USING WIRELESS TECHNOLOGY: SEQURITY MEASURES

R.S. Volkov, *student, group IN-53*

In recent years, wireless networking has become more available, affordable, and easy to use. Home users are adopting wireless technology in great numbers. On-the-go laptop users often find free wireless connection in places like coffee shops and airports. However, there are security threats people may encounter using such type of connection.

When someone uses a wireless router or access point to create a home network, he trades wired connectivity for connectivity delivered via a radio signal. Unless you secure this signal, strangers can access your internet connection or, even worse, monitor your online activity or modify files on your hard drive. By taking the following actions people can help secure their wireless home network against these threats:

- change the default system ID of wireless access point or router;
- change the default password for a system;
- turn off identifier broadcasting;
- encrypt wireless communications (WPA-based encryption offers better protection than WEP-based encryption.);
- use router built-in firewall to restrict access to a network;
- keep your wireless system patched and up to date.

Accessing a wireless connection from a coffee shop or airport terminal may be convenient and even fun, but people should note that public access points (frequently called hot spots) are often insecure. The following are some steps anyone should consider taking before connecting to a public access point:

- use a virtual private network (VPN) if possible;
- avoid using passwords and providing personal information to web sites;
- encrypt your files;
- be aware of your surroundings.

G.I. Lytvynenko, *EL Advisor*