JEL CLASSIFICATION: L81, G32, C10, C12, C18

# CONSTRUCTION OF A GENERALIZED MODEL OF THREATS TO INTERNET-BANKING

**Maryna M. VOITKO**
*Chief engineer, The National Bank of Ukraine, graduate student of the University of Banking of the National Bank of Ukraine (Kyiv)*

*Summary. This article is devoded to investigation of generalized model of threats for Internet-banking systems, which is based on interrelation of operation risks and information security risks.*

***Key words:*** *Internet-banking, operationalrisk, information security risks, threat model, source of threats, offender model.*

In the context of the global development of the market economy and increased competition it has become popular to use a relatively new tool for the management of bank accounts of Internet banking.

The development of Internet banking attack concepts, means and methods for their implementation is conditioned by growth of the number of Internet users at an exponential rate in the world and clients of Internet banking systems. The solutions that are currently used in those systems cannot fully ensure their protection during attacks.

The purpose of this paper is to analyze the possible sources of threats to information security in Internet banking systems, and based on that, to improve generalized threat model for further evaluation of security of the mentioned systems in the performance of bank payments as well as to develop the methodological risk assessment systems related to information security risks that are available in Internet banking systems.

The aim of the article is to study the interrelation between operational risks and information security risks in the Internet banking system and based on this interrelation to improve the generalized threat model for Internet banking systems.

In order to develop a methodological system to assess risks related to information security risks (IT-risks) that exist in Internet banking systems, the priority is to build the threat model. The threat model in Internet banking system is generalized information on detailed analysis of potential threats, determination of their characteristics, mechanisms and impacts.

In order to build such a model, the Internet banking system is considered as the one that consists of geographically dispersed clients, the web server of the bank, the bank's application server, the bank's core banking server and "Client-Bank" server and ensure the functioning of Internet banking system.

It was defined as the interrelationship of operational risk and information security risk. On the basis of the mentioned interrelationship the model of threats to Internet banking systems was built.

An integral part in improving the construction of a threat model for IB systems is the model of the likely offender, which should be adequate to the real offender of this type of system, it was considered some categories of possible infringers of IT security systems.

*References*

1. Pro zatverdzhennia Polozhennia pro orhanizatsiiu operatsiinoi diialnosti v bankakh Ukrainy, zatverdzhene Postanovoiu Pravlinnia Natsionalnoho banku Ukrainy vid 18.06.2003 № 254 [On approval of the operational activity of banks of Ukraine, approved by the National Bank of Ukraine 18.06.2003 № 254]. Retrieved from http://zakon.nau.ua/doc/?uid=1078.8029.0.

2. Valentsovoi N. Y. (2008) Bankovskie riski [Banking risk]. M. : KNORUS.

3. Lyst Departamentu informatyzatsii bankakh Ukrainy 03.03.2011 № 24-112/365/ [Letter to the Department of Informatization banks of Ukraine 03.03.2011 № 24-112/365/]. Retrieved from http://www.zakon.rada.gov.ua.

4. SOU N NBU 65.1 SUIB 2.0:2010 "Metody zakhystu v bankivskii diialnosti. Zvid pravyl dlia upravlinnia informatsiinoiu bezpekoiu" (ISO/IES 27002:2005, MOD) ["Methods of protection in the business. Code of Practice for Information Security Management"]. Retrieved from http://www.zakon.rada.gov.ua.

5. Postanova Pravlinnia Natsionalnoho banku Ukrainy vid 28.10.2010 № 474 "Pro nabrannia chynnosti standartamy z upravlinnia informatsiinoiu bezpekoiu v bankivskii systemi Ukrainy" [Resolution of the Board of the National Bank of Ukraine dated 28.10.2010 № 474 "On the effective date of standards for information security management in the banking system of Ukraine"]. Retrieved from http://www.zakon.rada.gov.ua.

6. SOU N NBU 65.1 SUIB 1.0:2010 "Metody zakhystu v bankivskii diialnosti. Zvid pravyl dlia upravlinnia informatsiinoiu bezpekoiu" (ISO/IES 27001:2005, MOD). [JMA H NBU 65.1 ISMS 1.0: 2010 "Methods of protection in the business. Code of Practice for Information Security Management" (ISO / IES 27001 : 2005, MOD)] http://www.zakon.rada.gov.ua.

7. ND TZI 1.1-002-99 Zahalni polozhennia shchodo zakhystu informatsii v kompiuternykh systemakh vid nesanktsionovanoho dostupu. Zatverdzheno nakazom DST·SZI SB Ukrainy vid 28.04.1999 № 22. [Sun Heat 1.1-002-99 General provisions for the protection of information in computer systems from unauthorized access. Approved by DSTSZI Security Service of Ukraine from 28.04.1999 № 22.]

8. Kapustian M. V., Orlenko V. S., Khoroshko V. O. (2006) Stvorennia modeli zahroz informatsii ta mekhanizmu yii efektyvnoho zakhystu [Creating models of threat information and the mechanism for its effective protection]. Avtomatyka, vymiriuvannia ta keruvannia: Visnyk natsionalnoho universytetu "Lvivska politekhnika". № 551, 58–63.

9. Kudinov V. A., Khoroshko V. A. (2004) Korporatyvna merezha OVS Ukrainy ta modeli yii zakhystu vid porushnykiv bezpeky [Corporate network ATS Ukraine and models of protection against violators of safety]. Information Security. 1, 26-36.

10. Liamyn L. V. (2006) Analiz faktorov riska, sviazannykh s internet-bankinhom [Analysis of risk factors, sviazannyh with Internet banking]. Raschety i operatsionnaia rabota v kommercheskom banke. 5, 52-64.