УДК 338.054.23+004.056.53

Кобилянська Л.М.
кандидат економічних наук,
старший науковий співробітник відділу макроекономічного регулювання
та міжнародних економічних відносин
Академії фінансового управління

КІБЕРЗЛОЧИННІСТЬ ЯК ГЛОБАЛЬНА ЗАГРОЗА ЕКОНОМІЧНІЙ БЕЗПЕЦІ СУЧАСНОЇ ДЕРЖАВИ

У статті розглянуто явище кіберзлочинності, що завдає значних економічних збитків у світовому масштабі. Досліджено проблеми підрахунку втрат через кіберзлочини в кількісному виразі. Визначено можливості удосконалення системи протидії явищу кіберзлочинності на міжнародному рівні та в Україні.

Ключові слова: кіберзлочинність, економічна безпека, кібератака, протидія.

Кобылянская Л.Н. КИБЕРПРЕСТУПНОСТЬ КАК ГЛОБАЛЬНАЯ УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ СОВРЕМЕННОГО ГОСУДАРСТВА

В статье рассмотрено явление киберпреступности, которое наносит значительный экономический ущерб в мировом масштабе. Исследованы проблемы подсчета потерь вследствие совершения киберпреступлений в количественном выражении. Определены возможности совершенствования системы противодействия явлению киберпреступности на международном уровне и в Украине.

Ключевые слова: киберпреступность, экономическая безопасность, кибератака, противодействие.

Kobylyanska L.M. CYBERCRIME AS A GLOBAL THREAT TO MODERN STATE ECONOMIC SECURITY

The article deals with the cybercrime phenomenon, causing significant economic losses worldwide. The problems of losses accounting in quantitative terms caused by cybercrime are investigated. The opportunities of cybercrime resistance system improvement at the international level and in Ukraine are defined.

Keywords: Cybercrime, economic security, cyber attacks, resistance.

Постановка проблеми. Відомо, що кіберзлочинність у світових масштабах призводить до значних втрат, однак, єдиної методології розрахунку не існує, з цієї причини в оприлюднених статистичних даних спостерігаються значні розбіжності. Оцінка підрахунку збитків від кіберзлочинів залишається наразі надзвичайно важливою і, водночас, складною проблемою.

Аналіз останніх досліджень і публікацій. Дослідженням окремих аспектів явища кіберзлочинності, зокрема, термінології займалися іноземні науковці Дж. Ліпман, Ф. Крамер, питання наслідків здійснення кіберзлочинів на національному та міжнародному рівнях вивчали Р. Олдріч, М. Шмідт. Серед вітчизняних дослідників проблематики кіберзлочинності можна відзначити таких фахівців як П. Біленчук, В. Голубев, Д. Дубов, С. Кавун, В. Носов, О. Манжай.

Постановка завдання. Основним завданням даної публікації є визначення масштабів загроз явища кіберзлочинності в глобальному форматі. Надзвичайно актуальним питанням залишається створення ефективної системи протидії явищу кіберзлочинності у світовому вимірі та в Україні.

Виклад основного матеріалу дослідження. Тотальна комп'ютеризація, мережа Інтернет, цифрові технології стрімко увірвались в усі сфери людської діяльності. Розвиток ІКТ значно спрощує виробничі, управлінські, організаційні процеси та збереження інформації, водночас, активізуючи такий різновид незаконної діяльності як кіберзлочинність у віртуальній мережі.

Кіберзлочинність щорічно завдає глобальних економічних збитків, отже, основною мотивацією поширення даного різновиду злочинної діяльності залишається отримання доходів. Ще в жовтні 2000 р., на конференції країн Великої вісімки, присвяченої проблемам кіберзлочинності йшлося про те, що збитки від кіберзлочинів сягають 100 млрд німецьких марок у рік, а за оцінками Рахункової палати уряду США щорічний збиток від розкрадань і шахрайств, здійснених за допомогою інформаційних технологій лише через Internet, досягав 5 млрд дол. [1].

Відомо, що обсяги фінансових збитків через кібератаки з року в рік зростають. Так, згідно з інформацією Комісії з внутрішніх справ палати громад парламенту Великобританії, втрати світової економіки від злочинів, скоєних за допомогою інформаційно-комунікаційних технологій, досягли в 2013 р. 388 млрд дол., обійшовши за своїм розмахом світовий наркотрафік, річний оборот якого оцінюється в 288 млрд дол. [2].

Згідно з методикою розрахунків Центру стратегічних і міжнародних досліджень CSIS (США) та фірми безпеки McAfee, щорічні втрати світової економіки від кіберзлочинів варіюються в межах від 300 млрд дол. до 1 трлн дол. США і складають 0,4%-1,4% світового ВВП [3]. За даними вищезазначених організацій, у результаті кібердіяльності лише економіка США щороку втрачає 100 млрд дол. і 508 000 робочих місць [4]. У звітах організацій, що проводять дослідження такого явища як кіберзлочинність, серед основних висновків є такий – більшість урядів та бізнесменів недооцінюють збитки та ризики зростання кількості кіберзлочинів. Відомо також, що найбільша частина правопорушень, вчинених завдяки сучасним цифровим технологіям та мережам телекомунікацій, залишається за рамками статистики, до офіційних даних потрапляє лише десять, у кращому випадку, двадцять відсотків скоєних злочинів.

Як повідомляє Центр прийому скарг про кіберзлочинність (Internet Crime Complaint Center – IC^3) що діє під контролем ФБР, у 2013 р. було отримано 262813 скарги від споживачів про збитки в результаті кібердіяльності (рис. 1), загальний обсяг яких складав 781,841611 дол.

Список країн-лідерів за загальною кількістю скарг, що надійшли до IC^3 у 2013 р., складали США – 90,63%, Канада – 1, 38%, Великобританія – 0,85%, Індія – 0,71%, Австралія – 0,69% [5].

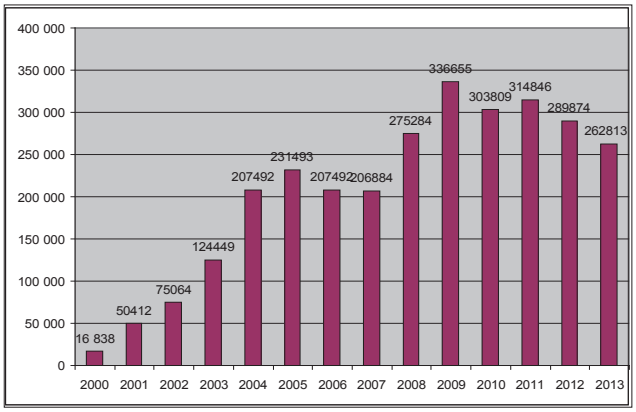

Рис. 1. Кількість щорічних повідомлень про кіберзлочини в Центрі прийому скарг про кіберзлочинність, США

Джерело: 2013 Internet Crime Report. [Електронний ресурс]. – Режим доступу: http://www.ic3.gov/media/annualreport/2013_ic3report.pdf

Однак, згідно з даними досліджень компанії «Norton», щодня у світі 1,5 мільйона людей або 18 осіб у секунду піддаються атакам кіберзлочинців. Впродовж 2012 р. тільки в США 71 млн осіб стали жертвами кіберзлочинів. Найбільшу кількість постраждалих було зафіксовано в Росії (92%), Китаї (84%) і Південній Африці (80%). За оцінками компанії, 556 мільйонів дорослих жителів світу мають досвід атак кіберзлочинців, серед яких 21% користувачів онлайн-мереж стали жертвами соціальних злочинів чи мобільних технологій, 15% користувачів скаржилися на викрадання коштів з власних рахунків, кожен десятий користувач став жертвою підроблених посилань або шахрайства [6].

Оцінка підрахунку збитків від кіберзлочинів залишається наразі надзвичайно важливою і, водночас, складною. Йдеться, передусім, про промислове шпигунство, незаконне копіювання матеріалів інтелектуальної власності, безпосередні крадіжки коштів через мережу. Так, дослідниками явища кіберзлочинів у США з'ясовано, що шпигунство та крадіжки інтелектуальної власності генерують величезні втрати для національної економіки та призводять до деформації відносної економічної ефективності. Найбільше кіберзлочинність розповсюджена у фармацевтичній, біотехнічній та хімічній галузях промисловості, а також у сферах виробництва електроніки та комп'ютерних технологій.

Зазвичай компанії чи корпорації не в змозі оцінити реальні збитки через кіберзлочинну діяльність, адже незаконне привласнення інтелектуальної власності чи важливої ділової інформації важко піддається кількісній оцінці. Також надзвичайно складно визначити у вартісному вимірі втрати репутації банківських установ, адвокатських контор або юридичних компаній серед клієнтів. Значними є витрати на страхування суб'єктів господарювання та відновлення їх діяльності у випадку скоєння кіберзлочинів.

Водночас, з року в рік зростають додаткові витрати фізичних осіб, організацій та держав на оновлення операційних систем захисту персональних комп'ютерів, убезпечення діяльності підприємств, банківських установ від несанкціонованого втручання в роботу комп'ютерних систем.

Проте, йдеться не тільки про економічні наслідки. Торгівля підробними ліками та нанесення шкоди здоров'ю, торгівля людьми, розповсюдження порнографії, моральні травми, втручання в роботу державних електронних мереж та комунікацій стратегічних об'єктів, кібертероризм – це далеко не повний перелік проблем, пов'язаний з кіберзлочинами. Яскравими прикладами негативних наслідків світового масштабу є кібератака сайту «WikiLeaks», створення електронної шпигунської мережі «GhostNet» (завдяки якій відбувалось втручання в роботу міністерств закордонних справ і посольств Південної Кореї, Ірану, Бангладешу, Індії, Таїланду, Німеччини, Пакистану), злом групою осіб (група «LulzSec») сайту «Sony Playstation» та сайту ЦРУ, втручання угрупування «Anonymous» у роботу державних сайтів США, Польщі, Росії, Сирії, Ватикану, Угорщини, Франції, Австрії, Мексики, сайтів багатьох корпорацій та особистих сайтів урядовців. Все частіше новітні інформаційні технології застосовуються терористичними організаціями з метою залучення коштів, здійснення пропаганди або передачі секретної інформації. Окремі терористичні угруповання, такі як «Hezbollah», «Hamas», «The Abu Nidal Organization» використовують комп'ютерні системи, електронні мережі для шифрування та передачі інформації, фінансування та всілякої підтримки злочинної діяльності. Кібертероризм, як різновид зброї, дедалі активніше застосовується з метою виведення з ладу важливих державних та соціальних об'єктів.

Базовою основою міжнародного рівня з мінімізації загроз впливу кіберзлочинності є Конвенція Ради Європи про злочинність в кіберпросторі, прийнята 23 листопада 2001 р. у Будапешті (Будапештська конвенція). Серед основних питань, висвітлених у даному документі – криміналізація правопорушень, здійснених завдяки комп'ютерним пристроям з метою втручання в роботу комунікаційних мереж та викрадення даних; вдосконалення національного законодавства в боротьбі з кіберзлочинністю; розвиток міжнародного співробітництва.

Згідно з класифікацією, що прийнята вищезазначеною Конвенцією, кіберзлочини поділяються на п'ять різновидів: правопорушення проти конфіденційності, цілісності і доступності комп'ютерних даних і систем; правопорушення пов'язані з комп'ютерами; правопорушення, пов'язані зі змістом інформації; правопорушення, пов'язані з порушенням авторських і суміжних прав; дії расистського і ксенофобського характеру.

Протидія явищу кіберзлочинності вбачається в спільних діях державного і приватного сектора, вдосконаленні міжнародного та національного законодавства, організації міжнародних підрозділів та структур у боротьбі з кіберзлочинами. З цією метою в 2013 р. в ЄС створено Європейський центр боротьби з кіберзлочинністю (Гаага).

Наразі в Україні склалася неоднозначна ситуація через втручання в роботу електронних систем та скоєння кіберзлочинів. За даними дослідження Світового економічного форуму, Україна в 2013 р. посідала 81 місце з-поміж 148 країн світу за Індексом мережевої готовності (Networked Readiness Index), що характеризує рівень розвитку інформаційно-комунікаційних технологій (ІКТ) у країнах світу [7]. Однак, маючи один з найнижчих показників підключення до всесвітньої мережі Інтернет в Європі, Україна входить до списку п'ятнадцяти світових країн-лідерів, з території яких відбувається найбільша кількість кібератак, зокрема, таких як Росія, США, Китай, Тайвань, Німеччина, Велика Британія, Франція, Австралія, Нідерланди. За даними моніторингу оператора зв'язку Deutsche Telekom (Німеччина), у січні

2014 р. з території України було здійснено 52009 кібератак, у лютому – 110132, у березні – 111730, у червні – 62538, у липні – 31982, у вересні – 46832, у жовтні –116182 [8].

Кількість Інтернет-користувачів в Україні невпинно зростає. За даними Київського міжнародного інституту соціології, частка регулярних користувачів мережі Інтернет значно збільшилась – з 32% на початку 2011 р. [9] до 50% загальної кількості дорослого населення наприкінці 2013 р. [10], та зросла до 53,4% за перший квартал 2014 р. Вцілому, серед опитаних 58,5% українців мають вдома доступ до Інтернет-мережі [11].

У 2013 р. в Україні найбільш розповсюдженим видом кіберзлочинів було списання коштів з рахунків фізичних і юридичних осіб з використанням систем дистанційного банківського обслуговування та подальшою легалізацією незаконно отриманих доходів. За минулий рік правоохоронними органами зафіксовано 270 спроб злому систем на суму понад 100 млн грн. Із загальної суми зареєстрованих списань – понад 67 млн грн, власникам повернуто близько 47 млн грн. Впродовж 2011-13 рр. спостерігалось значне зростання кількості випадків застосування скіммінгових пристроїв. Співробітниками МВС України в 2011 р. було виявлено 45 таких пристроїв, у 2012 р. – 73, у 2013 р. – 160 [12].

Аналогічна ситуація спостерігається в 2014 р. Як зазначають фахівці Незалежної асоціації банків України, серед специфічних видів кіберзлочинів – підробка банківських карток, крадіжка конфіденційних даних банківських карт, шахрайство з банкоматами, злочинні дії в банківській системі он-лайн.

Українським зловмисникам належить авторство в розробці вірусних програм Carberp (за допомогою яких у світовій електронній мережі викрадено 250 млн дол.) та Gamker, а також нового віруса Neverquest, що мають модуль для крадіжки даних. Перелічені віруси вражають банківські системи та копіюють конфіденційну інформацію, пов'язану з фінансами.

Як повідомляє компанія-розробник програмного забезпечення в сфері комп'ютерної безпеки Trusteer (Ізраїль), нещодавно було виявлено нову троянську програму Zberp, котра є новою модифікацією Carberp та Zeus – хакерських програм, створених з метою автоматичної крадіжки персональних даних та проведення різноманітних несанкціонованих операцій. Zberp здатна робити скріншоти і відправляти їх на віддалений сервер, викрадати вхідні і вихідні дані FTP (протоколу передачі даних) і POP3 (поштового протоколу, завдяки якому користувачі отримують пошту з серверів), SSL-сертифікати (забезпечення встановлення безпечного з'єднання між клієнтом і сервером), а також інформацію користувачів при заповненні будь-яких форм online, втручатися в роботу браузера та копіювати інформацію на відкриті вебсайти [13]. На думку експертів, більшість антивірусних систем на момент виявлення троянської програми були не спроможні розпізнати Zberp.

У 2013-14 рр. почастішали випадки розповсюдження вірусів через мобільні пристрої користувачів, зокрема, телефони, смартфони, планшети. Згідно з експертними висновками фахівців компанії «Norton», небезпека криється в тому, що близько 49% споживачів використовують свої особисті мобільні пристрої водночас як для роботи, так і для гри, таким чином спрощуючи доступ хакерам до конфіденційної інформації. Близько половини смартфонів і планшетних пристроїв не оснащено навіть елементарними запобіжними заходами, зокрема, йдеться про використання паролів, безпекове програмне забезпечення, резервне копіювання файлів з мобільних пристроїв.

Пріоритетними напрямами створення державної стратегії в Україні в сфері забезпечення інформаційної безпеки та протидії кіберзлочинам є поєднання координаційних зусиль та взаємодії правоохоронних органів, спецслужб, судової системи, а також їх матеріально-технічне забезпечення, підготовка необхідної кількості фахівців, узагальнення слідчої та судової практики стосовно кіберзлочинів, розробка чітких рекомендацій щодо їх розслідування, налагодження механізму обміну інформацією правоохоронної системи України з правоохоронними органами іноземних держав, що здійснюють боротьбу з кіберзлочинністю.

Надзвичайно гостро постає необхідність удосконалення внутрішнього чинного законодавства України в сфері боротьби з кіберзлочинністю. У вітчизняному законодавстві панує невизначеність стосовно термінів «кіберзлочин», «кіберзлочинність», «кібератака» та існує лише узагальнене визначення цього типу злочинів як шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки (Стаття 190 Кримінального кодексу України); несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (стаття 361 КК України); створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (стаття 361^1 КК України); несанкціонованих дій з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинених особою, яка має право доступу до неї (стаття 362 КК України); порушень правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (стаття 363 КК України); перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (стаття 363^1 КК України).

Висновки з проведеного дослідження. Кіберзлочинність щорічно завдає глобальних економічних збитків, які надзвичайно складно визначити в кількісному виразі. Водночас, суб'єкти господарювання та уряди держав недооцінюють реальні виклики та загрози, пов'язані з кіберзлочинами в глобальному вимірі (йдеться про так званий прихований чи «тіньовий» Інтернет, кібертероризм, промисловий шпіонаж, функціонування бот-мереж та вірусних програм).

Боротьба з кіберзлочинністю в міжнародному форматі актуалізує необхідність координації дій державного і приватного сектора на основі об'єднання фінансових, технічних, комунікаційних і організаційних ресурсів, обмеження анонімності користувачів у всесвітній Інтернет-мережі, соціальних мережах та під час проведення банкінгових операцій, створенні міжнародних підрозділів та структур у боротьбі з кіберзлочинністю з наданням права передачі даних про рух інформації, екстрадицію, допомогу, розробку міжнародних чи транскордонних комунікаційних мереж для відстеження в реальному часі і передачі інформації про кіберзлочини.

Втручання в роботу телекомунікаційних систем в Україні потребує вжиття низки заходів протидії, зокрема: зменшення кількості авторизаційних лімітів, розширення використання чіпових карт, застосування сучасного мережевого захисту банківських систем, у тому числі систем додаткового підтвердження платежів через одноразові паролі та коди.

Небезпеку складає одночасне використання браузеру для ігор чи спілкування в соціальних мережах та здійснення Інтернет-банкінгу. Використання ліцензійного програмного забезпечення, новітні системи мережевого захисту фінансових установ та організацій, роз'яснювальна робота серед клієнтів у питаннях збереження конфіденційності інформації та індивідуальних даних сприяє зниженню кількості кіберзлочинів.

Існує потреба удосконалення внутрішнього чинного законодавства України шляхом доповнення термінології нормативно-правової бази в сфері кіберзлочинності.

Наразі в Україні відсутня єдина державна стратегія з кібербезпеки та цифрового суверенітету, виробництво власних програм та сучасної електронної комп'ютерної техніки, а також єдина національна операційна система обміну інформацією. За відсутності власної технічної, програмної бази країна з низьким рівнем обізнаності, інформаційної безпеки й надалі лишатиметься залежною і вкрай вразливою до глобальних загроз.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Біленчук П.Д. Організована транснаціональна комп'ютерна злочинність: глобальна проблема третього тисячоліття / П.Д. Біленчук [Електронний ресурс]. – Режим доступу : http://www.crime-research.ru/library/Bilukr.htm.
2. Офіційний сайт Незалежної асоціації банків України [Електронний ресурс]. – Режим доступу :http://www.anticyber.com.ua/article_detail.php?id=186.
3. The Economic Impact of Cybercrime and Cyber Espionage. Report // Center for Strategic and International Studies, July 2013 [Електронний ресурс]. – Режим доступу :http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf.
4. The Economic Times / Cyber-crime costs up to $500 billion to world economy [Електронний ресурс]. Режим доступу: http://articles.economictimes.indiatimes.com/2013-07-23/news/40749590_1_cyber-crime-cyber-attacks-global-economy.
5. 2013 Internet Crime Report [Електронний ресурс]. – Режим доступу : http://www.ic3.gov/media/annualreport/2013_ic3report.pdf.
6. 2012 Norton Cybercrime Report // http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf.
7. The Global Information Technology Report 2014 / The Networked Readiness Index 2014 [Електронний ресурс]. – Режим доступу : http://www3.weforum.org/docs/GITR/2014/GITR_OverallRanking_2014.pdf.
8. Overview of current cyber attacks // Top 15 of Source Countries [Електронний ресурс]. – Режим доступу : http://www.sicherheitstacho.eu/?lang=en.
9. Динаміка проникнення Інтернету в Україні [Електронний ресурс]. – Режим доступу : http://www.kiis.com.ua/?lang=ukr&cat=reports&id=80.
10. Динаміка використання Інтернет в Україні [Електронний ресурс]. – Режим доступу : http://www.kiis.com.ua/?lang=ukr&cat=reports&id=199&page=2.
11. В Україні більше людей стало користуватися Інтернетом [Електронний ресурс]. – Режим доступу: http://espreso.tv/news/2014/05/22/v_ukrayina_bilshe_lyudey_stalo_korystuvatysya_internetom.
12. В Украине растет финансовая киберпреступность [Електронний ресурс]. – Режим доступу : http://news.finance.ua/ru/~/2/0/all/2013/12/15/314801.
13. Новый банковский троян Zberp обнаружен экспертами [Електронний ресурс]. – Режим доступу : http://bin.ua/news/finance/banking/156921-novyj-bankovskij-troyan-zberp-obnaruzhen.html.

УДК 339.72

Колінець Л.Б.
кандидат економічних наук,
доцент кафедри міжнародної економіки
Тернопільського національного економічного університету

ФІНАНСОВА КРИЗА В АЗІЇ: ПРИЧИНИ ТА УРОКИ

Стаття присвячена висвітленню причин виникнення та перебігу фінансової кризи в Азії у 1997–1998 рр. Показано, що криза поєднувала у собі елементи різних типів кризи: розпочавшись як валютна, вона перетворилася в банківську і боргову кризи. Проведено аналіз основних факторів, що вплинули на розвиток кризи в Азії. Охарактеризовано уроки, які можна винести з даної кризи в Азії, та проведено аналогію з кризою в ЄС.

Ключові слова: фінансова криза, боргова криза, фінансова система, платіжний баланс, іноземний капітал.

Колинец Л.Б. ФИНАНСОВЫЙ КРИЗИС В АЗИИ: ПРИЧИНЫ И УРОКИ

Статья освещает причины возникновения и течения финансового кризиса в Азии в 1997–1998 гг. Показано, что кризис сочетал в себе элементы различных типов кризиса: начавшись как валютный, он превратился в банковский и долговой кризис. Проанализированы основные факторы, повлиявшие на развитие кризиса в Азии. Охарактеризованы уроки, которые можно извлечь из данного кризиса в Азии, и проведена аналогия с кризисом в ЕС.

Ключевые слова: финансовый кризис, долговой кризис, финансовая система, платежный баланс, иностранный капитал.

Kolinets L.B. ASIAN FINANCIAL CRISIS: CAUSES AND LESSONS

The article deals with causes and flow of the financial crisis in Asia in 1997–1998. It is shown that the crisis combines the elements of different types of crisis: it begun as a currency, it has grown into the banking and debt crisis. It has been analysed the main factors that influenced on the development of the crisis in Asia. It has been characterized the lessons to be learned from this crisis in Asia, and the analogy with crisis in the EU.

Keywords: financial crisis, debt crisis, financial system, balance of payments, foreign capital.