

МІЖРЕГІОНАЛЬНА
АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ



СТАНОВЛЕННЯ І РОЗВИТОК УКРАЇНСЬКОЇ ДЕРЖАВНОСТІ

Випуск 13

Матеріали

*Міжнародної науково-практичної конференції
“Управління бізнесом в умовах глобальної нестабільності”
м. Київ, МАУП, 26 березня 2015 р.*

Київ
ДП “Видавничий дім “Персонал”
2015

*Схвалено Вченою радою Міжрегіональної Академії управління персоналом
(протокол № 2 від 25.02.15)*

Редакційна колегія:

А. М. Подоляка (голова), д-р юрид. наук., проф.;
А. А. Ігнатченко (заступник голови), канд. техн. наук;
О. В. Баєва, д-р біол. наук., проф.;
І. П. Бідзюра, д-р політ. наук, проф.;
М. Ф. Головатий, д-р політ. наук., проф.;
В. Б. Захожай, д-р екон. наук, проф.;
А. С. Лисецький, д-р екон. наук., проф.;
К. В. Муравйов, канд. юрид. наук., доц.;
І. П. Розпутенко, д-р наук держ. упр., проф.;
Л. В. Романова, д-р екон. наук, проф.;
В. Є. Сафонова, д-р екон. наук;
Г. П. Ситник, д-р наук держ. упр., проф.;
Ю. П. Сурмін, д-р соц. наук, проф.;
Н. М. Чернуха, д-р пед. наук., проф.

Матеріали подано в авторській редакції.

Відповідальність за зміст та орфографію матеріалів несуть автори.

Становлення і розвиток української державності : [зб. наук. пр.] /
МАУП. — К.: ДП “Видавничий дім “Персонал”, 2008 —

С76 Вип. 13: Матеріали Міжнар. наук.-практ. конф. “Управління бізнесом в умовах глобальної нестабільності”, 26 березня 2015 р. / редкол.: А. М. Подоляка (голова) [та ін.]. — 2015. — 300 с. : іл. — Бібліогр. у кінці ст.

У пропонованому збірнику подано тези учасників науково-практичної конференції, присвяченої проблемам реформування системи управління бізнесом в умовах розгортання кризових ситуацій та глобальної нестабільності.

Для науковців і громадсько-політичних діячів, керівників та власників бізнесу, студентів, а також усіх, хто цікавиться розвитком Української держави і бізнесу.

ББК 63.3(4УКР)я43+67.9(4УКР)301я43

ЗМІСТ

СТІЙКИЙ РОЗВИТОК БІЗНЕСУ В УМОВАХ НЕСТАБІЛЬНОСТІ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ

Баєва О. В.

Система менеджменту безпеки та охорони здоров'я як складова інтегрованого управління якістю на підприємствах 8

Мовчан А. В.

Кібернетична безпека України в умовах нестабільності національної економіки 12

Захожай В. Б., Колесник В. М.

Шляхи підвищення ефективності управління витратами феросплавних підприємств 16

Баєв В. В.

Економічне обґрунтування розвитку медичного туризму в Україні 19

Давидов О. І.

Управління розвитком підприємств: вартісно-орієнтований підхід 22

Тьорло В. О., Приходько Г. Г.

Проблеми управління інвестиційною діяльністю компанії з імпорту в Україну нафтопродуктів за умов нестабільності національної економіки 25

Таранець В. О.

Критерії класифікації моделей економічного зростання й розвитку 29

Лобов С. П.

Продуктовий підхід до економічної оцінки управлінських інформаційних систем 35

Лопатенко Л. О., Лопатенко Д. Б.

Розвиток ринку автосервісу України в сучасних умовах 38

Бородін М. Ю.

Забезпечення енергетичної безпеки національної економіки 42

Головач Н. В.

Розвиток системи управління персоналом на підприємстві в умовах кризи 45

Левченко М. О.

Удосконалення асортименту продукції підприємств громадського харчування за рахунок використання нових видів сировини 49

Берестецька Л. М.

Тенденції розвитку інтернет-бізнесу в Україні 54

Середюк К. В.

Вдосконалення механізму бізнес-планування діяльності підприємств України: організаційні аспекти 60

КІБЕРНЕТИЧНА БЕЗПЕКА УКРАЇНИ В УМОВАХ НЕСТАБІЛЬНОСТІ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ

Становлення і розвиток української державності, вип. 13, с. 12–15

У 2014 році Україна пережила безпрецедентне поєднання політичної, фінансово-економічної та банківської криз. Конфлікт на сході України разом із накопиченими у попередні роки макроекономічними дисбалансами зруйнували макрофінансову стабільність держави, зокрема: ВВП скоротився на 6,7 %; дефіцит Зведеного бюджету України перевищив 10 % від ВВП; інфляція зросла майже на 25 %; дефіцит зведеного платіжного балансу сягнув 13 млрд дол. США; банківська система втратила третину депозитів [1].

Серед негативних факторів, що обумовлювали економічні тенденції в минулому році, були: військові дії на сході України та розрив міжрегіональних зв'язків унаслідок анексії АР Крим; низький зовнішній попит унаслідок гальмування економічного зростання країн — основних торговельних партнерів; ускладнені торговельні відносини з Російською Федерацією; зниження купівельної спроможності населення внаслідок зменшення реальних доходів; погіршення фінансових результатів підприємств, звуження кредитної активності, скорочення державного фінансування та високий рівень невизначеності.

У цих умовах кіберзлочинність стає однією з найбільших загроз національній безпеці України, зокрема, значного впливу на суспільне життя та економіку в нашій країні набули глобальні інформаційні мережі (передусім мережа Інтернет), які отримали в науковій літературі назву “кіберпростір”.

У Великому тлумачному словнику сучасної української мови термін “Інтернет” тлумачиться як “всесвітня асоціація комп'ютерних мереж, інтегрована мережна “павутина”, яка складається з різних фізичних неоднорідних комунікаційних мереж, об'єднаних в єдину логічну архітектуру” [2, 402].

У проекті закону “Про внесення змін до Закону України “Про основи національної безпеки України” щодо кібернетичної безпеки України” кібернетичний простір (кіберпростір) визначається як середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [3].

Нині кіберпростір використовується злочинними та терористичними угрупованнями для незаконної торгівлі наркотиками, зброєю, розповсюдження дитячої порнографії, підготовки та здійснення терористичних актів

і збройної агресії проти України, проведення різного роду екстремістської діяльності (зокрема, пропаганди тероризму, насильства, жорстокості, расової, національної, релігійної нетерпимості), порушення авторських прав, а також промислового шпигунства, конкурентної розвідки тощо.

Кількість злочинів, що вчиняється у кіберпросторі, зростає пропорційно числу користувачів комп'ютерних мереж. За оцінками Інтерполу, темпи зростання злочинності в глобальній мережі Інтернет є найбільшими, порівняно з іншими видами злочинів, включаючи торгівлю наркотиками та зброєю. Щорічно глобальна кіберзлочинність обходиться планеті в 114 млрд доларів. Як стверджує Р. Ноубл, кіберзлочинність уже увійшла до переліку найбільш серйозних загроз з тих, з якими доводиться стикатися поліції [4, 75].

За даними НБУ на території України зареєстровано 132 банківські установи, що здійснюють емісію платіжних карток, функціонує 38461 банкомат, 205799 платіжних терміналів, в обігу знаходиться понад 69 млн платіжних карток, зареєстровано 56,5 млн держателів платіжних карток, сума операцій із використанням платіжних карток за квартал становить понад 271 млрд грн [5].

Для здійснення платіжних операцій за допомогою мережі Інтернет використовуються системи на основі банківських карток, смарт-карток, інтернет-банкінгу або “електронних” грошей. Найбільш популярними платіжними системами, які використовуються в мережі Інтернет, є: WebMoney Transfer, E-Gold, PayPal, Яндекс, Інтернет-гроші, Portmone.

Виділяються чотири групи відомостей, які найбільш часто піддаються нападу з використанням шкідливих програм: 1) доступ до різних фінансових операцій (онлайн-банкінг, платіжні картки, електронні гроші), інтернет-аукціонів тощо; 2) доступ до поштових скриньок, які є складовою частиною ICQ-акаунтів, як і всі знайдені на комп'ютері адреси електронної пошти; 3) паролі, коди доступу до інтернет-пейджерів, сайтів тощо; 4) паролі, коди до онлайн-ігр.

Останніми роками спостерігається тенденція до збільшення шахрайських дій у мережі Інтернет, у тому числі отримання персональної інформації (паролів, банківських рахунків або дамнів з інформацією про власників кредитних карт тощо), шляхом розсилки електронних листів від імені банку, які містять посилання на підроблені сайти, що імітують роботу справжніх — так званого “фішингу”. Цьому сприяло стрімке розповсюдження Інтернет-аукціонів, “фінансових пірамід”, використання небанківських електронно-платіжних систем.

Зафіксовано непоодинокі факти несанкціонованого списання коштів з рахунків підприємств, учиненого шляхом втручання в роботу систем віддаленого обслуговування клієнтів. Зокрема, у Дніпропетровській області викрито групу осіб, які з використанням мережі Інтернет здійснювали втручання в роботу автоматизованої електронної системи Інтернет-магазину “WebMoney. ua”. Зловмисниками шляхом несанкціонованої зміни інформації було сформовано 58 підроблених платіжних доручень, за якими з елек-

тронного гаманця зазначеного магазину перераховано на свій електронний гаманець понад 1 млн грн [4, 76–77].

Службою безпеки України припинено діяльність групи кібершахраїв, якими за останні п'ять років викрадено понад 250 млн доларів США. Хакери за допомогою вірусу отримували доступ до систем інтернет-банкінгу, після чого переводили кошти компаній на рахунки підставних фірм. Тільки в Україні від їхніх дій потерпіли більше 30 компаній [6]. Нещодавно українські хакери викрали в закордонних банках понад 40 млн доларів. До діяльності зазначеного угруповання причетні близько 20 громадян України, п'ятеро з яких були затримані співробітниками СБУ [7].

Значного розповсюдження набуло використання кіберпростору для здійснення конкурентної розвідки та промислового шпигунства. Завдяки високим технологіям шпигувати за чужими промисловими секретами стало набагато простіше, ніж 10–15 років тому. Сучасні ІТ-технології дають можливість на відстані відстежувати діяльність конкурентів, зокрема: сервіс SEMrush дозволяє аналізувати конкурентні сайти, джерела трафіку, ключові слова, за якими конкуренти просуваються в Google; SemanticForce моніторить інформаційне поле і медійну активність конкурентів не тільки в соціальних медіа, а й в онлайн-виданнях, відстежує активність співробітників компанії.

Нині для конкурентної розвідки використовують хмарні технології, SaaS системи і серверні ферми Google. Колишній агент ЦРУ Едвард Сноуден наглядно показав усьому світу, що сервери багатьох популярних сайтів постійно перебувають під контролем [8].

В умовах жорсткої конкурентної боротьби провідні промислові та фінансові організації для захисту конфіденційної інформації застосовують комплексні системи безпеки. Зокрема, з метою забезпечення комерційної таємниці, для нових розробок зазвичай використовують комп'ютери, в яких немає технічної можливості вставити флеш-накопичувач, а всередині їх немає жорсткого диску (вони підключені до серверів, розташованих в окремому захищеному приміщенні). Обмін інформацією з іншими користувачами здійснюється за допомогою одного комп'ютера, а робота з кресленнями, програмним кодом тощо — на іншому, не підключеному до мережі Інтернет.

Отже, забезпечення кібернетичної безпеки України в умовах нестабільності національної економіки є одним із важливих складових забезпечення національної безпеки України і потребує здійснення комплексу заходів організаційно-правового і технічного характеру.

Література

1. *Банківська система 2015: виклики та перспективи* [Електронний ресурс]. — Режим доступу: <http://www.bank.gov.ua/doccatalog/document?id=14741673>
2. *Великий тлумачний словник сучасної української мови* / [упоряд. і голов. ред. В. Т. Бусел]. — К., Ірпінь: ВТФ: Перун, 2001. — 1440 с.

3. *Про внесення змін до Закону України “Про основи національної безпеки України” щодо кібернетичної безпеки України: проект Закону України* [Електронний ресурс]. — Режим доступу: <http://zakon.nau.ua/doc/?uid=1206.832.0>
4. *Зима Л. М.* Протидія кіберзлочинності у банківській сфері: стан, проблеми та шляхи їх вирішення / Л. М. Зима // Протидія злочинам, які вчиняються з використанням комп’ютерних мереж: матеріали Міжнар. наук.-практ. конф., 1–2 жовт. 2010 р.: тези доп. — Суми: ДВНЗ “УАБС НБУ”, 2010. — С. 74–80.
5. *Загальні показники розвитку ринку платіжних карток в Україні* [Електронний ресурс]. — Режим доступу: http://www.bank.gov.ua/control/uk/publish/category?cat_id=79219
6. *Обезврежена* група хакерів [Електронний ресурс]. — Режим доступу: <http://kommersant.ua/doc/2160535>
7. *Україну* визнали центром світової кіберзлочинності [Електронний ресурс]. — Режим доступу: <http://tsn.ua/article/groshi/>
8. *Биленко Ж.* Как спрятать секреты компаний [Електронний ресурс]. — Режим доступу: <http://finance.obozrevatel.com/trends/51746-kak-spryatat-sekretyi-kompanij.htm>