложного сигнала в ходе имитации вызова	Возможность определения протокола обмена	Система приема и управления приемом	Использование специальных маркеров идентификации и аутентификации в каждом кадре (блоке) сеанса связи
Передача ложного сигнала в ходе сеанса связи	Возможность выделения и определения идентификационных преамбул	Система приема и управления приемом	Использование дополнит. канала для передачи (ПРД) служебных маркеров, разнесение во времени ПРД контр. сумм и квитанций
Искажение сигнала передачи	Возможность вскрытия синхронизации и входа в канал без ее нарушения	Приемопереда-ющая система	Использование двойной синхронизации, в том числе по дополнительному каналу

Внедрение
в беспроводной канал сети



Два механизма защиты

- В БЛС стандарта 802.11 первоначально были реализованы 2 основных механизма защиты
- На канальном уровне ИОС (MAC) обеспечивался контроль доступа, а для шифрования использовался стандарт *WEP* (*wired equivalent privacy* – безопасность, эквивалентная проводным сетям)

Немного разрядов

- В основе 64-разрядного *WEP* лежит шифрование данных с помощью алгоритма *RSA RC*4 с 40-разрядным разделяемым ключом
- Двадцать четыре разряда отводятся под вектор инициализации (*IV – initialization vector*)

Только по списку

- Когда работает *WEP*, он защищает только пакет данных, а не заголовки физического уровня – их должны просматривать все абоненты сети
- Для контроля доступа каждый абонент имеет свой идентификатор *SSID (service set identifier*), а сервер хранит список (*ACL – access control list)* разрешенных *MAC*-адресов, обеспечивая доступ только тем абонентам, чьи адреса входят в этот список

Аутентификация в открытой системе

Потоки сообщений

Клиент старается получить доступ к сети

Запрос на аутентификацию посылается к ТД

ТД проводит аутентификацию

Клиент соединяется с сетью

Точка Доступа

Аутентификация с разделяемыми ключами

Потоки сообщений

Клиент старается получить доступ к сети

Запрос на аутентификацию посылается к ТД

Посылается сложный текст клиенту

Шифруется сложный текст и возвращается к ТД

ТД расшифровывает, проверяет точность и в случае совпадения, аутентифицирует станцию

При аутентификации клиент соединяется с сетью

Точка Доступа

Постоянная работа

- Серьезная работа ведется над созданием стандарта 802.11*i* , предусматривающего применение иного протокола шифрования *AES (advanced encryption standard* = усовершенствованный стандарт шифрования) на основе 128-разрядных ключей и динамическое изменение ключей