Information & Security: An International Journal

Ihor Chernukhin, vol.31, 2014, 79-86 http://dx.doi.org/10.11610/isij.3105

NEW CHALLENGES TO INFORMATION SECURITY CAUSED BY THE INTRODUCTION OF WI-FI TECHNOLOGIES

Ihor CHERNUKHIN

Abstract: Along with WIMAX, Wi-Fi technology is one of the standards for construction of broadband wireless networks, WLAN, and provides an opportunity to ensure data communication at the distance of up to 100 m with the rate of 11-300 Mbit/sec within the range of 2.4-2.5 or 5.9 GHz. Along with a number of advantages (rate of scanning, equipment commissioning, data communication, possibility of informatisation of rural and remote areas), the main disadvantage of Wi-Fi networks is the low level of protection against unauthorized access. The current article focuses on problems related to such use of the Wi-Fi technology posing a threat to information security. It elaborates on the main vulnerabilities of the Wi-Fi technology and points out drawbacks of a legal nature. Finally, it suggests solutions to increased cybersecurity on the background of the mounting use of Wi-Fi technology in Ukraine.

Keywords: Wi-Fi technology, cybersecurity, legislation measures.

Introduction

The rapid advancement in the field of information technologies which has been observed during the last 20 years has taken society to another level – the level of information society, the main characteristic of which is the production and dissemination of information, its transformation into a main type of services, into product and even into power.[1] Such concept has found its reflection in state policy of the majority of leading countries of the world. In Ukraine in 2013, the Cabinet of Ministers of Ukraine approved the *Strategy of Information Society Development*, which defines the basic principles and strategic purposes of information society development. Among others, the main direction of modern information infrastructure formation is the creation of networks of broadband access to Internet all over the territory of Ukraine, and provision of conditions for access to this network in all populated areas in order to achieve the indicators of information society development determined by the state by 2020 (the share of Internet users shall be 75 percent of the whole population of Ukraine).[2] The telecommunication and information sectors of other countries are characterised by the rapid development of the networks of Internet access and its penetration into the society (Norway – 94.8 %, Netherlands – 88.6 %, Great Britain – 82.5 %).[3] More and more frequently the users choose the wireless access or, in other words, the electric communication with the use of radio technologies. One of the most widespread ways of wireless access is networking with the use of Wi-Fi technology. Along with a number of advantages, which ensure the convenience of its use, the mentioned technology introduces a number of vulnerabilities which may negatively influence the information security.

Taking into consideration the fact that the issue of cyber space security is becoming more and more urgent against the background of the establishment of information society in many countries, preventing the use of Wi-Fi networks for destructive purposes requires taking of a range of organisational, legal, technical measures and profound scientific research.

The purpose of the current article is to study the problems related to such use of the Wi-Fi technology that might potentially pose a threat to the information security, and its tasks are: to determine the causes for appearance of threats, drawbacks of legal character in this sphere, and to substantiate the offers concerning improvement of legal and organisational measures for preventing the use of brand new technologies for destructive purposes.

Wi-Fi and Cyber (in)security

Along with WIMAX, the Wi-Fi technology is one of the standards for construction of broadband wireless networks (Wireless Local Area Network, WLAN), and gives the possibility to ensure data communication at a distance of up to 100 m with the rate of 11-300 Mbit/sec within the range of 2.4-2.5 or 5.9 GHz (depending on the relevant standard).[4]

Along with a number of advantages—rate of scanning, equipment commissioning, and data communication, possibility of informatisation of rural and remote areas—the main disadvantage of Wi-Fi networks is the low level of protection from unauthorised access (so called network "cracking"). It is possible to find instructions and software for Wi-Fi networks cracking without any difficulty in the Internet. Thus, according to the results of the study of the level of protection of 40 thousand Wi-Fi networks in Great Britain carried out by CPP insurance company and CryptoCard, half of them have not used any means of data protection (passwords), while most of the remaining networks have been cracked by specialists using software available in the Internet within 10 minutes.[5] Taking into consideration the extent to which the Wi-Fi technology is spread globally, similar negative aspects are typical of other countries as well. Thus, for instance, in developing countries one of the ways of ensuring access to the Internet in remote or mountainous areas is to create wireless broadband networks.

The negative aspects mentioned above create the threat of using the Internet access with the help of Wi-Fi equipment by persons with the purpose of illegal activity to the detriment of the security of a certain country. The author marks out two groups of threats which may be defined as “network monitoring” and “outside use of network.” Thus, unauthorised access to Wi-Fi network (network “crack”) or use of password-free access gives the criminal the possibility:

- to carry out “secret” monitoring (being out of visually controlled area of the access point owner) of data communication within the coverage area (i.e. “network monitoring”) which may cause leak of important information (passwords for access to e-mails, e-banking, bank details, personal data, etc.). This threat concerns the risks of use of Wi-Fi technology in the sphere of state governance of the leading countries of the world. First, the availability of Wi-Fi segment in the state network may cause the leak of state information about the activity of any governmental body, state enterprise, institution or organisation, including those with restricted access. Second, the network monitoring within Wi-Fi coverage area gives the criminal the possibility to study the spheres of personal interests of network users, as well as and their psychological traits;
- to use Wi-Fi access points for the purpose of committing destructive actions (“outside use of network”). This study identified main groups of such actions as follows:

    a) dissemination of information of unconstitutional and illegal character (calls for forcible change or overthrow of constitutional order, seizure of state power, violation of territorial integrity of the country; instructions of terrorist and extremist content; video products of pornographic character; harmful software; other manipulative information which destabilises social and political environment, e.g. by provoking the population towards mass protest actions involving violence);

    b) commitment of computer crimes (stealing money from banks; fraud; commitment of cyber-attacks on information systems of state bodies, cyber terrorism, etc.).

In the latter group of crimes the particular attention (as a brand new challenge to the cyber security) shall be paid to unauthorised interference into the work of information systems of technological control at industrial, municipal, transport, and energy sites which may lead to blocking of production processes and, as a result, to emergency situations of anthropogenic character which present a threat to the life and health of a large number of people, to blocking of operation or destruction of highly important life support sites and enterprises. Infringement on such objects via information technologies has resulted in actualisation of the problem of preventing cybercrimes at the state level. In particular, the US and European Union (EU) countries have introduced the concept of “critical infrastructure.”

According to the Directive of the US President No.63 (PDD 63, 1998) the critical infrastructure is defined as physical and information systems required for ensuring of minimal acceptable level of operation of economy and government. The critical infrastructure includes: telecommunications, energy, banking and finance, transport, water systems and emergency services.[6] In December 2006, the European Program of Critical Infrastructure Protection[7] was adopted with description of the aim, principles, and required protection measures. Then, the final List of European critical infrastructure sectors was defined to include Energy, Information, Communication Technologies, Water, Food, Health, Financial, Transport, Chemical and nuclear industry, Space and Research, etc. This author has explored the mentioned aspects more thoroughly in another study.[8]

Turning to the above-mentioned classification, the author does not claim it to be exceptional. The alternative is the classification of illegal actions, for example, according to the national criminal legislations which characterise the use of information technologies as a method and means of commitment of crimes.

For instance, according to the Criminal Code of Ukraine, an unauthorised use of Wi-Fi network may be a method of commitment of: actions aimed at forcible change or overthrow of constitutional order or seizure of state power (article 109), infringement of the territorial integrity and inviolability of Ukraine (article 110), sabotage (article 113), violation of privacy (article 182), fraud (article 190), distribution of pornographic products (article 301), unauthorised interference into the work of computer or telecommunication networks (article 361), distribution of harmful software (article 361-1).[9]

And for providers and law enforcement authorities, such illegal actions are committed on behalf of the Wi-Fi access point owner (traffic which goes from Wi-Fi access point via the Internet-provider is identified by one IP-address given to the user by the provider, i.e. by the specific person). This complicates the identification of the real criminal and decreases the efficiency of crimes detection.

For the future, the author predicts an increase in number of cybercrimes committed with the help of Wi-Fi wireless access technology due to:

- low level of knowledge and careless attitude of Wi-Fi access point owners (including telecommunication operators and providers) towards the implementation of protective measures;
- high rates of wireless access technology introduction and increase in the number of users. For example, in Ukraine today the development of Wi-Fi networks decreases the demand for data transfer services provided by mobile operators.[10] And this results not only from the development of the telecommunications market, but also from the state policy of the leading countries in the sphere of information society development, as well as from international obligations. For example, the Agreement of association between Ukraine and

EU, Chapter 14 ("Information society") provides for the promotion of the development of broadband access to telecommunication networks;[11]

- easiness of "cracking" the Wi-Fi radio channel, especially by hacker groups;
- anonymity of Internet users in democratic countries using both collective Wi-Fi access points and mobile communication networks;
- absence in some countries of legally determined mechanisms for regulation of economic objects which provide Internet access (telecommunication providers), their interaction with law enforcement authorities, traffic data storage for a certain period. Thus in Ukraine, according to article 39 of the Law of Ukraine "On Telecommunications," the demand to assist investigation and search operations and to prevent disclosure of organisational and tactical methods of such operations within telecommunication networks is applicable to telecommunication operators only.[12] This demand is not applicable to Internet providers.

The author points out these two last factors as the main ones which decrease the efficiency of response to illegal actions using information technologies, and do not give the possibility to detect the criminal in time and to prevent socially harmful consequences.

Measures for Enhancing Cybersecurity in Wi-Fi Context

At the same time, the provisions of the European Council Convention concerning cybercrimes give the possibility to reflect the mentioned issues in national legislations. Articles 16, 17, 19 of the Convention require the telecommunication providers to store the traffic data for a certain period, and to provide the access to such information and components of information and telecommunication systems to the law enforcement agencies.[13] Thus, the registration of installation data of telecommunication network users is used for the direct binding of mobile numbers, IP addresses and other identifiers to physical and legal bodies for the purpose of registration of the possible violations of the current law and calling the guilty persons to the account. Attention is also paid to the problem of safe functioning of Wi-Fi networks. In order to avoid risks of unauthorised interference into the work of such networks, some countries take administrative measures for the control of Internet access in public places.

Thus, in European countries in places of collective access to the Internet using Wi-Fi technology (coffee shops, restaurants, hotels, etc.) it is obligatory to install the systems of video surveillance and to warn of such method of data registration. In 2011, the Supreme Criminal Court of the Federal Republic of Germany obliged the owners of private wireless networks to use passwords. And in case of any computer crime committed via an unprotected access point, an administrative sanction in the form of a fine of 100 Euros is imposed on the owner of such access point.[14] In The Netherlands, according to the order of the State Communication Agency, hotels which provide Internet services using the Wi-Fi technology have to be registered as Internet providers.[15]

There are also countries with so called "strict" identification (complete identification of physical person). Thus, according to the Governmental Decree of the Republic of Belarus No.646 as of 2010, in collective access points the data transfer services are provided only in case of user identification by identity card.[16]

The author emphasises that in order to effectively oppose the use of new technologies, including Wi-Fi, for commitment of illegal acts, the national legislations shall take into account the positive experience of the leading countries in the sphere of cyberspace protection. In particular, the ways to improve the efficiency of prevention of Wi-Fi networks' use for destructive purposes are:

1) obligatory protection of access points using Wi-Fi technology in governmental telecommunication networks or non-use of such technology in governmental networks;
2) initiation in national legislation of norms according to which the owners of collective Internet access points using Wi-Fi technology in public places (coffee shops, restaurants, hotels, transport, etc.) shall ensure video registration of events in the access area with obligatory warning of such method of data registration;
3) introduction of licensing for providing services of Internet access and data communication;
4) assessment and control of the power levels of Wi-Fi access points.

At the same time, the adoption of the offered legal norms is a slow process due to the need to take into account the opinion of scientists, lawyers from different fields of law, positions of the central bodies of state power and the public and, first of all, of the Internet association of Ukraine.

Not the last place belongs to the organisational aspect of cybercrimes' prevention, which requires improvement of the methods of activity of law enforcement agencies and special services aimed at opposing the use of Wi-Fi networks for destructive purposes. Thus, the main efforts of such authorities shall be focused on arrangement of cooperation with partner special services and police structures of other countries, national telecommunication operators and providers, control of hacker environment with account of national legislation and investigation methods of police and special services. Of course, such actions shall be carried out in line with democratic rights and liberties, and public control.

Conclusion

The rapid development of information technologies leads to the transformation of the society into the new one – information society, characterised by the increase in volumes of information production, ensuring access to domestic and world information resources for the majority of people, primarily with the help of new information technologies and global data communication networks (Internet). The mentioned tendency is one of the directions of the state policy of the leading countries of the world and Ukraine, which aspires to increase its presence in the world information space and stimulates the construction of broadband wireless Internet access networks, including those using Wi-Fi technology.

Along with a number of advantages (rates of scanning, equipment commissioning, data transfer, and possibility of informatisation of rural and remote areas), the main disadvantage of such networks is the low level of protection from unauthorised access (so-called network "cracking") which creates favourable conditions for increase in number of computer crimes, and free use of new technologies for destructive and illegal purposes. In particular, unauthorised access to Wi-Fi network (network "cracking") or use of password-free access gives the criminal the possibility to carry out the "secret" monitoring of data communication (including for the purposes of study of personal characteristics of the person of interest) within the coverage area and/or to use the Internet access points for commitment of destructive actions.

Objective and subjective factors of development of the telecommunication market given in the article provide for the future increase in number of cybercrimes with the help of wireless Wi-Fi connection. The mentioned factors require the introduction of changes into the national legislation with the account of positive experience of other countries, international normative and legal acts, and improvement of the methods of activity of special services and police structures with the account of the national legislation and proper methods of investigation.

Notes

[1] Daniel Bell, "The Coming of Postindustrial Society," *System & Networking Engineering*, 2001, https://www.os3.nl/_media/2011-2012/daniel_bell_-_the_coming_of_post-industrial_society.pdf.

[2] Web Portal of Ukrainian Government, Resolution of Ukrainian Government 386-p, "Strategy of Information Society Development in Ukraine," 15 May 2013, http://www.kmu.gov.ua/control/npd/search rada.gov.ua.

[3] Internet World Stats, http://www.internetworldstats.com.

[4] ITU-T Work Programme, http://www.itu.int/itu-t/workprog/wp_a5_out.aspx?isn=2262.

[5] "50% Wi-Fi сетей можно взломать за несколько секунд" [Fifty percent of the Wi-Fi networks can be broken in in a few seconds], *C News*, 19 October 2010, http://www.cnews.ru/top/2010/10/19/50_wifi_setej_mozhno_vzlomat_za_neskolko _sekund_412774, in Russian.

[6] Presidential Decision Directive NSC-63, 22 May 1998, available at http://www.epa.gov/ watersecurity/tools/trainingcd/Guidance/pdd-63.pdf.

[7] European Commission, "Green Paper on a European Programme for Critical Infrastructure Protection," 17 November 2005, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52005DC0576.

[8] Oleksandr Dovgan and Igor Chernuhin, "Organizational and legal bases of critical infrastructure protection system construction against cyberattacks," in *Information Security of the Person, Society and State* (2012).

[9] *Criminal Code of Ukraine*, 05 April 2001, Web Portal of Verkhovna Rada of Ukraine, http://zakon4.rada.gov.ua/laws/show/2341-14.

[10] "Когда в Украине появится 4G и 5G-интернет" [When 4G and 5G Internet will appear in Ukraine], *Vesti*, 29 August 2013, http://vesti.ua/infografika/14693-kogda-v-ukraine-pojavitsja-4g-internet, in Russian.

[11] Association Agreement between the European Union and its Member States and Ukraine, 15 May 2013, www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2013/0290/COM_COM%282013%290290%28PAR2%29_EN.pdf.

[12] Law of Ukraine on Telecommunications 1280-IV, 18 November 2003, Web Portal of Verkhovna Rada of Ukraine, http://zakon4.rada.gov.ua/laws/show/1280-15.

[13] Website of the Council of Europe, Convention on Cybercrime, 23 November 2001, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[14] Geektimes, "Wi-Fi сети в Германии обязаны стать закрытыми" [Wi-Fi networks in Germany need to become closed], 13 May 2010, http://habrahabr.ru/post/93425, in Russian.

[15] "Голландским гостиницам придется получать лицензию провайдера" [Dutch Hotels would need to get a License as Providers], Open Systems Publications, 15 October 2010, accessed November 22, 2013, http://www.osp.ru/news/2010/1015/13003983/.

[16] Resolution of the Council of Ministers of the Republic of Belarus No. 646, 29 April 2010, Web Portal of the Council of Ministers of the Republic of Belarus, www.mpt.gov.by/ru/new_page_4_5_15099/print.

Igor CHERNUKHIN is an expert of the Security Service of Ukraine (SBU). He also conducts research at the National Academy of the Security Service of Ukraine. He is author of seven other peer-reviewed articles on various security issues. Mr. Chernukhin can be reached via the following e-mail: icd_info@ssu.gov.ua.

Bibliography

50% Wi-Fi сетей можно взломать за несколько секунд [Fifty percent of the Wi-Fi networks can be broken in in a few seconds](link is external). C News, 2010.

Association Agreement between the European Union and its Member States and Ukraine(link is external)., 2013.

Bell, Daniel. "The Coming of Postindustrial Society(link is external)." *System & Networking Engineering* (2001).

Convention on Cybercrime(link is external). Council of Europe, 2015.

Criminal Code of Ukraine(link is external). Web Portal of Verkhovna Rada of Ukraine, 2001.

Dovgan, Oleksandr, and Igor Chernuhin. "*Organizational and legal bases of critical infrastructure protection system construction against cyberattacks*." In *Information Security of the Person, Society and State*., 2012.

Green Paper on a European Programme for Critical Infrastructure Protection(link is external). Brussels: Commission of the European Communities, 2005.

Internet World Stats(link is external)., 2015.

ITU-T Work Programme(link is external)., 2015.

Law of Ukraine on Telecommunications(link is external). Web Portal of Verkhovna Rada of Ukraine, 2003.

Presidential Decision Directive NSC-63(link is external)., 1998.

Resolution of the Council of Ministers of the Republic of Belarus (link is external). Web Portal of the Council of Ministers of the Republic of Belarus, 2010.

Strategy of Information Society Development in Ukraine(link is external). Web Portal of Ukrainian Government, Resolution of Ukrainian Government 386-p, 2013.

Wi-Fi сети в Германии обязаны стать закрытыми [Wi-Fi networks in Germany need to become closed](link is external). Geektimes, 2010.

Голландским гостиницам придется получать лицензию провайдера [Dutch Hotels would need to get a License as Providers](link is external). Open Systems Publications, 2010.

Когда в Украине появится 4G и 5G-интернет [When 4G and 5G Internet will appear in Ukraine](link is external). *Vesti* (2013).