НТЦ ВУЛКАН

Москва • 3 декабря
КОНФЕРЕНЦИЯ WLAN & АКАДЕМИЯ БЕСПРОВОДНЫХ РЕШЕНИЙ

Обеспечение безопасности беспроводных сетей

Александр Кузнецов, руководитель отдела
Александр Товстолип, ведущий специалист

2013

Содержание

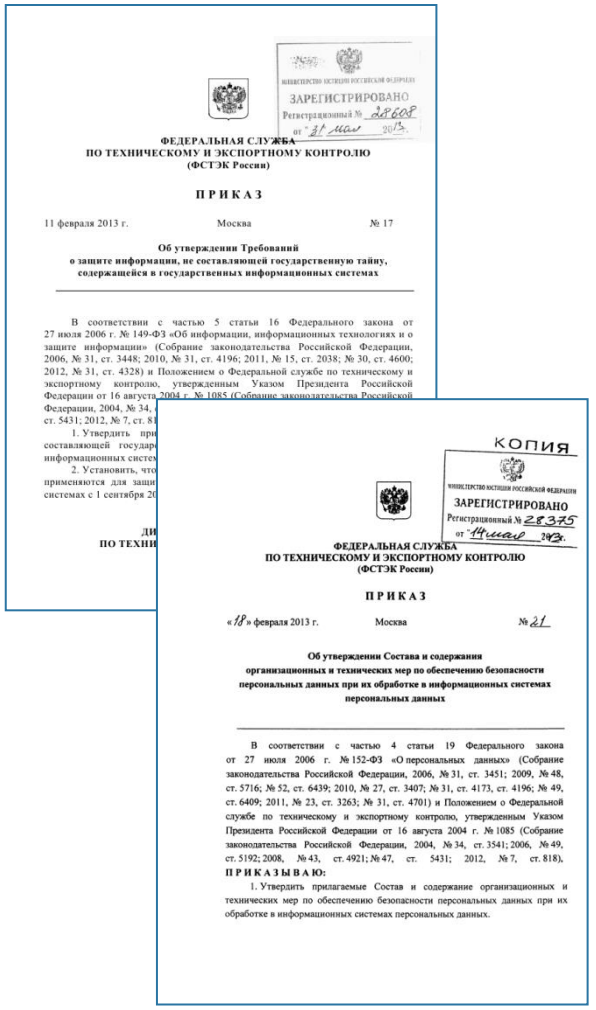
- Нормативно-правовое обеспечение вопросов защиты беспроводных сетей
- Классификация атак
- Ресурсы и инструменты злоумышленника
- Базовые уровни безопасности беспроводных сетей
- Дополнительные защитные меры

Нормативно-правовое обеспечение

- Конституция РФ
- Федеральные законы и кодексы
- Указы президента РФ
- Постановления и распоряжения Правительства РФ
- Нормативно-правовые акты министерств и ведомств
- Нормативно-правовые акты ассоциаций, союзов и иных объединений

Нормативно-правовое обеспечение

- УПД.14 Регламентация и контроль использования в ИС технологии беспроводного доступа
- ЗИС.3 Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
- ЗИС.20 Защита беспроводных соединений, применяемых в ИС



ЗАРЕГИСТРИРОВАНО
Регистрационный № 28608
от "31" мая 2013

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

ПРИКАЗ

11 февраля 2013 г. Москва № 17

Об утверждении Требований
о защите информации, не составляющей государственную тайну,
содержащейся в государственных информационных системах

КОПИЯ

ЗАРЕГИСТРИРОВАНО
Регистрационный № 28375
от "14" мая 2013

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

ПРИКАЗ

«18» февраля 2013 г. Москва № 21

Об утверждении Состава и содержания
организационных и технических мер по обеспечению безопасности
персональных данных при их обработке в информационных системах
персональных данных

Мировой опыт и лучшие практики

- Публикации
- Материалы вендоров
- Стандарты и рекомендации
- Веб-ресурсы

Классификация атак

- **Пассивные атаки (мониторинг коммуникаций):**
  - прослушивание
  - анализ сетевого трафика
- **Активные атаки:**
  - «маскарад» пользователя
  - ретрансляция сообщений под видом легального пользователя
  - модификация сообщений
  - отказ в обслуживании (DoS)
  - незаконное присвоение (хищение)

Ресурсы и инструменты злоумышленника

- **Сканирование сетей:**
  - CommView for Wi-Fi
  - Airodump-ng
  - Kismet
  - Inssider
- **Подбор паролей:**
  - Aircrack-ng
  - Wpacracker
  - Pyrit
  - Elcomsoft Wireless Security Auditor
- **Полезные дистрибутивы:**
  - BackTrack + Reaver
  - Kali Linux
  - AirSlax

ПОЧТИ ВСЕ АВТОМАТИЗИРОВАНО

reaver-wps
Brute force attack against Wifi Protected Setup

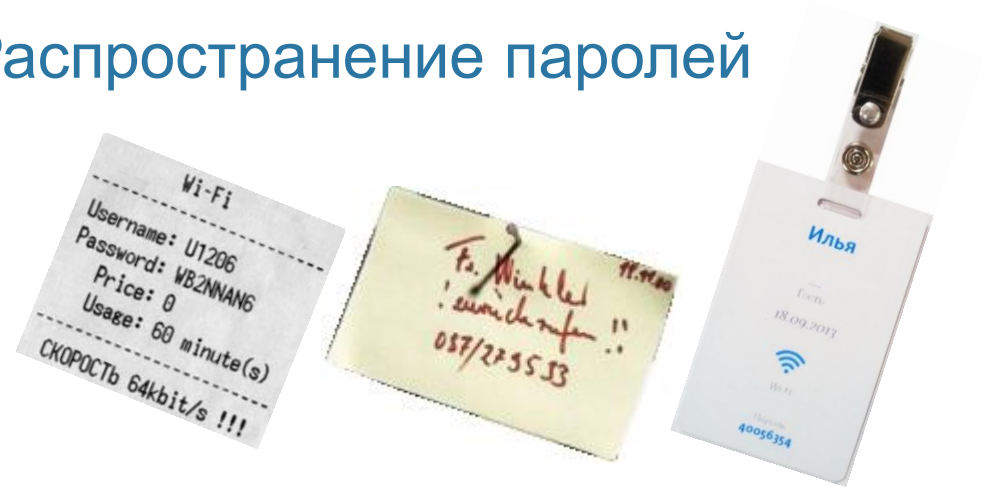
Базовые уровни безопасности

- **Аутентификация:**
  - Открытая аутентификация (Open system authentication)
  - Аутентификация с общим ключом (Shared key authentication)
  - Аутентификация по MAC-адресу (MAC address authentication)
  - Использование RADIUS-сервера
- **Обеспечение конфиденциальности и целостности:**
  - Wired Equivalent Privacy (WEP)
  - Wi-Fi Protected Access (WPA)
  - Wi-Fi Protected Access 2 (WPA2)
- **Фильтрация по MAC-адресам**
- **Манипуляции с SSID (Service Set Identifier)**

Пароли (Shared key authentication)

- Содержание пароля (*A-a, 1-0, !-#*)
- Длина пароля
- Частота смены пароля
- Распространение паролей

Нашел свой пароль?
Получи приз!!!



SSID

- SSID не должен содержать полезной для злоумышленника информации:
  - принадлежность к владельцу (Компании)
  - физическое расположение
  - технические характеристики точки доступа или т.п. сведения
- Скрытие SSID («Disable SSID Broadcast» или «No Guest Mode»)

Кадр из телепередачи «Comedy Club»

Дополнительные защитные меры

- Физическая безопасность точек доступа, контроллеров и др. устройств
- Управление учетными записями на устройствах
- Оптимизация зоны покрытия и уровня мощности
- Резервирование
- Выделение целевого VLAN для точек доступа
- Использование IDS/IPS-решений
- Мониторинг и аудит ИБ

Заключение

- Обоснованное решение применения беспроводных технологий
- Определение зон покрытия и физическая защита точек доступа
- Применение классических подходов к защите сетевого периметра с учетом специфики канала передачи данных
- Комплексность и непрерывность мониторинга и защитных мероприятий

Спасибо за внимание!

Вопросы …

Конференция: «Вокруг WLAN. Академия беспроводных решений»
Участник: ООО «НТЦ «Вулкан»
Адрес: 105318, г. Москва, ул. Ибрагимова, д. 31 (БЦ «Семеновский»)
Тел.: +7 (495) 663-9516
E-mail: info@ntc-vulkan.ru