УДК 658.012.8

И. П. Иванов, А. Ю. Успенский

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В РАДИОКАНАЛАХ СТАНДАРТА IEEE 802.11

С целью обеспечения безопасности данных, передаваемых в радиоканале, стандарт IEEE 802.11 предусматривает использование протокола WEP (Wired Equivalent Privacy), с помощью которого делается попытка достичь уровня защиты передаваемых данных, сравнимого с обеспечиваемым обычными проводными сетями. Рассмотрены особенности протокола WEP, возможные способы нарушения защиты информации и виды атак на радиосеть. Приведены рекомендации по преодолению недостатков WEP, и рассмотрены общие положения протокола WEP2, призванного устранить существующие проблемы.

Analysis of Data Protection Methods in IEEE 802.11 Radio Channels / I.P. Ivanov, A.Yu. Uspensky // Vestnik MGTU. Priborostroenie. 2002. № 4. P. 26–35.

To provide protection of data being transferred via radio channels, the standard IEEE 802.11 involves WEP (Wired Equivalent Privacy) protocol, with the help of which an attempt is made to achieve the transferred data protection level comparable to that of traditional networks. The WEP protocol peculiarities are considered as well as possible ways of the data protection violation and kinds of attacks against the radio network. Recommendations are given to overcome WEP weak points, and general provisions are considered of the WEP2 protocol which is to eliminate the existing problems. Refs.10. Figs.3.

СПИСОК ЛИТЕРАТУРЫ

1. Sandberg J. Hackers poised to land at wireless AirPort. – ZDNet, 2001 (February 5).
2. Zyren J., Petrick A. IEEE 802.11 Tutorial. – http: // www.wirelessethernet.org/whitepapers.asp.
3. Borisov N., Goldberg I., Wagner D. Intercepting Mobile Communications: The Insecurity of 802.11 // 7-th Annual International Conference on Mobile Computing and Networking. – 2001.
4. Borisov N., Goldberg I., Wagner D. Security of the WEP Algorithm. – http: // www.isaac.cs.berkeley.edu/isaac/wepfaq.html, University of California at Berkeley, February 2001.

5. Fisher D., Nobel C. Wireless LAN Holes. – eWeek, 2001 (February 11).
6. Garcia A. WEP Remains Vulnerable. – eWeek, 2001 (March 26).
7. Grogans C., Bethea J., Hamdan I. RC4 Encryption Algorithm. – http: // www.ncat.edu/~grogans/main.htm, North Carolina Agricultural and Technical State University, 2000 (March 5).
8. Pescatore J. Commentary: An Object Lesson in Managing Security Risks of New Technologies. – http: // www.techrepublic.com/article.jhtml?src=search&id=r00120010207ggp10.htm, TechRepublic, Inc., 2001 (February 7).
9. Uskela S. Security in Wireless Local Area Networks. – http: // www.tml.hut.fi/Opinnot/Tik-110.501/1997/wireless_lan.html, Helsinki University of Technology, 1997.
10. Zurko E. Listwatch: Items from Security-Related Mailing Lists. – http: // www.ieee-security.org/Cipher/Newsbriefs/2001/022001. ListWatch.html, IEEE, 2001 (February 16).

Статья поступила в редакцию 9.10.2002

Игорь Потапович Иванов родился в 1955 г., окончил в 1979 г. МВТУ им. Н.Э. Баумана. Канд. техн. наук, проректор по информатизации МГТУ им. Н.Э. Баумана. Автор более 20 научных работ в области информатизации.

I.P. Ivanov (b. 1955) graduated from the Bauman Moscow Higher Technical School in 1979. Ph.D. (Eng.), pro-rector for informatization of the Bauman Moscow State Technical University. Author of over 20 publications in the field of informatization.

Александр Юрьевич Успенский родился в 1977 г., окончил в 2000 г. МГТУ им. Н.Э. Баумана. Аспирант кафедры "Информационная безопасность" МГТУ им. Н.Э. Баумана. Автор 3 научных работ в области защиты информации, беспроводных коммуникационных технологий, операционных систем реального времени, робототехнических комплексов.

A.Yu. Uspensky (b. 1977) graduated from the Bauman Moscow State Technical University in 2000. Post-graduate of "Data Security" department of the Bauman Moscow State Technical University. Author of 3 publications in the field or data protection, wireless communication technologies, real time operating systems, robotic complexes.