УДК 330.34

А. В. Колодійчук

МОЖЛИВОСТІ ТА ЗАГРОЗИ НЕЙТРАЛІЗАЦІЇ ФІНАНСОВО-КРЕДИТНИХ РИЗИКІВ РОЗВИТКУ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ НА МІЖНАРОДНИХ РИНКАХ ГРОШЕЙ І КАПІТАЛУ

Ужгородський торговельно-економічний інститут Київського національного торговельно-економічного університету

Анотація. *У статті виділено можливості та окреслено загрози нейтралізації фінансово-кредитних ризиків розвитку національної економіки на міжнародних ринках грошей та капіталу.*

Ключові слова: фінансово-кредитні загрози, капітал, грошовий ринок, мережа, фінансова піраміда, новітні технології, національне господарство.

Abstract. *The article highlights the opportunities and threats to neutralize the financial and credit risks of the national economy development in the international money and capital markets.*

Keywords: financial and credit threats, capital, money market, network, pyramid scheme, latest technologies, national economy.

У ході побудови та реалізації макроекономічної моделі управління ризиками впровадження інформаційно-комунікаційних технологій (ІКТ) важлива роль відводиться з'ясуванню питання визначення можливостей та загроз нейтралізації фінансово-кредитних ризиків розвитку національної економіки [1-8] на міжнародних грошових та капітальних ринках.

ІКТ-можливості, які враховують у процесі пом'якшення негативного впливу фінансово-кредитних загроз національної безпеки економічного сектору, виглядають так: пакети прикладних програм проектного та портфельного аналізу з диверсифікації ризику інвестицій (наприклад, "Інвестиційний аналіз 2.0", "ProjectExpert"); техніко-інформаційне вдосконалення фінансово-кредитних механізмів реалізації державної економічної політики; спеціальне антивірусне програмне забезпечення, яке обслуговує діяльність трейдерів на фінансових біржах; інноваційний розвиток фінансових інструментів на фондових онлайн-біржах; повсюдна QR-кодифікація елементів банківської та суміжної інфраструктури; всебічне впровадження систем інтернет-банкінгу в торговельних мережах; періодичні тренінги для працівників установ фінансового сектору з питань забезпечення та удосконалення інформаційної безпеки; впровадження найновіших технологій криптографічного захисту банківських та інших фінансових даних; задовільна протокольна політика керування електронними базами корпоративної інформації на підприємствах і організаціях фінансової сфери; підвищений інтерес до комп'ютерної складової фінансової грамотності економічно активного населення.

Наприклад, транснаціональна корпорація "Facebook" разом з Міністерством цифрової інформації України започаткувала у листопаді 2020 року проект онлайн-допомоги малому і середньому бізнесу в умовах посткарантинного локдауну. Побудований сервіс "Boost with Facebook" за принципом "інтерактивні вебінари + креативний контент + приклади". У всесвітній мережі його можна знайти за гіперпосиланням https://www.facebook.com/business/boost/webinars-online-learning. Тематично сайт присвячений актуальним питанням бренд-менеджменту, онлайн-бізнесу, маркетингу та "паблік рилейшнз".

ІКТ-загрози, що поглиблюють фінансово-кредитні загрози національної економічної безпеки, містить наступні загрози: крупні DDos-атаки на інтернет-мережі банківських та інших фінансових установ (зокрема, вони бувають наступних типів: SYN-атаки – при пересиланні хакерами спеціального ACK-пакета, в результаті чого сервер не здатний приймати запити інших клієнтів; UDP-атаки – при автоматичному створенні сукупності протокольних повідомлень за допомогою 17 мов програмування; MAC-атаки – під час перевантаження сервера організації безліччю порожніх Ethernet-фреймів; ICMP-атаки – при складанні комп'ютерами хакерів повідомлень про помилки без

трансферу даних по каналу мережі; HTTP POST – передбачає перекодування даних з сервера і пересилання йому назад, в результаті чого він перевантажується; HTTP GET – відбувається "зациклення" сервера на файлі-вірусі, що зупиняє його нормальну роботу; HTTP-назва – стороннє втручання зловмисників в роботу проксі-серверів банків); порушення роботи національної інформаційної системи та ІКТ-інфраструктури через дії хакерів та інших зловмисників шляхом злому комп'ютерних систем; поштові бомби; низький рівень розвитку електронного урядування в фінансовому сегменті управління національним господарством; локальні нормативно-правові бар'єри на шляху інтернаціонального використання банківсько-платіжних систем TARGET, SWIFT; значне поширення смартфон-додатків, які самостійно списують кошти з банківських рахунків користувачів без їх відома; корпоративний банківський шпіонаж, націлений на електронні бази даних та іншу інсайдерську інформацію; можливий витік даних із хмарних сервісів через неправильне їх використання працівниками підприємств фінансового сектору національної економіки; втрати даних через фішингову діяльність зловмисників; невміння клієнтів банківських установ правильно та безпечно користуватися мобільними девайсами, що обслуговують банківські операції; хактивізм – суспільна популяризація хакерської діяльності не заради наживи, а задля цілей певної політичної ідеології, в результаті чого страждає національна банківська система; діяльність фінансових пірамід в цифровому просторі; загрози, які пов'язані з обігом криптовалют та функціонуванням криптогрошового онлайн-ринку.

Якщо говорити про державну статистику DDos-атак на офіційні владні органи та установи, то її проводять здебільшого на тижневому відтинку. Часто масштаби перебігу DDos-атак залежать від проведення суспільно-політичних подій, що відбуваються в Україні. Так, наприклад, напередодні місцевих виборів депутатів та голів міських, сільських й селищних рад у 2020 році, за тиждень 21-27 жовтня цього року було зафіксовано 22 DDos-атаки, що на 47% більше, ніж на попередньому тижні (15 DDos-атак). Загалом, за цей тиждень було знешкоджено 44,8 тис. кібератак різного типу, що на 28% менше, ніж за попередній тиждень. Якщо говорити про структуру загальної кількості кібератак, то 94% з них – це павутинні прикладні атаки, ще 4% – кібератаки, що носять назву "harvest attack". За аналізований період офіційного кібермоніторингу було виявлено біля 1,1 млн. підозрілих подій, а це на 10% більше, ніж на попередньому тижні (це нестандартні протоколи, павутинне сканування, запуск шкідливих програм тощо).

В умовах активізації міжнародної економічної діяльності та посилення глобалізаційних процесів все більше зростає роль інформаційно-комунікаційних технологій на міжнародному рівні. Не є виключенням в цьому плані і світовий фінансовий ринок, який включає міжнародні валютні ринки, міжнародні грошові ринки та міжнародні ринки капіталів [4]. До ІКТ-можливостей послаблення фінансово-кредитних загроз національної економічної безпеки на міжнародних ринках капіталів (інвестиційних ринках) відносяться: постійне розширення офіційного "чорного" списку сумнівних інвестиційних проектів та інвестиційних ідей, що періодично формується спеціалістами з Національної комісії з питань цінних паперів і фондового ринку (у кінці 2020 року їх нараховувалось біля 40 суб'єктів різних форм власності); цільовий продаж товарів, інформаційної продукції, реалізація послуг, в тому числі рекламних через відеохостинги YouTube, з допомогою професійних ютуб-менеджерів та ютуб-маркетологів (спеціальні калькулятори розкручування бренду на порталі http://7youtube.ru/calc).

У розрізі ІКТ-загроз, що сприяють негативному прояву фінансово-кредитних ризиків безпеки національної економіки на міжнародних ринках капіталів, слід виділити наступні: 1) махінації з процентними сертифікатами при купівлі електроніки, дорогоцінностей (наприклад, у бізнес-проектах "B2B Jewerly", "Eva" намічаються виплата 400% річних при купівлі сертифікатів, проте вони зараховуються на внутрішній електронний рахунок, вміст котрого практично неможливо перевести в готівку до терміну закінчення життєвого циклу проекту фінансової піраміди); 2) висока професійність реферальної команди (набирачів нових інвесторів в сумнівні короткострокові фінансові проекти з високою дохідністю вкладених інвестиційних засобів); крупні фінансові махінації зі книжковими сертифікатами (у проекті "Wecauto" пропонується придбати знижковий річний сертифікат на купівлю автомобіля за 30%-вартістю, в оборот схеми вдалося залучити близько 2000 вкладників); 3) експлуатація рядом фінансових пірамід теми новітніх і високих технологій (квантові технології інвестування у піраміді "QubitTech", технології криптовалютного майнінгу у кропивницькому дата-центрі "Mining Express"), що приваблює інноваційно орієнтованих, але не підготовлених вкладників.

Розглянемо ключові ІКТ-можливості для зменшення негативного впливу фінансово-кредитних ризиків національної безпеки на міжнародних грошових ринках (ринок короткострокових позик та міжнародних грошових розрахунків). Вони включають різноманітні системи захисту банківської та іншої фінансової інформації клієнтів фінансово-кредитних установ та організацій різних форм власності, QR-кодифікацію тощо.

В частині сучасних і актуальних ІКТ-загроз, які поглиблюють фінансово-кредитні загрози національної безпеки на міжнародних грошових ринках, ми маємо: діяльність міжнародної хакерської бот-мережі "EMOTET", яка працювала на 90 серверах у різних країнах світу (в т.ч. США, Великобританії, Франції, Голландії, ФРН, Литви) і незаконно оволоділа грошовими коштами фінансових та підприємницьких установ на 2,5 млрд. $. Механізм функціонування цієї мережі полягав у спам-розсиланні вірусного програмного забезпечення через doc.- та xls-документи та вилучення конфіденційної банківської інформації клієнтів фінансово-кредитних установ.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Боди З. Финансы: учеб. пособие / З. Боди, Р. Мертон; пер. с англ.. – М., 2000. – 592 с.
2. Гаврилко П. П., Колодійчук А. В., Важинський Ф. А., Гуштан Т. В., Чобаль Л. Ю. Економіка туризму в цифрову еру: еволюція, маркетографія, перспективи: монографія. Львів, 2021. 163 с.
3. Гаврилко П. П., Колодійчук А. В., Важинський Ф. А., Індус К. П. Міжнародні фінанси і фінансовий менеджмент в задачах та прикладах: навчальний посібник. Львів: Вид-во ННВК "АТБ", 2020. 161 с.
4. Гаврилко П. П., Колодійчук А. В., Лазур С. П., Важинський Ф. А. Міжнародна економіка в таблицях, схемах, формулах, задачах і прикладах: навчальний посібник. Львів: Вид-во ННВК "АТБ", 2019. 258 с.
5. Колодійчук А. В., Чобаль Л. Ю., Молнар О. С., Данило С. І. Транснаціональні корпорації в таблицях і схемах: навчальний посібник. Львів: Вид-во ННВК "АТБ", 2020. 182 с.
6. Нижник Н. Р., Ситник Г. Л., Білоус В. Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): навч. посіб. К.: Преса України, 2000. 304 с.
7. Ноздріна Л. В., Ящук В. І., Полотай О. І. Управління проектами: підручник. К.: Центр учбової літератури, 2010. 432 с.
8. Kolodiychuk A.V. Entrepreneurial risk theories as component of the theoretical foundations of informatization processes in the national economy / A.V. Kolodiychuk // Институт за икономически изследвания при БАН «Списание «Икономически изследвания» – Vol. 26(6). – 2017. – С. 104-117. – Available from: https://www.researchgate.net/publication/323412759_ Entrepreneurial_risk_theories_ as_component_of_the_theoretical_foundations_of_informatization_processes_in_the _national_economy [accessed Apr 18 2018].

Колодійчук Анатолій Володимирович, кандидат економічних наук, доцент, доцент кафедри менеджменту туристичного та готельно-ресторанного бізнесу, Ужгородський торговельно-економічний інститут Київського національного торговельно-економічного університету, Ужгород, e-mail: kolodiychuka@i.ua

Kolodiychuk Anatoliy V. – Ph.D. in Economics, Associate Professor, Associate Professor of the Department of Tourism, Hotel and Restaurant Business Management, Uzhhorod Trade and Economic Institute of Kyiv National Trade and Economic University, Uzhhorod, e-mail: kolodiychuka@i.ua