

# Обеспечение безопасности беспроводных сетей

Александр Кузнецов, руководитель отдела  
Александр Товстолип, ведущий специалист

## Содержание

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

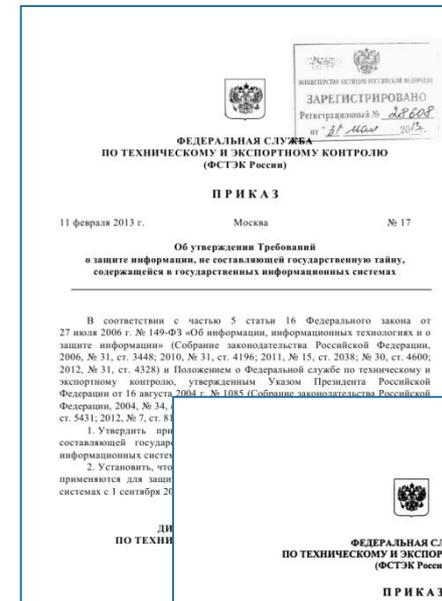
# Нормативно-правовое обеспечение

- 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



# Мировой опыт и лучшие практики

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

Андрей А. Владимиров  
Константин В. Гавриленко  
Андрей А. Михайловский

NT PRESS

## Wi-фу: «БОЕВЫЕ» ПРИЕМЫ ВЗЛОМА И ЗАЩИТЫ

УДК 004.056

Белорус Дмитрий Иванов  
Корсаков Михаил Сергеевич  
ООО «РЯКОМ» - Москва  
E-mail: belarus@ryacom.ru, korsov@ryacom.ru  
Wi-фу в угрозе информационной безопасности

УДК 004.056

А.С. МАРКОВ, доктор кафедры информационной безопасности  
ИИЭТ им. Н.Э. Баумана, г.м.  
В.В. РАДЧЕН, старший ИИЭТ им. Н.Э. Баумана  
А.А. ФАДВИ, старший ИИЭТ им. Н.Э. Баумана

### СОСТОЯНИЕ И ПЕРСПЕКТИВЫ АНАЛИЗА ЗАЩИЩЕННОСТИ WI-FI СЕТЕЙ

Введение статьи Wi-Fi, обзор безопасности, анализ современных беспроводных сетей, IEEE 802.11.

© Copyright 2005 The CWNP® Program www.cwnp.com Page 1

### A Guide to Wireless Network Security

By Mitchell Ashby

Operations of all sites are installing and operating wireless networks, known as wireless local area networks (WLANs) or Wi-Fi networks. Low cost, ease of installation, flexibility – these are the benefits that are driving wireless technology's growing popularity. These advantages include:

**Wireless Advantages**  
The operational advantages described give rise to a number of advantages that are driving wireless technology's growing popularity. These advantages include:

### Security, Audit and Control Issues for Managing Risk in the Wireless LAN Environment

By Richard A. Stanley, Ph.D., PE, CISSP

**Business Drivers**  
Today, wireless technologies is a common method of data transmission for cellular phones, wireless personal digital assistants (PDAs), BlackBerries, text pagers and wireless local area networks (WLANs). While these technologies offer many advantages, they also present a number of risks that can be evaluated periodically to ensure that all of the appropriate measures are taken for each system to secure the desired level of quality and security. However, security is not an absolute. It is impossible to eliminate all risks completely, but it is possible to reduce the risk to an acceptable level.

### Securing IEEE 802.11 Wireless LANs

by

**NIST**  
National Institute of Standards and Technology  
U.S. Department of Commerce

Special Publication 800-153

### Guidelines for Securing Wireless Local Area Networks (WLANs)

**Recommendations of the National Institute of Standards and Technology**

Murugiah Souppaya  
Karen Scarfone

### Best Practices for Wireless Network Security

By Susan Kennedy, CISA, CIB

Networking technology is dramatically changing the world of computing, creating considerable business opportunities as well as increasing security risks. One such technology, wireless networks, also known as broadband networks or WLANs, are increasing in popularity at the organizational and consumer levels. While these technologies offer many advantages, they also present a number of risks that can be evaluated periodically to ensure that all of the appropriate measures are taken for each system to secure the desired level of quality and security. However, security is not an absolute. It is impossible to eliminate all risks completely, but it is possible to reduce the risk to an acceptable level.

**Risk 2: Access Constraints**  
By design and out of necessity, Wi-Fi especially need not require a wireless device to connect to the network. This means that anyone with a laptop or other device can connect to the network. This is a significant security risk because it allows unauthorized users to access the network. To mitigate this risk, organizations should consider the importance of vigilance. It is important to monitor the network for unauthorized access and to take appropriate action if such access is detected.

Set up and maintain secure wireless networks  
Find out how hacker's break in – and how to stop them  
Avoid attacks and prevent vulnerabilities

Microsoft  
**Windows Server 2003**

### Проблемы безопасности в беспроводных ЛВС IEEE 802.11 и решения Cisco Wireless Security Suite

White Paper (version 1.0)

© Copyright 2005 Cisco Systems, Inc. All rights reserved. Cisco Confidential

**1. Введение**  
С появлением стандарта IEEE 802.11 в 1999 году беспроводные ЛВС получили широкое распространение. Сегодня их можно встретить во многих офисах, конференц-залах, на промышленных объектах, в торговых центрах, кафе и других публичных местах.

Беспроводные ЛВС стандарта IEEE 802.11b предоставляют собой ряд новых проблем для администраторов сетей и систем безопасности. В отличие от проводных сетей Ethernet, беспроводные ЛВС стандарта IEEE 802.11 используют общедоступный радиоканал для связи и взаимодействия. Этот факт создает и создает новые риски безопасности, включая проблемы, связанные с конфиденциальностью информации стандарта IEEE 802.11.

С целью обеспечения безопасности, производители стандарта IEEE 802.11 в первоначальной версии IEEE 802.11b, IEEE 802.11a, IEEE 802.11g включили механизмы защиты на сетевой стороне. Однако, как было отмечено в предыдущих документах, эти механизмы не обеспечивают достаточной безопасности информации (конфиденциальности, целостности, конфиденциальности данных) в беспроводной среде.

В настоящее время:

- для обеспечения конфиденциальности и целостности данных;
- решения проблемы этих механизмов являются неэффективными;
- производители стандарта IEEE 802.11b, IEEE 802.11a, IEEE 802.11g включили механизмы защиты на сетевой стороне, включая Cisco Wireless Security Suite (WSSS) для решения проблемы безопасности в беспроводных ЛВС;
- производители стандарта IEEE 802.11b, IEEE 802.11a, IEEE 802.11g включили механизмы защиты на сетевой стороне IEEE 802.11n, и их производители в беспроводной ЛВС.

**2. Аутентификация в IEEE 802.11 и ее реализация**  
Беспроводные ЛВС, имея их неограниченный радиус, требуют реализации дополнительных механизмов для:

Cisco Systems, Inc.  
All rights reserved. Cisco Confidential  
1.0

## 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**



# 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»)

*Нет сети  
«Наша сеть»?*

*Наша сеть -  
«Kalipso1703»*



## 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](mailto:info@ntc-vulkan.ru)