Міністерство внутрішніх справ України
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

# ЕКОНОМІЧНА ТА ІНФОРМАЦІЙНА БЕЗПЕКА: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

***Матеріали***
***Міжнародної науково-практичної конференції***
*(м. Дніпро, 27 квітня 2018 р.)*

Дніпро
2018

УДК 33 + 004 + 351.741
Е 45

*Рекомендовано до друку*
*науково-методичною радою*
*Дніпропетровського державного*
*університету внутрішніх справ*
*(протокол № 8 від 17 квітня 2018 р.)*

**Е 45 Економічна та інформаційна безпека: проблеми та перспективи :** матеріали Міжнар. наук.-практ. конф. (м. Дніпро, 27 квіт. 2018 р.). – Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. – 276 с.

ISBN 978-617-7665-14-3

Збірник містить матеріали однойменної міжнародної науково-практичної конференції. У заході взяли участь науковці, викладачі та здобувачі вищих навчальних закладів та наукових установ України і зарубіжжя, а також фахівці-практики правоохоронних органів. Тематика публікацій охоплює актуальні питання економічної та інформаційної безпеки.

Матеріали конференції можуть бути використані в науково-дослідній роботі та навчальному процесі спеціалізованих ВНЗ, а також у законотворчості та правоохоронній діяльності.



*Факти, судження й висновки, викладені авторами публікацій,*
*не завжди підтверджуються та поділяються редакційною колегією.*

ISBN 978-617-7665-14-3 УДК 33 + 004 + 351.741

## ЗМІСТ

***Шановні гості та учасники конференції!***

Радий Вас вітати від імені науково-педагогічного колективу Дніпропетровського державного університету внутрішніх справ та від себе особисто на Міжнародній науково-практичній конференції «Економічна та інформаційна безпека: проблеми та перспективи». Статус заходу є міжнародним і це підтверджує актуальність питань, що нами розглядаються.

Сучасний вік - вік інформації - не тільки відкриває можливості, а й ставить нові завдання та потребує вирішення нових проблем. Тому необхідно адекватно реагувати на подібні виклики. Можна сміливо стверджувати, що економічна та інформаційна небезпека перетворилася на один з найбільш небезпечних видів загроз, і свідченням цього є постійне обговорення проблем економічної та інформаційної безпеки як науковою спільнотою, практиками, так і на офіційних зустрічах на найвищому політичному рівні.

Наш університет має певні досягнення в цьому напрямі. За останній час створений економіко-правовий факультет для підготовки курсантів для підрозділів захисту економіки Національної поліції за спеціалізацією фінансово-економічна безпека. Відкриті нові спеціальності для підготовки студентів в області менеджменту із спеціалізацією «економіко-фінансова безпека» і економіки із спеціалізацією «захист економіки».

Зважаючи на сучасні реалії, тема нашого обговорення є надзвичайно актуальною, глибокою і водночас складною.

Складність і глобальний характер завдань вимагають розробки ґрунтовного наукового супроводження і консолідації зусиль представників наукової спільноти.

Отже, виходячи з зазначеного, сьогоднішній науковий захід має на меті обговорити такі питання:

- інформаційно-правові проблеми безпеки;
- використання інформаційних технологій в діяльності поліції;
- забезпечення інформаційної безпеки;
- науково-методичні, нормативно-правові та програмно-технічні аспекти безпеки у інформаційній та економічній сфері;
- сучасний стан, проблеми та перспективи розвитку фінансової та економічної безпеки підприємств, регіонів, суспільства;
- корупційні ризики в економічній сфері;
- попередження та розслідування економічних злочинів;
- вітчизняний та зарубіжний досвід підготовки фахівців з фінансово- економічної та інформаційної безпеки.

Саме для отримання відповідей на ці проблемні питання та удосконалення практичних і теоретичних навичок проводиться цей захід.

Завдяки присутності на заході фахівців різних сфер науки і практики, а

саме – економіки, менеджменту, інформаційних технологій, економічної та інформаційної безпеки, юриспруденції, бізнесу та правоохоронних органів ми маємо виняткову можливість перейняти позитивний досвід у зазначеній сфері, а також поділитися власним досвідом.

Переконаний, що наукова дискусія при обговоренні визначених питань матиме глибокий та плідний характер і сприятиме розвитку вітчизняної науки, подальшому підвищенню рівня протидії злочинності в економічній та інформаційній сферах.

Від імені оргкомітету конференції хочу щиро подякувати вам за те, що знайшли час прийняти участь у конференції з цієї, безперечно актуальної на сьогодні проблематики.

Особливо хочу завдячити шановним гостям конференції, які прибули до Дніпропетровського державного університету внутрішніх справ зі Львова, Харкова, Сєвєродонецька, Запоріжжя, Одеси. У дистанційному відео-форматі з нами на зв'язку будуть Кишинів, Київ, Харків, Одеса. Очікуємо на включення зі Сполучених Штатів Америки. Взагалі на конференцію надійшли матеріали 72 учасників, серед яких 60 вчених, 16 представників практичних підрозділів, в тому числі з Польщі, Молдови та Білорусі.

Висловлюю вдячність учасникам міжнародної конференції, бажаю всім плідної співпраці та сподіваюся на те, що ми отримаємо професійне задоволення від результатів нашої роботи.

*Ректор Дніпропетровського*
*державного університету*
*внутрішніх справ*
***Фоменко Андрій Євгенович***

**Фоменко Андрій Євгенович,**
к.ю.н., ректор Дніпропетровського державного
університету внутрішніх справ

**Вишня Володимир Борисович,**
д.т.н., проф., професор кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

**Бойко Дмитро Дмитрович,**
к.ю.н., начальник ТСЦ-12/42
по Дніпропетровській області

**Гавриш Олег Степанович,**
викладач кафедри економічної
та інформаційної безпеки Дніпропетровського
державного університету внутрішніх справ

# ПЕРЕДАЧА ВІДЕОПОТОКІВ В СИСТЕМІ УПРАВЛІННЯ МОБІЛЬНИМИ НАРЯДАМИ ПАТРУЛЬНОЇ СЛУЖБИ

Реформування правоохоронних органів і створення патрульної поліції є найбільш важливою і вдалою реформою, що здійснив наш уряд за останні роки. Розбудова мобільних патрульних нарядів Національної поліції України, які першими реагують на виклик про допомогу, або повідомлення про вчинене правопорушення чи злочин є дієвим викликом в протидії злочинності в побутових умовах та на вулицях міст і селиш.

Разом з тим, незважаючи на існуючу скорочену система підготовки патрульних поліцейських, постійно відчувається їх нестача. Крім того, не завжди якісно здійснюється керівництво мобільними патрульними нарядами зі сторони диспетчера із-за відсутності у останніх відеоінформації з міста події та дій поліцейських при виконання завдання. Вирішення цього питання стане дієвою допомогою патрульним нарядам.

Найбільш вдосконаленим технічним рішенням даної проблеми є створення системи централізованого управління нарядами патрульної служби (“ЦУНАМІ”), що являє собою комплекс апаратних та програмних засобів, а також персоналу, призначений для управління силами й засобами мобільних нарядів поліції. Він включає пов’язані між собою блоки оператора 102, диспетчера, чергового районного відділу поліції, та обладнання автопатруля у вигляді блока керування та відображення (у подальшому – планшет) з системою супутникового GPS-позиціонування і особистого відеорегістратора патрульного. Диспетчер системи є оперативним черговим і куратором кожного конкретного райвідділу поліції, відповідального за організацію реагування на злочини та пригоди в рамках району. Оператор 102 здійснює прийняття і ре-

єстрацію повідомлень про злочини та події, виконує попередню їх кваліфікацію. Заповнена оператором 102 електронна картка надходить до диспетчера - чергового відповідального за управління мобільними нарядами поліції, де призначається екіпаж мобільного патруля для реагування на сповіщення, що надійшло. Одночасно електрона картка поступає черговому районного відділу поліції, до території якого відноситься звернення, де повідомлення громадян реєструється у журналі "Єдиного обліку злочинів і правопорушень районного управління".

Як вказувалося вище, при ефективної взагалі роботи системи проявляється суттєвий недолік – відсутня можливість у диспетчера оперативно відслідковувати ход подій та дії патрульного безпосередньо при виконанні отриманого їм завдання. Тим самим виключається можливість у чергового диспетчера, в разі необхідності, вмішуватися в хід виконання завдання нарядом, оперативно коригувати дії наряду, виключити випадки некваліфікованих дій патрульних.

В основу вдосконалення системи управління нарядами мобільної патрульної служби пропонується, шляхом уведення нових зв'язків елементів, забезпечити можливість відображення у диспетчера інформації, яка попадає у поле зору об'єктиву відеорегістратора патрульного. Це дозволяє диспетчеру в режимі реального часу оперативно контролювати дії патрульного поліцейського в процесі відпрацювання поставленого завдання і, при необхідності, своєчасно втручатися в його роботу, і за рахунок цього підвищити ефективність та безпеку діяльності патрульного наряду.

Поставлена задача вирішується тим, що у відомій системі централізованого управління нарядами патрульної служби, що включає пов'язані між собою блоки оператора 102, чергового районного відділу поліції, диспетчера, планшет мобільного патрульного наряду з системою супутникового GPS-позиціонування та блок особистого відеорегістратора патрульного, вводяться канали передачі відеопотоків, якими сполучено відповідно блок особистого відеорегістратора патрульного до планшету мобільного патрульного наряду, від нього – до блоку диспетчера з можливістю висвітлення кожномоментно на моніторі диспетчера місця події з об'єктиву особистого відеорегістратора патрульного при відпрацюванні завдання [1].

На рис. 1 представлена схема удосконаленої системи управління нарядами мобільної патрульної служби, яка включає блок 1 оператора 102, вхід якого приєднаний до телефонної мережі зв'язку, а виходи підключені відповідно до першого входу блока 2 диспетчера та першого входу блока 3 чергового райвідділу поліції, другий вхід якого зв'язаний з телефонною мережею зв'язку. В той же час, вихід блоку 3 чергового райвідділу поліції підключений до другого входу блока 2 диспетчера, третій вхід якого (сумісний з виходом) зв'язаний з планшетом 4 мобільного патрульного наряду, до якого приєднаний перший канал передачі відеопотоку 6 від особистого відеорегістратора патрульного 5 та другий каналу передачі відеопотоку 7 планшету 4 до блоку диспетчера 2.

Система реалізується в такий спосіб. Сповіщення поліції про злочини

та події або виклик допомоги, що здійснюються за телефоном 102, приймаються і обробляються оператором 102 (блок 1). В результаті створюється електронна картка повідомлення, яка відразу надходить до диспетчера 2 – чергового відповідального за управлінням мобільними нарядами патрульної поліції, який призначає вільний екіпаж мобільного патруля для реагування на повідомлення. Одночасно, електронна картка повідомлення надсилається черговому (блок 3) райвідділу поліції, до території якого відноситься звернення, яке реєструється у журналі Єдиного обліку злочинів і правопорушень райвідділу. Слід відмітити, що повідомлення громадян може поступити безпосередньо на телефон чергової частини райвідділу (блок 3). В цьому разі воно реєструється в журналі райвідділу і пересилається до оперативного диспетчера (блок 2) для реагування.

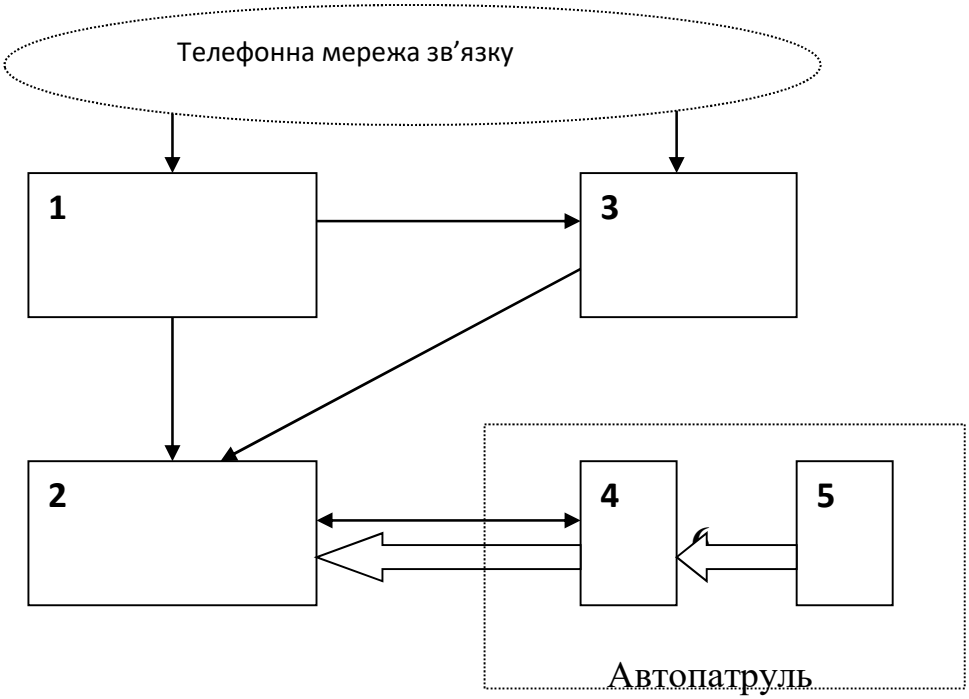



*Рис. 1. Удосконалена система управління нарядами мобільної патрульної служби*

Виділений диспетчером 2 мобільний патрульний наряд (автопатруль) приступає до виконання отриманого завдання. На протязі усієї роботи екіпаж за допомогою планшету 4 підтримує голосовий або автоматичний зв'язок з диспетчером (блок 2), відмічає етапи виконання завдання. Зокрема, після прибуття наряду на місце вказане в повідомлені громадян в планшеті 4 фіксується час прибуття і патрульним активізуються канали передачі відеоінформації 6 і 7 відповідно між особистим відеорегістратором 5 патрульного і планшетом 4, та між планшетом 4 і блоком 2 диспетчера. С цього моменту по цім каналам диспетчеру передається відеоінформація, яка попадає в об'єктив відеорегістратора 5 патрульного. По завершенню виконання завдання в

планшеті 4 робиться відповідна відмітка і канали передачі відключаються.

З метою зменшення витрат на експлуатацію системи доцільно побудувати перший канал передачі 6 в стандарті “Wi-Fi” (безкоштовне користування), а другий канал передачі 7 – на платформі 4G або 5G.

Перевагою запропонованої системи управління нарядами мобільної патрульної служби є можливість диспетчера системи спостерігати в режимі “On Line” за місцем події або злочину і діями патрульних, корегуючи їх при необхідності, рекомендувати вірні управлінські рішення.

Разом з тим запропонована система управління відеоканалами має певні недоліки, зокрема, в існуючої системі управління відсутня можливість автоматичного включення каналів передачі відеопотоків по прибуттю наряду на місце події, що не дозволяє виключити вплив людського фактору при активізації каналів системи**.**

З метою подальшого вдосконалення системи управління нарядами мобільної патрульної служби, нами пропонується ввести додаткові нові елементи, які забезпечать можливість автоматичного включення каналів передачі відеопотоків і відображення на моніторі у диспетчера інформації, з об’єктиву особистого відеорегістратора патрульного при відпрацювання завдання, залишив, при цьому, можливість особистого управління цими каналами диспетчеру і патрульному.

Для цього, у відомій системі управління нарядами мобільної патрульної служби, вводиться блок прийому координат (адреси) події (завдання), вхід якого підключено до першого виходу диспетчера, а вихід блоку прийому координат події зв’язаний с другим входом модуля порівняння, перший вхід якого підключений до виходу системи супутникового GPS-позиціонування, а вихід модуля порівняння підключено до першого входу логічної схеми АБО, другий вхід якої приєднаний до виходу планшету, а третій – до другого виходу диспетчера, при тому, що вихід логічної схеми АБО підключений до входу блока формування сигналу на відкриття першого і другого каналів передачі відеопотоків, вихід якого приєднаний до першого входу планшету, другий вхід якого підключено до виходу блока формування сигналу на закриття першого і другого каналів передачі відеопотоків, а вхід його зв’язаний з третім виходом блока диспетчера.

На рис. 2 представлена схема запропонованої системи управління нарядами мобільної патрульної служби. Вона включає блок 1 оператора 102, вхід якого приєднаний до телефонної мережі зв’язку, а перший та другий виходи підключені відповідно до першого входу блока 2 диспетчера та першого входу блока 3 чергового райвідділу поліції, другий вхід якого зв’язаний з телефонною мережею зв’язку. В той же час, вихід блоку 3 чергового райвідділу поліції підключений до другого входу блока 2 диспетчера, третій вхід якого (сумісний з виходом) приєднаний до планшету 4 мобільного патрульного наряду, який оснащений системою 8 супутникового GPS-позиціонування, та на якому побудовано перший канал передачі відеопотоку 6 від особистого відеорегістратора патрульного 5 до планшету 4 та другий канал передачі відеопотоку 7 від планшету 4 до блоку диспетчера 2.

Крім того система додатково включає блок 9 прийому координат (адреси) події (завдання), вхід якого підключено до першого виходу блоку 2 диспетчера, а вихід блоку 9 прийому зв'язаний с другим входом модуля порівняння 10, перший вхід якого підключений до виходу системи 8 супутникового GPS-позиціонування, а вихід модуля порівняння 10 підключено до першого входу логічної схеми АБО 11, другий вхід якої приєднаний до виходу планшету 4, а третій – до другого виходу блоку 2 диспетчера, при тому, що вихід логічної схеми АБО 11 підключений до входу блока 12 формування сигналу відкриття першого 6 і другого 7 каналів передачі відеопотоків, вихід якого поступає на перший вхід планшету 4, другий вхід якого підключено до виходу блока 13 формування сигналу закриття першого 6 і другого 7 каналів передачі відеопотоків, вхід якого зв'язаний з третім виходом блоку 2 диспетчера.

Система реалізується в такий спосіб. Сповіщення поліції про злочини та події, або виклик допомоги, що здійснюються за телефоном 102, приймаються і обробляються оператором 102 (блок 1). В результаті створюється електронна картка повідомлення, яка відразу надходить до блоку 2 диспетчера – чергового відповідального за управлінням мобільними нарядами патрульної поліції, який призначає вільний екіпаж мобільного патруля для реагування на повідомлення. Одночасно, електронна картка повідомлення надсилається черговому (блок 3) райвідділу поліції, до території якого відноситься звернення, яке реєструється у журналі "Єдиного обліку злочинів і правопорушень" райвідділу. Слід відмітити, що повідомлення громадян може поступити безпосередньо на телефон чергової частини райвідділу (блок 3). В цьому разі воно реєструється в журналі райвідділу і пересилається до оперативного диспетчера (блок 2) для реагування.

Виділеному диспетчером 2 мобільному патрульному наряду (автопатруль) пересилається на планшет 4 завдання та на блок 9 прийому координати місця події. Наряд приступає до виконання отриманого завдання. Місце знаходження наряду постійно відслідковується системою 8 супутникового GPS-позиціонування і відповідний сигнал подається на перший вхід модуля порівняння 10.

По прибутті наряду на місце вказане в повідомлені громадян в планшеті 4 фіксується час прибуття, а сигнали на обох входах модуля порівняння 10 співпадають і на його виході формується сигнал, який поступає на перший вхід логічної схеми АБО 11 і далі на вхід блоку 12 формування сигналу відкриття каналів передачі відеопотоків. По прибутті наряду на місце вказане в повідомлені громадян в планшеті 4 фіксується час прибуття, а сигнали на обох входах модуля порівняння 10 співпадають і на його виході формується сигнал, який поступає на перший вхід логічної схеми АБО 11 і далі на вхід блоку 12 формування сигналу відкриття каналів передачі відеопотоків.

На виході блока 12 формується сигнал, який поступає на перший вхід планшету 4 і автоматично активізуються канали передачі відеопотоків 6 і 7 відповідно між особистим відеорегістратором 5 патрульного і планшетом 4 та між планшетом 4 і блоком 2 диспетчера.

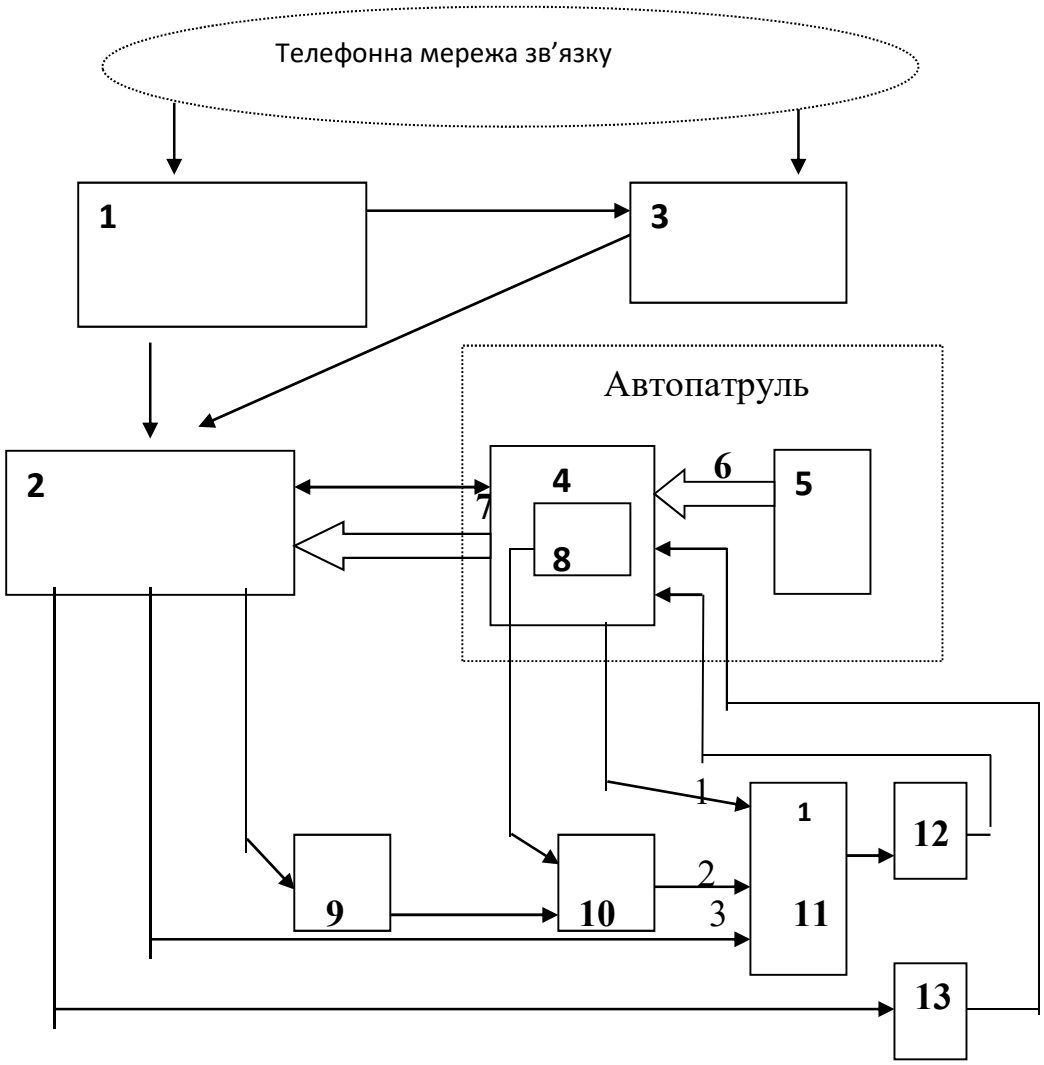



*Рис.2. Модернізованна система управління нарядами мобільної патрульної служби*

С цього моменту на монітор диспетчера передається відеоінформація місця події з об'єктиву особистого відеорегістратора 5 патрульного. По завершенню виконання завдання в планшеті 4 робиться відповідна відмітка, яка надсилається в блок 2 диспетчеру, з третього виходу якого, через блок 13 формування сигналу закриття каналів передачі відеопотоків, на другий вхід планшету 4 поступає сигнал на відключення каналів 6 і 7 передачі відеопотоку.

Слід відмітити, що окрім автоматичного включення каналів передачі відео потоків 6 і 7, система допускає особисту активізацію каналів 6 і 7 за командою диспетчера подачею сигналу з другого виходу блока 2 диспетчера на третій вхід логічної схеми АБО 11 і далі, з її виходу, через блок 12 формування сигналу відкриття каналів передачі відеопотоків, на перший вхід планшету 4, та – за командою патрульного подачею сигналу з виходу планшету 4 на другий вхід логічної схеми АБО 11 і далі, з її виходу, через блок 12 формування сигналу відкриття каналів передачі відеопотоків, на перший вхід планшету 4.

Перевагою запропонованої системи управління нарядами мобільної патрульної служби є можливість автоматичного включення каналів передачі відеопотоків з міста події або злочину до диспетчера, бо, інколи, патрульним приходиться негайно вмішуватися в ліквідацію обставин, що виникли при правопорушеннях. Важливим аспектом діяльності системи є також можливість, у любий момент, активізувати канали передачі відеопотоків безпосередньо командою диспетчера або патрульного, що посилює надійність функціонування визначеної операції системи. Також надійність роботи каналів зв'язку підвищиться за рахунок повного впровадження на території України стандарту 4G, а згодом і 5G, який має не тільки швидкісну перевагу але буде покриватиме усю територію країни, а не лише великі міста. Цього вимагало Міністерство інфраструктури України. В умовах видачі ліцензії обов'язково необхідно вказати, що компанія зобов'язана покрити всю територію України. В чому у нас є проблема з 3G – оператори обирають найбільш рентабельні об'єкти: міста чи невеликі містечка, а села і дороги просто забувають. «Дороги у нас не повністю покриті», - наголосив Володимир Омелян [2], а згодом така вимога була прописана в тендерній документації. Тому незабаром якісний зв'язок буде і в селах, і в горах, і, що найголовніше, на всіх дорогах країни що значно підвищить якість реагування Національної поліції. А при запровадженні стаціонарних станцій 4G в автомобілях Національної поліції, швидкість роботи каналів зв'язку 6 та 7 збільшиться до 1 Гігабіт/сек, що дасть змогу швидкісного відеозв'язку у любій точці України та дозволить більш якісно реагувати на всі ситуації де доступ до інформації відіграє важливу і необхідну роль в роботі Національної поліції України.

1. Система управління нарядами мобільної патрульної служби /Вишня В.Б., Глуховеря В.А., Золотоноша О.В., Рижков Е.В.// Патент України на корисну модель № 118449. Україна. Заявка № u201701677, МПК H04B 1/04. Бюл. №15, 10.08.2017.

2. Мобільних операторів необхідно зобов'язати покривати всю територію України якісним зв'язком. –Володимир Омелян // Міністерство інфраструктури України [Електронний ресурс]. –Режим доступу: https://mtu.gov.ua/news/28853.html.

**Andriichenko Zhanna Olehivna**
PhD, Associate Professor
of Simon Kuznets Kharkiv
National University of economics

## THE INTERNATIONAL ASSESSMENT OF ANTI-MONEY LAUNDERING AND TERRORISM FINANCING SYSTEM IN UKRAINE

At the beginning of 2018 MONEYVAL declared the results of the Fifth Round Mutual Evaluation in Ukraine, which had continued from 2016.

MONEYVAL – the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism is a permanent monitoring

body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards to counter money laundering and the financing of terrorism and the effectiveness of their implementation, as well as with the task of making recommendations to national authorities in respect of necessary improvements to their systems. Through a dynamic process of mutual evaluations, peer review and regular follow-up of its reports, MONEYVAL aims to improve the capacities of national authorities to fight money laundering and the financing of terrorism more effectively.

The system of mutual assessments is based on the special FATF Methodology for assessing technical compliance with the FATF Recommendations and the effectiveness of Anti-Money Laundering and the Counter-Financing of Terrorism systems.

The Methodology relates to two assessment components of FATF international standards implementation: 1) technical compliance; 2) results, indicators, data and other factors, which are used for measures implementation effectiveness assessment.

According to Methodology, effectiveness is the key component in the compliance degree assessment of the country by FATF international standards. The assessment process should consider the effectiveness evaluation and technical compliance as well. The effectiveness evaluation is aimed at attention increasing to results and the determination of what goals of FATF international standards has been achieved by National System AML/CFT, and detection of system disadvantages. It enables countries to pay priority attention to their systems improving measures.

Consequently, the summary MONEYVAL Report clarifies the state of technical compliance and the effectiveness of anti-money laundering, terrorism financing, and weapons of mass destruction proliferation countering measures in Ukraine.

This international document presents the analysis of Ukrainian legislation level of compliance to actual FATF recommendations, practicality and effectiveness assessment of the financial monitoring system in Ukraine, and gives the recommendations for its improving.

The general result, which was conducted on the Fifth Round Mutual Evaluation of financial monitoring system in Ukraine, is positive. It was stated in prepared MONEYVAL Report that Ukraine is reliable jurisdiction in anti-money laundering, terrorism financing, and weapons of mass destruction proliferation countering and doesn't need to conduct special measures by Council of Europe Committee MONEYVAL and FATF [2].

Taking into account that Ukraine has been in "black" and "grey" FATF lists twice, this result proves the certain progress in national financial monitoring system construction.

It was determined by the technical compliance assessment results that Ukrainian legislation totally meets (Compliant) 12 FATF Recommendations, mainly meets (Largely compliant) 20 of them, partly meets (Partially compliant) 7 and the only 1 Recommendation isn't used in Ukraine (Non-compliant) [1].

By the level of effectiveness, according to established ratings, Ukraine got the grade "Substantial" for 2 results, the grade "Moderate" for 8 results and a "Low" score for 1 indicator [1].

The main MONEYVAL remarks were aimed at the necessity of effectiveness increasing:

– law enforcement system, particularly in the improving of practical measures for investigation criminal proceedings, arresting and criminal proceeds confiscation;

– the measures for regulation and supervision of non-financial institutions and professions;

– the procedure implementation for checking the reliability of the data on the final beneficial owners;

– the measures for the prevention and counteraction of terrorism financing and awareness of private and non-profit sectors with corresponding threats, vulnerability and risks, which are related to their professional activity;

– the measures for comprehensive, authentic and continuous administrative reporting in the field of financial monitoring;

– transformation of legislation base relative to crimes of terrorism financing and targeted financial sanctions to the international standards, etc.

Comments and suggestions of MONEYVAL Committee for Ukraine mostly are corresponded with the results of National risks assessment in the field of preventing and countering legalization (laundering) of proceeds of crime and financing of terrorism (NRA) 2016, which were made by State Financial Monitoring Service, for example, for corruption risks, organized crimes, high cash flow, terrorism manifestations, the absence of sector assessment of financial sector risks, inefficient sanction policy, the activity of law enforcement system, etc. [5].

In accordance to the Fifth Round Mutual Evaluation Report, Ukraine faces considerable money laundering risks due to the corruption and illegal economic activities, including fictitious entrepreneurship, tax evasion and fraud. The sheer size of the shadow economy exacerbated by the widespread use of cash makes the country especially vulnerable. Among the prevalent mechanisms to launder money in Ukraine are the so-called conversions centers through which funds are siphoned from the real to the shadow economy, and which are used to convert proceeds into cash and transfer them out of the country [2].

Since the last evaluation in 2009, Ukraine has taken a number of welcome steps, namely the adoption of a dedicated law in 2014 strengthening the procedure of financial monitoring and enhancing efforts to fight corruption through the establishment of the National Anti-Corruption Bureau of Ukraine (NABU) and the National Corruption Prosecutors Office. Other positive initiatives, the report reads, include "very significant efforts" by the National Bank of Ukraine to remove criminals from having controls of banks, and the successful development of complex money laundering cases [2].

It should be emphasized that Ukraine is at the same level with such FATF countries-members like Australia, the USA, Canada, Singapore, Denmark, Sweden and Switzerland in the rating of monitoring mode.

For the comparison, there were considered the Mexican and Portuguese reports of Mutual Evaluation at the regular FATF Plenary Session (1-3/10/2017). Following the discussion, Mexico got the enhanced monitoring with the necessity to yearly account to FATF Plenary Session. The Portuguese National System AML/CFT was recognized as sufficiently efficient and the country will present the information about its progress in three years. Delegates also admitted the significant progress of Austria, Brazil and Uganda in conformity to Recommendations.

According to results of FATF Plenary Session, the "black" list of FATF remained unchanged: Iran and North Korea (countermeasures are used only in North Korea). The "grey" list replenished with Trinidad and Tobago, Tunisia and Sri-Lanka. This list includes Bosnia and Herzegovina, Vanuatu, Iraq, Yemen Syria and Ethiopia for December 2017.

On the 6th April, 2018, FATF published the summary table of ratings, which were formed by the results of Mutual Assessments of National Systems AML/CFT, which were made by FATF and regional groups like FATF by Technical Conformity to FATF Recommendations Evaluation Methodology and systems effectiveness AML/CFT in the editorial office 2013 [1].

The National Systems of 47 countries has been already assessed by the new Methodology by now.

In the part of Technical Compliance to FATF Recommendations Assessment, which represents the biggest interest for Ukrainian financial market (R1 "Risks evaluation and the application of risk-oriented approach", R10 "Proper customer verification", R11 "Data storage", R13 "Correspondent banks", R14 "The services of funds and valuables transferring", R16 "E-transfers of money", R17 "Trust in third-party measures", R18 "Internal control, foreign affiliates and subsidiaries", R26 "Regulation and financial institutions supervision", R27 "Empowering of supervisory authorities" and R35 "Sanctions"), the countries got the following ratings:

Countries were able to demonstrate the best results in the part of compliance to R11, R13 and R14: only Australia didn't conform to R13among all the FATF countries-members.

The highest scores for all three recommendations were assigned to Armenia, Cuba, Honduras, Fiji, Macao, China, Spain and Trinidad and Tobago.

The low ratings for R1, R16 and R35 were obtained by almost all the countries. Spain was the only one country that was able to demonstrate that its legislation base properly fixes the responsibilities by risks assessment AML/CFT and application of risk-oriented approach. It is necessary to notice that R1 is "cross-cutting" recommendation: rating, which was obtained for R1 compliance, usually influences on the ratings for conformity to other FATF Recommendations. Rating for partly compliance to R1 was gotten by Australia, Austria, Armenia, Denmark, Norway, Serbia, Slovenia and the USA [1].

It is noticeable that ratings of compliance and significant compliance to R16 was obtained by Austria, Bahama, Barbados, Bhutan, Armenia, Costa Rica, Cuba, Ethiopia, Fiji, Jamaica, Macao, China, Malaysia, Nicaragua, Mongolia, Panama,

Singapore, Trinidad and Tobago, Tunisia, Spain, Ukraine at the same time when Australia, Belgium, Denmark, Canada, Norway, Italy, Portugal, the USA, Switzerland and Sweden got the rating for partly compliance.

Most countries failed to demonstrate the sufficient conformity and restrictive kind of sanctions, which can be used to the people who don't meet the requirements of legislation (AML/CFT): the rating of compliance to R35 was obtained only by Austria, Macao, China, Slovenia and Spain.

According to summary results gotten by estimated countries, which present the level of FATF standards performance effectiveness, the lowest ratings were assigned for IO 3 (the financial sector and DNFBP sector supervision) and IO 4 (financial sector and DNFBP requirements to AML/CFT sector supervision). Hence, no country got the high-level rating, 6 countries got the rating of substantial effectiveness level of IO 3 (Ireland, Spain, Canada, Macao, China and Malaysia) and only Armenia got the rating for IO 4 of substantial efficient level [1].

Therefore, according to the Fifth Round Mutual Evaluation, Ukraine significantly improved the effectiveness of financial monitoring system at the global level. Hence, it should be emphasized that, according to the results of evaluation, MONEYVAL Committee approved the significant level of operational and institutional ability of national Financial Intelligence Unit – State Financial Monitoring Service – in all the rating parameters.

However, the number of problems still exists and needs the solution. Ukraine must report back to MONEYVAL at the first Plenary in 2019 about the implementation of its recommendations under enhanced follow-up procedures.

Thereby, State Financial Monitoring Service starts the process of the Action Plan preparation in order to continue the improving of financial monitoring system in Ukraine, according to the results of the MONEYVAL Fifth Round Mutual Evaluation.

However, drawing up the Action Plan it should be noticed that the population access increasing to financial services is still the priority for FATF and highly cautious approach to the prevention measures of AML/TF can cause the unwanted exclusion of legal business and the number of customers in official financial system.

---

1. An up-to-date overview of the ratings on both effectiveness and technical compliance for all countries assessed against the 2012 FATF Recommendations and using the 2013 Assessment Methodology [Electronic resource]. – Access mode : http://www.fatf-gafi.org/media/fatf/documents/4th-Round-Ratings.pdf.

2. Fifth Round Mutual Evaluation Report on Ukraine [Electronic resource]. – Access mode : https://rm.coe.int/fifth-round-mutual-evaluation-report-on-ukraine/1680782396.

3. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation [Electronic resource] : The FATF Recommendations. February 2012. – Access mode : http://www.fatf-gafi.org/media/fatf/documents / recommendations/ pdfs/FATF_Recommendations.pdf.

4. Methodology for assessing technical compliance with the FATF Recommendations and the effectiveness of AML/CFT systems [Electronic resource]. – Access mode : http://www.fatf-gafi.org/media/fatf/documents/methodology /FATF%20Methodology%2022%20Feb%202013.pdf

5. National Risk Assessment Report [Electronic resource]. – Access mode : http://www.sdfm.gov.ua/content/file/Site_docs/2017/20170113/nra.pdf.

**Баранник Лілія Борисівна**
д.е.н., проф., завідувач кафедри
оподаткування та соціального забезпечення
Університету митної справи та фінансів,
м. Дніпро

# РОЗВИТОК МЕДИЧНОГО СТРАХУВАННЯ В УКРАЇНІ ЯК ФАКТОР ПОСИЛЕННЯ СОЦІАЛЬНО-ЕКОНОМІЧНОЇ БЕЗПЕКИ

Соціально-економічна безпека країни нерозривно пов’язана зі станом здоров’я її населення. Поняття «здоров’я» має набагато глибший зміст, ніж зазвичай думають. У Преамбулі статуту ВООЗ (1948р.) поняття «здоров’я» визначено, як стан повного фізичного, духовного та соціального благополуччя, а не лише відсутність хвороб і фізичних дефектів. Розглядаючи людину як цілісну систему, виділяють такі види здоров’я: фізичне, психічне, моральне, соціальне. Порушення будь-якого з них негативно впливає на якість життя, на стан суспільних відносин.

Охорона здоров’я населення в будь-якій розвиненій країні є найбільш пріоритетною задачею держави. Україна дотримується цього курсу. У Законі України «Основи законодавства України про охорону здоров'я» говориться, що «кожна людина має природне невід'ємне і непорушне право на охорону здоров'я. Суспільство і держава відповідальні перед сучасним і майбутніми поколіннями за рівень здоров'я і збереження генофонду народу України, забезпечують пріоритетність охорони здоров'я в діяльності держави, поліпшення умов праці, навчання, побуту і відпочинку населення, розв'язання екологічних проблем, вдосконалення медичної допомоги і запровадження здорового способу життя» [1].

Разом з тим, сучасний стан охорони здоров’я в Україні є вкрай незадовільним. За даними ВООЗ, Україна ввійшла в так звану «червону зону». За рік від неінфекційних захворювань в Україні померло 605 тис. осіб, що становить приблизно 90% від усіх смертей [2]. В 2017 році, за рейтингом британського аналітичного центру «The Legatum Institute», за рівнем охорони здоров’я наша країна зайняла 135 місце з 148 можливих (в 2016 р. – 107 місце, в 2015 р. – 70 місце) [3, с.61]. За даними Світового банку, витрати 7% ВВП на медицину в Україні не відповідають якості послуг [4].

Такі оцінки визнаних міжнародних організацій небезпідставні. Близько 2/3 бюджетних коштів, які виділяються в нашій країні на охорону здоров’я, йдуть на утримання медичних закладів, непотрібних приміщень та оплату праці лікарів. Без перебільшення можна сказати, що наразі медицина є найбільш корумпованою сферою соціального буття. Наразі в тіньовому секторі медичної галузі знаходиться 3,5% ВВП (і не зрозуміло, чому держава не може залучати ці тіньові кошти). Бідність основної частини населення не дозволяє йому отримувати своєчасне й якісне медичне обслуговування за рахунок добровільного медичного страхування. Поганий стан здоров’я грома-

дян, «тіньова медицина» й інші вади сфери охорони здоров'я криють в собі значні загрози як для соціального здоров'я українського суспільства, так і для економічного розвитку країни. Економіка несе значні людські й матеріальні втрати через лікарняні, інвалідність й смертність. Тривалість життя українця майже на десять років менше, ніж іспанця або канадця. Очікувана тривалість життя українця – 66,3, а українки – 76,1 року. Ризик для чоловіка померти у віці до 60 років – 40%, тоді як в Швейцарії не доживають до 60 років всього 8% чоловіків. Це означає, що зі 100 народжених хлопчиків в Україні до пенсії доживуть лише 60, а в Швейцарії – 92 [5].

Звичайно, такий стан медичної галузі виник не сьогодні. Потреби населення у медичних послугах фінансувались і раніше за залишковим принципом. Останніми роками фінансова ситуація значно погіршилась. Як визнає прем'єр-міністр України В. Гройсман, 4% ВВП Україна витрачає на обслуговування зовнішнього боргу, а це понад 100 млрд грн щорічно, близько 5,5 млрд дол щорічно витрачається з бюджету на покриття дефіциту Пенсійного фонду, 5% ВВП - на безпеку та оборону [6]. У 2018 р. видатки Державного бюджету на охорону здоров'я сягатимуть 86 млрд грн., що становить 9,1% від державного бюджету та 2,6% від ВВП (зазначимо, що частка витрат, рекомендованих ВООЗ, мінімальних 6%). А це означає, що у Державному бюджеті України на 2018 рік закладено лише 25% необхідних коштів для лікування онкохворих, 30% - пацієнтів із серцево-судинними захворюваннями.

В Україні фінансування охорони здоров'я здійснюється переважно за рахунок Державного бюджету. Ця фінансова модель була закладена ще в 30-ті роки й отримала назву «моделі Семашка» або «піраміди Семашка», на ім'я тодішнього наркома охорони здоров'я Радянської Росії. Головними принципами цієї системи були: централізація системи охорони здоров'я; доступність медичних послуг для всіх громадян; особлива увага материнству і дитинству; єдність профілактики і лікування; ліквідація соціальних основ хвороб; залучення громадськості до справи охорони здоров'я. Контролюючим органом був наркомат охорони здоров'я, в підпорядкуванні якого перебували всі медичні установи. Приватна медицина була ліквідована, але багато платних поліклінік все ж залишилося. Таким чином, у той час вишикувалася рівна система медичних установ, яка не тільки існує, а й діє в наші дні. Нині можна багато дискутувати з приводу того, чи правильно був обраний вектор розвитку цієї галузі. Напевне, на той час з урахуванням складної ситуації в країні, домінуванням сталінського курсу на одержавлення економіки така політика щодо розвитку медицини була прийнятною. І вона дозволити досягти високого рівня медичного обслуговування громадян.

Ставши суверенною державою, Україна на початку 90-х років почала створювати власну систему охорони здоров'я. Системні зміни у відносинах власності, ліквідація державної монополії на засоби виробництва, розвиток підприємницької діяльності вплинули на появу страхування. У 1993 р. із прийняттям Декрету Кабінету Міністрів України «Про страхування» почався новий етап розвитку страхового ринку України, одним із сегментів якого стало медичне страхування. Високий рівень інфляції зумовив поширення

змішаного страхування життя. Проте цей вид страхування не мав достатнього законодавчого та методологічного обґрунтування, через що багато страхових компаній збанкрутіли, а застраховані особи не отримали належних виплат. У 1997 році у медичних закладах країни було впроваджено платні медичні послуги. Згодом їх перелік розширився. Однак це не дало позитивного ефекту. Навпаки, воно стало гальмом для розвитку приватної медицини, тому що викликало негативне ставлення населення до неї.

Медичне соціальне страхування намагаються впровадити з 2001 року, але постійно відтерміновують, бо жоден із запропонованих законопроектів (яких за ці роки було більше 20) не знаходив підтримки одночасно всіх трьох сторін соціального діалогу, тому що проекти були зорієнтовані не на соціальний захист громадян, а на інтереси комерційних клінічних, фармацевтичних або страхових компаній тощо. А джерело фінансування змінювалось з держбюджету на кошти соціального страхування.

Вирішальну роль у реформуванні системи охорони здоров'я України відіграє перехід до обов'язкового медичного страхування (ОМС), яке стане додатковим джерелом фінансування галузі. Наразі в Україні є обов'язкове страхування спортсменів вищої ліги, спеціалістів ветеринарної медицини, деяких інших професій, пов'язаних з безпекою навколишнього середовища і людства. Обов'язковим є страхування пасажирів авіаперевезень, водного транспорту, таксі та інших видів перевезень, які діють за ліцензією. Але масово соціальним видом страхування здоров'я і життя громадян воно ще не стало. На сьогодні в Україні розгляд ОМС для всіх працівників відкладено на невизначений термін.

Добровільне медичне страхування (ДМС) в Україні розвивається, хоча ним користуються нині лише 5-6% українців. Послуги такого страхування є дуже дорогими. Цей вид страхування здійснюють в основному юридичні особи. Це великі компанії, які створюють додаткові комфортні умови для своїх працівників з метою їх заохочення. ДМС не може працювати окремо від держави. Необхідно поєднувати систему державного забезпечення та систему ДМС. Схожа модель працює в США, де послугами ДМС користуються близько 70% працюючих осіб, які заключають саме колективні договори, тому що даний вид страхування передбачає знижки до тарифів та мотивує офіційно влаштовуватись на роботу. Щоправда, існують країни й без державної медицини. Наприклад, в Ізраїлі немає державної системи медичного обслуговування. 94% його населення охоплено всебічним страхуванням здоров'я, яке здійснюється в рамках медичного страхового фонду профспілкового об'єднання Гістадрут (83% випадків), а також інших фондів медичного страхування (17%). Медичні заклади знаходяться під контролем різних установ, головними з яких є профспілки та уряд [7, с.10].

ДМС здійснюється страховими компаніями, які в установленому порядку отримали ліцензію на страхування життя. ДМС має ряд переваг: широкий вибір аптек, лікарів, медичних закладів з поліпшеними умовами перебування; страхування ризиків тимчасової втрати працездатності, пологів тощо. Переліки страхових ризиків та відповідна тарифікація останніх здійснюється

індивідуально до кожного клієнта, що дає можливість регулювати суму витрат індивіда на покриття лікування. Однак, типовою є ситуація, коли в страхову компанію за послугою індивідуального страхування звертаються люди з низьким рівнем здоров'я, а це впливає на кінцеву вартість страхування здоров'я або ж страхові компанії відмовляють у придбанні поліса.

Більшість страхових компаній орієнтована на корпоративний сегмент через те, що в компаніях-замовниках корпоративного страхування, не можуть працювати люди з важкими захворюваннями. Компанії, які ведуть боротьбу за кращі кадри, включають медичний захист здоров'я своїх співробітників в соціальний пакет. Як сподівається Ю. Добренкова, співробітник СК Крона, «в 2018 році буде зростати попит на корпоративні програми зі страхування здоров'я співробітників. Компаніям середнього і малого бізнесу необхідно конкурувати за висококваліфікований персонал, а соціальний пакет все більш значущий для талановитих працівників. Буде розвиватися "точність" прогнозування страхового пакету, яка буде залежати від рівня здоров'я працівників компаній. Це дозволить зробити вартість пакетів медичного страхування більш доступною» [8].

На нашу думку, нині єдиною ефективною моделлю системи охорони здоров'я України, за допомогою якої можна вирішити проблему недофінансування і неефективного використання наявних фінансових ресурсів, є модель державно-приватного партнерства з обов'язковою участю приватних страхових компаній.

Медична реформа, яка розпочалась в Україні в 2018 р., має створити необхідну платформу (передумови) для запровадження ОМС й виправити негативну тенденцію, яка склалася з медичним обслуговуванням населення.

Основними положеннями даної реформи є:

1) право громадянина самостійно обрати собі сімейного лікаря чи терапевта, підписавши з ним декларацію, незалежно від місця проживання;

2) право пацієнта безкоштовно отримувати послуги у свого лікаря первинної ланки, визначені державою: прийом лікаря, оформлення листків непрацездатності, виписаний лікарем рецепт, базові аналізи крові, сечі, електрокардіограма (ЕКГ) та інші послуги, передбачені програмою медичних гарантій;

3) медичні послуги поділяються на повністю оплачувані та платні за рахунок пацієнта або спільно зі страховою компанією;

4) оплата гарантованих медичних послуг буде здійснюватися за рахунок бюджетних коштів, якими буде розпоряджатись Національна служба здоров’я України.

Реформа є першим кроком до вдосконалення системи охорони здоров’я, але існує ряд питань та недостатня поінформованість населення щодо порядку надання вторинної і третинної допомоги, регулювання цін на медичні послуги та фінансування усієї медичної системи в цілому. Існує ризик неплатоспроможності населення покривати витрати на медицину. Тому паралельно з медичною реформою необхідно розвивати сектор страхування, який вирішить питання забезпечення належного рівня лікування та обслуговуван-

ня на всіх рівнях медичної допомоги.

ОМС повинне запрацювати на рівні всієї держави. Механізм же буде ідентичний зі страховою компанією, де гарантований пакет медичних послуг (буде сформований протягом 2019 р.) - це той самий страховий ліміт. При цьому страхова компанія формує поліс в рамках зібраних коштів конкретної людини на відповідний рік, держава буде робити також, але з податків всього населення країни. Поліс буде розроблятися щорічно, виходячи з потреб людей. Незмінним буде тільки одне - в гарантований пакет послуг із року в рік будуть переходити екстрена медична допомога і невідкладна медична допомога, а також всі ті види, що серйозно впливають на показники захворюваності та смертності.

Варто зазначити, що в Україні вже є успішні приклади корпоративного ДМС. Зокрема, ПАТ «Українська залізниця» має успішний досвід протягом 17 років. У 2000 р. було запроваджено багатоканальне фінансування й ДМС для працівників і пенсіонерів залізниці. Нині в цій системі близько 900 тис. застрахованих осіб. З них 326,5 тис. — працівники, 300,6 тис. — пенсіонери, 300 тис. — члени родин. Люди застрахувалися добровільно. Підприємство співпрацює з більше ніж 25 компаніями, є лікарняна каса [9].

Отже, у перспективі впровадження медичного страхування дасть можливість досягти належного рівня фінансування системи охорони здоров'я.

1. Основи законодавства України про охорону здоров'я: Закон України від 19.11.1992 № 2801-XII [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/2801-12

2. ВООЗ опублікував рейтинг найздоровіших країн: Україна потрапила в "червону зону" [Електронний ресурс]. – Режим доступу: http://expres.ua/news/ 2017/09/28/264335-vooz-opublikuvav-reytyng-nayzdorovishyh-krayin-ukrayina-potrapyla-chervonu

3. The Legatum Prosperity Index 2017 [Електронний ресурс]. – Режим доступу: https://www.li.com/activities/publications/the-2017-legatum - prosperity-index

4. Расходы 7% ВВП на медицину в Украине не соответствуют качеству услуг, - Всемирный банк [Електронний ресурс]. – Режим доступу: https://ru.espreso. tv/news/2017/07/14/raskhody_7_vvp_na_medycynu_v_ukrayne_ne_sootvetstvuyut_kachestvu_uslug_vsemyrnyy_bank

5. Україна в світових рейтингах [Електронний ресурс]. – Режим доступу: https://ukr.segodnya.ua/ukraine/ukraina-v-raznyh-reytingah-kak-zhivetsya-ukraincam--1049597.html

6. Україна щорічно витрачає понад ₴100 млрд на обслуговування зовнішнього боргу [Електронний ресурс]. – Режим доступу: https://zaxid.net/ukrayina_shhorichno_vitrachaye_ponad_100_mlrd_na_obslugovuvannya_zovnishnogo_borgu__groysman_n1431708

7. Баранник Л.Б. Фінансові аспекти медичного страхування в Україні / Л.Б. Баранник // Вісник ДДФА. – 2012. – № 1 (27). – С. 10-14. (Сер.: Економічні науки).

8. Добренкова Ю. Про перспективи медичного страхування в Україні [Електронний ресурс]. – Режим доступу: https://ua.korrespondent.net/business/ 3922841-yuliia-dobrenkova-pro-perspektyvy-medychnoho-strakhuvannia-v-ukraini

9. Запровадження загальнообов'язкового соціального медичного страхування в Україні. Матеріали круглого столу 15 листопада 2017 р. [Електронний ресурс]. – Режим доступу: https://www.umj.com.ua/article/117332/ zaprovadzhennya-zagalnoobov-yazkovogo-medichnogo-strahuvannya-chasu-na-rozdumi-nemaye

**Бідняк Ганна Сергіївна**
старший викладач кафедри криміналістики,
судової медицини та психіатрії

**Форостян Олександр Сергійович**
курсант факультету підготовки фахівців
для органів досудового розслідування
Дніпропетровського державного
університету внутрішніх справ

# ОКРЕМІ АСПЕКТИ ВИКОРИСТАННЯ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ ПІД ЧАС ОГЛЯДУ МІСЦЯ ПОДІЇ

Огляд місця події є ключовою інформативно-пошуковою слідчою-розшуковою дією. Вона часто проводиться як першочергова слідча (розшукова) дія після внесення відомостей до Єдиного реєстру досудових розслідувань. Так, відповідно до ч. 3 ст. 214 Кримінального процесуального кодексу України огляд місця події у невідкладних випадках може бути проведений до внесення відомостей в ЄРДР, що здійснюється негайно після завершення огляду. Таке виключення для даної слідчої (розшукової) дії зроблено законодавцем тому, що нерідко тільки завдяки огляду місця події можна встановити наявність ознак злочину й прийняти рішення щодо відкриття кримінального провадження.

Враховуючи важливість проведення даної слідчої (розшукової) дії ті помилки, які допускають слідчі, особливо за браком досвіду, при огляді місця події негативно впливають на результативність, швидкість та повноту досудового розслідування. Більше того, повторний або додатковий огляд місця події не завжди може дати результат, внаслідок багатьох факторів, зокрема: зміну обстановки на місці події, втраті об'єктів, слідів або через їх зміну.

Так, помилки, які допускають слідчі під час огляду місця події можна поділити на 3 види: процесуальні (передбачені кримінально-процесуальним законодавством Україні); тактичні (пов'язані с послідовністю методів, прийомів огляду місця події) та технічні (помилки у порядку та способів використання технічних засобів та криміналістичної техніки). Ми звернемо увагу, на тактичних та технічних типових помилках, які допускають слідчі під час здійснення огляду місця події.

К технічним помилкам можна віднести, неправильність використання спеціалістом та слідчим технічних засобів та криміналістичну техніку, наприклад несправність фотоапарата та відеокамери, що унеможливлює здійснення фото та відео фіксацію.

Так, наприклад для встановлення наявності та вилучення видимих слідів, огляд поверхонь предметів і слідів спочатку проводять при природному освітленні без застосування будь-яких заходів технічного оснащення. Другим етапом оглядають предмети при штучному освітленні у косо падаючих променях за допомогою криміналістичних луп та ультрафіолетових освітлюва-

чів. Зазвичай застосовується лупа з великим полем зору і невисоким ступенем збільшення (2,5-х). Особливо зручна лупа з підсвічуванням, що є в комплекті науково-технічних засобів для слідчого. Дрібні деталі вивчаються за допомогою 10-кратної вимірювальної лупи, що кріпиться на штативі зі шкалою, що дозволяє проводити виміри з точністю до 0,1 мм. Спостереження люмінесценції під впливом ультрафіолетових променів здійснюється в затемненому приміщенні. Для дослідження невеликих об'єктів, можна затемнити будь-яку частину кімнати. При роботі з ультрафіолетовим освітлювачем необхідно зважати на те, що деякі речовини починають люмінесціювати не одразу після опромінення, тому не слід поспішати з переміщенням освітлювача з одного об'єкта на інший. Найбільший ефект люмінесценції виникає при спрямуванні пучка променів перпендикулярно до досліджуваної площини. Робота в затемненому приміщенні потребує деякого звикання (адаптації зору), у зв'язку з чим ефективне спостереження можливо через кілька хвилин після настання темряви. Ультрафіолетовий освітлювач слід увімкнути за 3–5 хвилин до використання, щоб його лампа ввійшла в стабільний режим випромінювання [2, с.15].

Науково-технічним засобом, який забезпечує комплексну фіксацію оточуючої обстановки із здійсненням точного відображення зовнішнього вигляду, форми, вимірюванням відстаней між об'єктами, їх взаємного розташування та розмірів, є лазерний 3D сканер. За допомогою відповідного програмного забезпечення, використання 3D сканеру дозволяє протягом невеликого проміжку часу створити точну фотореалістичну модель ділянки місцевості, розглянути її з будь-якого ракурсу та відстані як в цілому, так й окремі об'єкти. Важливим є й те, що дане програмне забезпечення дає можливість проводити реконструкцію об'єкту та здійснювати різного роду операції з окремими об'єктами як у 3D моделі, так і окремо від неї, імпортувати у 3D модель місця, що скановано, інші трьохвимірні об'єкти для ілюстрації їх розташування в певні проміжки часу [4].

Серед основних напрямів таких інноваційних застосувань виділяють:

– візуалізацію приміщень зі створенням найбільш реалістичної картини відсканованих просторів і можливістю за допомогою відповідних комп'ютерних програм проводити вимірювання для будь-якої точки у межах об'єкта сканування;

– огляд місця події з певної точки: 3D-сканування дозволяє проводити огляд

місця злочину з точки, в якій перебував правопорушник або його жертва, і наочно продемонструвати саме те, що було видно з цієї точки;

– аналіз слідів крові: 3D-сканування дозволяє криміналістам створювати зображення слідів крові у тривимірному зображенні, відтворювати траєкторії бризок крові і переглядати їх у межах місця події;

– техніку дактилоскопіювання: 3D сканування дозволяє прискорити процедуру дактилоскопіювання (сканер витрачає менше ніж одну секунду на палець); у подальшому розробники обіцяють збільшити його швидкість за рахунок сканування усіх десяти пальців за один раз. Відсутність контакту зі

сканером зменшує забруднення поверхні скла або «змазання» відбитка через випадкове смикання пальцем, а отже, підвищує якість сканування. У базі даних відбиток зберігається у вигляді тривимірної моделі;

– балістичні експертизи: експерти мають змогу вивчати не плоске зображення

кулі, а її повноцінну 3D-модель, на поверхні якої чітко відтворюються жолобки і борозенки, залишені після пострілу, за якими експерти можуть з достовірністю ідентифікувати застосовану зброю. Крім цього, за допомогою 3D-моделювання можна точно розраховувати і наочно продемонструвати траєкторію кулі;

– реконструкцію ДТП: відновлення сценаріїв і причин дорожньо-транспортних

пригод, детальне зображення та збереження усіх пошкоджень і доказової бази для подальшого розслідування [3].

Незважаючи на свої переваги, сучасна техніка також має свої недоліки. Зокрема, велика вартість зазначених пристроїв обумовлює вельми повільне впровадження їх в практичну діяльність.

Таким чином, слід зазначити, що огляд місця події є досить складною та водночас важливою слідчою (розшуковою) дією, яка дає основні вихідні дані, необхідні для визначення можливих напрямів розслідування. Задля неприпустимості втрати інформації він повинен проводитися з дотриманням вимог процесуального законодавства та криміналістичних рекомендацій та з використанням сучасних інноваційних технологій.

1. Кримінальний процесуальний кодекс України : наук.-практ. коментар / [за заг. ред. професорів В. Г. Гончаренко, В. Т. Нора, М. Є. Шумила]. / К. : Юстініан, 2012, 1224 с.

2. Огляд місця події: виявлення та вилучення об’єктів біологічного походження: Методичні рекомендації / Міністерство внутрішніх справ України, Державний науково-дослідний експертно-криміналістичний центр; [авт.-упоряд.: С. І. Перлін, С. О. Шевцов, Н. М. Косміна, В. В. Іонова]. / Х.: Х.: ФО-П Чальцев О. В., 2009, 100 с.

3. Непорада А.С. Новітні технології в криміналістиці: 3D-сканування під час огляду місця події / Криміналістичний вісник : наук.-практ. зб. / [голов. ред. В.В. Чернєй] / ДНДЕКЦ МВС України; НАВС. / К. : ПК «Типографія від «А» до «Я», 2016. / No 2 (26). / с. 141-144.

4. Офіційний сайт компанії Panorama Tools graphical user interface [Електронний ресурс]. / Режим доступу : http://www.ptgui.com.

**Varianychenko Alina Olegovna**
wykładowca Uczelni Łazarskiego
w Warszawie uczestnik seminarium doktoranckich
Uczelni Łazarskiego w Warszawie
aplikant adwokacki przy Okręgowej Radzie
Adwokackiej w Warszawie

# WYKORZYSTYWANIE PRZEZ POLICJĘ INFORMACYJNYCH TECHNOLOGII W KONTROLI OPERACYJNEJ A OCHRONA KONSTYTUCYJNYCH I KONWENCYJNYCH PRAW CZŁOWIEKA W SYSTEMIE PRAWNYM RZECZPOSPOLITEJ POLSKIEJ

Z uwagi na istotną pozycję w systemie bezpieczeństwa państwa, Policja Rzeczpospolitej Polskiej posiada uprawnienia o szczególnym charakterze, do których zaliczają się złożone formy działania i wykorzystywane w ich ramach specjalne metody i środki techniczne, uregulowane w ustawie z dnia 6 kwietnia 1990 r. – o Policji (Dz.U. Nr 30, poz. 179; dalej: PolU).

Intencją ustawodawcy było, aby uprawnienia te służyły Policji do zwalczania przestępstw o najwyższym ciężarze gatunkowy. Dlatego też to wyłącznie w sprawach o umyślne przestępstwa enumeratywnie wymienione w art. 19 ust. 1 PolU może zostać zarządzone wszczęcie czynności operacyjno-rozpoznawczych. Ustawodawca posiadający przymiot racjonalności postanowił zawęzić spektrum typów czynów zabronionych, w stosunku do których kontrola operacyjna może być prowadzona przez Policję. Nie ma zatem argumentów do dowolnego rozszerzania tego katalogu na inne jeszcze przestępstwa. Fakt podobieństwa czy też podobnego poziomu zagrożenia ustawowego przestępstw zawartych w omawianym katalogu do innych przestępstw, nie może przesądzać o odstąpieniu od ścisłej wykładni literalnej art. 19 ust. 1 PolU. To ustawodawca, na podstawie m.in. testu proporcjonalności, doprecyzowuje ten katalog, odbierając w tym zakresie swobodę organom ścigania bądź sądom. Stosowanie argumentacji *per analogia* przy dokonywaniu wykładni art. 19 ust. 1 PolU bezsprzecznie stanowiłoby zakazane w demokratycznym państwie prawa działanie na niekorzyść osoby podejrzanej i od samego początku postępowania pozbawiłoby ją prawa do rzetelnego procesu.

Zakres czynności możliwych do podjęcia w ramach kontroli operacyjnej, która do tej pory obejmowała przede wszystkim kontrolę korespondencji, przesyłek i treści rozmów telefonicznych oraz przy pomocy sieci telekomunikacyjnej został znacznie rozszerzony tzw. ustawą inwigilacyjną, która weszła w życie 07 lutego 2016r. Policji zostały nadane dodatkowe uprawnienia w ramach kontroli operacyjnej, pozwalające wykorzystywać technologii informacyjne przy realizacji ustawowych zadań tej służby bezpieczeństwa państwa.

W świetle aktualnie obowiązujących przepisów niejawna kontrola operacyjna może polegać również na uzyskiwaniu i utrwalaniu treści korespondencji prowadzonej za pomocą środków komunikacji elektronicznej,

uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych.

W toku kontroli operacyjnej można pozyskać nie tylko informacje z rozmów telefonicznych prowadzonych czy to w sieci stacjonarnej lub mobilnej, lecz także inne informacje przesyłane za pomocą sieci telekomunikacyjnych, tj. SMS-ów czy innego rodzaju tekstów, faksów, obrazów, filmów, wreszcie informacji zawartych w poczcie elektronicznej. Wszystkie te informacje są przesyłane za pomocą sieci telekomunikacyjnej. Zgodnie bowiem z art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. Nr 171, poz. 1800; dalej: PrTel) sieć telekomunikacyjna oznacza systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju.

Wcześniej podmioty wykonujące działalność telekomunikacyjną oraz podmioty świadczące usługi pocztowe były obowiązane do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Policję kontroli operacyjnej. Obecnie podmioty wykonujące działalność telekomunikacyjną oraz podmioty świadczące usługi pocztowe są obowiązane do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Policję kontroli operacyjnej (art. 19 ust. 12 PolU). W związku z art. 19 ust. 12 PolU pozostają odpowiednie postanowienia Prawa telekomunikacyjnego i Prawa pocztowego. Zgodnie z art. 179 ust. 3 pkt 1 PrTel operator jest obowiązany do zapewnienia warunków technicznych i organizacyjnych dostępu i utrwalania, zwanych dalej warunkami dostępu i utrwalania, umożliwiających jednoczesne i wzajemnie niezależne uzyskiwanie przez Policję dostępu do przekazów telekomunikacyjnych, nadawanych lub odbieranych przez użytkownika końcowego lub telekomunikacyjne urządzenie końcowe i posiadanych przez przedsiębiorcę danych związanych z przekazami telekomunikacyjnymi. Analogiczne obowiązki przewiduje ustawa – Prawo pocztowe.

Przewidziane w art. 19 PolU działania ingerują bezpośrednio w sferę praw i wolności obywatela. Niezwykle istotne jest więc przeprowadzanie tych czynności w sposób w pełni zgodny z przepisami prawa. Sąd Apelacyjny w Białymstoku w wyroku z 18.3.2010 r., II AKA 18/10, trafnie wskazał, że wartości chronione przez art. 5 i art. 7 Konstytucji RP (ochrona wolności i praw człowieka i obywatela oraz zasada Państwa Prawnego), a w szczególności nałożone przez ustawę zasadniczą w art. 9 zobowiązanie, że Rzeczpospolita Polska przestrzega wiążącego ją prawa międzynarodowego, czyni niedopuszczalne wykorzystywanie przez organy państwowe – pod jakąkolwiek postacią oraz w jakiejkolwiek formie i celu – informacji o obywatelach, które są pozbawione atrybutu legalności.

Dowody z kontroli operacyjnej, zwłaszcza te, uzyskane za pomocą wykorzystywania informacji technologicznych, jako najbardziej ingerujące w swobodę komunikowania się i inne związane z tym wartości konstytucyjne w zasadzie nie mogą stanowić dowodu, który można wykorzystać w postępowaniu

karnym, chyba że spełnione zostaną wymogi legalizujące takie działania, ustalone w art. 19 PolU.

Dlatego też nie sposób uznać za trafny wyrok Sądu Najwyższego z 2.3.2012 r., V KK 270/11, który stwierdził, że nawet trafne – w jakiejś mierze – zastrzeżenia do podstaw czy sposobu kontroli operacyjnej w postaci podsłuchu telefonicznego nie powinny automatycznie wykluczać utrwalonych rozmów z kręgu dowodów mogących stanowić podstawę orzeczenia, gdy działania organów ścigania były pierwotnie legalne, tzn. oskarżeni byli podsłuchiwani legalnie, policjanci mieli prawo dostępu do rozmów i przestępny charakter zachowań oskarżonych "rzucał się w oczy" oraz gdy funkcjonariuszom towarzyszyła dobra wiara i ich działania nie zasługiwały na napiętnowanie.

Celem nienarażania się na zarzut naruszenia praw człowieka przewidzianych w Konwencji Europejskiej należy bezwzględnie przyjąć, że niezbędnym warunkiem uznania materiałów, zdobytych w rezultacie czynności operacyjno-rozpoznawczej, za dowód w postępowaniu karnym jest stwierdzenie, że do jego uzyskania i utrwalenia doszło w sposób odpowiadający ustawowym rygorom, właściwym dla różnych kategorii zagrożeń porządku prawnego, w związku z którymi czynności te są podejmowane.

Po pierwsze więc, jak już zostało zaznaczone powyżej, wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych przez Policję w celu zapobieżenia, wykrycia, ustalenia sprawców, a także uzyskania i utrwalenia dowodów ściganych z oskarżenia publicznego, umyślnych przestępstw, enumeratywnie wymienionych w art. 19 ust. 1 pkt 1–8. W orzecznictwie Sądu Najwyższego trafnie się podkreśla, że zezwolenia na możliwość wykorzystania każdego dowodu – a więc i dowodu na popełnienie przestępstwa tzw. pozakatalogowego – uzyskanego w czasie trwania kontroli operacyjnej w postępowaniu karnym, jest zupełnie chybione (wyrok Sądu Najwyższego z 3.7.2013 r., V KK 412/12).

Po drugie, musi istnieć realne, a nie tylko hipotetyczne niebezpieczeństwo popełnienia jednego z przestępstw wskazanych w art. 19 ust. 1 albo musi istnieć realna możliwość wykrycia lub ustalenia sprawców tego przestępstwa czy też dostarczenia dowodów jego popełnienia. Użyte przez ustawodawcę sformułowanie „uzyskanie dowodów” należy rozumieć jako odnoszące się do „informacji mogących mieć znaczenie dowodowe”, dopiero w toku procesu karnego informacje takie mogą nabrać pełnej wartości dowodowej, lecz poza procesem jeszcze dowodami nie są. Powyższe stwierdzenie wywodzi się z treści art. 167 ustawy dnia 6 czerwca 1997 r. - kodeks postępowania karnego, zgodnie z którym dowody przeprowadza się w czasie procesu. W sprawach o przestępstwa ścigane z urzędu, w zakresie odpowiedzialności karnej, wykrywanie, zbieranie i wydobywanie dowodów jest obowiązkiem organów procesowych. Organy operacyjno−rozpoznawcze nie są organami procesowymi i nie prowadzą procesu karnego, zatem wyniki ich pracy nie mogą mieć znaczenia dowodowego. Jak słusznie wskazuje Sąd Najwyższy w wyroku z dnia 14 stycznia 2004 r., dopiero zeznania w charakterze świadka osoby realizującej czynność operacyjno-rozpoznawczą będą stanowiły dowód.

Jako trzeci, niezbędny, warunek, umożliwiający wszczęcie kontroli operacyjnej, jest zaistnienie sytuacji, w której inne środki okazały się bezskuteczne lub zachodzi wysokie prawdopodobieństwo, że będą nieskuteczne.

Po czwarte, przeprowadzenie kontroli operacyjnej jest dopuszczalne zasadniczo na mocy postanowienia sądu okręgowego (art. 19 ust. 2 PolU). Kontrola zarządzana jest na pisemny wniosek Komendanta Głównego Policji, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego. Wniosek o kontrolę operacyjną powinien być przedstawiony wraz z materiałami uzasadniającymi potrzebę zastosowania kontroli operacyjnej (art. 19 ust. 1a PolU). W przypadkach niecierpiących zwłoki, jeżeli mogłoby to spowodować utratę informacji lub zatarcie albo zniszczenie dowodów przestępstwa, Komendant Główny Policji lub Komendant Wojewódzki Policji może zarządzić, po uzyskaniu pisemnej zgody właściwego prokuratora, tj. Prokuratora Generalnego lub prokuratora okręgowego, zwracając się jednocześnie do właściwego miejscowo sądu okręgowego z wnioskiem o wydanie postanowienia w tej sprawie. W razie nieudzielenia przez sąd zgody w terminie 5 dni od dnia zarządzenia kontroli operacyjnej, organ zarządzający wstrzymuje kontrolę operacyjną oraz dokonuje protokolarnego, komisyjnego zniszczenia materiałów zgromadzonych podczas jej stosowania (art. 19 ust. 3 PolU). W doktrynie za kontrowersyjny uznaje się wyrok Sądu Najwyższego z 16.10.2010 r., V KK 414/11, zgodnie z którym, dla oceny dopuszczalności dowodu z materiałów z kontroli operacyjnej istotny jest kierunek tego dowodu. Jeśli jego celem jest wykazanie niewinności oskarżonego lub uzyskanie dowodów świadczących na jego korzyść, to może być on przeprowadzony niezależnie od faktu, że wobec tego oskarżonego nie wydano postanowienia w trybie art. 19 ust. 3 PolU, ani też określonego w art. 19 ust. 15c PolU postanowienia o zgodzie następczej. Z takim stanowiskiem Sądu Najwyższego należy się jednak zgodzić.

Po piąte, istotne jest również, iż za dowód w postępowaniu karnym mogą zostać uznane informację uzyskane w trakcie kontroli operacyjnej przeprowadzanej przez ustawowo dozwolony okres czasu. Kontrolę operacyjną zarządza się na okres nie dłuższy niż 3 miesiące. Sąd okręgowy może jednak, na pisemny wniosek Komendanta Głównego Policji lub Komendanta Wojewódzkiego Policji, złożony po uzyskaniu pisemnej zgody właściwego prokuratora, na okres nie dłuższy niż kolejne 3 miesiące, wydać postanowienie o jednorazowym przedłużeniu kontroli operacyjnej, jeżeli nie ustały przyczyny tej kontroli. W uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawców i uzyskania dowodów przestępstwa, sąd okręgowy, na pisemny wniosek Komendanta Głównego Policji, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może, również po upływie tych okresów wydawać kolejne postanowienia o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, których łączna długość nie może przekraczać 12 miesięcy. Kontrola operacyjna powinna być zawsze zakończona niezwłocznie po ustaniu przyczyn jej zarządzenia, najpóźniej jednak z upływem okresu, na który została wprowadzona.

Problem ustalenia zakresu stosowania czynności operacyjno-rozpoznawczych oraz możliwości wykorzystania ich wyników w procesie karnym

będzie zawsze budził żywe kontrowersje.

Nie sposób całkowicie kwestionować możliwości, a nawet potrzeby stosowania różnych form inwigilacji. Wymóg ochrony bezpieczeństwa nie ma jednak charakteru bezwzględnego i wyłącznego, co oznacza, że może i powinien podlegać ograniczeniom. Działania nakierowane na ochronę bezpieczeństwa obywateli nie mogą w sposób nieograniczony ingerować w prawo do prywatności. Zbyt duży zakres dopuszczalnej ingerencji oznacza ryzyko poważnych nadużyć. Jest to szczególnie istotne w przypadku danych internetowych i tworzenia stałych łączy do ich pozyskiwania.

Pomimo tego, że kontrolę operacyjną może stosować Policja i niektóre inne służby w Polsce, w żadnym jednak wypadku interes publiczny nie powinien usprawiedliwiać bezkrytycznego użycia dowodów pochodzących z wykonywania czynności operacyjno-rozpoznawczych. Oznacza to konieczność wskazania w akcie normatywnym, upoważniającym funkcjonariuszy państwa do ingerencji w konstytucyjne prawa osób, jakimi jest m.in. wolność i bezpieczeństwo osobiste oraz prawo do prywatności, zakresu, w jakim prawa te doznają ograniczenia. Ustawodawca nie może poprzez niejasne formułowanie przepisów ustawy pozostawiać organom mającym je stosować nadmiernej swobody działania.

Przede wszystkim wskazać należy, że przesłanki dostępu służb do danych telekomunikacyjnych czy internetowych są bardzo szerokie, i uzasadniają powstanie wątpliwości, czy spełniają one wymóg przewidywalności wkroczenia w prawo do prywatności, chronione przez Konwencję Europejską. Ustawodawca powinien wprowadzić normy prawne, które sprecyzowałyby i ograniczyły szeroki dostęp służb do danych.

Ponadto, przepisy powinny zostać uzupełnione o określenie, w jakich sytuacjach możliwe jest korzystanie z tych danych – np. gdy inne, mniej inwazyjne środki okazały się nieskuteczne. Konieczne wydaje się być wprowadzenie zasady *ultima ratio* wykorzystywania przez Policję danych telekomunikacyjnych i internetowych.

Dane pozyskiwane w ramach dostępu do danych internetowych powinny być również poddane skutecznemu systemowi kontroli przez niezależny organ.

Zakwestionować również należy brak przepisów prawnych, przewidujących następcze powiadamianie osoby, której dane były sprawdzane lub pobierane.

Dopuszczalny okres przeprowadzania kontroli również należy uznać za niezasadnie długi. Zgodnie ze znowelizowanymi przepisami kontrola operacyjna będzie mogła trwać aż do 18 miesięcy. Oznacza to, że przez półtora roku służby policyjne i służby specjalne będą mogły ustalać treść korespondencji obywateli niezależnie od tego, czy ostatecznie zostanie uruchomione na tej podstawie postępowanie karne.

Powyższe prowadzi do wniosku, że choć znowelizowana ustawa o Policji miała na celu wykonać wyrok Trybunału Konstytucyjnego z lipca 2014 r., który uznał szereg przepisów dotyczących funkcjonowania policji i służb specjalnych za niezgodne z Konstytucją i ustawa ze stycznia 2016 r. w znacznym stopniu realizuje rekomendacje i zalecenia płynące z wyroku Trybunału Konstytucyjnego, pozostało wiele braków, które powinny zostać przez polskiego ustawodawcę naprawione.

**Волков Юрій Михайлович,**
викладач кафедри
тактико-спеціальної підготовки
Дніпропетровського державного
університету внутрішніх справ

# ПРОБЛЕМА ПІДГОТОВКИ ФАХІВЦІВ КІБЕРБЕЗПЕКИ ДЛЯ ОРГАНІВ НАЦІОНАЛЬНОЙ ПОЛІЦІЇ

На сьогоднішній день наше існування неможливе без тісної взаємодії з кібертехнікою, коли комп'ютери і телекомунікаційні системи охоплюють всі сфери життєдіяльності людей і держави. Але людство, поставивши собі на службу телекомунікації і глобальні комп'ютерні мережі, не передбачало, які можливості для злочинних діянь створюють ці технології. На сьогодні жертвами злочинців, що діють у віртуальному просторі, можуть стати не лише люди, але і цілі країни. При цьому безпека тисяч користувачів інтернет простору залежна від декількох злочинців. Кількість злочинів, що здійснюються в кіберпросторі, зростає пропорційно числу користувачів комп'ютерних мереж, і, за оцінками Інтерполу, темпи зростання злочинності в глобальній мережі Інтернет, є найшвидшими на планеті.

Небезпеку 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 загроз національній безпеці України в інформаційній сфері.

Створення підрозділу з висококваліфікованими працівниками у сфері кібербезпеки є, однією з актуальних проектів, так як дана сфера є найбільш незахищеною і привертає увагу багатьох осіб, які посягають на приватне життя та інші блага пов'язанні з інтернет простором.

Першим кроком, у розвитку безпеки громадян та захисту їх конфіденційної інформації на законодавчому рівні, було затвердження "Стратегії кібербезпеки України" указом президента України станом на 15 березня 2016 року. Даний указ закріплює забезпечення безпеки у кіберпросторі, шляхом застосування сукупності правових, організаційних, інформаційних заходів, що, безпосередньо, базуються на принципах верховенства права і поваги до прав та свобод людини і громадянина, забезпечення національних інтересів України.

Якщо аналізувати даний нормативний документ, а саме у четвертому положенні указу, стає зрозуміло, що майже усі можливі дії та заходи, щодо вдосконалення захисту у сфері кіберпростору, вжиті з боку законодавця, серед яких є:

– розробка та оперативна адаптація державної політики в сфері кібербезпеки, досягнення сумісності з відповідними стандартами ЄС і НАТО;

– створення національної нормативно-правової та термінологічної основи в цій сфері, гармонізація нормативних актів у сфері електронних кому-

нікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів та стандартів ЄС і НАТО і т.д.[1]

Вищезазначені положення, безумовно, мають чимале значення у гарантуванні безпеки в кіберпросторі, так як стали гарантом діяльності органу кібербезпеки, але впровадження надійного апарату протидії злочинам у кіберпросторі є проблемним, через низький рівень підготовки здобувачів освіти, оскільки дана сфера вимагає знання:

– теоретичних основ кібернетичної безпеки;

– правових та організаційних засад протидії кіберзлочинності;

– методів та засобів протидії кіберзлочинності;

– програмного забезпечення систем кібернетичної безпеки;

– криптографічних механізмів кібернетичної безпеки;

– кібернетичної безпеки підприємств; − основ кібернетичної безпеки держав тощо.

Але у ВНЗ діючих на території України не існує відповідних дисциплін, які, на думку багатьох науковців, могли б надати такий багаж знань. Проте впровадження таких дисциплін, як: "Кібернетичний простір", "Інформаційні технології та системи кібернетичного простору", "Технологія організації збору та добування інформації у кіберпросторі, її обробки аналізу і синтезу", "Основи автоматизації процесів інформаційної діяльності у кібернетичному просторі" – значно змінили б становище майбутніх фахівців, у сфері кібербезпеки. Ввівши вище зазначені дисципліни у ВНЗ зі специфічними умовами навчання системи МВС, здобувачі освіти у цих закладах можуть отримати:

– здатність розуміти сутність і значення інформації в розвитку сучасного інформаційного суспільства, застосовувати досягнення інформатики й обчислювальної техніки, проводити цілеспрямований пошук і збір інформації з відкритих, а також її добування з відносно-відкритих і закритих електронних джерел;

– здатність виявляти ознаки стороннього кібернетичного впливу, а також моделювати можливі ситуації такого впливу та прогнозувати їх можливі наслідки;

– здатність організовувати й підтримувати комплекс заходів щодо забезпечення інформаційної і кібербезпеки з урахуванням їх правової обґрунтованості, адміністративно-управлінської й технічної реалізуємості й економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації;

– здатність протидіяти несанкціонованому проникненню протиборчих сторін до власних ІТ систем і мереж, забезпечити стійкість їх роботи, а також відновлення їх нормального функціонування після здійснення кібернападів;

– здатність організовувати проведення атестації об'єкта на відповідність вимогам державних або корпоративних нормативних документів;

– здатність брати участь у розробці підсистем управління інформаційною і кібербезпекою, здійснювати їх адміністрування й експлуатацію;

– здатність до проведення попереднього техніко-економічного аналізу

й обґрунтування проектних рішень по забезпеченню кібербезпеки;

– здатність оформлювати технічну документацію з урахуванням діючих нормативних і методичних документів в області інформаційної і кібербезпеки [2].

Отже, підготовка фахівців у даній сфері має вагоме значення у гарантованій безпеці кіберпростору, але проблема підготовки, справді, висококваліфікованих кадрів, що підготовленні до усіх реалій у цій сфері й посягань на блага людини та держави, залишається відкритою.

1. Указ Президента України "Про рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України" від 27 січня 2016 року прийнятий 15 січня 2016 року № 96/2016. – Режим доступу., Електронний ресурс: http://zakon3.rada.gov.ua/laws/show/96/2016;

2. Бурячок В.Л. "Рекомендації щодо розробки та запровадження профілю навчання «Кібернетична безпека» в Україні"// Кібербезпека та захист критичної інформації інфраструктури., - 2014 р., С. 126-131.

**Воронов Ігор Олександрович**
д.ю.н., с.н.с., провідний науковий
співробітник Одеського державного
університету внутрішніх справ

## ВИКОРИСТАННЯ ПРОГРАМНИХ КОМПЛЕКСІВ У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Концепція "інформаційного суспільства" розкрила принципово важливу рису суспільства, відкрила нові властивості інформації та підкреслила її зростаючу роль. Основними рисами, що характеризують інформаційне суспільство, є постійне збільшення ролі інформації і знань, постійний розвиток комунікацій, продуктів та послуг, глобального інформаційного простору.

Поява та розвиток високих інформаційних технологій являє собою масштабний динамічний процес, який має постійний та цілеспрямований характер. Внаслідок цього невпинно удосконалюються і створюються нові засоби та способи обробки інформації.

Важливого значення набувають методи або способи обробки інформації, зокрема її візуального аналізу даних та виявлення прихованих зв'язків.

Одержувані з різноманітних джерел відомості повинні всебічно вивчатися й оцінюватися з погляду їхньої значущості та можливості подальшого використання для забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку.

Реалізація наявного інформаційного матеріалу – наступний етап процесу оперативно-розшукової діяльності. Її успішність визначається насамперед якісним рівнем, на якому перебуває організація збирання й аналізу інформації.

Специфікою сучасних вимог до продуктивної переробки інформації є те, що:

- дані мають значний обсяг;

- дані є різнорідними (кількісними, якісними, текстовими);
- необхідні конкретні та зрозумілі результати;
- інструменти для обробки даних повинні бути простими у використанні.

З одного боку, інтелектуальний аналіз даних являє собою процес виділення з неструктурованої інформації даних, придатних для використання. З іншого, інтелектуальний аналіз – це форма існування і систематизації результатів пізнавальної діяльності людини, складова теорії штучного інтелекту. Врешті, інтелектуальний аналіз ґрунтується на таких технологіях, як візуальний аналіз, виявлення прихованих зв'язків, моделювання, передача та зберігання даних тощо.

Програмні комплекси для побудови концептуальних схем інформаційних звязків між обєктами знайшли широке застосування в багатьох напрямах людської діяльності, насамперед, у комерційній сфері. Вони активно застосовуються приватними структурами, які професійно займаються корпоративною безпекою та проводять внутрішні розслідування інцендентів.

Стає очевидним, що інформаційно-аналітичне забезпечення протидії злочинності потребує розробки нових рішень в аналізі великих обсягів даних і виявлення прихованих зв'язків.

Значна частина аналітичної роботи в даному напряму полягає у виявленні зв'язків між об'єктами. Основними поняттями моделі даних стають "об'єкт" і "зв'язок". Така інформація здебільшого не може бути агрегована, що робить традиційні засоби представлення інформації у вигляді екранних форм і таблиць неефективними.

Слід також враховувати, що дані можуть поступати з взаємозв'язаних або абсолютно незалежних один від одного джерел. В цьому випадку виникає проблема в зручному і надійному способі ідентифікації інформаційних об'єктів і їх ефективної селекції з подібних джерел даних, оскільки об'єм дублюючих даних може бути значним.

Таким чином, на перший план виходять візуальні засоби аналізу і такі графічні представлення даних як специфічні діаграми: зв'язків, послідовності подій і трансакцій. При цьому не повинна втрачатися можливість роботи з окремим об'єктом для виявлення його зв'язків і взаємин з іншими об'єктами.

Відомо, що класифікація є єдиною універсальною формою представлення і систематизації знань, яка дозволяє звести усе різноманіття об'єктів, процесів і явищ реальній дійсності, їх численних зв'язків і взаємних залежностей, що знаходяться в безперервному русі (зміні), до кінцевої спостережуваної безлічі класифікаційних об'єктів і їх ознак.

Під технологіями візуального аналізу даних та виявлення прихованих зв'язків автором пропонується розуміти методи та способи представлення даних в залежності від їх об'єму, кількості джерел та послідовності подій.

Програмні продукти, істотним чином відрізняючись архітектурно, використовують одну і ту ж модель даних – "об'єкт-зв'язок" і значною мірою перетинаються функціонально, оскільки так чи інакше намагаються вирішувати одні і ті ж завдання візуального аналізу даних, зберігання даних, що з'являються під час розслідування, використання даних, що зберігаються в

зовнішніх базах даних, а також роботи з неструктурованими даними.

Основний компонент дозволяє швидко та ефективно проводити аналіз системи взаємопов'язаних об'єктів і динаміки послідовних подій, відображаючи при цьому результати дослідження у вигляді зручних для розуміння схем та діаграм. Інформація може відображатися у вигляді об'єктів, до яких у разі необхідності можливо додати додаткові атрибути і картки даних з коментарями.

Використання систем інтегрованого управління даними дозволить не лише адекватніше вирішувати завдання ідентифікації дубльованих даних про об'єкти, як у власних, так і в зовнішніх базах даних, але і істотно підвищити якість самих даних, допомагаючи виявити помилки введення, порушення логічних зв'язків і цілісності посилань.

Вживання технологій візуального аналізу і виявлення прихованих зв'язків дозволить не просто консолідувати інформацію про об'єкти в одному сховищі під час первинного завантаження, але і забезпечувати незалежне функціонування підсистем, що виконують роль джерел даних, не втрачаючи погодженого уявлення про об'єкт. Крім того, можливий пошук дороги між об'єктами, як на схемі, так і в базі даних, що дозволяє виявити ланцюжок об'єктів і зв'язків між ними.

Дані, представлені в графічному вигляді, дозволять виявляти окремі явища на декілька порядків швидше, ніж аналіз табличної або текстової інформації. Ефективність візуальної обробки інформації виражається в тому, що вона дозволяє підключити до активної роботи по ухваленню рішення резерви образного, асоціативного мислення. Представлення ситуації у вигляді образів узагальнює інформацію і дозволяє приймати рішення у предметній галузі.

Програмні продукти можуть ефективно використовуватися при вирішення багатьох завдань, а саме:

- при фіксації, узагальненні або структуризації оперативно-розшукової інформації (візуалізації даних незалежно від об'єму та формату);
- для класифікації джерел оперативно-розшукової інформації;
- для ефективної групової роботи за обраним напрямом діяльності;
- для створення схем послідовності подій;
- для виявлення прихованих зв'язків між об'єктами та подіями, що становлять оперативний інтерес;
- ефективно здійснювати обмін фіксованими результатами аналізу з іншими підрозділами.

Таким чином, поліція здійснюватиме інформаційно-аналітичну діяльність у сучасному форматі обробки й повноцінного використання різноманітних даних, успішно виконуючи покладені на неї функції й завдання.

**Гаврилюк Руслан Валерійович,**
к.ю.н., начальник Придніпровського управління
кіберполіції Департаменту кіберполіції
Національної поліції України

## СУЧАСНІ ТЕНДЕНЦІЇ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ

У наші дні використання інформаційних технологій не має меж. Однак, нажаль, віртуальний простір переймає й злочинність у її нових формах та проявах.

Все частіше підпадають під загрозу персональні дані, банківські рахунки, паролі, конфіденційна інформація як фізичних осіб, так і державного сектору, що виступають об'єктами кіберзлочинів.

Найпоширеніші злочинні схеми пов'язані з кардингом, фішингом, вішингом, соціальною інженерією тощо.

Існують чотири основні напрямки діяльності у сфері протидії злочинам, які вчиняються з використанням високих інформаційних технологій.

Перший напрямок - шахрайства, що вчиняються в мережі Інтернет, складають більше половини – приблизно 60%. Різноманіття шахрайських схем вражає, починаючи від банального використання інтернет-аукціонів та торговельних платформ накшталт OLX, закінчуючи створенням фейкових інтернет-магазинів, візуально схожих на відомі, так звані "брендові" ресурси.

Друга група – це безпосередньо злочини, які вчиняються з використанням спеціальних ІТ знань – хакерські атаки, викрадення інформації, блокування роботи систем з метою вимагання коштів тощо.

Третя група – це злочини у сфері платіжних систем, що пов'язані з використанням банківських платіжних карток, шахрайства з використанням скіммінгових пристроїв (пристрої для зчитування інформації на магнітній смузі карти, прикріплюються до банкоматів) і "білого пластику" (дублікати карток клієнтів закордонних банківських установ).

І четверта група злочинності – це протидія протиправному контенту, перш за все – розповсюдженню дитячої порнографії та припинення порушення авторських та суміжних прав.

Однак, сьогодні спостерігається тенденція зростання активності окремих осіб та груп, які спеціалізуються на виготовленні та використанні шкідливого програмного забезпечення:

- для блокування роботи комп'ютерів та комп'ютерних мереж підприємств у комерційних цілях;
- для отримання банківської інформації та використання її для несанкціонованого управління рахунками;
- отримання конфіденційної інформації, в тому числі й з метою вимагання коштів від потерпілих осіб за її нерозголошення;
- для інформаційного дезорієнтування населення та пропаганди населення з використанням комп'ютерів та їх мереж;

- для отримання стратегічно значущої інформації тощо.

Аналіз статистичних даних показав, що незважаючи на ужиті підрозділами кіберполіції заходи, кількість осіб, які вчиняють кіберзлочини зростає, та становить 56 осіб, яким вручені повідомлення про підозру у 2015 році, 87 осіб у 2016 році, 117 осіб у 2017 році та вже 25 осіб у поточному році.

Сучасний світ дуже тісно пов'язаний із використанням електронних пристроїв та комп'ютерної техніки, і це ще одна причина, чому кількість саме кіберзлочинів зростає. Натомість зростаюча кількість користувачів цієї техніки – не підготовлена.

Працівниками кіберполіції на постійній основі уживаються заходи з попередження указаної категорії злочинів, активно використовуються можливості як спеціальних агентів Департаменту кіберполіції, так і допомога осіб, які володіють спеціальними знаннями у сфері високих інформаційних технологій та організована на засадах взаємодії та партнерства.

*Як позитивний приклад такої роботи слід відзначити задокументовану злочинну діяльність мешканця м. Запоріжжя, який із використанням шкідливого програмного забезпечення, отримував доступ до управління смартфонами громадян, в результаті чого блокував ці пристрої та для відновлення їх роботи вимагав сплату грошових коштів на заздалегідь підготовлені карткові рахунки. Фігуранту повідомлено про підозру за ч. 1 ст. 189, ч. 1 ст. 361 КК України та обвинувальні акти надіслано до суду.*

Наразі, на базі Департаменту кіберполіції Національної поліції України впроваджені новітні технології та сервіси, які дозволяють миттєво реагувати на інформація від громадян про кіберзлочини чи кібератаку.

Департаментом кіберполіції створено цілодобовий «call-центр» для прийому заяв та звернень від громадян про злочини та правопорушення, що вчиняються в глобальній мережі, однак лише зусиль працівників кіберполіції у цьому напрямку не завжди достатньо. Захист українських користувачів від посягань кіберзлочинців залежить не тільки від роботи поліції, але й від того, наскільки користувачі обізнані з найпростішими правилами використання електронних пристроїв, сервісів та комп'ютерної техніки; наскільки відповідально відносяться до зберігання особистої або комерційної інформації, яка міститься в електронних носіях та сервісах тощо.

Для захисту інформації, що використовується підприємствами у своїй діяльності, працівниками кіберполіції акцентується увага підприємцям на кібербезпеці як окремій складовій бізнесу, що полягає у підтримці використовуваного програмного забезпечення в оновленому стані, використання антивірусних засобів та засобів контролю і моніторингу стану захищеності комп'ютерних мереж.

Кіберполіцією проводиться активна робота по інформуванню населення про способи та методи, що використовуються для вчинення кіберзлочинів, адже у 90% випадків злочини вчиняються через необізнаність громадян та при безпосередній участі потерпілих осіб, які тим чи іншим способом сприяють вчиненню злочинів: від завантаження шкідливого програмного забезпечення, до надсилання шахраям персональних даних, що використовуються

для вчинення карткових та інтернет-шахрайств.

Наразі, кіберполіцією переймається позитивний досвід протидії указаній категорії злочинів, що використовуються поліцейськими іноземних держав та проводиться активна робота з впровадження у практичну діяльність новітніх розробок у сфері високих інформаційних технологій.

**Грибан Віталій Григорович**
д.біол.н., проф., заслужений працівник
народної освіти України,
професор кафедри фізичного виховання

**Казначеєв Дмитро Георгієвич**
к.ю.н., доц., доцент кафедри фізичного виховання

**Хрипко Людмила Володимирівна**
к.н.ф.в. та с., доц.,
завідувач кафедри фізичного виховання
Дніпропетровського державного
університету внутрішніх справ

## БЕЗПЕКА ПРАЦІ ТА ОСОБИСТА БЕЗПЕКА ПРАЦІВНИКІВ НА СУЧАСНОМУ ЕТАПІ СТАНОВЛЕННЯ УКРАЇНИ

Людина в Україні, як правовій, демократичній державі, визнана найвищою соціальною цінністю [1]. Держава гарантує людині гідний рівень життя, здійснює соціальну політику на засадах соціальної справедливості і в інтересах усього суспільства, дає можливість людині працювати та забезпечує належні умови праці.

У Міжнародному пакті про економічні, соціальні й культурні права, прийнятого Генеральною Асамблеєю ООН 16 грудня 1966 року [2], зазначається, що право на працю - це право кожної людини отримати можливості заробляти собі на життя працею, яку вона вільно обирає або на яку вільно погоджується. Праця має особливий характер і потребує певної організації. З фізіологічної точки зору - це витрати фізичної і розумової енергії людського організму. Праця є необхідним і корисним процесом, за якого, проте, при певних умовах діяльності людина може піддаватися дії небезпечних і шкідливих факторів виробничого процесу, що негативно відбивається на її здорові [3]. Конституція України гарантує кожній особі право на належні, безпечні і здорові умови праці. Це конституційне положення стало своєрідним принципом, на якому вибудовується цілий комплекс правових, соціально-економічних, санітарно-гігієнічних і лікувальнопрофілактичних заходів та засобів, що формують систему охорони праці усіх зайнятих громадян. Але не дивлячись на це в Україні кількість нещасних випадків або надзвичайних подій, що трапляються на виробництві або у ході виконання службових

обов'язків, внаслідок яких працівники отримують травми або навіть гинуть, залишається дуже великою [4].

За останні роки кількість працюючих в умовах, що не відповідають установленим нормам з охорони праці, зросла з 15 до 30 відсотків від загальної чисельності працівників і складає майже 3 млн. людей.

Важливо відмітити, що на роботах з такими умовами праці ¼ таких працівників - жінки. Це негативно позначається на стані їх здоров'я, визиває порушення перебігу вагітності, викликає вади розвитку плоду та патологію серед народжених, що призводить до незадовільної демографічної ситуації в Україні

В середньому в шкідливих та небезпечних умовах праці на сьогоднішній день працює майже кожен третій робітник.

Продовжується негативна тенденція до збільшення кількості вперше виявлених профзахворювань, число яких складає 5000-7000 щорічно.

Майже 17 тис. громадян щороку стають інвалідами праці, понад 300 тис. осіб одержують компенсацію за відшкодування шкоди внаслідок трудового каліцтва або професійного захворювання. З них близько 50 тис. осіб отримують компенсацію у зв'язку з втратою годувальника.

За офіційними даними 5.5 млн працівників сфери малого і середнього бізнесу в Україні перебувають «у тіні», тобто працюють без юридичного оформлення трудових відносин з роботодавцями. Вони практично позбавлені права на цільове медичне обслуговування, пільги та компенсації за важкі та шкідливі умови праці, допомоги у разі нещасного випадку.

Небезпечна тенденція склалася в державі протягом останніх десяти років і з станом виробничого травматизму, коли більшість нещасних випадків, які сталися на підприємствах. приховуються від обліку та розслідування (більш ніж 70%), що призводить до порушення законних прав та інтересів потерпілих і не сприяє підвищенню рівня безпеки та посиленню профілактики виробничого травматизму. Протягом 2011 – 2015 років в Україні на виробництві щорічно реєструється в середньому до 13 тис. нещасних випадків. Із них майже 10 % - зі смертельним наслідком Набули масового характеру випадки, коли під тиском роботодавців про звільнення або пониження на роботі, потерпілі дають неправдиві свідчення, що дає змогу переводити нещасні випадки, які сталися на виробництві, до розряду таких, що не пов'язані з виробництвом, або до таких, що сталися у невиробничій сфері.

Ще гіршими є стан справ під час **розслідування** нещасних випадків зі смертельними наслідками, за результатами яких відповідні комісії пов'язують з виробництвом в середньому лише 42% таких нещасних випадків. Це в свою чергу залишає травмованих без належного соціального захисту, а сім'ї загиблих – без матеріальних відшкодувань у зв'язку з втратою годувальника, а фактично – без засобів для існування.

За рівнем смертності на виробництві, Україна випереджає всі країни ЄС і має найгірші показники, навіть в порівняльні з колишніми країнами СНГ (наприклад, Молдова, Естонія).

Одна людина гине: в Україні - із 10 травмованих, у Німеччині – із 1260

травмованих, у Словаччині – із 208 травмованих, у Польщі –із 145 травмованих

За такими показниками смертності на виробництві ситуація в Україні гірше у 126 разів ніж у Німеччині, майже у 20 разів ніж у Словаччині.

Крім людських втрат зазнає великих збитків і економіка країни. Величезні суми з резервних державних, Фондів соціального страхування та самих власників підприємств витрачаються на ліквідацію наслідків промислових аварій, нещасних випадків, профзахворювань та допомоги потерпілим та сім'ям загиблих на виробництві.

За останні десять років Фондом соціального страхування від нещасних випадків на виробництві та професійних захворювань України виплачено страхових виплат потерпілим на виробництві (членам їх сімей), реабілітацію та лікування потерпілих, оплату пільг і компенсацій працівникам за роботу у важких та шкідливих умовах праці понад 20 млрд. гривень.

Разом з цим, виправдовуючись кризою, Урядові структури, більшість підприємців почали економити на безпеці праці, знижуючи і без того мізерні відрахування на ці цілі, прагнучи досягти якомога більших прибутків за будь-яку ціну та саме сьогодні.

Гострою соціальною проблемою залишається також високий травматизм невиробничого характеру. За оцінкою фахівців Інституту демографії та соціальних досліджень НАН в Україні щорічні втрати економіки тільки внаслідок травмування і загибелі громадян у сфері, не пов'язаній з виробництвом, перевищують 10 млрд. грн., зокрема внаслідок загибелі – 9,2 млрд., а травмування, що призвело до тимчасової непрацездатності, – 1,12 млрд. грн. Це становить близько 2,5% ВВП України.

Щороку в Україні зникає від трьох до п'яти тисяч людей, із них, кожного п'ятого так і не вдається знайти. Великий травматизм має місце і на дорогах України. Так у 2016 році на автошляхах України мало місце 158776 ДТП, у тому числі 26782 пригоди з постраждалими, в яких отримали травми 37041 особа, з них 3410 загинули.

Наявність цих проблем створює негативний вплив на результати проведення економічних та соціальних реформ з відновлення економічного зростання і модернізації економіки держави. За модульною оцінкою Міжнародної організації праці в розвинутих країнах світу внаслідок нещасних випадків на виробництві та професійних захворювань, ліквідації наслідків промислових аварій щорічно в середньому втрачається близько 4% відсотки ВВП

Український ВВП складає близько 1,5 трильйона гривен, відтак відповідно до методик та розрахунків МОП та країн ЄС: кожного року Україна втрачає, принаймні 60 мільярдів гривень від негативних наслідків небезпечного виробничого середовища та поганих умов праці.

На сьогоднішній день є нагальна необхідності розроблення та реалізації такої політики у сфері охорони праці та особистої безпеки, яка б забезпечила встановлення нормативів і параметрів безпеки праці, визнаних міжнародним співтовариством, та обсягів фінансування організаційних та технічних заходів на кожному робочому місці, які б звели до мінімуму ризики травмування

і професійного захворювання, а також здійснення заходів з відновлення втраченого здоров'я працівників.

Професійна діяльність працівників правоохоронної галузі становить гостру проблему щодо їх безпеки. Викликані багатьма соціальними, економічними та іншими чинниками загострення кримінальної обстановки, зростання злочинності в її найбільш агресивних формах призводять до того, що випадки виникнення екстремальних ситуацій, коли життю або здоров'ю працівника цієї галузі загрожує реальна небезпека, стають все частішими. Від 7 до 12 % працівників під час виконання службових обов'язків зазнають тяжких фізичних та психічних травм.

Дані науково-дослідницького інституту НАВСУ вказують на те, що з 1990 по 1997 рр. за різних обставин загинуло 564 та поранено 3769 працівників ОВС України. Серед усіх надзвичайних подій випадки загибелі працівників становили у середньому 25 чоловік на рік. В останні роки ці показники не зменшились, а навпаки, зросли. Зростає кількість нещасних випадків серед суддів, адвокатів, прокурорів та іншитх фахівців права, повязаних з їх професійною діяльністю. Останній трагічний випадок з правозахисницею Іриною Ноздовскою, яка була умисно вбита 1 січня 2018 рокуза свою професійну діяльність.

Колегія та керівництво МВС України неодноразово вказували на визнання безумовності пріоритету життя і здоров'я особового складу над будь-якими інтересами чи завданнями оперативно-службової діяльності і на необхідність запобігання надзвичайним подіям, пов'язаним із втратами та пораненнями працівників органів внутрішніх справ (рішення розширеного засідання колегії МВС України № 6 КМ/2 та № 9 КМ/1 за 1997, 2001 рр.).

Дотримання Закону «Про охорону праці» і Кодексу України про працю, Закону України «Про національну поліцію», навчання курсантів, студентів, працівників щодо охорони праці та профілактична своєчасна робота є запоруком того, що кількість виробничих травм і професійних захворювань людей зменшиться як на виробництві, так і поза ним.

Основними заходами щодо охорони праці та особистої безпеки в правоохоронній діяльності є:

1. Професійні заходи передбачають набування та удосконалення досвіду службової, бойової, оперативної підготовки, з метою його умілого використання.

2. Духовні заходи передбачають дотримання культури поведінки з колегами по роботі, з громадянами, з особами, які підозрюються у вчиненні злочинів, в сім'ї та стійку моральну поведінку в різних ситуаціях.

3. Правові заходи – це відповідність правової нормативної бази об'єктивним умовам і завданням професійно-службової діяльності. Вони передбачають знання правових норм, тримання їх при виконанні службових обов'язків та розробку відповідних нормативних актів.

4. Тактичні заходи – знання тактики дій злочинців, і з урахуванням цього уміле застосування своїх тактичних дій з метою затримання злочинця, одержання перемоги над ним з мінімальними втратами і максимальними

прибутками.

5. Психологічно-педагогічні заходи – передбачають мобілізованість психіки, настроєність на більш доцільні, активні, рішучі дії та готовність до дій в складних чи небезпечних для життя чи здоров'я ситуаціях.

6. Фізичні заходи – вміння застосовувати заходи протидії злочинним посяганням на життя і здоров'я . Вони передбачають фізичний розвиток, володіння прийомами рукопашного бою , а також формування стійкого психомоторного стану до зовнішніх проявів небезпеки, з метою захисту виконання професійних дій.

7. Індивідуальні заходи – сукупність індивідуальних якостей і властивостей співробітника, його здатність ефективно застосовувати необхідні заходи і засоби з метою забезпечення особистої безпеки.

1. Конституція України від 28 червня 1996 р. –К., 2007.

2.. Скринька. Д. В Міжнародний пакт про економічні, соціальні та культурні права 1966 // Українська дипломатична енциклопедія: У 2-х т./Редкол.: Л. В. Губерський (голова) та ін. — К.: Знання України, 2004.

3. Грибан В.Г. Охорона праці в галузі права: Навчальний посібник Грибан В.Г.,Глуховеря В.А.). Д.:Дніпропетровський університет внутрішніх справ, 2016.- 252 с.

4. https://pon.org.ua/novyny/4608-stan-oxoroni-praci-v-ukrayini-ekonomiya-na.html

**Дубницький Володимир Іванович**
д.е.н., проф., професор кафедри
теоретичної та прикладної економіки
ДВНЗ «Український державний
хіміко-технологічний університет», м. Дніпро

**Колодинський Сергій Борисович**
д.е.н., доц., професор кафедри менеджменту
та управління проектами
ДВНЗ «Одеська державна академія
будівництва та архітектури», м. Одеса

**Овчаренко Ольга Вікторівна**
аспірант, викладач кафедри
теоретичної та прикладної економіки
ДВНЗ «Український державний
хіміко-технологічний університет», м.Дніпро

## ОСНОВНІ МЕТОДОЛОГІЧНІ ПІДХОДИ ДО ДОСЛІДЖЕННЯ ОЦІНКИ ЕКОНОМІЧНОЇ БЕЗПЕКИ РЕГІОНУ

Економічна безпека є найбільш важливою складовою структури національної безпеки країни, оскільки без достатнього економічного забезпечення не може йти мова про національну стабільність, стійкість розвитку, самодостатність господарства. Без її забезпечення практично неможливо вирішити

жодної із задач, що стоять перед країною, як у внутрішньодержавному, так й у міжнародному плані.

Економічна безпека є основою життєдіяльності суспільства, його соціально-політичної й національно-етнічної стабільності і являє собою складне, багатогранне соціально-економічне явище, що відображає комплекс динамічних умов всіх соціально-економічних процесів, що виникають у суспільстві.

Аналіз зовнішніх і внутрішніх факторів забезпечення економічної безпеки показує, що причини складних загроз економічної безпеки країни мають яскраво виражений регіональний характер і диференційовані по регіонах.

Регіональна економічна безпека має чітко виражену специфіку, обумовлену сукупністю різних унікальних умов: географічним положенням, кліматом, ступенем забезпеченості природними ресурсами, чисельністю населення, розвиненістю інфраструктури й ін.

Заходи, що здійснюються державою в теперішній час, по створенню системи державного керування економічною безпекою вже призвели до певних результатів: на рівні країни прийнята концепція національної безпеки й стратегія економічної безпеки. На жаль, реалізовані заходи на регіональному рівні носять фрагментарний характер, не у всіх регіонах займаються питаннями економічної безпеки, крім того, зберігається цілий ряд серйозних проблем, що здійснюють стримуючий вплив на її забезпечення.

Вирішальне значення для забезпечення економічної безпеки регіону має попередження загроз, що зароджуються, а не пасивне слідування наслідкам їхнього впливу. Для розробки превентивних заходів необхідно чітко визначити показники й індикатори соціально-економічної безпеки регіону, які дозволять визначити природно-ресурсний потенціал регіону: рівень ефективності використання в регіоні виробничих фондів, капіталу й праці; конкурентоздатність економіки, а також стан соціальної стабільності в регіоні й умови запобігання й вирішення можливих соціальних конфліктів.

Показники економічної безпеки - це найбільш значимі параметри, що дають уяву про стан економічної системи в цілому, її стабільність й мобільність. Система показників, що характеризують стан економічної безпеки регіонів, не може бути єдиною для всіх й, крім загальноприйнятих значимих параметрів, повинна оцінювати, насамперед, специфічні особливості економіки регіону й ті її сфери, де велика ймовірність настання загроз.

Незважаючи на важливість системи індикаторів безпеки в забезпеченні й підвищенні рівня економічної стабільності регіону, в Україні на сьогоднішній день не існує єдиної прийнятої й законодавчо закріпленої методики розрахунку індикаторів й їхніх граничних значень для нормалізації показників економічної безпеки на рівні регіону.

Для оцінки регіональної економічної безпеки використовуються різні методи, кожний з яких має певні недоліки й переваги. Вивчення методик вітчизняних учених по оцінці економічної безпеки регіону дозволило авторам виділити й систематизувати основні методологічні підходи до дослідження розглянутої проблеми (табл. 1)

Таблиця 1

Класифікація сучасних методів оцінки економічної безпеки регіону

| Метод (методика) | Представники | Основні положення | Недоліки |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| Динамічний – оцінка динаміки розвитку регіону по темпах росту його основних макроекономічних показників | І.В. Долматов, І.М. Мухітов, І.А. Соколов | Головними індикаторами економічної безпеки прийняті соціальні індикатори | Не конкретизовано показники. Відсутні показники, що характеризують ситуацію в економіці регіону і їхні граничні значення |
| Эконометричний – оцінка на основі багатомірного статистичного аналізу методу найменших квадратів й ін. | І.В. Дюженкова, О.С. Філеткін | Використання інтегральних показників, що характеризують економічну й соціальну сферу регіону | Методики громіздкі й у деяких випадках піддається сумніву взаємозв'язок між окремими |
| | | | показниками, часто відсутні граничні значення |
| Макроекономічний – порівняння основних макроекономічних показників з їхніми граничними значеннями | І.М. Воронін, І.В. Новікова, Н.І. Красніков, З.З. Абдулаєва | Застосовуються показники, що характеризують розвиток економіки й соціальної сфери регіону | Губиться унікальність (специфіка) регіону, тобто його показники зрівнюються з усередненими по країні, або з максимальними значеннями |
| Експертно-рейтинговий – рейтингові, бальні й експертні оцінки при ранжируванні регіонів за рівнем загроз | С.В. Гук, С.И. Волков | Використання рейтингових, бальних експертних оцінок, інтегральних показників | Відсутні граничні значення, велика ймовірність суб'єктивізму, неможливості довести результати, отримані на його основі, точними характеристиками |
| Економіко-математичний – оцінка наслідків загроз через кількісний вимір шкоди | Л.И. Гончаренко, Э.А. Уткін, А.Ф. Денисов | Функціональний аналіз безпеки території, заснований на оцінці ймовірності настання окремих негативних подій і ймовірній величині шкоди | Дана методика більше підходить для окремого підприємства, а не для регіону |
| Комплексний – комплексна оцінка економічної безпеки регіону | Г.А. Олейніков, В.С. Сальников, И.В. Дюженкова | Застосовуються різні комбінації перерахованих вище методик | Поєднує й сполучає в собі розглянуті в інших методах недоліки |

На основі порівняльної характеристики розглянутих методик виявлені їхні базові положення й властиві їм недоліки:

- відсутність єдиної системи індикаторів і граничних значень;
- застосування складних і громіздких розрахунків при визначенні окремих показників з використанням багатомірних статистичних методів;
- використання функціонального аналізу, характерного для окремого підприємства, а не для регіону;
- широке використання експертних оцінок, при застосуванні яких велика ймовірність суб'єктивізму, неможливість довести результати, отримані на їх основі, точними характеристиками.

Таким чином, можна констатувати, що практично в жодній з розглянутих наукових праць не пропонується система індикаторів й їхніх граничних значень для оцінки економічної безпеки регіону, що відображають його специфічні особливості.

Запропоновано інтегральний показник рівня економічної безпеки регіону ($К_{РЕБР}$), сформований на основі окремих показників, згрупованих по стратегічних напрямках.

Для об'єднання окремих нормованих даних у єдиний інтегральний показник методом «згортки» пропонуємо використати формулу простої середньої арифметичної, застосування якої припускає, що всі ключові показники взаємозамінні й зниження значення одного з нормованих показників повністю компенсується в інтегральній оцінці іншою позитивною зміною значення нормованого показника (формула 1):

$$К_{РЕБР}=\frac{\sum К_i}{n} \qquad (1)$$

де n - число стратегічних напрямків аналізу економічної безпеки регіону.

Застосування середньої арифметичної обґрунтоване з математичної точки зору, оскільки ми розглядаємо систему показників, що не перебувають у функціональній залежності і мають однакову вагу, що визначається умовою підбора показників.

Рівень значимості для кожного окремого показника пропонується визначити як співвідношення фактичних і граничних значень показників. Даний прийом дозволяє перейти до єдиної безрозмірної величини, що дуже важливо для системи запропонованих показників, які мають різні одиниці виміру й провести нормування щодо граничного значення, яке приймається за одиницю.

Коефіцієнт значимості (співвідношення) розраховується як відношення фактичного значення до граничного, якщо бажано збільшення відповідного показника економічної безпеки ($Кі_1$) і навпаки, якщо бажано його зниження ($Кі_2$) (формули 2 й 3):

$$Кі_1=\frac{Уф_1}{Уп_1} \qquad (2)$$

$$Ki_2 = \frac{Уп_1}{Уф_1} \qquad (3)$$

де $Ki_1$ й $Ki_2$ – коефіцієнти значимості (співвідношення) фактичного й граничного значення показника;

$Уф_i$ – фактичне значення показника;

$Уп_i$ – граничне значення показника

Основними задачами керування економічною безпекою є: оцінка й розробка напрямків діяльності по забезпеченню економічної безпеки; розробка пропозицій щодо вдосконалювання взаємодії між учасниками системи; планування й проведення контрольних і профілактичних заходів щодо безпеки.

У зв'язку з тим, що основним бар'єром на шляху виникнення кризових ситуацій в економічній безпеці регіону повинна стати скоординована діяльність органів влади, виникає необхідність у визначенні інструмента реалізації ними своїх функцій і повноважень по забезпеченню безпеки. Таким інструментом повинна стати регіональна цільова програма по забезпеченню економічної безпеки.

Таким чином, забезпечення економічної безпеки регіонів вимагає розробки й здійснення комплексу заходів у рамках програм соціально-економічної безпеки й стійкого розвитку регіону.

**Дубницький Володимир Іванович**
д.е.н., проф., професор кафедри
теоретичної та прикладної економіки

**Науменко Наталія Юріївна**
к.т.н., доц., доцент кафедри теоретичної
та прикладної економіки

**Тутаєва Ольга Володимирівна**
інженер І категорії кафедри
теоретичної та прикладної економіки
ДВНЗ «Український державний
хіміко-технологічний університет»

## АСПЕКТИ ПРОЦЕСУ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Управління інформаційною безпекою займає все більш значиме місце у функціонуванні будь-якої організації, застосовує сучасні технології збору, зберігання і обробки інформації. Даний процес ґрунтується на періодичному проведенні аналізу інформаційних ризиків, який дозволяє своєчасно виявити

загрози інформаційної безпеки, уразливості інформаційної системи, впроваджувати відповідні заходи по їх нейтралізації та, як наслідок, постійно відстежувати стан інформаційної безпеки в організації, з огляду на попередній досвід і нові загрози і вразливості.

Інформаційна безпека – це захищеність інформаційних систем й інформаційних ресурсів від зовнішніх та внутрішніх загроз, ускладнюють ефективне використання інформації суспільством, державою, окремими особистостями. Інформаційна безпека повинна вирішувати такі завдання:

– виявлення, оцінка й запобігання загроз інформаційним системам та інформаційним ресурсам;

– захист прав юридичних та фізичних осіб на інтелектуальну власність, а також збір, накопичення і використання інформації;

– захист державної, службової, комерційної та особистої таємниці.

Інформаційна безпека тісно пов’язана з функціонуванням інформаційного ринка, найбільш розгалуженою частиною якого є область інформації, а її головним сектором виступає економічна інформація, яка, в свою чергу, безпосередньо зв’язана з проблемою забезпечення економічної безпеки країни та її регіонів в цілому, різних господарюючих суб'єктів, людської особистості. Світовий досвід розвитку інформаційного ринку показує, що управлінська та підприємницька діяльність має велику потребу в економічній інформації, а також інформації соціального характеру.

Ціль процесу оцінювання ризиків полягає у визначенні характеристик ризиків по відношенню до інформаційної системи (ІС) та її ресурсам (активам). На основі отриманих даних можуть бути обрані необхідні засоби захисту. При оцінюванні ризиків враховуються багато факторів: цінність ресурсів, оцінка значущості загроз та вразливостей, ефективність існуючих й плануючих засобів та багато іншого.

Використання інформаційних технологій (ІТ) в бізнес-процесах сучасних організаціях є ефективним інструментом підвищення продуктивності праці. Однак, ІС організацій часто має неструктурований характер, що тягне за собою зростання вразливостей і ризик порушення інформаційної безпеки (ІБ).

Базовий рівень безпеки (baseline security) – обов’язків мінімальний рівень захищеності для ІС. В ряді країн існують критерії для визначення цього рівня. В якості приклада наведемо критерії Великобританії – CCTA Baseline Security Survey, що визначають мінімальні вимоги в області ІБ для державних установ цієї країни. У Німеччині ці критерії викладені в стандарті BSI.

Базовий (baseline) аналіз ризиків ІС – аналіз ризиків проводиться відповідно до вимог базового рівня захищеності. Найбільш трудомісткім є процес оцінювання ризиків, який умовно можна розділити на наступні етапи: ідентифікації ризику; аналіз ризику; оцінювання ризику. На мал. 1 надана концепт-модель процесу оцінки ризику ІБ.

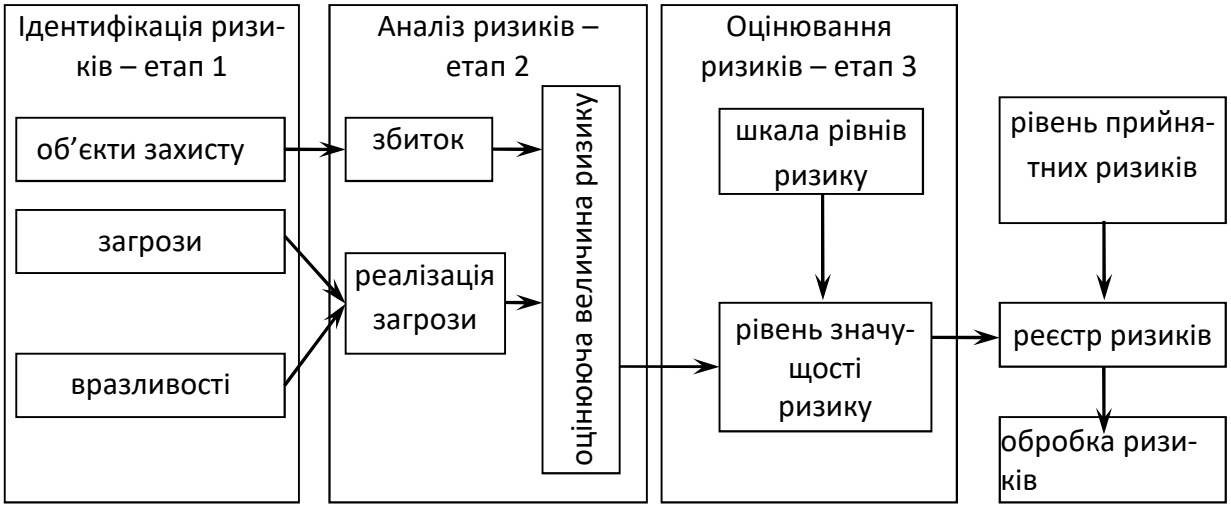



*Рис. 1. Концепт-схема процесу оцінки ризиків інформаційної безпеки*

Ідентифікація ризику в рамках ІС полягає в складанні переліку та описі елементів ризику: об'єктів захисту, загроз, вразливостей. Прийнято виділяти такі типи об'єктів захисту: інформаційні активи; програмне забезпечення; фізичні активи; сервіси; люди, а також їх кваліфікації, навички й досвід; нематеріальні активи (НМА), також як репутація та імідж організації. Як правило, на практиці розглядають перші три групи. Решта об'єктів захисту не розглядаються в силу складності їх оцінки. На етапі ідентифікації ризиків ІБ (мал. 1) так само виконується ідентифікація загроз і вразливостей. В якості вихідних даних для цього використовуються результати аудитів: дані про інциденти ІБ; експертні оцінки користувачів, фахівців з ІБ, ІТ-фахівців та зовнішніх консультантів.

На рис. 2 представлена концепт-модель побудови системи інформаційної безпеки. Представлена модель ІБ – це сукупність об’єктивних зовнішніх та внутрішніх факторів та їх вплив на стан інформаційної безпеки на об’єкті та на збереження матеріальних чи інформаційних ресурсів. Розглядаються наступні об’єктивні фактори:

– загрози ІБ, які характеризуються імовірністю виникнення та імовірністю реалізації;
– вразливості ІС чи системи контрзаходів (системи ІБ), які впливають на імовірність реалізації загрози;
– ризик-фактор, який відображає можливий збиток організації в результаті реалізації загрози ІБ: витоку інформації та її неправомірного використання(ризик в кінцевому підсумку відображає імовірні фінансові втрати - прямі або непрямі), а також інтелектуально-технологічні втрати та т.д.

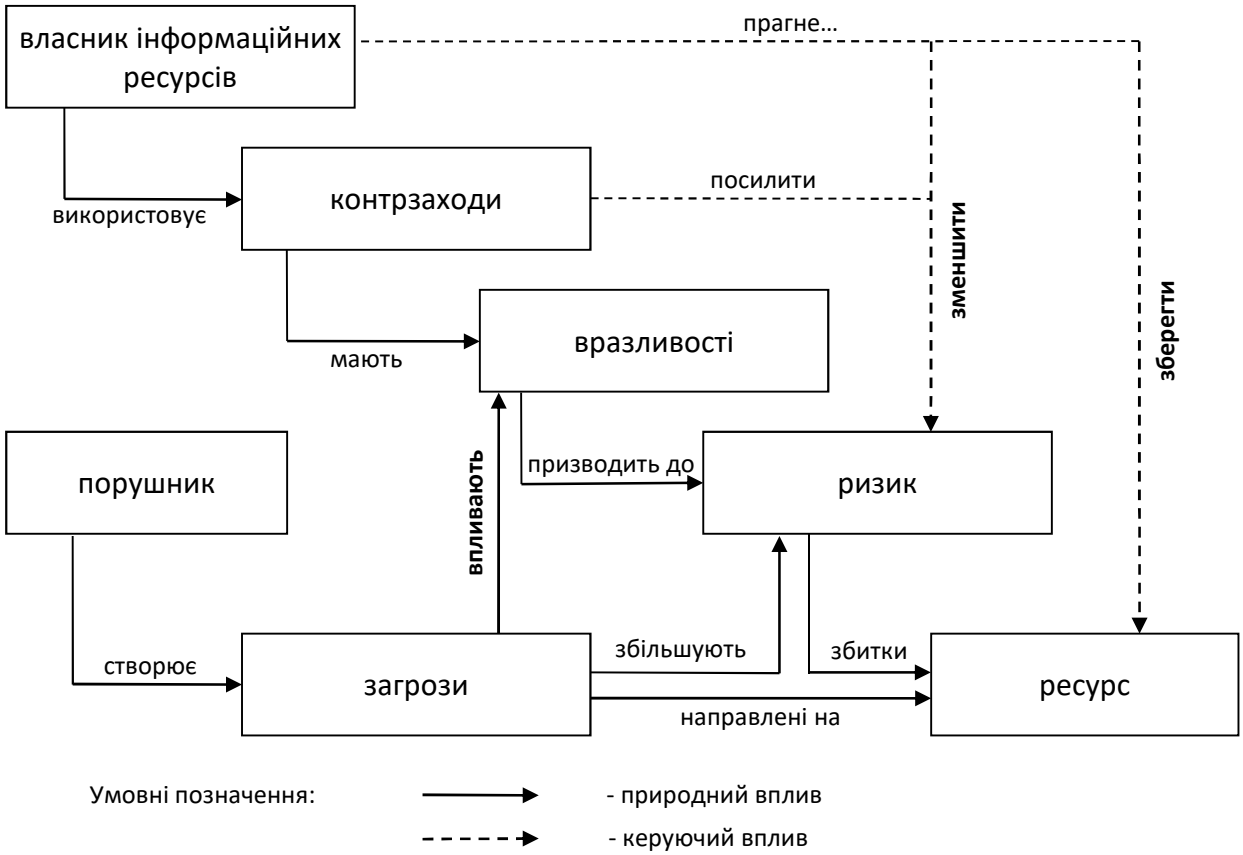



*Рис. 2. Концепт-модель будови системи ІБ*

Для будови збалансованої системи ІБ передбачається спочатку провести аналіз ризиків в області ІБ. Потім визначити оптимальний рівень ризику для організації на основі заданого критерію. Систему ІБ (контрзаходи) належить побудувати таким чином, щоб досягти заданого рівня ризику. Система інформаційної безпеки об'єкта виявиться ефективною, якщо вона буде надійно підтримувати виконання правил політики безпеки, і навпаки. Кроками побудови організаційної політики безпеки є:

– внесення до опису об’єкта автоматизації структури цінності та проведення аналізу ризику;

– визначення правил для будь-якого процесу використання даним видом доступу до ресурсів об'єкта автоматизації, які мають даний ступінь цінності.

Ризик ІБ в рамках функціонуючої ІС – це комплексна величина, що визначається як функція (або функціонал) ряду факторів, таких загроз ІБ, потенційно можливий збиток і уразливості ІС. Аналіз інформаційних ризиків, незважаючи на наявні специфічні для нього нюанси в різних сферах діяльності, являє собою упорядкований алгоритм, що складається з однакових етапів, на кожному з яких можуть бути застосовані свої методи (мал. 3). Аналіз потоків даних ефективно реалізується з допомогою сучасних структурних методів [1, 2]. Наприклад, в працях [3, 4] для розробки функціональної моделі, описуючий інформаційні процеси використовується методологія IDEFO.

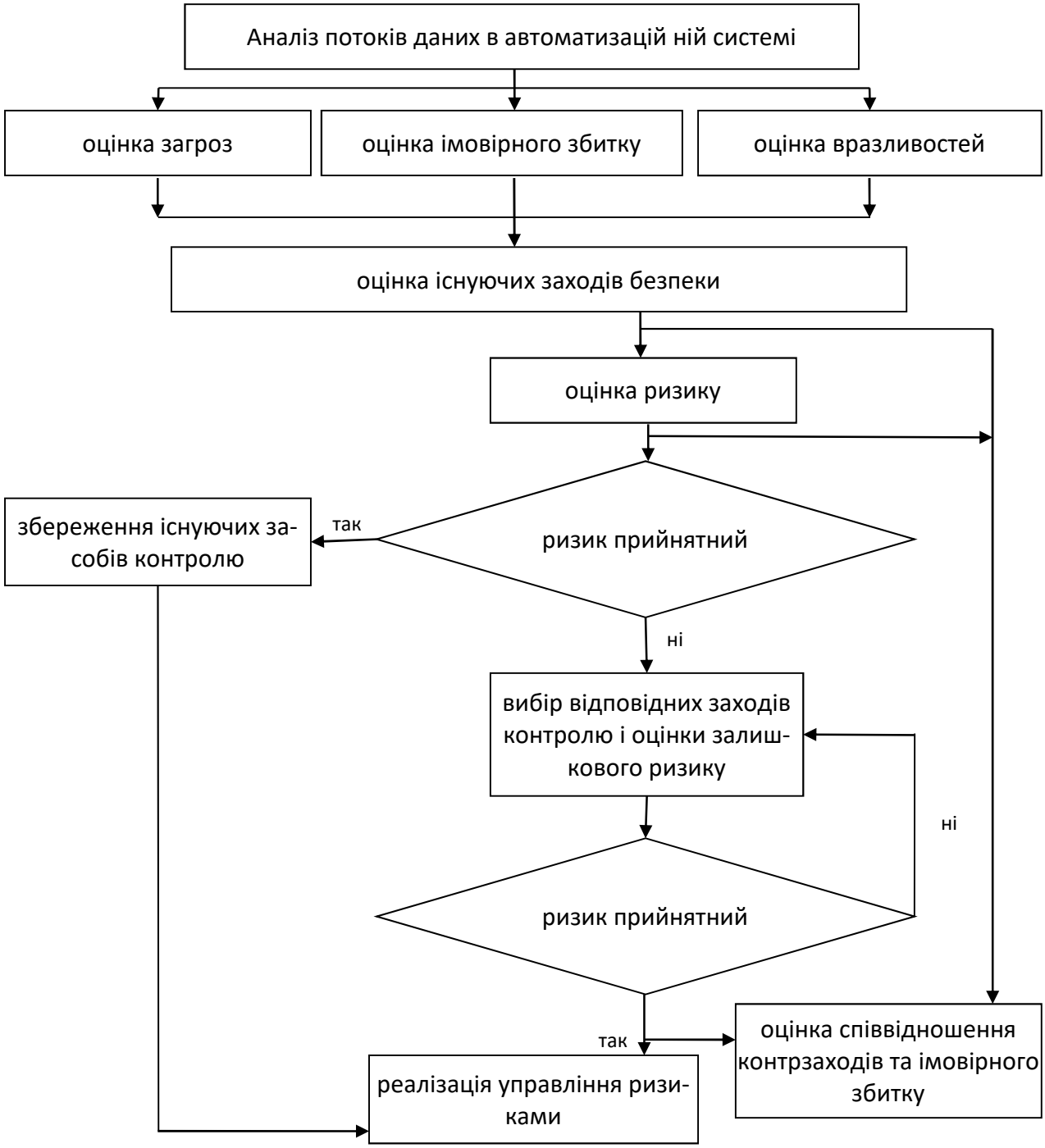



*Рис. 3. Процес аналізу інформаційних ризиків в рамках ІС*

1. Миков Д.А. Анализ методов и средств, использованных на различных этапах оценки рисков ИБ. // Вопросы кибербезопасности. – 2014. - №4(7). – С. 49-54.

2. Велигура А.Н. О выборе методики оценки рисков ИБ. // Information Security / Информационная безопасность. – 2008. - №4. – С. 16-17.

3. Баранова Е.К. Методики анализа и оценки рисков ИБ. // Обозревательніе ресурсі и технологи. – 2015. - №1(9). – С. 73-79.

4. Корченко А.Г., Архипов А.Е., Казмирчук С.В. Анализ и оценивание рисков информационной безопасности. – К.: «Лазурит-Полиграф», 2013. – 275 с.

**Евчук Сергей Алексеевич**
сотрудник forensic manager

**Неделков Кирилл Юрьевич**
сотрудник forensic investigator,
Общество с ограниченной ответственностью
«Группа информационной безопасности «ФС ГРУП»,
г. Одесса

## COMPUTER FORENSIC INVESTIGATOR - КОГДА НУЖНА ЭКСПЕРТИЗА

Вы директор/бухгалтер предприятия и обнаружили, что с счета были несанкционированно списаны деньги (или попытка) путем создания электронного платежа. Самая распространенная схема кражи денег через системы ДБО.

Вы стали жертвой мошенничества (пополняли счет, осуществляли платежи) в интернете, отправляли одному отправили другому (фишинг).

Файлы на компьютере зашифрованы вы их не видите/не можете получить доступ, и преступники вымогают деньги за раскодирование. (Криптор).

Во время запуска компьютера появляется окно с требованиями перечислить деньги за возможность использования операционной системы (Локер).

На почту пришло подозрительное сообщение с файлом или ссылкой, и вы открыли их, после чего компьютер стал медленно работать или вести себя “странно” - скорее всего ваш компьютер был заражен трояном (вирусом), который может похитить Ваши данные и использовать Ваш компьютер как часть сети для совершения других преступлений. (Бот-нет, трояны)

Страница Вашего сайта была изменена (дефейс) - хакеры получили доступ к вашему сайту с правами администратора (использовали уязвимость, эксплоиты, залили шелл), т.е. могли скопировать все данные и использовать Ваш сайт для массового заражения пользователей/рассылки спама/использовать для других киберпреступлений. (Дефейс, заливка shell`a, exploit).

Информация на сервере/компьютере Вашей компании была удалена/изменена/похищена. Вы хотите узнать, что произошло, когда, кто мог сделать (инсайдер или из вне).

Кто-то похитил Ваши логин/пароль от соц. сетей, почты, др. сайтов - скорее всего на компьютере или моб. устройстве имеется вирус (стиллер, кейлоггер) и все вводимые данные перехватываются хакерами. (steeller, keylogger) или ваш браузер изменен/подменен/инфицирован, что также дает возможность перехватывать вводимые данные.

Вы являлись владельцем домена, но теперь Ваш домен принадлежит другому, и он требует деньги за возврат домена (вымагательство не обязательно) - это увод домена http://www.vedomosti.ru/newspaper/articles/2015/03/19/derzhi-vora-domenov

На каком-то ресурсе вы увидели информацию о себе или о своей компании и хотите, используя юридические рычаги заблокировать/удалить/изменить информацию, но Вам нужно правильно (по закону, в соответствии с правовыми нормами) оформить факт наличия данной инфор-

мации на сайте (портале, форуме, и т.п.) для последующего обращения в суд/полицию/др. инстанции.

Вы являетесь владельцем (или по поручению владельца защищаете интересы) объекта интеллектуальной собственности, но обнаружили, что кто-то, нарушая Ваши права использует их в своих интересах и собираетесь восстановить нарушенные права через суд/полицию и Вам, нужно зафиксировать данный факт нарушения.

В результате проведения экспертизы, готовится вывод по исследованию с описанием и результатом, полученным в ходе экспертизы, который правильно оформлен (по закону, в соответствии с правовыми нормами) для последующего обращения в суд/полицию/др. инстанции.

Исследование компьютерной техники и программных продуктов. http://rase.minjust.gov.ua/

Исследование телекоммуникационных систем (оборудования) и средств. https://www.eccouncil.org/programs/computer-hacking-forensic-investigator-chfi/

**Іванова Марина Іллівна**
к.е.н, доц., доцент кафедри
цивільно-правових дисциплін
Дніпропетровського державного
університету внутрішніх справ

## УПРАВЛІННЯ КОРУПЦІЙНИМИ РИЗИКАМИ В СУЧАСНИХ УМОВАХ

Корупція в Україні є системним явищем, що супроводжує соціально-економічний розвиток будь якої країни світу. Ускладнення офіційно можливих та законних шляхів отримання бажаного змушує людей шукати більш складних, заплутаних та тіньових схем реалізації корумпованих схем.

Згодні із Ю.В. Дмитрієвим, що нашій державі необхідно звернути увагу на розгляд передових європейських систем управління корупційними ризиками у сфері державного управління, які довели на практиці свою ефективність, з метою запозичення зарубіжного досвіду. При цьому за умов масштабної корупції акцент повинно бути зроблено саме на виявленні та усуненні причин, а не боротьбі з конкретними її проявами. Зокрема, для правових систем деяких розвинених країн взагалі нехарактерне використання в законодавстві терміна «боротьба», законодавці закладають в нормативно-правовому акті принципи (або механізми) оцінювання та мінімізації корупційних ризиків, що стосуються певної сфери діяльності [1].

За Д.А. Красніковим сфера національної економіки завжди виступає саме тим полігоном, на якому й розгортається найбільша боротьба за незаконні прибутки, винагороди, економічні переваги. Корумпованість економіки призводить до ослаблення фінансової системи держави, оскільки приватний бізнес переходить у тіньовий сектор, від цього не працюють на повну силу

система оподаткування і правила підприємницької діяльності, постійно порушується законодавство, що у свою чергу підриває довіру до державного апарату в цілому та завдає фінансових втрат державному бюджету [2].

Відтак, авторське бачення зводиться то того, що ***корупційними ризиками*** доцільно вважати ймовірність втрат державного бюджету через вплив на систему державного управління сукупності умов та факторів, що сприяють можливості виникнення корупції і продукують небезпеку прояву негативних наслідків для життєдіяльності як окремої особи, так, і суспільства, і держави.

Для мінімізації втрат державного бюджету і вище згаданих негативних наслідків корупційними ризиками необхідно управляти. При цьому вважаємо, що це управління повинно базуватися на аналізі ризику під час прийняття управлінських рішень, що демонструє рис. 1

Усі втрати держаного бюджету доцільно класифікувати за такими видами:

1) фінансові втрати – це прямий грошовий збиток, що може бути нанесений державі через реалізацію корупційного ризику;

2) матеріальні втрати – це непередбачені державним бюджетом додаткові витрати чи прямі втрати окремих виробничих комплексів тощо;

3) втрати часу – це такі втрати, що пов’язані з нераціональним його використанням внаслідок виникнення корупційного ризику. Втрати часу розділяють на дві групи втрат:

- трудові втрати – втрати робочого часу, які викликані випадковими обставинами;
- неефективна організація – це такі втрати, що виникають у тому випадку, коли процес будь-якої господарської діяльності здійснюється повільніше, ніж це було узгоджено раніше;

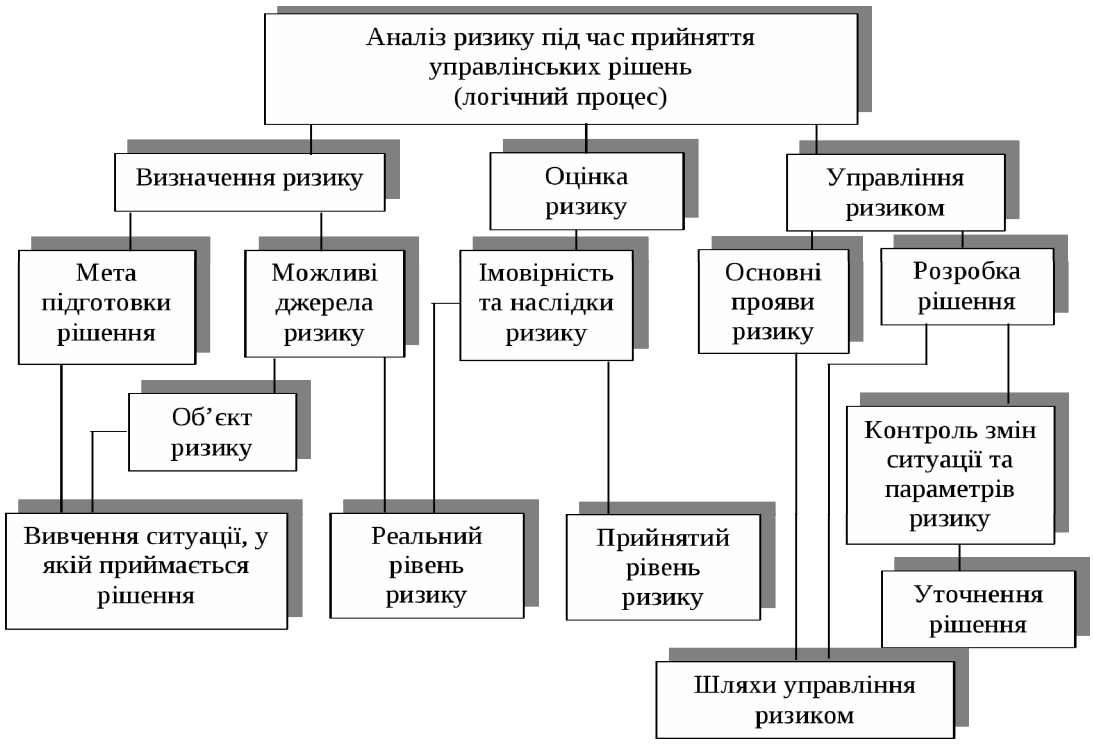



*Рис. 1. Аналіз корупційного ризику як необхідна складова управління*

4) соціальні втрати – це такі види втрат, що пов'язані з нанесенням збитку здоров'ю і життю людей – громадян України;

5) екологічні втрати – це нанесення шкоди навколишньому природному середовищу. Ці витрати поділяються на прямі і непрямі:

- прямі – це втрати, що виникають безпосередньо в країні, та відчуваються через короткий проміжок часу;
- непрямі втрати – виникають в тому випадку, якщо шкідливий вплив на навколишнє середовище буде впливати на функціонування держави через тривалий час;

6) морально-психологічні втрати – обумовлені тим, що будь-який корупційний механізм впливає на наявну соціальну систему, а порушення рівноваги цієї системи призводить до небажаних наслідків.

Аналіз корупційного ризику здійснюється з точки зору їх якісної та кількісної оцінки.

Якісний аналіз є найбільш складним і вимагає ґрунтовних знань, досвіду та інтуїції в даній сфері економіко-політичної діяльності. Його головна мета – визначити чинники, сферу корупційного ризику, після чого ідентифікувати усі можливі прояви. Кількісний аналіз ризику, тобто кількісне (числове) визначення ступеня корупційного ризику в цілому, є достатньо складною проблемою, яка потребує використання спеціального інструментарію.

1. Дмитрієв Ю.В. Європейські механізми управління корупційними ризиками в системі державного управління / Ю.В. Дмитрієв // Теорія та практика державного управління. – 2016. - Вип. 2. – С. 199–205.

2. Красніков Д. А. Наслідки корупції для фінансової системи держави / Д. А. Красніков // Теорія та практика державного управління. – 2013. – Вип. 2. – С. 206–212.

**Ісмайлов Карен Юрійович**
к.ю.н., завідувач кафедри кібербезпеки
та інформаційного забезпечення

**Балтовський Олексій Анатолійович**
д.т.н., доц., професор кафедри
кібербезпеки та інформаційного
забезпечення Одеського державного
університету внутрішніх справ

## ПІДХОДИ ТА ЯВИЩА ДЛЯ ОПТИМШЗАЦІЇ УПРАВЛІННЯ БД ІАСУ

Удосконалення управління організаціями вимагає організації інформації, на основі якої здійснюється: аналіз; корегування ходу роботи об'єкта управління; прийняття рішень для виправлення ситуації, що утворилася, і виведення об'єкта управління на заплановані показники; планування і ухва-

лення рішень по оперативному управлінню роботою організацій.

Основне завдання оперативного управління полягає в узгодженні всіх елементів загального процесу в часі та просторі з необхідним ступенем деталізації. Тому інформаційне забезпечення необхідно розглядати як діяльність, в процесі якої відбувається об'єднання інформаційних ресурсів з інформаційними процесами, що дозволяють довести інформацію в чистому або перероблену вигляді до споживача.

Інформація повинна мати певну структуру і характеризувати об'єкт або предметну область як в кількісному, так і в якісному відношенні.

Для забезпечення ефективного оперативного управління організацій необхідно заздалегідь визначити тип моделей даних і сучасний підхід до створення баз даних.

В теперішній час для зберігання, обробки і управління даними використовують різні підходи до побудови баз даних, найбільш вивченим і поширеним, з яких є реляційний підхід.

Проте при використанні такого підходу в нетрадиційних додатках з складною структурою даних виявляється його деяка надмірність.

Тому, зараз, коли для управління організаціями використовуються інтегровані автоматизовані системи управління (ІАСУ) таких областей стає все більше, досліджуються напрями, що виходять за межі реляційної моделі даних.

Вироблення управлінських рішень можливе лише на основі обліку всього комплексу задач управління організацій. Більшість авторів [1-6], досліджують в своїх роботах окремі сторони проблеми і йдуть по шляху моделювання окремих процесів управління. Проте моделювання і вирішення приватних задач не вирішує проблему комплексного управління організацій. У зв'язку з цим самостійний інтерес представляє розробка баз даних для оперативного управління організацій з використанням ІАСУ.

Сучасний етап розвитку інформаційних процесів характеризується тим, що процедури збереження великих масивів інформації і пошук необхідних відомостей здійснюється за допомогою створення баз і банків даних, що відображають стан об’єкта або множини об’єктів, їх властивості і взаємовідношення.

Розробка моделі бази даних вимагає визначення і опису таких складових елементів бази, як атрибути, відносини, залежність і оператори, що характеризують дану предметну область, а також визначення форм і видів вхідної і вихідної документації, що використовується для підтримки бази даних в робочому стані і здійснення оперативного управління організацій.

Бази даних є єдністю, з одного боку, сукупності операційних даних, що характеризують діяльність організацій, що зберігаються в пам'яті електронної обчислювальної машини (ЕОМ) і, з другого боку, набору прикладних програм пакетної обробки, призначених для вибірки і обробки цих даних з можливістю оновлення, доповнення, виключення.

Формування і корегування бази даних здійснюються на основі «вхідної інформації», що вводиться ззовні і поточної. Результатом обробки бази даних є «вихідна інформація». Обробка проводиться по певним алгоритмам.

Архітектура системи бази даних може бути розділена на зовнішній, внутрішній і концептуальний рівні:

*Зовнішній рівень* - є інформаційним вмістом бази даних в тому вигляді, в якому вона з'явилася перед користувачем.

*Внутрішній рівень* - визначається як збережена база даних і може бути описаний за допомогою внутрішньої схеми, тобто структури зберігання. Часто під поняттям «база даних» розуміють саме зберігання даних.

Інформаційне забезпечення ІАСУ включає: єдину систему класифікації та кодування техніко-економічних показників діяльності об'єкта управління; уніфіковану систему первинної інформації; масиви інформації, що використовуються для розв'язання задач управління.

Внутрішні інформаційні масиви підрозділяють на постійні, допоміжні, проміжні, поточні:

*Постійні масиви* – директивні, нормативні, довідкові і інші рідко змінні відомості.

*Допоміжні масиви* - одержувані на основі перетворення (сортування, об'єднання, виділення і ін.) постійних масивів. Допоміжні масиви забезпечують різні поєднання показників і повинні зберігатися той же час, що і постійні масиви.

*Проміжні масиви* - одержувані на стику рішення різних задач, при яких результат попереднього розрахунку виступає як початковий результат подальшого розрахунку, які в необхідних випадках можуть зберігатися (якщо вони мають самостійне значення).

*Поточні масиви* – це змінна робоча інформація про стан керованого об'єкта. Серед поточних масивів слід виділити накопичувані інформаційні масиви, в яких дані не виключаються, не виправляються, не замінюються, а тільки доповнюються новими і повністю обновляються тільки або на початку наступного циклу, або через декілька циклів.

*Службові масиви* - містять інформацію, необхідну для переробки інформації вище названих масивів (каталоги систем інформаційних масивів, програми ЕОМ, транслятори, машинні довідники і т. п.).

*Концептуальний рівень* - є абстрактною формою інформаційного змісту бази даних і в теперішній час є, як правило, об'єднанням всіх представлень даних окремими користувачами з додатком процедур контролю повноважень і перевірки.

«Система управління базою даних» (СУБД) відповідає за контроль повноважень користувача, проведення процедур перевірки, знаходження збережених записів, формування концептуальної моделі, а також за здійснення необхідної обробки даних по заданим алгоритмам, тобто перетворення даних і, нарешті, вивід одержаних в результаті обробки інформації даних в найбільш зручній формі, для подальшого використання.

Залежно від способу організації даних розрізняють наступні типи баз даних: дореляційні, реляційні, пісреляційні.

**Дореляційні БД**

Дореляційні БД діляться на наступні три групи: засновані на інвертова-

них списках, ієрархічні і мережні:

*БД засновані на інвертованих списках* відрізняються від реляційних тим, що збереженні таблиці і шляхи доступу до них видно користувачам.

*БД ієрархічні* складаються з впорядкованого набору дерев; більш точно, з впорядкованого набору декількох екземплярів одного типу дерева.

*БД мережні* – є розширенням ієрархічних баз даних. В мережній структурі даних нащадок може мати будь-яке число предків, тоді як в ієрархічній нащадок може мати лише одного предка.

До числа *достоїнств* дореляційних БД слід віднести: розвинуті засоби управління даними в зовнішній пам'яті на низькому рівні; можливість побудови вручну ефективних прикладних систем; можливість економії пам'яті за рахунок розподілу об’єкта на підоб'єкти.

До числа *недоліків* дореляційних БД слід віднести: складність використання; фактично необхідні знання про фізичну організацію бази даних (прикладні системи залежать від цієї організації); їх логіка переобтяжена деталями організації доступу до БД.

**Реляційні бази даних**

Реляційний підхід до формування даних характеризується тим, що вся інформація в БД як «об'єкт», так і «зв'язки» представляється в єдиній уніфікованій формі, формі таблиць, що робить реляційну структуру найбільш доступною для розуміння.

Реляційні бази даних забезпечують відображення всіх даних у в двовимірних таблицях. Рядки таблиці складені з полів, наперед відомих базі даних. Кожний рядок в таблиці відповідає одному запису. Положення даного рядка може змінюватись разом з вилученням або вставкою нових рядків.

Оскільки таблиці повинні містити постійне число полів наперед певних типів, доводиться створювати додаткові таблиці, що ураховують індивідуальні особливості елементів, за допомогою зовнішніх ключів. Такий підхід ускладнює створення складних взаємозв'язків в базі даних.

Побудова реляційної бази даних для управління організацій може розглядається як з позиції управлінського персоналу, так і працівників фінансових служб і бухгалтерії, зобов'язаних відповідно до переліку загальних і спеціальних задач здійснювати оперативне управління виробництвом.

Оскільки працівники фінансових служб або бухгалтерії лише вводять в систему прості параметри або викликають певні дані, то такі користувачі можуть бути визначені як параметричні, що мають справу тільки із зовнішньою моделлю даних, яка для них визначається операційно. Оперативне управління фінансами підприємств припускає можливість за допомогою набору форм, що висвічуються на екрані дисплея, вводити або запрошувати дані і «меню» операцій, доступних користувачу.

До числа *переваг* реляційних баз даних можна віднести: наявність невеликого набору абстракцій, які дозволяють порівняно просто описати велику частину поширених предметних областей і допускають точні формальні визначення залишаючись інтуїтивно зрозумілими; наявність простого і в то ж час могутнього математичного апарату, що опирається головним чином на

теорію множин і математичну логіку і реляційного підходу до організації баз даних; можливість ненавігаційного маніпулювання даними без необхідності знання конкретної фізичної організації баз даних в зовнішній пам'яті; можливість формулювання і підтримки обмежень цілісності даних. При визначенні переваг використання реляційної бази даних необхідно відмітити, що відношення може бути розглянуто як спеціальний випадок ієрархії, а ієрархія – як спеціальний випадок межі. Таким чином, реляційний підхід до побудови бази даних є переважним внаслідок того, що вся інформація в базі представляється з використанням тільки однієї конструкції - таблиці, при цьому забезпечується не надмірність представлення даних і уніфікованість.

До числа *недоліків* слід віднести: ускладнення створення складних взаємозв'язків в базі даних, оскільки таблиці повинні містити постійне число полів наперед заданих типів, то доводиться створювати додаткові таблиці ураховуючи індивідуальні особливості елементів за допомогою зовнішніх ключів; деяка обмеженість при використанні в так званих нетрадиційних областях тобто в системах, які вимагають гранично складні структури даних; неможливість адекватного віддзеркалення семантики предметної області.

**Пісреляційні бази даних**

В нетрадиційних додатках в базі даних з'являється безліч таблиць, над якими постійно виконуються операції з'єднання, необхідні для відтворення складних структур даних, властивих предметній області. Усвідомлюючи ці обмеження і ураховуючи недоліки реляційних систем, дослідники в області баз даних розробляють проекти, засновані на ідеях, що виходять за межі реляційної моделі даних.

В результаті досліджень можна виділити наступні пісреляційні системи: *розподілені СУБД, системи клієнт-сервер, інтегровані* або *федеральні системи даних*, орієнтовані і об'єктно-реляційні СУБД.

Основна задача систем управління *розподіленими базами даних* полягає в забезпеченні засобу інтеграції локальних баз даних, розташованих в деяких вузлах обчислювальної межі, з тим, щоб користувач, що працює в будь-якому вузлі межі, мав доступ до всіх цих баз як до єдиної бази даних. При цьому повинні забезпечуватися: простота використання системи; можливості автономного функціонування при порушеннях зв'язності межі або при адміністративних потребах; високий ступінь ефективності.

Можливі однорідні і неоднорідні розподілені бази даних: в *однорідному* випадку кожна база даних управляється однією і тією ж СУБД, *в неоднорідній системі* локальні бази даних можуть відноситися навіть до різних моделей даних.

Основною задачею інтеграції неоднорідних баз даних є надання користувачам інтегрованої системи глобальної схеми БД, представленої в деякій моделі даних, тобто автоматичне перетворення операторів маніпулювання БД глобального рівня в оператори, зрозумілі відповідним локальним СУБД. В теоретичному плані проблеми перетворення піддаються реалізації.

Найбільш перспективними вважаються дослідження об'єктно-орієнтованого (ОО) і об'єктно-реляційного підходів (ОР). Перспективи ОР

підходу відкривають нові можливості для збереження і управління різними типами даних, зберігаючи при цьому звичні табличні структури. На відміну від чисто об'єктних баз даних, перехід до об'єктно-реляційних систем не вимагає масового перепрограмування.

Найбільш важливими новими об'єктно-реляційними можливостями є: визначені користувачами типи; визначенні користувачами функції; інфраструктура (методи індексації і доступу, а також вдосконалені способи оптимізації).

Все це показує перспективність подальшого розвитку об'єктно-реляційних систем баз даних, відкриває нові можливості для збереження і управління різними типами даних, дозволяючи використовувати їх в різних нетрадиційних предметних областях, зберігаючи при цьому звичне представлення даних.

**Висновки**:

Положення, сформульовані у даній статті, доповнюють науково-практичну систему знань щодо методів і принципів розробки баз даних для оперативного управління промисловим виробництвом.

Результати статті можуть бути використанні при створенні обґрунтованої методології розробки баз даних для ІАСУ організаціями.

1. Бойко В.В., Савинков В.М. Проектирование баз данных информационных систем. – М.: Финансы и статистика, 1989. – 351 с.

2. Куликовский Л.Ф., Мотов В.В. Теоретические основы информационных процессов. – М.: Высш. шк., 1987. – 248 с.

3. Мерстюк В.Г., Иоадесян А.Н. Автоматизация управления финансами, сущность и проблематика //Вестник ХГТУ. – 2002. - №1(14). – С. 151 – 155.

4. Мартин Дж. Организация баз данных в вычислительных системах. – М.: 1980. – 662 с.

5. Четвериков В.Н. Базы и банки даннях. – М.: Высш. шк.., 1987. – 248 с.

6. Шолье Ж. Банки данных: Использование электронной вычислительной техники / Пер. с франц., под ред. Б.А. Щукина. – М.: Энергоиздат, 1981. – 72 с.

**Ісмайлов Карен Юрійович**
к.ю.н., завідувач кафедри
кібербезпеки та інформаційного
забезпечення Одеського державного
університету внутрішніх справ

## ДЕЯКІ ПИТАННЯ ІНФОРМАЦІЙНО-ПРАВОВОЇ ВІДПОВІДАЛЬНОСТІ В УКРАЇНІ

Актуальність питання про формування нового різновиду юридичної санкції у вигляді інформаційно-правової відповідальності обумовлена тим, що у юриспруденції, до цього часу, означений різновид державного примусового заходу не розглядався вченими в системі теорії юридичної відповіда-

льності, як самостійний.

Сучасне інформаційне право в Україні набуває від цілого комплексу інших галузей певні правові інститути, в тому числі й інститут інформаційно-правової відповідальності, що формується з норм, які розташовані в адміністративному, цивільному, кримінальному праві та в самому інформаційному праві і відповідно інформаційному законодавстві. З одного боку це дає додаткових підстав відносити інформаційне право до комплексної галузі права. З другого – це підтверджує комплексний характер інформаційного права та наявність тісних взаємозв'язків між різними галузями права і законодавства. Відтак, логічно передбачати, що головна мета інформаційно-правової юридичної відповідальності – максимальний захист та відновлення порушеного права на інформацію суб'єктів інформаційно-правових відносин.

На питання про інформаційно-правову відповідальність в національній юриспруденції в своїх публікаціях вже звертали увагу такі науковці, Л.П. Коваленко, В.А. Ліпкан, Г.М. Писаренко, А.А. Письменицький, О.О. Тихомиров, О.К. Тугарова.

Так, В.А. Ліпкан сформулював в своїх дослідженнях цілу низку відповідних інформаційно-правових категорій: Інформаційна деліктологія — самостійна підгалузь інформаційного права, що містить сукупність знань про інформаційні делікти і деліктність як масове негативне явище, що містить в собі детермінанти протиправної поведінки делінквента, їхньої особистості з метою вироблення і використання адекватних заходів для протидії інформаційних правопорушень [1].

Л.П. Коваленко вбачає в широкому розумінні, інформаційно-правову відповідальність, як вид юридичної відповідальності, якому притаманні всі ознаки останнього, вона є складовою частиною державного примусу, це накладення на правопорушників (фізичних і юридичних осіб), загальнообов'язкових правил, які діють в інформаційній сфері, стягнень, що тягнуть за собою для цих осіб обтяжливі наслідки юридичного характеру.

У вузькому розумінні, інформаційно-правова відповідальність - це вид юридичної відповідальності, який полягає в застосуванні до фізичних і юридичних осіб, які вчинили інформаційні проступки, особливих санкцій - інформаційних стягнень [2].

Г.М. Писаренко зазначає, що у теорії права існує думка, що нині приступити до вивчення юридичної відповідальності з позиції інформаційних відносин важко, оскільки визначення інформаційної відповідальності не існує на законодавчому рівні, а також відсутній єдиний кодифікований нормативно-правовий акт, у якому містився б перелік інформаційних правопорушень і визначалася б специфічність санкцій інформаційного права [3].

Найбільш комплексним є підхід до питання про інформаційно-правову відповідальність у публікаціях і монографіях доцента А.А. Письменицького, який розробив в Україні, ще з 1993 року, фактично основу теорії інформаційного права. Зокрема його бачення категорії інформаційно-правової відповідальності було оформлено в одній із наукових публікацій 2017 року у наступній дефініції: Інформаційно-правова відповідальність – це система заходів

примусового характеру, передбачених чинним законодавством, що призводять до претерпівання порушником інформаційного законодавства певних обмежень в інформаційних правах і свободах та не охоплюються іншими видами юридичної відповідальності. Правові наслідки інформаційно-правової відповідальності проявляються у тому, що суб'єктом інформаційних правовідносин втрачаються чи обмежуються можливості щодо: пошуку, одержання, створення, використання, зберігання, поширення або захисту інформації у будь-який вільно обраний спосіб і не залежно від кордонів [4].

Останнім часом найбільш поширена практика застосування примусових заходів інформаційно-юридичного характеру в сфері діяльності таких органів державної влади, як Рада національної безпеки і оборони України та Національна рада з питань телебачення та радіомовлення.

Упродовж 2015 року Національною радою з питань телебачення і радіомовлення проводився моніторинг програм іноземного виробництва. Через виявлення порушень із Переліку іноземних програм, зміст яких відповідає вимогам Європейської конвенції про транскордонне телебачення [6] і законодавства України було вилучено 10 телеканалів Російської Федерації: «24 Техно», «МИР 24», «Страна», «Русский иллюзион», «Дом кино», «Оружие», «Многосерийное ТВ», «Школьник ТВ», «Феникс+кино», «Иллюзион +». В даному випадку було застосовано положення Європейської конвенції про транскордонне телебачення, що встановлює порядок, за яким у випадках, якщо порушення має очевидний, серйозний і тяжкий характер, а також призводить до виникнення складних громадських проблем.

В ефірі згаданих вище російських мовників також було зафіксовано трансляцію: телевізійних фільмів та серіалів, які заборонені для розповсюдження і демонстрування на території України Державним агентством України з питань кіно; передач, у яких популяризувалися стратегічні об'єкти Російської Федерації, а також висвітлювалися найновітніші види російського озброєння і засоби ведення бою; сюжетів новин і фрагментів передач, які містили заклики до зміни конституційного ладу у країні, рекламу миротворчих сил Російської Федерації, пропаганду війни та порушення територіальної цілісності України; передач з інтерактивними конкурсами, зміст яких суперечить вимогам частини третьої статті 6 Закону України «Про телебачення і радіомовлення» [5, ч.3 ст.6]. Зокрема, 2015 року до п'яти провайдерів програмної послуги було застосовано санкцію «оголошення попередження» у зв'язку з ретрансляцією програм, не передбачених відповідним актом Національної ради.

Так, Рішенням Ради національної безпеки і оборони України від 25.01.2015 року «Про надзвичайні заходи протидії російській загрозі та проявам тероризму, підтримуваним Російською Федерацією», затвердженої Указом Президента України [6] було передбачено «ужити за участю Національної ради України з питань телебачення і радіомовлення невідкладних заходів щодо припинення російської інформаційної агресії, здійснюваної з використанням іноземних та вітчизняних засобів масової інформації» [7, п. 1. 5].

У 2015 році до п'яти провайдерів програмної послуги було застосовано

санкцію «оголошення попередження» у зв'язку з ретрансляцією програм, не передбачених цим актом Національної ради з питань телебачення і радіомовлення. Також 2015 року було тимчасово припинено розгляд питань щодо визнання змісту програм адаптованим до вимог законодавства України, правовласники (виробники) яких підпадають під юрисдикцію Російської Федерації. Таке рішення було прийнято, зважаючи на ведення бойових дій на сході України, військову та інформаційну агресію проти України, визнання законодавством України Російської Федерації державою-окупантом та державою-агресором, беручи до уваги антиукраїнську позицію цієї держави щодо територіальної цілісності, суверенітету України в цілому, з метою забезпечення інформаційної безпеки та захисту територіальної цілісності України [8].

17 травня 2017 року, набув чинності Указ Президента України Петра Порошенка про введення санкцій відносно ряду російських інформаційних продуктів, зокрема соцмережі «ВКонтакте» і «Одноклассники», ІТ-компаній, «Яндекса» (та його української «дочки») і поштового сервісу Mail.ru, а також бухгалтерської програми 1С [9].

У цьому акті значними для інформаційної безпеки і кібербезпеки України є не лише кількість осіб, щодо яких застосовано санкції (1228 фізичних та 468 юридичних осіб), а й види застосованих обмежень [10].

Щодо заборони інтернет-провайдерам надання послуг з доступу користувачам мережі інтернет до ресурсів/сервісів на певних доменах, то це захисний інструмент чинного законодавства, що застосовується на загальнодержавному рівні вперше. Одночасно, це є й одним з видів нової генерації юридичної відповідальності, що сучасні науковці визначають як інформаційно-правову.

Так, стаття 4. Закону України «Про санкції» дає перелік видів санкцій і у пункті 9 передбачає, що окремим різновидом такого державного примусу є обмеження або припинення надання телекомунікаційних послуг і використання телекомунікаційних мереж загального користування [11]. Це, в свою чергу, відсилає нас до іншого закону – Закону України «Про телекомунікації», що визначає телекомунікаційну мережу загального користування, як телекомунікаційну мережу, доступ до якої відкрито для всіх споживачів. В свою чергу саме поняття телекомунікаційної мережі, Закон характеризує, як комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням [12].

Усі вище перераховані приклади підтверджують широке застосування владними органами заходів примусового характеру, що спрямовуються на обмеження прав допуску суб'єктів професійної інформаційної діяльності до інформації, заборону їм поширювати певну інформацію, обмеження прав на розповсюдження певної інформації, та призупинення інформаційної діяльності. Всі ці заходи мають певні спільні ознаки, що виокремлюють означені санкції серед різновидів юридичної відповідальності в самостійну групу. Зок-

рема, всі ці приклади застосування інформаційно-юридичного впливу, здебільше, вимагали прийняття окремих нормативно-правових актів, починаючи від Законів України і до окремих рішень Національної ради з питань телебачення і радіомовлення. Це було обумовлено, переважно, відсутністю у національному законодавстві, до того часу, необхідних важелів примусового впливу на суб'єктів інформаційних відносин, які систематично, або з важкими наслідками порушують права інших суб'єктів на інформацію і раніше не несли за це ніяких правових наслідків у вигляді обмежень, або втрат в інформаційній свободі. Вектор спрямування означених санкцій направлений не на матеріальний прояв прав і свобод сторін у інформаційних відносинах, а саме, на їх право на інформацію. Тобто, якщо стороною відносин здійснювалось зловживання правом на інформацію, в певному аспекті, що обмежувало це право у інших сторін, то санкціями здійснювалось обмеження або скасування саме цієї частини права на інформацію винного суб'єкта.

Таким чином, інформаційно-правова відповідальність – це система заходів примусового характеру, передбачених чинним законодавством, що призводять до претерпування порушником інформаційного законодавства певних обмежень в інформаційних правах і свободах.

Зазначена характеристика і розуміння інформаційно-правової відповідальності дає підстави вважати, що основною метою такого виду відповідальності виступає забезпечення більшої повноти реалізації інформаційних прав і свобод іншим суб'єктам інформаційних правовідносин.

1. Ліпкан В.А. Вікіпедія. Електронна інтернет-енциклопедія // [Електронний ресурс]. - Режим доступу: https://uk.wikipedia.org/wiki/18.10.2017.

2. Коваленко Л.П. Юридична відповідальність за правопорушення у сфері інформаційної діяльності / Л.П. Коваленко // Проблеми законності. - 2012. - Вип. 120. - С. 165-172.

3. Писаренко Г.М. Юридична відповідальність в інформаційній сфері: окремі аспекти становлення // Наук. вісник Ужгородського національного університету, 2016. Серія ПРАВО. Випуск 36. Том 2. – С. 55-58.

4. Письменицький А.А. До теоретико-правового концепту кібербезпеки та інформаційної юридичної відповідальності // Кібербезпека в Україні: правові та організаційні питання: матеріали всеукр. наук.-практ. конф., м. Одеса, 17.11.2017 р. – Одеса : ОДУВС, 2017. – С. 162-165.

5. Про телебачення і радіомовлення. Верховна Рада України. Закон від 21.12.1993 № 3759-XI // Відомості Верховної Ради України, 1994, N 10, ст. 43

6. Про рішення Ради національної безпеки і оборони України від 25 січня 2015 року "Про надзвичайні заходи протидії російській загрозі та проявам тероризму, підтримуваним Російською Федерацією".; Указ Президента України від 14.02.2015 № 85/2015 // [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/85/2015.

7. Про надзвичайні заходи протидії російській загрозі та проявам тероризму, підтримуваним Російською Федерацією. Рішення Ради національної безпеки і оборони України від 25.01.2015 // [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/n0001525-15

8. Звіт Національної ради України з питань телебачення і радіомовлення за 2015 рік // [Електронний ресурс]. – Режим доступу: http://www.nrada.gov.ua/userfiles/file/2016/Zvitna%20informacia

9. Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року "Про застосування персональних спеціальних економічних та інших обмежувальних захо-

дів (санкцій)". Указ Президента України від 15.05.2017 № 133/2017 // Урядовий кур'єр від 17 травня 2017 року // [Електронний ресурс]. Режим доступу: http://zakon3.rada.gov.ua/laws/show/133/2017.

10. Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій). РНБО; Рішення від 28.04.2017 // [Електронний ресурс]. Режим доступу: http://zakon3.rada.gov.ua/laws/show/n0004525-17/paran2#n2.

11. Про санкції. Закон України; від 14.08.2014 № 1644-VII // Відомості Верховної Ради (ВВР), 2014, № 40, ст.2018.

12. Про телекомунікації. Закон України від 18.11.2003 № 1280-IV // Відомості Верховної Ради (ВВР), 2004, N 12, ст.155. Редакція від 04.06.2017, підстава 1834-19, 1983-19.

**Коренюк Петро Іванович**
д.е.н., проф., завідувач кафедри
менеджменту організацій
і адміністрування Дніпровського
державного технічного університету

**Коренюк Людмила Володимирівна**
к.е.н., доцент**,** доцент кафедри
фінансів та економічної безпеки
Дніпропетровського національного
університету залізничного
транспорту імені В. Лазаряна

## ОСОБЛИВОСТІ ФОРМУВАННЯ КОНКУРЕНТНОЇ РОЗВІДКИ У КОНТЕКСТІ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

У сучасних ринкових умовах в бізнесі зростає значимість аналізу можливих ситуацій, з'ясування домінуючих тенденцій, розрахунок можливих ризиків при ухваленні господарських рішень. Недостатньо володіти інформацією у вигляді результатів маркетингових досліджень або бізнес-довідок про потенційних партнерів і конкурентів. Виникає потреба з метою виживання дати відповідь на питання: хто або що є причиною виникнення подій, звідки виходить або може виходити загроза, як її уникнути або мінімізувати? Нагальна потреба у вирішенні таких задач і стала причиною виникнення конкурентної розвідки. За сутністю та змістом конкурентна розвідка не є промисловим шпигунством, адже вона функціонує виключно в рамках чинного законодавства. Але джерела інформації для конкурентної розвідки завжди «відкриті» і загальнодоступні, хоча не завжди опубліковані.

Проблему фінансово-економічної безпеки та конкурентної розвідки прямо та опосередкована досліджена у працях О. Г. Білорус [1], О. Р. Бойкевич [2], Т. Г. Васильціва [2], В. І. Волошина [2], В. О. Голубєва [4], Т. В. Давидюк [3], В. В. Каркавчук [2], В. А. Ліпкан [6], О. В. Логінова [6], В. Г. Лукашевич [4], О. М. Марченко [5], І. П. Мойсеєнко [5], А. В. Товксиса [8],

Л. С. Харченка [6], Г Хофмана [7], Л. А. Чвертко [8], А. М. Штангрета [9] та інших вітчизняних та закордонних вчених.

Конкурентна розвідка з економічного середовища трансформується в один з узаконених соціальних інститутів суспільства. В той же час глобалізація бізнесу і поширення інформаційних технологій сприяють інституціоналізації конкурентної розвідки і розширенню сфери її застосування, але вирішальною умовою є праця професіоналів конкурентної розвідки, що обумовлює включення конкурентної розвідки у корпоративну систему прийняття рішень. Різні рівні менеджменту, особливо топ-менеджмент, мають вчасно реагувати на ініціативи конкурентів, законодавців і появу новітніх технологій. Як свідчить світовий досвід, добре організована конкурентна розвідка забезпечує стійкий ріст компанії і її прибутків і виступає незамінним елементом системи забезпечення фінансово-економічної безпеки підприємства. У роботі самої групи конкурентної розвідки, особливо на початковому етапі її діяльності на підприємстві, коли репутація та робочі зв'язки ще не сформовані, поширеними помилками є крайнощі у сприйнятті результатів власної діяльності. Це або занадто критичний підхід, що межує з недостатньою впевненістю у власних силах, або ж нерозсудливість та самовпевненість.

Цілісний підхід до конкурентної розвідки також вимагає, щоб у її програмі були представлені всі компоненти циклу конкурентної розвідки. Компанії, що спираються лише на опубліковану вторинну інформацію й ігнорують одержання даних через особисті контакти або не мають ефективних аналітичних інструментів, не зможуть одержати від програми конкурентної розвідки повну віддачу. Internet в його нинішній формі є конгломератом різних за виглядом, значимістю, достовірністю та цінністю джерел інформації. Так, значна частка його ресурсів є інформаційним сміттям, але уміння орієнтуватися в цьому безмежному інформаційному болоті є половиною успіху справи. Крім цього, фахівець з конкурентної розвідки має і повинен отримувати потрібну інформацію з стрічок інформаційних агентств в режимі реального часу (on-line). Переваги є в тому, що має місце мінімум коментарів в повідомленнях. Для аналітиків це важливо, оскільки дозволяє аналізувати безпосередньо події, а не їх трактування.

В той же час інформація на сайтах традиційних засобах масової інформації носить менш оперативний характер і видозмінюється журналістами, тим самим розбавляються первісні відомості. Відмітимо, що переважна частина традиційних газет і журналів мають сьогодні свої Internet-сервери. Велике значення мають спеціалізовані бази даних, які досить важко поповнювати, що під силу лише інформаційним підрозділам крупних компаній.

Досвідчені фахівці надають важливе значення торговим виставкам, на яких можна отримати первинну інформацію про конкурентів і, відповідно, змінити тактику поведінки у чітко визначеному ринковому сегменті. Наприклад, в США понад 50 відсотків учасників виставок, що проводяться Центром експонування промислових, шукають нові ідеї, партнерів та готові

ділитися своєю інформацією. До 60 відсотків учасників вперше присутніх на таких заходах, а це полегшує встановлення нових контактів. Близько 34 відсотків фірм, що беруть участь на виставках, представлені своїми керівниками, а 84 відсотки учасників входять в керівні органи, що ухвалюють корпоративні рішення. І всі вони на виставці відкриті до спілкування. Нарешті, виставки відвідуються багатьма аналітиками, експертами і представниками преси. Це сприяє встановленню контактів з людьми, які добре розбираються в проблемах сегменту ринку, що цікавить вас. Готуючись до роботи на торговій виставці, потрібно захистити свою організацію від розвідувальних акцій її конкурентів і, в той же час, продумати способи встановлення корисних контактів.

Підходячи до стенду конкурента, не слід викликати підозри, знімаючи значок з вказівкою своїй приналежності, але так же бажано не повідомляти зайвих відомостей. Збираючи дані про конкурента краще скористатися послугами третіх осіб. Потрібно перевірити всі отримані дані за іншими джерелами, адже виставкова інформація про нову продукцію часто є рекламною.

В умовах глобалізації світової економіки конкурентна розвідка являється невід'ємною складовою частиною діяльності щодо забезпечення економічної безпеки підприємства. Лише на основі всебічної інформації яка стосується процесів що відбуваються в зовнішньому середовищі можливо створити ефективну систему безпеки підприємства та протистояти сучасним небезпекам , загрозам та ризикам. Конкурентна розвідка забезпечує вищих керівників підприємства інформацією про процеси, що відбуваються на ринку. Без цієї інформації неможливо вчасно приймати вірні рішення, пов'язані з посиленням ринкових позицій підприємства і його подальшим розвитком. Фахівець в галузі конкурентої розвідки повинен використовувати всі засоби та джерела для отримання інформації: засоби масової інформації, інформацію з стрічок інформаційних агентств, торгові виставки, Internet та інші джерела. Дана інформація має поступати з альтернативних джерел і неодноразово ситемно перевірятися з метою підвищення достовірності.

І саме головне, ефективність конкурентної розвідки може бути досягнута в умовах високої довіри до неї з боку керівництва підприємства. Така довіра може бути виправдано при вірному підборі керівника підрозділу конкурентної розвідки й забезпечення її необхідними ресурсами для реалізації різних варіантів збору й аналітичної обробки інформації.

1. Білорус О.Г. "Глобалізація і безпека розвитку". – Монографія. - К.: КНЕУ, 2001. – 733 с.

2. Васильців Т.Г. Фінансово-економічна безпека підприємств України: стратегія та механізми забезпечення: монографія [Електронний ресурс] / Васильців Т. Г., Волошин В.І., Бойкевич О. Р., Каркавчук В. В., [за ред. Т.Г. Васильціва]. – Львів: Ліга-Прес, 2012. – 386 с. – Режим доступу: http://lv.niss.gov.ua/content/articles/files/mono_2012-d47ce.pdf.

3. Давидюк Т.В. Фінансово-економічна безпека або фінансова складова економічної безпеки: епістемологічний підхід / Т. В. Давидюк // Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу. Сер. : Бухгалтерський облік, контроль і аналіз. – 2013. – Вип. 1. – С. 39-52. - Режим доступу: http://nbuv.gov.ua/j-pdf/ptmbo_2013_1_6.pdf.

4. Лукашевич В. Г., Голубєв В. О. – "Напрямки удосконалення кримінальної

відповідальності за злочини у сфері комп`ютерної інформації" // Інформаційні технології та захист інформації.- Запоріжжя: Юридичний ін-т МВС України,2002 – 311 с.;

5. Мойсеєнко І.П. Управління фінансово-економічною безпекою підприємства: навч. посібник / І.П.Мойсеєнко, О.М.Марченко. – Львів, 2011. – 380 с.

6. Харченко Л.С., Ліпкан В.А., Логінов О.В. – Інформаційна безпека України: Глосарій". – К.: "Текст", 2004. – 136;

7. Хоффмаг Герд – "Советы по предотвращению преступлений в бизнесе и на производстве" – Hoffmann Investigations, Amsterdam, 2005. – 246 с.

8. Чвертко Л.А. Конкурентна розвідка в системі забезпечення економічної безпеки банків / Л.А. Чвертко, А.В. Товксис // Управління фінансово-економічною безпекою. – 2015. – № 1. – С. 65–68.

9. Штангрет А.М. Методичні засади здійснення конкурентної розвідки в системі економічної безпеки підприємства / А.М. Штангрет // Науковий вісник НЛТУ України. – 2013. – Вип. 23.4. – С. 302–307.

**Каблуков Андрій Олександрович**
к.т.н., доц., доцент кафедри

**Мурзіна Олена Анатоліївна**
к.пед.н., асистент кафедри
медичної і фармацевтичної
інформатики та новітніх технологій
Запорізького державного
медичного університету

## ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ПРОТИДІЇ ЗЛОЧИННОСТІ В УКРАЇНІ

Сьогодні кримінальна ситуація в Україні відрізняється особливою складністю. Криміногенні чинники економічного, соціального, політичного та морально-психологічного характеру продовжують чинити негативний вплив як на стан правопорядку, так і на особисту безпеку громадян, суспільну та державну безпеку. Так кількість злочинів скоєних в Україні в 2017 році досягла 523,9 тисяч [1].

Тому, коли масштаби злочинності набули загрозливого характеру, гостро постає завдання вироблення нових теоретичних підходів до вирішення відповідних проблем і практичних заходів щодо вдосконалення діяльності органів внутрішніх справ. Швидке освоєння і впровадження в практичну діяльність правоохоронних органів сучасних наукових досягнень дозволить більш успішніше протистояти росту злочинності.

До наукових досягнень в першу чергу можна віднести сучасні інформаційні технології з комп'ютерним обладнанням. Використання новітніх технологій дозволить підвищити професіоналізм українських поліцейських та поліпшити роботу оперативників і слідчих.

Зараз в МВС України існують комп'ютерні підрозділи, які підтримують роботу інформаційно-пошукових баз з обліку злочинців, автомототранспор-

ту, зброї тощо. Однак підвищення ефективності використання криміналістичних обліків в діяльності поліції неможливо без принципово нових засобів організації роботи з інформаційними масивами. Найбільш важкою буде завдання інформатизації самого процесу розслідування. Слідчий повинен переробити величезний масив інформації, виокремити з неї криміналістичну значиму і не допустити при цьому помилок, які пов'язані з недоліком цієї інформації та труднощами в її отриманні, так і з дефіцитом часу та часто невисоким професійним рівнем. При цьому вельми значний час витрачається на рутину роботу по складанню різних документів процесуального та непроцесуального характеру: протоколів, постанов, запитів та ін.

Для вирішення цієї проблеми необхідно здійснити наступні заходи:

- забезпечити комп'ютерною технікою в достатній кількості всіх підрозділив поліції;
- створити АРМ слідчих і оперативних співробітників, для надання можливості отримання криміналістичної інформації в повному обсязі;
- організувати навчання співробітників щодо використання нових спеціалізованих комп'ютерних програм;
- централізувати всі існуючи криміналістичні обліки. Для цього уніфікувати систему криміналістичної реєстрації з перекладом місцевих обліків в категорію централізованих;
- розробити та втілити нові види технологій для розкриття злочинів.

Для впровадження нових методів використання комп'ютерних технологій в слідчій діяльності України треба використовувати досвід інших держав. Використовуючи те, що більшість телефонів, планшетів і ноутбуків мають GPS, Wi-Fi і модуль мобільного зв'язку, за допомогою яких можна легко визначити місце розташування людини, якщо він приєднаний до однієї з цих мереж. Поліція міста Ролі (США) оголосила про співпрацю з Google [2]. Отримані від компанії дані допомогли швидше розкривати злочини. Так в одній справі Google показала всі смартфони, які перебували поруч з місцем події, при цьому компанія не розкрила особисті дані користувачів. В іншій справі вона вказала пристрої, які потрапили в зону розміром 68 квадратних кілометрів в момент вбивства.

МВС та СБУ України мають технічні можливості відслідковувати місце знаходження мобільних пристроїв злочинців, але технології визначення всіх мобільних пристроїв, що знаходилися поряд з місцем скоєння злочину, ще не використовувались.

З метою підвищення рівня інформаційного забезпечення поліцейських доцільно було б додатково створити нові обліки:

- облік осіб на основі використання фотознімків і анкетних даних;
- облік добової оперативної інформації, що міститься в рапортах співробітників підрозділів поліції, які несуть службу на вулицях міст, на дорогах і т.д.

**Висновок.** Для підвищення дієвості використання інформаційних технологій в боротьбі зі злочинністю доцільним є створення і використання в рамках України єдиної інтегрованої системи інформаційного забезпечення всіх правоохоронних органів (МВС, СБУ, прокуратури і т.д.).

1. Преступность в Украине: статистика за прошлый год. [Електронний ресурс]. – Режим доступа: https://ru.slovoidilo.ua/2018/02/16/infografika/obshhestvo/prestupnost-ukraine-statistika-proshlyj-godє..
2. Google передавала полиции GPS-данные пользователей. . [Електронний ресурс]. – Режим доступа: news.i.ua/theme/4732227/.
3. Использование GPS-трекеров в работе полиции. Источник: http://www.usfleettracking.com/blog/2015/06/01/why-law-enforcement-should-use-gps-trackers/.

**Калініченко Зоя Дмитрівна**
к.е.н., доц., доцент кафедри
цивільно-правових дисциплін
Дніпропетровського державного
університету внутрішніх справ

## ЗАКОНОПРОЕКТ ПРО ВВЕДЕННЯ ПОДАТКУ НА ВИВЕДЕНИЙ КАПІТАЛ ТА МОЖЛИВІ НАСЛІДКИ РЕФОРМУВАННЯ КОРПОРАТИВНОГО ОПОДАТКУВАННЯ

В Україні планується кардинально реформувати корпоративне оподаткування. Але у 2018 році відкладено подання до Верховної Ради законопроекту про введення податку на виведений капітал, яким обкладається не фінансовий прибуток, а розподілений прибуток та капітал підприємств. Раніше була заявлена готовність внести його до парламенту з посиланням на позитивний досвід міжнародних партнерів. МВФ наполегливо рекомендував не вносити на розгляд Верховної ради законопроект про заміну податку на прибуток податком на виведений капітал.

*Сьогодні потрібна чесна дискусія прихильників і противників податку на виведений капітал, з іноземними партнерами і асоціаціями малого і великого бізнесу. Існує переконання, що* **нова податкова політика може кардинально змінити інвестиційний клімат.**

Треба почати діалог із МВФ, який є ключовим кредитором та міжнародним партнером України, і програма співпраці із МВФ є важливою для макростабілізації та проведення важливих реформ. Позиція МВФ, можливо нажаль, є стриманою та консервативною. За участі авторів законопроекту та Ukrainian Institute for the Future, МВФ взяв паузу на вивчення законопроекту, та спочатку позитивно відреагував на готовність скорочувати державний бюджет, як компенсатор запровадження ПВК протягом перших років. Це дійсно нагальна потреба для країни, бо видатки зростають швидше доходів. Паралельно тривають переговори із асоціаціями, членами яких є міжнародні транснаціональні корпорації, частина з яких виступає проти податку на ВК.

В рамках Закону № 1797 «Про внесення змін до Податкового кодексу України щодо покращення інвестиційного клімату в Україні», який є части-

ною антикорупційного пакету податкових змін, група у складі представників Міністерства фінансів України, бізнесу, експертів та народних депутатів підготувала законопроект щодо введення податку на виведений капітал.

Спочатку текст потрібно було узгодити із змінами до податкового кодексу, які було прийнято із бюджетом в грудні 2017, потім вичистити закон від різних псевдо-компенсаторів, які обмежували бізнес, потрібно було викреслити надмірні повноваження ДФС, узгодити з НБУ як запровадити автоматизований процес сплати ПВК в момент проведення транзакції. Нарешті, юристи повинні були опрацювати закон щодо стандартів нормотворення та юридичних узгоджень.

Головна мета - запровадити оподаткування прибутку підприємств, розподіленого у формі дивідендів чи прирівняних до них платежів та відмовитися від податку з доходів нерезидентів.

Запровадження податку на виведений капітал замість податку на прибуток здійснюється з метою допомогти бізнесу реінвестувати кошти у розвиток. Одночасно очікується, що це спростить правила оподаткування та процедуру адміністрування і покращить інвестиційний клімат в країні.

Проте, як зазначають науковці та фахівці фіскальної служби, реалізація норм законопроекту найближчим часом може привести до втрат державного бюджету в сумі 26,0 млрд. грн. та місцевих бюджетів – 5,4 млрд. гривень [1].

Міністерство фінансів, очікуючи таке недоотримання надходжень до бюджету, підтримує запровадження податку на виведений капітал лише за умови, якщо державний бюджет залишиться збалансованим. Тому розглядаються можливі шляхи компенсації бюджетних втрат, такі як значне підвищення ставок податків або скорочення видатків. Міністерство фінансів виступає категорично проти підвищення ставок податків та вважає єдиним шляхом для пошуку компенсаторів – це скорочення державних витрат та більш ефективне використання бюджетних коштів.

Сплата податку на виведений капітал передбачає, що такі кошти підприємство має сплатити державі, коли почне виводити гроші, сплачуючи дивіденди. Дивіденди — частина чистого доходу підприємства (після всіх виплат, зокрема й заробітних плат своїм працівникам), прибуток якого розподіляється між акціонерами такого підприємства. Розмір їхніх виплат залежить не тільки від чинного статуту такої фірми, а й від зборів акціонерів (тобто що вони вирішать, — у нас часто такі збори вирішують взагалі не сплачувати жодних дивідендів). Ось із таких операцій і стягуватиметься новий податок у розмірі 15%.

Є платежі, прирівняні до дивідендів, і їх також обкладатимуть податком на виведений капітал. Якщо компанія або підприємство захотіло виплатити роялті (своєрідну плату у вигляді відсотків комусь за його роботу, яку той робив для цього підприємства), виплатити своїм нерезидентам якісь гроші (тобто юридичним особам, у яких їхнє підприємство не зареєстровано в Україні), донарахувати щось за трансфертним ціноутворенням (це перерозподіл загального прибутку групи осіб, що перебувають у державах з нижчи-

ми доходами) або інвестувати що-небудь за кордон, то в цьому разі компанія повинна буде сплачувати такий податок на виведений капітал у розмірі 20%.

З одного боку, виходять з того, що підприємство дозволить собі накопичувати кошти, не сплачуючи податку на прибуток. З іншого боку, більшість експертів та підприємці побоюються того, що вони не знають, що може бути взагалі зараховано до таких дивідендів (а їхній список може бути значно розширений), і тоді доведеться сплачувати податок на виведений капітал з набагато більшого переліку операцій.

У деяких країнах світу, зокрема в Естонії, є позитивний досвід упровадження цього податку. Податок на виведений капітал дає змогу активно боротися з ухильниками від сплати коштів до скарбниці. Це й засвідчив досвід Естонії. У цій країні не використовували в таких величезних масштабах, як в Україні, практику виведення грошей в офшори. Тому для нас такий податок дозволить її практично викорінити. Адже ті заходи, що сьогодні розписано в законопроекті про податок на виведений капітал, будуть мати негативні наслідки перш усього саме для таких компаній.

Адміністрування податку полягає в перевірці вузького, конкретного переліку операцій, що обмежені виключно операціями платника податку на виведений капітал з неплатником.

Крім Естонії, де аналогічна система працює і має позитивні наслідки вже 17 років, є позитивний досвід Гонконгу — принцип звільнення від оподаткування реінвестованих коштів там посприяв економічному ривку. З 2017 р. на такий податок перейшла Грузія, яка вже отримала 1,2% додаткового зростання ВВП. Також податок на виведений капітал з 2018 р. застосовує Латвія, яка, до речі, взяла за основу ту модель, яку запропонували впровадити в Україні вітчизняні економісти в співпраці з європейськими колегами.

Противники введення в практику податку на виведений капітал кажуть, що естонський досвід, сьогодні є мало не єдиним позитивним. При цьому відзначають, що усі країни, що впроваджували в практику цей податок, зіткнулися в перші два-три роки з величезним недоотриманням бюджету. Різко знизилися обсяги надходжень від сплати податків. Не було й різкого надходження іноземних інвестицій уже після трирічної перерви. Те, що таке сталося в Естонії, свідчить більше, що саме після входження цієї країни до ЄС туди просто «потекли» європейські інвестиції, як у нову країну спільноти. Тобто однозначно запевняти, що саме податок на виведений капітал привів до естонського «дива», не можна. Від цього податку, до речі, свого часу відмовилися Швейцарія, США, Македонія, Молдова й інші країни.

Не виключено, що підприємства вкотре підвищення ПДВ покладуть на плечі споживачів, збільшивши ціни на свою продукцію. Як вважають окремі фахівці, нібито саме за «допомогою» такого податку державі легше буде розпочати скасування єдиної, тобто спрощеної, системи оподаткування.

До аргументів за податок на виведений капітал відносять, наприклад, те, що втрати бюджету в перші роки функціонування податку на виведений капітал не перевищать певної межі і можна знайти досить просто джерела перекриття втрат. Так, це може бути прибуток НАК «Нафтогаз України» (там саме 25 млрд

грн, які забирає державний бюджет у вигляді податків). Можна також упорядкувати ринок землі, додатково заробивши на земельному податку 5 млрд грн, закрити схеми з блокуванням податкових накладних – 10-12 млрд грн.

У 2017 р. надходження від податку на прибуток підприємств становили близько 64 млрд грн, або лише трохи більше 10% від загальної суми податкових надходжень. Це саме пов'язано з тим, що від цього податку відносно просто ухилятися підприємствам.

Розглянемо, яка ціна питання заміни податку на прибуток. Податок на прибуток дає в бюджет близько 2% ВВП або до 9% від усіх податкових надходжень до бюджету. Зокрема, в 2017 році він забезпечив понад 64 млрд гривень. Вже в поточному році, згідно з прогнозами Кабінету міністрів, надходження зростуть ще на 22%. Таким чином, в уряді очікують отримати від податку на прибуток 82 млрд гривень [2].

Введення ПВК докорінно змінить корпоративне оподаткування. З економічної точки зору, ПВК є податком на розподілений прибуток у вигляді дивідендів та прирівняних до них платежів, а не фінансових прибутків, як у випадку ППП. Вживання поняття "податок на виведений капітал" замість поняття "податок на дивіденди" означає, що з метою запобігання ухилянню від сплати податків будь-який рух капіталу від платників ПВК неплатникам ПВК буде обкладатися ПВК.

ПВК базується на міжнародному нестандартному виді корпоративного оподаткування. Вперше він був запроваджений в Естонії у 2000 році. Такий податок вводили в низці країн, зокрема, в Македонії й Молдові, але згодом його скасували. Естонія залишається єдиною країною, у якій цей податок працює багато років. Грузія ввела схожий до естонського податок у 2017 році.

Існують дві причини, які спонукають до докорінної реформи податкової системи. Перша – збільшення інвестицій. Оскільки нерозподілені прибутки не оподатковуються, це повинно сприяти інвестиційній діяльності. Друга – зменшення адміністративного навантаження. Замість фінансових прибутків податковою базою є операційні доходи. Вважається, що оподаткування операційних доходів полегшує адміністративне навантаження підприємств та податкових органів.

Ключовою відмінністю між ПВК та ППП є те, що база оподаткування, тобто вартість активів об'єктів оподаткування, складатиметься не із скоригованих фінансових прибутків підприємств, а з окремих операцій, що підлягають оподаткуванню. Це радикальна відмінність, адже відтепер податкове регулювання буде спрямоване на окремі платежі, а не на перевірку всієї фінансової звітності платників податків.

ПВК матиме дві основні ставки: 15% — для розподілу прямих прибутків, 20% — для розподілу прихованих прибутків — "умовних дивідендів". Це стимулюватиме платників використовувати для розподілу прибутку "нормальні" дивіденди.

Хоча ці ставки ПВК начебто наближаються до поточної ставки ППП у розмірі 18%, ПВК передбачатиме зменшення податкових ставок на розподілений прибуток. Оскільки з дивідендів не будуть стягуватися податок на до-

ходи фізичних осіб та військовий збір, ставка знизиться до 11% для прибутків, розподілених між фізичними особами через дивіденди, але за умовними дивідендами ставка зросте на 2%.

Підприємства, що підпадають під дію ПВК, повинні будуть звітувати лише про оподатковувані операції, а не подавати податкову декларацію на основі повної фінансової звітності. Звіти про виплату дивідендів та операції з виведення капіталу повинні надаватися щомісяця, якщо протягом цього місяця такі операції відбулися.

Більшість концепцій запобігання ухилянню від сплати податків, які використовуються в рамках ППП, такі як контроль трансфертного ціноутворення або моніторинг відсоткових платежів, залишаться актуальними і в рамках ПВК.

Ті, хто є прихильниками податку на виведений капітал, впевнені, що всі розмови про масові негативні сторони податку на виведений капітал поширюються від імені керівників ДФС (адже роботу після скасування податку на прибуток можуть втратити чимало співробітників інспекцій, що адміністрували його) та великих компаній, які щільно «сидять» на офшорах.

Маніпуляції в нарахуванні та сплаті податку на прибуток зустрічаються досить часто. Є думка, що нерідко підприємці взагалі не знають, як і що вони платять за цим видом податку.

Отже, однозначної відповіді щодо запобігання від хронічного недофінансування бюджету, прискореного розвитку підприємств та інших економічних «див» від впровадження в практику податку на виведений капітал немає. Дискусія триває, й експерти зобов'язані ретельно вивчити всі питання, пов'язані і з чинним податком на прибуток, і з поки що новим для України податком на виведений капітал.

Очевидно,що потрібна допомога у переконані МВФ та інших міжнародних партнерів, а також інвесторів та транснаціональних корпорацій у важливості впровадження ПВК. Ми не програли бій, а лише вимушені взяти паузу, адже у поточній ситуації роль МВФ у проведені реформ дуже важлива.

Крім того, зміна системи оподаткування не зменшує потребу у проведенні значно актуальнішої реформи, яка полягає в докорінній перебудові податкової системи, підвищенні потенціалу Державної фіскальної служби та боротьбі з корупцією.

1. Закон № 1797 «Про внесення змін до Податкового кодексу України щодо покращення інвестиційного клімату в Україні» //Відомості Верховної Ради (ВВР), 2017 - № 5-6, ст.48.

2. Кабмін зробив додаткові кроки для покращення інвестиційного клімату//[Ел.ресурс].Режим доступу https://ligazakon.net/lawnews/doc/EN171381.

3. Податок на виведений капітал голосуватимуть в пакеті зі скороченням видатків бюджету//Режим доступу://news.dtkt.ua/taxation/profits-tax/47533.

**Карпенко Роман Валерійович**
викладач кафедри
цивільно-правових дисциплін
Дніпропетровського державного
університету внутрішніх справ

# РОЗКРИТТЯ ТА РОЗСЛІДУВАННЯ ЕКОНОМІЧНИХ ЗЛОЧИНІВ: ПРОБЛЕМНІ ПИТАННЯ

Вагомий внесок у вирішення проблем попередження та розслідування економіч- них злочинів зроблено такими вченими як О. Абрамов, О. Бандурка, Г. Клімов, А. Новицький, В.Швець, В. Шендрик, В. Шиканов та ін. Але, незважаючи на вагомий вне- сок зазначених вчених, зростання кількості правопорушень в економічній сфері обумовлює необхідність проведення подальших досліджень із цієї проблематики. В умовах економічної стагнації в країні та світі спостерігається зростання злочинів, пов'язаних з легалізацією (відмиванням) грошових коштів та іншого майна, здобутих злочинним шляхом, шахрайств з платіжними картками, викраденням паролів та пограбування банківських рахунків, маніпу- люванням з фінансовою звітністю з метою ухилення від сплати податків, незаконним заволодінням чужим майном, крадіжками інформації з комп'ютеризованих баз даних фінансово-кредитних установ та суб'єктів господарювання тощо

Тенденція до збільшення кількості правопорушень в економічній сфері, що спостерігається протягом останніх років, визначає пріоритетну роль правоохоронних органів, зокрема органів внутрішніх справ, одним з основних завдань яких є захист економічних прав і інтересів суспільства, суб'єктів господарювання усіх форм власності та громадян, збереження економічного суверенітету та економічної цілісності України. При цьому ефективність роботи правоохоронних органів, зокрема органів внутрішніх справ, багато в чому залежить від можливості використання новітніх технологій оперативно-розшукової діяльності, що обумовлено, по-перше, еволюційним розвитком науки і техніки та накопиченням практичного досвіду, по-друге, появою новітніх форм та способів вчинення злочинів. На думку академіка О.М. Бандурки, одним з основних завдань щодо підвищення ефективності оперативно-розшукової діяльності є підняття ступеня готовності оперативних підрозділів до роботи з інформаційними системами, до активного використання ними новітніх інформаційних технологій у своїй професіональній діяльності, переосмислення традиційних підходів та методів, формування нового – системного мислення, оволодіння умінням бачити в нових інформаційних технологіях не тільки систему знань, але і сукупність практичних прийомів, методів і засобів, що розширюють межі можливостей користувачів таких систем [1; 2]. Основою розкриття будь-яких злочинів, у тому числі й економічних, є наявність попередньої інформації про злочин і особу, яка його вчинила, що використовується у процесі попередження, виявлення, розкриття і розслідування

економічних злочинів. На думку Міллера Л.Ю., інформаційне забезпечення процесів розкриття і розслідування злочинів, а іноді і їх виявлення, є основним фактором підвищення ефективності оперативно-розшукової діяльності органів внутрішніх справ [3; 4]. Стрімкий розвиток інформаційних технологій, що спостерігається протягом останніх років, підвищує вимоги до засобів отримання, збереження та передачі інформації в процесі розкриття економічних злочинів. Це пояснюється специфікою економічних злочинів, обумовленою документопотоками та документообліком, що супроводжують економічні та фінансові операції, механізмом утворення слідів, виявлення місць їх локалізації, встановлення напрямів та форм руху слідової інформації, а також складністю злочинності в економічній сфері. Крім того новий Кримінальний процесуальний кодекс України передбачає розширення підслідності правопорушень, які розслідують органи внутрішніх справ, і віднесення до їх компетенції досудового розслідування кримінальних правопорушень в економічній сфері, які раніше відносилися до компетенції органів прокуратури та Служби безпеки України.

Таким чином, протидія економічним злочинам є важливим напрямом забезпечення економічної безпеки держави та укріплення законних економічних основ державної системи України. Ефективність розкриття та розслідування економічних злочинів, що характеризуються складністю, багатоаспектністю та постійною зміною форм вчинення, багато в чому визначається існуючими методиками, технологіями та спеціальною технікою, що використовується оперативними працівниками та слідчими в оперативно-розшуковій діяльності. Постійна зміна форм та способів вчинення економічних злочинів підвищує роль та значення інноваційних технологій оперативнорозшукової діяльності, що створюють сприятливе середовище для протидії економічним злочинам. Позитивним аспектом також є вивчення досвіду боротьби з економічними злочинами у міжнародній практиці та визначення механізмів взаємодії з іншими відомствами та структурними підрозділами правоохоронних органів.

1. Аналітичний огляд організації роботи поліції зарубіжних країн щодо протидії злочинам у сфері високих технологій. – [Електронний ресурс]. – Режим доступу: http://42827.ncbint00.web.hosting-test. net/?p=883.

2. Бандурка О.М. Оперативно-розшукова діяльність. Частина І: підручник / О.М. Бандурка. – Х: Вид-во Нац. ун-ту внутр. справ, 2012. – 436 с.

3. Зарубіжні правоохоронці ознайо- милися з роботою тренінгового центру. – [Електронний ресурс]. – Режим доступу: http://mvs.gov.ua.

4. Миллер Л.Ю. Интеграционный метод в теории и практике оперативно- розыскной деятельности органов внутренних дел: препринт монографии / Под общ. ред. д-ра юрид. наук, проф., засл. деятеля науки РФ Г.К. Синилова. – М.: Издатель- ский дом Шумиловой И.И., 2013. – 54 с.

**Касян Сергій Якович**
к.е.н.,доц., доцент кафедри
економічної теорії та маркетингу

**Жованик Оксана Володимирівна**
студентка факультету міжнародної економіки
Дніпровського національного
університету імені Олеся Гончара

# БЕЗПЕКА КОМУНІКАЦІЙНОЇ ВЗАЄМОДІЇ ПІДПРИЄМСТВ ІЗ ДОВКІЛЛЯМ НА ОСНОВІ КОНЦЕПЦІЇ ЕКОЛОГІЧНОГО МАРКЕТИНГУ

На сьогодні, економічна та інформаційна безпека у світі та Україні базується на дотриманні безпечної екологічної взаємодії із довкіллям. В умовах інтенсифікації інформаційних потоків забезпечення інформаційної безпеки поряд із розв'язанням екологічних проблем сприяє досягненню збалансованого суспільного розвитку. Відмітимо значне розповсюдження у світі концепції екологічного маркетингу, яка дозволяє толерантно управляти бізнесом, не завдаючи шкоди довкіллю. Проблеми та перспективи дотримання економічної та інформаційної безпеки під час бізнес-взаємодії підприємств на концентрованих товарних ринках певною мірою фокусуються на комплексній екологізації маркетингової діяльності.

І. М. Смоленський, Г. С. Степанюк визначають екологічний маркетинг (англ. green marketing) як прикладну типологію маркетингу, який базується на досягненні й підтриманні екологічного вектору орієнтації споживчого і промислового попиту, що забезпечить позитивні потоки прибутку, який має спрямовуватися на соціально орієнтоване управління і збереження довкілля [1].

Змістовна безпека від запровадження концепції екологічного маркетингу полягає у досягненні економічної гармонізації взаємодії соціальних і економічних агентів, що комплексно застосовують процедури і моделі, спрямовані на координацію безпечного природокористування. При цьому ефективність екологічної безпеки системно вписується у концепцію сталого розвитку, що сприяє досягненню збалансованості під час кругообороту основних ресурсних потоків та організації логістики рециклінгу.

Тетяна Примак справедливо підкреслює вагомість соціальної реклами, як сучасного інструменту спрямованого впливу на інформаційне суспільство, коли акцентується на емоційному контексті сприймання реклами й побудово на основі цього споживчої моделі ухвалення рішення. Виокремлюються причини прояву шкідливого способу життя, забруднення довкілля, серед яких варто згадати не модність, не достатність інформації, відсутність належної альтернативи стосовно зміни атрибутів споживчої поведінки. Вона зазначає, що у певному аспекті людина здійснює дії підсвідомо, тому вплив соціальної реклами при цьому є проблематичним, оскільки людини сприймає фізично необхідним такий стиль життя. Саме тому, соціальна реклама передусім спрямова-

на на людей, усвідомлюють мотиви і зміст своєї поведінки [2, с. 19, 20].

Отримавши спонукальні інформаційні мотиви від соціальної реклами, людина приймає зважене рішення. Якщо людина викидає сміття на вулицю й ніколи не замислювалася над цим, реагуючи на соціальну рекламу, що пропагує збереження довкілля, позначає наслідки його забруднення, людина зверне на це увагу. При цьому пересічний споживач може обговорювати це питання із своїм оточенням та може змінити свої ставлення до аспектів безпечної взаємодії з довкіллям [2, с. 20].

Науковець наголошує на ретельному обиранні спрямування соціальної реклами, коли вибирається вектор зміни сумнівного задоволення на альтернативне: людина буде знати альтернативні способи дії, спектр задоволення нових ефектів. Поділяємо точку зору щодо розв'язання певних гострих проблем завдяки шоковій рекламі, вплив якої охоплює населення, спричиняючи обговорення проблеми серед людей та пошук шляхів її розв'язання [2, с. 21]. Отже, у світі, системне використання соціальної реклами підвищує рівень безпеки у суспільстві, що змушує людей замислитися про актуальні питання господарського розвитку, про які вони навіть і не замислювалися, безпечної взаємодії з довкіллям. Це дає поштовх ефективно діяти, удосконалювати екологічний маркетинг, змінювати конфігурацію сил на ринку.

Н. В. Зіновчук, А. В. Ращенко визначає низку принципів екологічного маркетингу, а саме: орієнтацію на споживача, постійності, прозорості, рівноцінності, комплексності, прагматичності, інтегративності та залучення. Науковці підкреслюють, що застосування таких принципів дозволяє сучасним споживачам бути обізнаними щодо суспільних пріоритетів розвитку, підприємствам формувати пропозицію екологічних та енергозберігаючих продуктів [3].

В Україні проблема екологічно безпечного господарювання, поводження з твердими й рідкими побутовими відходами завжди була актуальною, через відомі не найкращі практики на території країни. На сьогодні відношення держави до екологічної ситуації має вплив на становлення і розвиток екологічного маркетингу, що створює підґрунтя для удосконалення соціально значущої і безпечної маркетингової діяльності. О. О. Веклич зазначає, що фінансове забезпечення природоохоронної діяльності в Україні перебуває на задовільному рівні. Раціонально створена податкова база за забруднення навколишнього середовища, природокористування, за рахунок яких поповнюється бюджет для здійснення природоохоронної діяльності. Безперечне, держава прагне розв'язувати проблеми в тих сегментах екології, що мають критичне становище. Цим державне адміністрування стимулює підприємства проводити екологічно чисту економічну діяльність, проводячи постійний перегляд її аспектів та дбаючи про захист навколишнього середовища [4, с. 20-22].

Науковець комплексно виокремлює наявні проблеми досягнення ефективного фінансового забезпечення природоохоронної діяльності, а саме:

– держава не завжди визначає чітких пріоритетів щодо використання фінансових ресурсів, що акумульовані й спрямовуються на певні екологічні цілі;

– не повна поінформованість про реальний стан екологічних збитків

для суспільства;

– низька бюджетна дисципліна у сфері природоохоронної діяльності.

Переглянувши функціонування механізму фінансування природоохоронної діяльності, усунувши недоліки, держава зможе покращити безпеку й стан навколишнього середовища на базі впровадження концепції екологічного маркетингу. При цьому важливо зацікавити підприємства до проведення такої маркетингової діяльності, показавши, що держава цікавиться цим питанням та заохочує його розвиток [4, с. 20-22, 32]. На наш погляд, в таких умовах вітчизняні підприємства мають системно застосовувати інструменти й складові екологічного маркетингу, що дає змогу поліпшувати безпеку маркетингової взаємодії з довкіллям.

У світі споживачі приділяють значну увагу підвищенню екологічної поінформованості, оскільки на основі маркетингових комунікаційних важелів прагнуть завжди дбати про навколишнє середовище. На основі інтегрування концепції еко-маркетингу з відповідним логістичним і комунікаційним забезпеченням підприємства розширюють ринки збуту товарів і послуг [5].

Отже, досягнення безпеки економічної взаємодії підприємств із довкіллям є можливе на застосування основі концепції екологічного маркетингу. При цьому ефективність екологічної безпеки системно вписується у концепцію сталого розвитку, що сприяє досягненню збалансованості під час кругообороту основних ресурсних потоків та організації логістики рециклінгу.

1. Смоленський І. М. Стратегічно-операційний маркетинг екологізації виробництва / І. М. Смоленський, Г. С. Степанюк // Економіка України. – 2006. – № 9. – С. 74–79.

2. Примак Тетяна Якою має бути соціальна реклама? / Тетяна Примак // Маркетинг в Україні. – 2006. – №5. – С. 19–23.

3. Зіновчук Н. В. Екологічний маркетинг : навч. посіб. / Н. В. Зіновчук, А. В. Ращенко. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 190 с.

4. Веклич О. О. Сучасні тенденції фінансового забезпечення природоохоронної діяльності в Україні / О. О. Веклич // Фінанси України. – 2009. – №11. – С. 20–34.

5. WPP companies [Електронний ресурс]. – Режим доступу: http://www.wpp.com/wpp.

**Карчевський Микола Віталійович**
д.ю.н., проф.
*(Луганський державний університет внутрішніх справ імені Е.О. Дідоренка)*

## КРИМІНАЛЬНЕ ПРАВО ТА НОВІ ТЕХНОЛОГІЇ: ВІД «КОМП'ЮТЕРНИХ» ЗЛОЧИНІВ ДО СОЦІАЛІЗАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ

Найбільш помітні соціальні зміни пов'язані з інформатизацією. Розвиток та розширення сфери застосування інформаційних технологій обумовили в тому числі істотні трансформації правового регулювання. Нібито очевидні положення, але відповідь на питання «Що саме змінилося?» не є простою.

Спробуємо сформулювати власне бачення цієї проблеми для сфери кримінально-правового регулювання.

1. Необхідність кримінально-правового стимулювання позитивних та мінімізації негативних наслідків інформатизації обумовила появу відносно самостійної групи суспільних відносин, які можна розглядати як новий родовий об'єкт злочину. Для позначення цієї групи будемо використовувати термін «інформаційна безпека» та визначимо його наступним чином: система суспільних відносин щодо реалізації інформаційної потреби особи, суспільства, держави. Складається дана система з трьох взаємопов'язаних та взаємообумовлених елементів: відносини в сфері використання інформаційних технологій, відносини в сфері забезпечення доступу до інформації, відносини в сфері формування інформаційного ресурсу.

2. На сьогодні можна казати про існування «класичних» проблем кримінально-правового регулювання кожної з означених груп. Ці проблемні аспекти достатньо добре досліджені та підтверджені емпіричним даними.

3. Стосовно так званих «комп'ютерних злочинів» головне питання полягає у відсутності чітких критеріїв суспільної небезпечності на рівні законодавчих визначень. Через це в сфері дії кримінальної юстиції опиняються не тільки діяння, що дійсно є суспільно небезпечними, але й ті, які такими не є. Ефективність протидії кіберзлочинності зменшується. Через вал роботи щодо розслідування діянь зі спірною суспільною небезпечністю певною мірою втрачаються і перспективи вдосконалення діяльності правоохоронців. Красномовними тут буде порівняння даних про облікові кримінальні правопорушення в сфері використання інформаційних технологій (ст.ст. 361 – 363-1 КК України) з кількістю вироків даної категорії, представлених у Єдиному державному реєстрі судових рішень (таблиця 1). Для того, щоб мати можливість оцінити результати роботи правоохоронців в контексті темпів інформатизації, ми також додали дані щодо проникнення Інтернету. Цей показник є одним з універсальних маркерів інформатизації, обчислюється у відсотках та представляє собою частку населення країни, яка користується Інтернетом. Як можна побачити, із зростанням аудиторії Інтернету відбувається зростання кількості облікованих правопорушень, що цілком природньо оскільки чим більше людей використовує сучасні інформаційні технології тим більше «комп'ютерних» злочинів може бути вчинено. Але разом із зростанням кількості облікованих правопорушень спостерігається зменшення кількості судових вироків відповідної категорії. Можна казати про рівень матеріально-технічного та кадрового забезпечення розслідування, брати до уваги необхідність спеціальних знань у судів та прокурорів тощо. Проте основна, фундаментальна причина ситуації, що склалася саме у якості законодавства.

Таблиця 1

**Статистичні дані щодо протидії злочинам в сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку**

| Показник | 2013 | 2014 | 2015 | 2016 |
|---|---|---|---|---|
| **Абсолютні дані** | | | | |
| Кількість вироків у Єдиному державному реєстрі судових рішень | 56 | 40 | 39 | 25 |
| Обліковано кримінальних правопорушень | 568 | 418 | 556 | 912 |
| Кримінальні правопорушення, у яких особам вручено повідомлення про підозру | 245 | 194 | 250 | 514 |
| Проникнення Інтернету (КМІС) | 49 | 54 | 57 | 62 |
| **Відносні дані (відсотки від базового рівня – 2013 р.)** | | | | |
| Кількість вироків у Єдиному державному реєстрі судових рішень | 100 | 71 | 70 | 45 |
| Обліковано кримінальних правопорушень | 100 | 74 | 98 | 161 |
| Кримінальні правопорушення, у яких особам вручено повідомлення про підозру | 100 | 79 | 102 | 210 |
| Проникнення Інтернету (КМІС) | 100 | 110 | 116 | 127 |

4. Проблеми кримінально-правового регулювання наступної групи відносин інформаційної безпеки – відносин в сфері забезпечення доступу до інформації – стосуються головним чином розбалансованості законодавства, існуванні численних конкуруючих норм, надмірного рівня кількості кримінально-правових заборон у даній сфері. Необхідною є оптимізація означеної системи норм, заміни наявної розосередженої системи спеціальних кримінально-правових заборон такими, які б забезпечували регулювання більш широких сегментів інформаційної безпеки.

5. Основне питання кримінально-правового регулювання в сфері формування інформаційного ресурсу полягає у чіткому та послідовному визначенні межі можливостей ефективного впливу на суспільні відносини засобами кримінального права. У суспільно-політичному дискурсі, в науці небезпеки інформаційних впливів та зловживань обговорюються достатньо широко. Багатомірність та масштабність шкоди від неконтрольованого інформаційного простору не викликає сумнівів. Разом з цим розв'язання означених проблем шляхом доповнення КК новими нормами навряд чи є доцільним. Неодноразово пропонувалося встановлювати покарання за різноманітні форми маніпуляції суспільною свідомістю. Такі пропозиції є спірними через прогнозовану неефективність і декларативність, їх невідповідність принципам кримінально-політичної адекватності, а також співрозмірності позитивних і негативних наслідків криміналізації. Крім того, поширення глобальних інформаційних технологій взагалі робить методи обмеження або заборони контенту все менш ефективними. Яскравим прикладом тут може слугувати

відомий «ефект Стрейзанд». Розв'язання проблеми знаходиться поза межами кримінально-правового регулювання і, на нашу думку, передбачає в першу чергу системну роботу в системі освіти та формуванні конкурентних інформаційних продуктів. Додаткових аргументів на користь освітнього вектору розв'язання наведених проблем інформаційної безпеки можуть свідчити і питання, які стали предметом суспільної уваги під час встановлення обставин загибелі учасників мережевої групи «Синій кіт». Самостійним напрямом особистої інформаційної безпеки підлітків, який знову ж таки підтверджує тезу про обмежену ефективність кримінально-правових засобів, є протидія кібербулінгу. Зарубіжна практика свідчить про те, що негативні наслідки образ, цькування неповнолітніх за допомогою соціальних мереж або електронної пошти (власне кібербулінг) долаються головним чином шляхом формування навичок безпечної комунікації.

В означеному контексті неможливо не згадати рішення про обмеження доступу до певних російських сайтів та соціальних мереж. З одного боку маємо очевидні позитивні аспекти: .тимчасове зменшення ефективності інформаційних операцій проти України та відчутні фінансові втрати російських ІТ-компаній (експертні оцінки втрат Яндекса - $124,4 млн.). З іншого – значні негативні наслідки як для інформаційної безпеки країни, так і громадян. По-перше, обмеження поведінки, що фактично є соціальною нормою, актуалізує питання стимулювання правого нігілізму, веде до чергового «витку» інфляції нормативно-правових актів. По-друге, обмеження можливостей правоохоронних органів щодо оцінки, аналізу та контролю за антидержавною діяльністю з використанням заблокованих ресурсів. Сподіватися на те, що всі одразу перестануть користуватись забороненими ресурсами безвідповідально. В той же час кількісна та якісна оцінка даного процесу надзвичайна ускладнена, моніторинг національної аудиторії заборонених ресурсів став складним технічним завданням. По-третє, створення «комфортної» «сірої зони» для інформаційних впливів через ускладнення їх правової оцінки. Ще раз зазначимо, величезна аудиторія не скоротиться миттєво. Чи можна сьогодні розглядати пост у соціальних мережах, доступ до яких обмежено, як «публічний заклик» в контексті відомих статей Особливої частини КК? Непросте питання, яке може розглядатися як технологія ухилення від відповідальності. По-четверте, нові небезпеки широкого розповсюдження шкідливого програмного забезпечення, зловмисники (в першу чергу шахраї, «фішери») отримали значну цільову аудиторію. Потреба отримувати доступ до заблокованих ресурсів за наявності для цього достатньо простої технічної можливості, створює попит на різноманітні програмні засоби. Під виглядом таких програмних засобів значна частка національної аудиторії заблокованих ресурсів може отримати «троянське» програмне забезпечення. В подальшому їх комп'ютери та інтернет-пристрої можуть бути використані, наприклад, для масштабних атак відмови від обслуговування.

6. Варто зауважити, що проблематика інформаційної безпеки є однією з найдинамічніших. Новітні технології розвиваються та поширюються досить швидко та, відповідно, викликають появу нових соціальних практик,

формують нові потреби у правовому регулюванні. Тому, сформулювавши як зазначалося раніше «класичні» проблеми інформаційної безпеки, вважаємо за необхідне звернути на нові виклики, що проявилися останнім часом достатньо рельєфно. Одним з таких є новітні можливості незаконних дій щодо матеріальних цінностей або з ними.

7. Сферою широкого застосування комп'ютерної техніки є банківська діяльність та платіжні системи тому велика частка злочинів проти власності так чи інакше пов'язана зі злочинами в сфері використання комп'ютерної техніки. Йдеться про: «злам» електронної пошти з метою отримання реквізитів доступу до банківських рахунків (ст. 361 КК); блокування інтернет-ресурсу з метою вимагання (ст. 361 або 363-1 КК); використання «скімерів» (спеціальних пристроїв, що приховано встановлюються зловмисниками на банкомати) для отримання реквізитів платіжних карток або розробка та використання шкідливих програмних засобів, призначених для незаконного віддаленого доступу до бухгалтерського програмного забезпечення підприємств, установ чи організацій (ст. 361-1 КК); збут клієнтських баз даних скомпрометованих фінансових установ (ст. 361-2); введення банківськими працівниками до автоматизованих систем банківського обслуговування неправдивих відомостей щодо здійснених фінансових операцій (ст. 362 КК); невжиття необхідних технічних заходів інформаційної безпеки, що призвело до компрометації автоматизованої системи фінансової установи (ст. 363 КК) тощо. Разом з оновленням способів вчинення та приховування слідів злочинів проти власності істотні зміни спостерігаються й у питанні предмету злочину проти власності. Доволі дискусійним як для науковців так і для практиків стало питання юридичного змісту таких категорій як «безготівкові гроші», «електронні гроші», «криптовалюта».

8. Категорія «безготівкові гроші» найчастіше зустрічається в контексті злочинів проти власності, що вчиняються з використанням платіжних карток або їх реквізитів. Фактично вони представляють собою зобов'язання банка-емітента платіжної картки, відомості про які обліковано на картковому рахунку держателя картки. В термінах розділу Особливої частини КК «Злочини проти власності» стосовно безготівкових грошей найбільш обґрунтовано використовувати поняття «право на майно». Тому переважна більшість посягань, пов'язаних з незаконними операціями з платіжними картками або їх реквізитами правильно розглядається як один з видів шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки (ч. 3 ст. 190 КК). Найбільш дискусійний момент такої кваліфікації полягає у питанні можливості «обманути комп'ютер». Проте наявний емпіричний матеріал та аналіз законодавства дозволяють наступним чином сформулювати особливості об'єктивної сторони даного виду шахрайства. По-перше, направляючи несанкціонований законним держателем картки запит на здійснення платежу і використовуючи існуючу платіжну систему і встановлені в ній правила автоматизованої обробки запитів законних держателів карток, зловмисник обманює банківську установу (банк-емітент) щодо необхідності виконання останнім зобов'язань, обумовлених договором, укла-

деним між банком і законним держателем картки. По-друге, внаслідок цього введення в оману банк-емітент здійснює необґрунтоване списання безготівкових коштів з рахунку законного держателя картки, що призводить до заподіяння останньому збитків у вигляді зменшення кількості безготівкових грошових коштів, врахованих на картрахунку[1] Варто зазначити, що не всі посягання в сфері використання платіжних систем, банкоматів слід кваліфікувати за ч. 3 ст. 190 КК. Наприклад, достатньо поширеним є так званий cash trapping, заволодіння готівкою, що знаходиться у банкоматі за допомогою спеціального пристрою («виделки»), або клейкої стрічки. Подібні випадки слід кваліфікувати як крадіжку, але такі виключення лише підтверджують правильність наведених раніше міркувань.

9. Електронні гроші «одиниці вартості, які зберігаються на електронному пристрої, приймаються як засіб платежу іншими особами, ніж особа, яка їх випускає, і є грошовим зобов'язанням цієї особи, що виконується в готівковій або безготівковій формі»[2] Вони з'явилися як реакція ринку банківських послуг на проблеми безпеки використання платіжних карток та потребу в новому, більш гнучкому, зручному і захищеному платіжному інструменті для оплати товарів та послуг через Інтернет[3]. Цим зумовлюються особливості електронних грошей, які відрізняють їх від безготівкових: електроні гроші не є універсальними і приймаються виключно користувачами відповідних платіжних систем; емісію грошей здійснює виключно НБ, емісія електронних грошей здійснюється банківськими установами; внаслідок переказу електронних грошей їх одержувач набуває право грошової вимоги до того ж суб'єкта, що й платник; електронні гроші існують в рамках однієї платіжної системи і не здатні до переведення їх в інші платіжні системи у незмінному вигляді[4]. Враховуючи означені особливості електронних грошей питання кваліфікації незаконних дій щодо них мають розв'язуватися аналогічно з описаним раніше підходом щодо безготівкових грошей.

10. Криптовалюта представляє собою наступний крок у розвитку технологій розрахунків з використанням сучасних інформаційних технологій. Найбільш відомою криптовалютою є Bitcoin. У науковій та популярній літературі представлено достатньо інформації щодо технічних та організаційних

[1] Дудоров О.О., Карчевський М.В. Шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки // Азовські правові читання – 2017: Матеріали міжнародної науково-практичної конференції, м. Бердянськ, 28–29 квітня 2017 р. – Бердянськ: ТОВ «Модем-1», 2017. – С. 5–12.

[2] Положення про електронні гроші в Україні // Постанова Правління Національного банку України від 04.11.2010 № 481

[3] Фінансова грамотність : навч. посібник / авт. кол. ; за ред. д-ра екон. наук, проф. Т. С. Смовженко. – Вид. 2-ге, випр. і доп. – К., 2013. – С. 74.

[4] Більш докладно див.: Шимон С. Електронні гроші: форма грошей чи майнові права вимоги? / С. Шимон // Юридична Україна. – 2015. – № 9. – С. 36–41; Куцевич М. Неправомірний випуск й використання електронних грошей, що вчиняються у системах інтернет-розрахунків (проблеми кримінально-правової кваліфікації) / М. Куцевич, П. Берзін // Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки. - 2013. - Вип. 4. - С. 13-16.

особливостей функціонування Bitcoin, зупинимося на тих, які вважаємо ключовими для відповіді на питання щодо можливостей кримінально-правового регулювання в даній сфері. По-перше, криптовалюта фізично представляє собою певний набір даних згенерований на підставі складного математичного алгоритму. По-друге, платіжна система Bitcoin організована за принципом піринговоі мережі (p2p, pear to pear – рівний рівному), записи щодо всіх транзакцій розподілені між всіма учасниками системи, єдиний центр координації мережі відсутній, у вільному доступі представлено інформацію щодо всіх здійснених транзакцій. Такий метод організації платіжної системи забезпечує майже абсолютний захист інформації щодо транзакцій, робить систему стабільною та надійною. По-третє, для реєстрації в платіжній системі не використовуються персональні дані, транзакції здійснюються між деперсоніфікованими «електронними гаманцями». По-четверте, Bitcoin - нефіатні гроші, їх вартість нічим не забезпечена і визначається ситуативно на підставі попиту та пропозиції, єдиний орган, що встановлює курс до національних валют, відсутній. Тим не менше, корисні властивості криптовалюти (захищеність, конфіденційність, децентралізація, майже миттєвий переказ у будь-яку частину світу) забезпечує стабільний попит на неї та стійке зростання курсу до національних валют. Лише з грудня 2016 року по квітень 2017 вартість Bitcoin зросла з 750 до 1450 доларів США. За таких умов не дивно, що криптовалюта набуває значного поширення в Україні. При цьому Національний банк України (лист від 8 грудня 2014 р. №29-208/72889) розглядає Bitcoin як «грошовий сурогат, який не має забезпечення реальною вартістю і не може використовуватися фізичними та юридичними особами на території України як засіб платежу, оскільки це протирічить нормам українського законодавства». Маємо ситуацію, коли фактично існуючі та динамічні суспільні відносини опиняються поза межами правового регулювання за умови очевидної необхідності такого. Наприклад, особа вимагає певну суму у Bitcoin або отримує хабар у такій формі. Яким чином встановити ознаки предмета злочину? Чи можна розглядати відомості інтернет-джерел щодо курсу Bitcoin як достатній доказ для встановлення економічної ознаки відповідних предметів злочинів? На сьогодні чіткої відповіді на поставлені питання не має. Досвід зарубіжних країн дуже різноманітний, містить приклади від офіційного визнання криптовалюти (Японія, Німеччина) до аналогічного національному підходові ігнорування. Очевидно криптовалюти будуть дедалі частіше використовуватися для вчинення злочинів або ставати їх предметом. В таких умовах найбільш доцільно сформулювати прості та прозорі правила для сфери кримінально-правового регулювання, зокрема передбачити механізм оцінки. Представлення у процесуальній формі даних про криптовалюти створить нові умови для якісного оновлення діяльності правоохоронців. Виникнуть принципово нові види тактичних операцій, що збільшить можливості протидії злочинності. Варто зазначити, що ці питання слід розглядати як складові більш загальної проблеми – можливості використання технологій Big Data у

правоохоронній діяльності[5].

11. Таким чином, для продовження дискусії щодо змісту обумовлених інформатизацією змін в сфері кримінально-правового регулювання можемо сформулювати наступні положення: розпочалося та триває формування нового предмету кримінально-правового регулювання – інформаційної безпеки; «класичними» проблемами цього процесу є недостатність визначеності законів про кримінальну відповідальність за «комп'ютерні» злочини, необхідність оптимізації системи кримінально-правого регулювання в сфері доступу до інформації, відсутність консенсусу у питанні меж доцільності кримінально-правового регулювання в сфері інформаційної безпеки; існують складнощі кримінально-правового регулювання, обумовлені появою нових видів матеріальних цінностей; інформатизація створює нові можливості для підвищення ефективності роботи правоохоронців, однак їх реалізація передбачає прийняття організаційно-правових рішень, які б дозволили збирати та використовувати надвеликі обсяги персональних даних з метою протидії злочинності.

12. Разом з цим, одним з найпомітніших трендів сучасної юридичної науки стала проблема соціалізації штучного інтелекту.

Передумовою ефективної наукової дискусії з правового регулювання соціалізації роботів є визначення структури досліджуваного проблемного поля, *формулювання ключових питань, які підлягають першочерговому аналізу*. Спробуємо запропонувати один з можливих підходів до розв'язання означеного завдання.

*Перше питання* правового регулювання розвитку штучного інтелекту стосується доцільності заборони (обмеження) наукових розробок у даній сфері. Розуміючи небезпеки некерованого розвитку штучного інтелекту деякі вчені наполягають на забороні відповідних досліджень та контролі за поширенням технологій настільки суворим як в атомній енергетиці[6]. Інші вчені кажуть про неможливість зупинити розвиток технологій. Як справедливо зазначає знаний український вчений В.І. Борисов, технології, які б небезпечні вони не були, обов'язково будуть винайдені та розповсюджені незалежно від нашого бажання та відношення до них. На нашу думку такий підхід є більш прагматичним та реалістичним. Заборона досліджень в сфері штучного інтелекту принципово не може стати дієвою. На відміну від досліджень в сфері ядерної зброї, розробка систем автономного озброєння в рази дешевше, отже

[5] Карчевський М.В. Можливості Big Data та кримінально-правова комунікація // Матеріали Міжнародної науково-практичної конференції "Політика в сфері боротьби зі злочинністю" [Текст]. - Івано-Франківськ, 2017. – С. 52-58.

[6] Autonomous Weapons: An Open Letter from AI & Robotics Researchers [Electronic resource] // Future of Life Institute. – Mode of access: http://futureoflife.org/open-letter-autonomous-weapons/; Бондаренко А. Искусственный интеллект против человечества: Маск, Хокинг и Возняк предостерегают, что пора остановиться [Электронный ресурс] / А. Бондаренко // AIN.UA – 27.07.2015 – Режим доступа : http://ain.ua/2015/07/27/593911; Хейнс К. Доклад Специального докладчика по вопросу о внесудебных казнях, казнях без надлежащего судебного разбирательства или произвольных казнях [Електронний ресурс] / Кристоф Хейнс // Платформа стратегічного судового захисту. – Режим доступу: http://precedent.in.ua/index.php?id=1405161984

є більш доступною. З розвитком інформаційних технологій дана діяльність ставатиме ще доступнішою, а отримані зразки зброї – ще більш небезпечними. В таких умовах законодавча заборона розробки автономної зброї приведе до ситуації, коли органи безпеки та правопорядку будуть оснащені на порядок гірше ніж злочинці, терористичні організації тощо.

Таким чином, відповідь на перше питання правового регулювання соціалізації штучного інтелекту наступна: попри ризик небезпек, абсолютна заборона розробки систем штучного інтелекту є неможливою, правове регулювання в даній сфері має забезпечувати стимулювання соціально ефективного використання технологій та мінімізацію ризиків зловживання технологією.

13. В той же час людство має забезпечити контроль за розвитком технологій. *Наступне питання правового регулювання* в сфері соціалізації штучного інтелекту – яким чином здійснювати правове регулювання використання штучного інтелекту.

Як зазначалося раніше, у науковій літературі представлено два підходи. У класичній системі юридичних координат вже сьогодні маємо певні рішення: визначаються права та обов'язки розробників, власників та осіб, що експлуатують роботів. У такий спосіб розв'язуються питання використання автономних транспортних засобів (autonomous vehicles), так званих «соціальних» (care robots) та хірургічних роботів, інноваційних засобів протезування тощо[7].

Інший підхід полягає у розгляді роботів як суб'єктів права. Сьогодні таке рішення може виглядати як фантастика з ознаками безпідставного юридичного романтизму. Найбільш вагомий аргумент у тому, що створений штучно робот слідує закладеній програмі та, відповідно, не має свободи вибору, свободи волі. Оскільки остання є атрибутом суб'єкта права, питання нібито закрите. Проте, не викликає сумнівів, що на певному етапі розвитку технологій та ускладнення відносин в сфері робототехніки, процес прийняття рішення роботом, нехай і на підставі програми, стане настільки складним, що його можна буде розглядати як акт поведінки людини. Тут варто зазначити, що Європейський парламент у січні 2017 року взяв до розгляду проект резолюції про правовий статус роботів як "електронної особистості (електронної особи)"[8].

Отже, представлені підходи не є взаємовиключними, їх можна розглядати як різні етапи правового регулювання робототехніки. Зрозуміло, що розгляд досліджуваних питань за класичною схемою «розробник-власник-користувач» є актуальним та затребуваним для сучасного рівня технологій. Запропоновані в межах цього розуміння, рішення можуть забезпечити достатньо ефективне юридичне забезпечення сучасних військових, промислових, соціальних роботів тощо. Очевидно і те, що ускладнення технологій вимагатиме переходу до нової, більш складної схеми правового регулювання. Ско-

[7] D6.2 Guidelines on Regulating Robotics [Electronic resource] – Mode of access : http://www.robolaw.eu

[8] Коваль М. Електронна особистість: навіщо ЄС обговорює права роботів [Електронний ресурс] / Марія Коваль // Європейська правда – 24.01.2017 – Режим доступу : http://www.eurointegration.com.ua/experts/2017/01/24/7060539/

ріше за все правове регулювання соціалізації штучного інтелекту пройде шлях від розгляду робота як об'єкта відносин до наділення його правами та обов'язками.

14. Якщо перше питання правового регулювання соціалізації штучного інтелекту стосувалося стратегічної проблеми заборони або регулювання штучного інтелекту. Друге питання пов'язане з тим як забезпечити нормативно-правове відображення використання роботів. Третє, в свою чергу, пов'язане з організацією виконання норм, що регулюють використання штучного інтелекту. Збереження можливості контролювати суспільні процеси потребуватиме від людства створення ефективної системи юстиції для роботів.

З отриманням роботами статусу суб'єкта права виникнуть нові сфери юстиції. Крім традиційної юстиції можна буде казати про появу двох нових видів, умовно назвемо їх «змішана юстиція» та «юстиція штучного інтелекту». До змішаної юстиції будуть відноситися форми вирішення правових спорів між фізичними, юридичними особами, суспільством та роботами. До юстиції штучного інтелекту будуть відноситися форми вирішення правових спорів між роботами. Крім цього функціонування даної системи юстиції буде забезпечувати протидію роботам, що представляють загрозу для соціального розвитку та стабільності.

Цілком зрозуміло, що копіювати людську систему юстиції для штучного інтелекту немає сенсу. Принципово різні фізичні характеристики та потреби вимагають апріорі відмовитися від такого підходу. Разом з цим створення даної системи є необхідною умовою для того, щоб забезпечити людству можливість контролювати розвиток суспільних процесів. Скоріше за все юстиція штучного інтелекту буде створена на основі роботів. Фізичних та інтелектуальних даних людини очевидно буде недостатньо для ефективного функціонування даної системи юстиції. Створення такої системи передбачає узагальнення в чіткі алгоритми досвіду, отриманого за час існування традиційної юстиції. Таке узагальнення має стати одним з основних напрямків сучасної юридичної науки.

15. Наприкінці варто зауважити, що сформульовані пропозиції ґрунтуються на гіпотезі про розвиток штучного інтелекту. У роботі ми спробували сформулювати перспективні напрями правового регулювання беручи до уваги гіпотезу появи автономного штучного інтелекту. Можливе й інше бачення. Наприклад, технічний прогрес може піти шляхом фізичної інтеграції людини та технологій. Як у такому випадку зміниться правовий статус людини, що підсилює свої можливості численними технологічними імплантатами? Як бути у випадку використання імплантатів із штучним інтелектом? Чи всі аспекти такого бачення розвитку робототехніки отримають якісне юридичне відображення в «класичній» схемі (власник-розробник-користувач)? Отже, перспективним напрямом подальших досліджень в сфері правового регулювання соціалізації штучного інтелекту варто визнати також проблематику фізичної інтеграції людини й технологій.

**Катан Володимир Олександрович**
к.ф-м.н., доц., доцент кафедри
економічної кібернетики Дніпровського
національного університету імені Олеся Гончара

# МАТЕМАТИЧНА МОДЕЛЬ СИСТЕМНОЇ ДИНАМІКИ ДЛЯ АНАЛІЗУВАННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ

У буремному сьогоденні проблема забезпечення національної безпеки є надзвичайно актуальною. Основними показниками стану національної безпеки є рівень щорічного оновлення озброєння, військової та спеціальної техніки, рівень забезпечення військовими та інженерно-технічними кадрами, рівень безробіття, децильний коефіцієнт, рівень зростання споживчих цін, рівень державного зовнішнього та внутрішнього боргу (% від внутрішнього валового продукту (ВВП)), рівень забезпечення ресурсами охорони здоров'я, культури, освіти та науки (% від ВВП) [1].

Існують різні методологічні підходи до дослідження економічної безпеки країни з урахуванням політичного аспекту національної безпеки в цілому. До недоліків запропонованих систем індикаторів та показників безпеки треба віднести: емпіричний підхід, приділення головної уваги статистичним взаємозв'язкам замість причино – наслідковим залежностям, суб'єктивізм при відборі показників, відсутність загальної всеохоплюючої картини явища, статична інтерпретація економіко – політичних явищ без врахування їх динамічної складової, що призводить до формування неадекватної оцінки соціально – економічної та політичної ситуації в країні, що може привести до помилок при прийнятті рішень. У теперішній час існує математичний апарат, що дозволяє моделювати та прогнозувати показники національної безпеки для різних часових інтервалів [1].

Модель системної динаміки [2-3] дозволяє відслідковувати причино – наслідкові зв'язки в системі і складається із системних рівнів, які представляють собою накопичення в ланцюгах зворотного зв'язку, потоків, що переміщують вміст одного рівня до іншого, процедур розв'язків , які регулюють темпи потоків між рівнями, а також каналів інформації, що з'єднують процедур розв'язків з рівнями.

Дія окремого потоку накопичується, визначаючи рівень системи. Інформація про рівень складає основу для регулювання швидкістю потоку. До змінних рівня відноситься рівень інфляції, чисельність населення, пропозиція праці та розмір податкового навантаження, кожний з яких є результатом накопичення внутрішніх та зовнішніх потоків, що зв'язують однорідні рівні. Зростання або спадання рівнів визначається тільки темпами потоку. Один рівень може впливати на інший рівень тільки темпом потоку.

Математично модель системної динаміки представляє собою систему звичайних диференціальних нелінійних рівнянь першого порядку, яка в залежності від часу визначає зростання або спадання величин, що характери-

зують системні рівні, а саме рівень щорічного оновлення озброєння, військової та спеціальної техніки, рівень забезпечення військовими кадрами, рівень забезпечення інженерно-технічними кадрами, рівень безробіття, децильний коефіцієнт, рівень зростання споживчих цін, рівень державного зовнішнього боргу, рівень державного внутрішнього боргу, рівень забезпечення ресурсами охорони здоров'я, рівень забезпечення ресурсами культури, рівень забезпечення ресурсами освіти та науки. У правих частинах диференціальних рівнянь для характеристики темпів зростання та спадання використовуються відомі функціональні залежності між рівнем безробіття та рівним споживчих цін, між рівнем безробіття та рівним державного зовнішнього боргу, між рівнем безробіття та децильним коефіцієнтом, а також між рівнем безробіття та рівним державного внутрішнього боргу [1]. Вказані функціональні залежності можуть бути представлені у вигляді таблиць або за допомогою наближених аналітичних виразів, а також апроксимовані сплайнами. Для розв'язання отриманої системи звичайних диференціальних нелінійних рівнянь використовувалися методи прогнозу та корекції, а також методи Рунге-Кутта [2].

Проведено обчислювальний експеримент за період 2001 – 2016 рр., початковими даними для якого було взято дані відповідних рівнів за 2001 р. Отримані дані порівнювалися з даними статистики [4] та з даними регресивної моделі, коефіцієнти якої були визначені за допомогою методу найменших квадратів. Для деяких рівнів, наприклад, для рівня безробіття, погодженість задовільна. Найбільше розходження відмічалось для рівня забезпечення ресурсами освіти та науки. Особливої уваги потребує моделювання в період з початку 2014 року по перший квартал 2016 року, коли всі показники системних рівнів зазнали різких пікових змін.

Таким чином, розроблена математична модель може бути використана для реалізації імітаційного моделювання та прогнозування показників стану економічної безпеки країни. Запропоновано алгоритм визначення показників національної безпеки із розв'язків системи звичайних нелінійних диференціальних рівнянь. Для перевірки адекватності створеної динамічної моделі проведено порівняння зі статистичними даними та результатами розрахунків регресивної моделі.

1. Городня Т.А. Математичні методи в економічній діагностиці / Т.А. Городня, Щербак А.Ф. – Львів: Магнолія 2006, 2010. – 200 с.

2. Гетьман О.О. Економічна діагностика / О.О. Гетьман, В.М. Шаповал. – К.: Центр навчальної літератури, 2007. – 307 с.

3. Форрестер Дж. Мировая динамика / Дж. Форрестер. М.: Наука, 1978. 230 с.

4. Статистичний щорічник України за 2016 рік / За редакцією І. Є. Вернера. Київ: Державна служба статистики України. 2017. – 610 с.

**Кахович Юлія Олександрівна**
доцент Університету
митної справи та фінансів

**Кахович Олена Олександрівна**
к.н.д.у., доц., доцент кафедри
цивільно-правових дисциплін
Дніпропетровського державного
університету внутрішніх справ

## ВПЛИВ ТНК НА ФІНАНСОВУ ТА ЕКОНОМІЧНУ БЕЗПЕКУ ПІДПРИЄМСТВ УКРАЇНИ

Глобалізація поглиблює диференціацію в соціально-економічному розвитку економічних систем, зумовлюючи кардинальні зміни в їх розвитку. Вона приводить до зниження ролі кордонів, відстаней і регіонів, а з іншого боку, викликає зростання значення кожного регіону як на національному, так і на світовому рівні. Глобалізація об'єднує весь світ у відкриту систему взаємовідносин. Фінансово-економічні, суспільно-політичні, екологічні і культурні зв'язки сьогодні є потрібними і неминучими. Новітні технології які формуються на основі потреб суспільства є основою цих зв'язків.

Світова економічна система розвивалася під впливом процесів поглиблення міжнародного поділу праці, розвитку процесів міжнародної спеціалізації, кооперування й інтернаціоналізації виробництва. Вона зазнавала змін, ускладнювалася за рахунок формування нових внутрішніх структур і зв'язків. Ця система завжди мала свою ієрархію зі своїми лідерами й аутсайдерами, відбувалася лише зміна лідерів, змінювалася геополітична роль тих або інших держав, але сам ієрархічний характер зберігався. Проте світ як система не є продуктом глобалізації, його системність пов'язана із виникненням світового господарства. В системі якого діють закони міжнародної конкуренції. Результати якої вливають на національний ринок, його економіку, підприємства.

**Підприємство** – це самостійний суб'єкт господарювання, створений у порядку, встановленому законодавством, для виробництва продукції, виконання робіт і послуг з метою задоволення суспільних потреб та отримання прибутку, що залишається в нього після сплати податків та інших обов'язкових платежів.

Роль підприємства в суспільному виробництві полягає в тому, що воно забезпечує:

1) випуск товарів і послуг – вирішує: що і скільки виробляти;
2) поєднання факторів виробництва – вирішує, які фактори необхідні для виробництва продукції;
3) зв'язок між товарними і ресурсними ринками – вирішує: де брати ці фактори для виробництва продукції, де і кому продавати готову продукцію і в який спосіб (яку форму зовнішньої торгівлі обрати).

Не можна сказати, що глобалізація якимось чином змінила системну

сутність світової економіки, вона стала всього лише ще одним етапом розвитку цієї системи. В зв'язку з міжнародними відносинами про явище глобалізації заговорили активно економісти бо зафіксували, що транснаціональні корпорації досягли оборотів, які перевищують ВВП більшості держав, а крім того, вони через транснаціональну діяльність отримали можливість йти з-під національного контролю з боку державних і громадських структур окремої країни. Їх ресурси дозволили транснаціональним корпораціям (ТНК) впливати на внутрішнє становище в десятках держав, фактично обмежуючи тим самим їх суверенітет. Найбільші ТНК завищують економічну вагу щодо національних економік в чотири рази. Але навіть після внесення відповідної поправки виявляється, що по «економічної могутності» в 2010-2011рр. компанія «Wal-Mart Stores» була порівнянна з В'єтнамом, «Royal Dutch Shell» переверщувала Марокко, а «ExxonMobil» трохи відставала від Словаччини.

Таблиця. Найбільші десять ТНК зі списку Fortune Global 500 за 2017 рік

| № | **Назва** | **Країна** | **Галузь** | **Річна виручка (млн. дол., на рік)** |
|---|---|---|---|---|
| 1. | Walmart | США | Роздрібна торгівля | 485,873 |
| 2. | State Grid | Китай | Енергетика | 315,199 |
| 3. | Sinopec Group | Китай | Паливна | 267,518 |
| 4. | China National Petroleum | Китай | Паливна | 262,573 |
| 5. | Toyota Motor | Японія | Виробництво автомобілів | 254,694 |
| 6. | Volkswagen | Німеччина | Виробництво автомобілів | 240,264 |
| 7. | Royal Dutch Shell | Нідерланди | Паливна | 240,033 |
| 8. | Berkshire Hathaway | США | Страхування | 223,604 |
| 9. | Apple | США | Комп'ютерні технології | 215,639 |
| 10. | Exxon Mobil | США | Паливна | 205,004 |

*Джерело: складено за даними рейтингу Fortune Global 500.*

Нерівномірність розвитку в країнах посилюється завдяки діяльності ТНК котрі, з одного боку, зацікавлені у капіталовкладеннях у свої дочірні компанії, що базуються у більшості країн світу, а з іншого – науково-технічні винаходи, новітні технології концентрують у материнських компаніях і не імпортують у країни базування їхніх філій. Крім того, інновації стосуються не технологій, а самих продуктів та розширення ринків їхнього збуту. До основних недоліків ТНК в Україні можна віднести:

1) У багатьох випадках транснаціональні корпорації використовують українську економіку як сировинну базу, передаючи українським партнерам не відповідні їхньому рівню розвитку технології з жорсткими обмеженнями

на продаж.

2) Ведення бізнесу у видах економічної діяльності, які вигідні міжнародним компаніям, а не економіці України. Поряд з активною діяльністю ТНК у галузях зі швидким оборотом капіталу й забезпеченими ринками збуту спостерігається недостатній рівень інвестицій у інші, дуже важливі для української економіки, види економічної діяльності.

3) ТНК демонструють свою соціальну відповідальності в Україні, проте на практиці дуже часто порушуються певні права національної робочої сили, використовуються недоліки українського законодавства у сфері охорони навколишнього середовища і ін.

4) Міжнародні компанії уникають сплати податків шляхом внутрішнього переливу капіталу в країни з нижчим рівнем оподатковування. У 2012 р. Державна податкова служба Україні порушила питання щодо вирішення проблем з ухиленням податків національними та міжнародними компаніями через механізми трансферного ціноутворення.

5) Спроможність ТНК впливати на ціноутворення в країні, що призводить до поглинання або банкрутства вітчизняних виробників, а також робить залежною українську економіку від діяльності міжнародних компаній.

Глобалізацію характеризують не тільки форми зовнішньоекономічних зв'язків, а й наступні процеси, що підсилюють їх інтенсивність: технологічний прогрес; лібералізація торгівлі й інші форми економічної лібералізації; розширення сфери діяльності організацій на основі застосування нових засобів комунікацій; єдині стандарти ринкової економіки та вільної торгівлі; перехід від традиційних форм спілкування до прогресивно-технологічних комунікацій.

Глобалізація не принесла очікуваного результату країнам, що розвиваються. Якщо глобалізація не досяг успіху в скороченні бідності, то ще менш вона досягла успіху в забезпеченні стабільності. Кризи в Азії і Латинській Америці загрожували економіці і стабільності всіх країн, що розвиваються. Захід, який підштовхнув бідні країни до ліквідації торговельних бар'єрів, зберігши при цьому свої власні, перешкоджаючи експорту сільськогосподарської продукції країн, що розвиваються і тим самим позбавляючи їх такого необхідного експортного доходу. Підприємства України повинні відповідати рівню цих корпорацій. Тобто йти такими темпами, щоб не тільки наздогнати, а й опереджати. Такий темп витримають не всі. Необхідним є вироблення стратегії розвитку та захисту підприємств України, тому що глобалізація має і позитивний ефект, так для західних країн: збереження власних торгових бар'єрів; відмова відкрити свої ринки для товарів країн, що розвиваються, збереження своїх квот на безліч товарів; плюс для західних банків від ослаблення контролю над ринками капіталу в Латинській Америці та Азії.

1. Хантингтон С. Столкновение цивилизаций /С. Харингтон // Поліс. – 2004. – №1. – с. 33-48.

2. Held D. Globalization. – Cambridge: Polity. – 2007. – 304.

**Кіндзерський Юрій Вікторович**
д.е.н., ст.н.с, провідний науковий співробітник
ДУ «Інститут економіки та прогнозування
НАН України» (м. Київ)

# ІМПЕРАТИВИ ПОЛІТИКИ НЕОДУСТРІАЛІЗАЦІЇ В КОНТЕКСТІ ПІДВИЩЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Деіндустріалізація української економіки [1] стала суттєвим фактором послаблення національної безпеки країни загалом та і її окремих складових – економічної, соціальної, політичної і воєнної безпеки, – зокрема. Без подолання явища деіндустріалізації не варто сподіватися на покращення безпекових параметрів розвитку нашої держави та забезпечення її стійкості як у внутрішньому виміри, так і по відношенню до зовнішніх воєнно-політичних і кон'юнктурних викликів. Тому відродження вітчизняного промислового комплексу на сучасній технологічній і організаційні основі постає як ніколи гостро на порядок денний [2], а перехід на якісно вищий рівень розвитку промисловості має супроводжуватись переглядом промислової політики.

Ця політика повинна поєднувати у собі інструментарій як «вертикальної», так і «горизонтальної» нормативних моделей. Інструментарій «вертикальної» моделі слід використати для зміни структури виробництва, його технологічної модернізації і створення нового виробництва переважно на основі масштабних технологічних запозичень [3]. Водночас, активізація підприємницької та інноваційної діяльності суб'єктів має досягатися інструментами «горизонтальної» моделі політики. Важливою рисою вітчизняної модифікації промислової політики має стати акцент на створенні та використанні державою спеціальних інститутів розвитку для стимулювання як попиту, так і пропозиції у пріоритетних секторах.

При формуванні галузевої і технологічної структури промисловості, слід виходити із перспективної, вигідної для країни, спеціалізації у глобальному, європейському та внутрішньому вимірі, ураховуючи наявні ресурси, внутрішні і зовнішні загрози. Україна може спеціалізуватися:

– по відношенню до глобальної економіки – як виробник і постачальник якісних продуктів харчування глибокої переробки;

– у регіональному вимірі – як головний транс'європейський міжнародний транзитер у напрямах «Захід–Схід» та «Північ–Південь», провідний лікувально-оздоровчий та науково-технологічний центр Європи;

– у внутрішньому вимірі – як ефективна держава – соціальний архітектор і менеджер для власного населення.

Цільовими безпековими орієнтирами реформ у вітчизняній промисловості відповідно до пропонованої спеціалізації країни можуть виступити такі:

– мінімізація зовнішньої вразливості та нестійкості господарської системи країни, утворених внаслідок залежності економіки, з одного боку, від імпорту енергоресурсів та цін на них, з іншого – від суттєвих коливань попи-

ту на світових ринках на вітчизняний монопродуктовий експорт;

– технологічна модернізація вітчизняного виробництва та інфраструктури, створення і підтримка транспортних коридорів переважно за рахунок відновлення чи започаткування випуску власного устаткування, техніки і транспортних засобів інвестиційного та інфраструктурного призначення;

– суттєве розширення виробництва готової продукції для внутрішнього споживчого ринку, в тому числі виробництва складної технічної продукції, виробів медичного призначення та ліків, орієнтація на завоювання домінуючих позицій вітчизняного виробника на внутрішньому споживчому ринку;

– гарантування продовольчої безпеки країни і досягнення статусу світового виробника продовольства шляхом розширення і модернізації галузей переробки сільськогосподарської продукції, переважної орієнтації на виробництво готових до вживання харчових продуктів;

– забезпечення воєнної безпеки країни через модернізацію ЗСУ за рахунок відродження вітчизняного ОПК і запуску у виробництво новітніх зразків військової техніки і озброєння; утилізація застарілої техніки та боєприпасів, вирішення соціальних проблем військовослужбовців;

– забезпечення енергетичної безпеки через модернізацію та розширення мережі енергогенеруючих підприємств традиційної та альтернативної енергетики за рахунок виробництва власного енергетичного обладнання та устаткування, впровадження енергоощадних технологій виробництва.

Реструктуризація промислового виробництва має здійснюватись на основі державного стратегічного планування. Воно передбачає розробку системи довго-, середньо- та короткострокових прогнозів, визначення низки взаємопов'язаних цілей соціально-економічного і технологічного розвитку першого, другого і третього порядку, розроблення довгострокових концепцій, середньострокових програм та індикативних планів, створення інститутів організації і виконання намічених завдань, методів контролю та механізмів відповідальності за досягнення результатів.

Напрямами реформування промисловості мають стати, по-перше, оптимізація структури промислового виробництва з його переважною орієнтацією на потреби внутрішнього ринку та матеріально-технічне забезпечення зовнішньої спеціалізації країни; по-друге, ліквідація критичного зносу та інноваційно-технологічна модернізація виробництва; по-третє, інвестиційне забезпечення структурних змін і технологічної модернізації.

Тактика структурних змін має вибудовуватись із необхідності орієнтації, з одного боку, на конкретні сегменти внутрішнього і зовнішнього ринків, де вітчизняні товаровиробники мають або можуть швидко отримати конкурентні переваги, спираючись на внутрішні сприятливі умови і державну підтримку, з іншого – на кардинальне розширення власного виробництва до досягнення паритету або переважання у тих секторах внутрішнього ринку, де сьогодні переважає імпорт, здійснюючи політику активного імпортозаміщення.

При виборі галузевих пріоритетів основна увага має бути зосереджена на відновленні потенціалу вітчизняного машинобудування та легкої промисловості, диверсифікації та розширенні асортименту продукції хімічної про-

мисловості та гірничо-металургійного комплексу, їх пристосуванні до потреб внутрішнього ринку та забезпечення прийнятної для країни спеціалізації на світовому ринку.

Машинобудування має стати локомотивом розвитку усієї промисловості та забезпечення безпеки країни. Його зростання має забезпечити умови для структурної перебудови і технічного переоснащення всіх галузей економіки. Основний вектор розвитку машинобудування мають визначати:

– виробництво авіаційної та ракетно-космічної техніки, зокрема: запуск серійного виготовлення пасажирських та вантажних літаків різних класів для міжнародних перевезень, внутрішнього регіонального авіасполучення, започаткування виробництва власних вертольотів різного призначення (пасажирських, вантажних, бойових і т.п.), сучасних бойових та воєнно-транспортних літаків різних типів для військової авіації, безпілотних літальних апаратів різного призначення;

– транспортне машинобудування, зокрема виробництво транспортних засобів для автомобільних, водних та залізничних пасажирських та вантажних перевезень з огляду на перспективи забезпечення країною спеціалізації міжнародного транзитера;

– сільськогосподарське машинобудування – виготовлення складної сільськогосподарської техніки підвищеної ергономічності та економічності для обробки ґрунтів та рослин, посіву та збору врожаю, механізації у тваринництві, технологічне устаткування для меліорації земель, зберігання врожаю у сховищах, переробки сільгосппродукції та харчової промисловості;

– енергетичне машинобудування – збільшення виробництва продукції для модернізації існуючих і будівництва нових атомних, теплових та гідроелектростанцій, розширення чи започаткування випуску технологічного устаткування для виробництва електроенергії з альтернативних джерел, зокрема для вітрової, сонячної, водневої енергетики;

– верстатобудування і виробництво технологічного устаткування для модернізації основних галузей промисловості – вугільної, машинобудівної, металургійної, хімічної, фармацевтичної, легкої, деревообробної, целюлозно-паперової, будівельних матеріалів, – із підвищеними показниками ресурсо- та енергозбереження, екологічності та автоматизації технологічних процесів.

– «екологічне» машинобудування – спеціальні машини і устаткування для очистки ґрунтів, стічних промислових та побутових вод, повітря, роздільної переробки та утилізації промислових відходів, побутового сміття, старих предметів вжитку (побутової техніки, автомобілів, одягу і т.п.); системи контролю за рівнем забруднення навколишнього природного середовища;

– приладобудування – прилади контролю, вимірювання і регулювання для систем транспорту і зв'язку, управління технологічними процесами і роботизованими комплексами, створення джерел світла на основі нових матеріалів, удосконалення керуючих електронних систем авіаційної, корабельної, залізничної та автомобільної техніки, розвитку навігаційних систем. Значна увага має бути приділена виготовленню медичного діагностичного і лікувального обладнання та апаратури.

*Оборонно-промисловий комплекс* повинен мати пріоритет у державній підтримці та розвиватися за такими напрямами, як:

– терміновий (у короткостроковій перспективі) запуск виробництва боєприпасів різних типів для Збройних сил України, ураховуючи високу ймовірність тривалого військового протистояння з РФ; якнайскоріша розробка та запуск у виробництво нової та модернізація існуючої військової техніки та озброєння;

– виробництво військової техніки та озброєння на експорт;

– утилізація військової техніки та боєприпасів з вичерпаним строком експлуатації, що не можуть бути залучені для потреб оборони.

Використання державних холдингових компаній і державного замовлення має стати ключовим елементом державного стимулювання випереджаючого розвитку виробництва продукції переробних галузей, насамперед наукомістких і високотехнологічних виробництв, які замикають на собі міжгалузеві технологічні ланцюги й можуть розглядатись як «точки зростання». Великі інтегровані структури у пріоритетних високотехнологічних секторах сприятимуть підвищенню стійкості вітчизняних підприємств в умовах загострення міжнародної конкуренції. При цьому окремим способом консолідації за стимулюючої ролі держави може бути викуп останньою частини акцій підприємств у обсягах, які дозволяють контролювати або блокувати їх діяльність з подальшим створенням на базі цих підприємств інтегрованих корпоративних об’єднань зі змішаною (державно-приватною) або державною формою власності.

Формування ємких ринків на продукцію створених за участю держави інтегрованих компаній може відбутись як мінімум у два способи. По-перше шляхом штучного створення нових ринків через застосування державного замовлення на певні види продукції. По-друге, введенням захисних заходів для доступу на внутрішній ринок аналогічних іноземних товарів через квотування їх обсягів або застосування до них протекціоністських імпортних мит. Слід відзначити, що обмеження імпорту може супроводжуватись вимогами держави до іноземних компаній щодо розміщення виробництв з виготовлення відповідної продукції у середині країни шляхом створення своїх дочірніх компаній, не виключаючи при цьому можливості участі держави у формуванні їх капіталу.

Державне замовлення доцільно застосувати для створення ринків авіаційної, суднобудівної, вагонобудівної, фармацевтичної промисловості, медичного приладобудування, енергетичного машинобудування, автомобілебудування (у таких сегментах як міський комунальний транспорт, комунальна техніка), виробництва сільськогосподарської техніки, оборонно-промислового комплексу. Саме в цих галузях також можуть бути створені згадані державні корпоративні об’єднання. Їх формування є доцільним принаймні на перших порах становлення потужного корпоративного сектору, оскільки вони вирізняються високим ступенем концентрації і технологічної інтеграції своїх виробництв, а тому здатні забезпечити бажані структурні зміни в промисловості. Присутність державного капіталу в таких об’єднаннях має визначатись

особливістю ринків, на яких вони діють, а також з огляду на доцільність формування з них своєрідного структурно-виробничого каркасу економіки, який підвищуватиме її стійкість до зовнішніх деструктивних впливів.

Технологічна модернізація промисловості неможлива без суттєвої активізації інноваційної діяльності її суб'єктів. Першочерговими мають стати заходи щодо надійного законодавчого захисту прав власності, що унеможливить її рейдерське захоплення, дозволить зменшити ризики інноваційної діяльності та стимулює суб'єктів до пошуку можливостей власного розвитку на основі фактора інновацій. Слід забезпечити формування повноцінної цілісної національної інноваційної системи; переглянути підходи до формування структури досліджень і розробок у промисловості; здійснювати надання державного фінансування на прикладні розробки на умовах державного замовлення та їх обов'язкового подальшого впровадження; запровадити економічні, насамперед податкові, стимули для інноваційної діяльності суб'єктів і впровадження інновацій у виробництво; створити умови для інтеграції державних наукових установ із виробничими структурами, об'єднаних спільним ринком, з подальшим утворенням науково-виробничих комплексів і застосуванням державного замовлення на їх продукцію.

Проведення структурно-технологічної модернізації виробництва неможливе без зростання інвестиційної активності суб'єктів. Тому напрямами інвестиційної політики мають стати такі, як: створення умов для зростання обсягів власних коштів підприємств та їх використання на інвестиційні цілі через запровадження інвестиційних податкових кредитів, пільг і премій; розширення обсягів державного інвестування пріоритетних сфер; створення грошово-кредитного механізму довгострокового інвестиційного кредитування у вигляді цільового рефінансування Національним банком України спеціально визначених комерційних банків під розширення пропозиції «довгих» грошей для реалізації інвестиційних програм і проектів; створення механізму міжгалузевого перетікання капіталу із сировинних і низько технологічних секторів у переробні високотехнологічні, що належать до пріоритетних.

Успіх розбудови вітчизняної промисловості неможливий без кардинального підвищення якості державного управління, запровадження механізмів персональної відповідальності урядовців за виконання намічених цільових показників розвитку, відокремлення функцій держави як суб'єкта економічної політики і як власника. Функції регулятора необхідно залишити за виконавчою владою, а функції власника зосередити у приналежних державі корпоративних об'єднаннях, які стануть основою формування прогресивної структури виробництва і суттєвого підвищення рівня національної безпеки України.

1. Кіндзерський Ю. Деіндустріалізація та її детермінанти у світі та в Україні / Ю. Кіндзерський // Економіка України. – 2017. – № 11. – С. 48–72.

2. Національна модель неоіндустріального розвитку України : моногр. / ред. В.П. Вишневський; НАН України, Ін-т екон. пром-сті. – Київ, 2016. – 519 с.

3. Полтерович В. Стратегии модернизации, институты и коалиции / В. Полтерович // Вопросы экономики. – 2008. – № 4. – С. 4–24.

**Кіріленко Федір Олександрович**
к.ю.н., заступник начальника управління
медіакомунікацій Міністра Департаменту
організаційно-апаратної роботи
Міністерства внутрішніх справ України

## ПЛАТФОРМИ ДЛЯ ОНЛАЙН-НАВЧАННЯ

На сьогоднішній день вимоги до вмінь і знань сучасної людини дуже високі. Окрім того, що працівник кожен день виконує свою роботу, йому ще потрібно постійно бути «в тренді» і розвиватися – проходити навчання на курсах підвищення кваліфікації, шукати нові методики, відвідувати різні заходи тощо. Все це потребує багато затрат як часу, так і матеріальних витрат. За допомогою платформ масових відкритих онлайн-курсів Massive open online course (далі – МООС) тепер все це можна робити не виходячи з дому та набагато швидше.

Платформи МООС – це електронні ресурси, які дозволяють покращити рівень знань, пропонують вдосконалити навички та слугують прекрасним помічником для саморозвитку. Вони дають можливість прослухати велику кількість курсів найкращих університетів світу.

Приємним бонусом до навчання може бути отримання сертифіката про проходження курсу або, у разі досягнення учнем високих результатів – сертифікат про завершення навчання. Такі сертифікати є хорошим доказом володіння необхідними навичками, і багато людей почали вказувати в своїх резюме інформацію про наявність сертифікатів з освітніх платформ. Ще однією приємною особливістю є те, що курси проходять в сучасній формі онлайн-навчання, при якому надається максимально гнучкий графік без відриву від роботи.

Проте, при всіх перевагах МООС існує і ряд недоліків, адже люди прагнуть не просто отримати інформацію щодо певної теми, а бажають оволодіти відповідними навичками чи знаннями.

На жаль МООС має певну обмеженість, а саме:

у завданнях, які можна надавати студентам (надаються лише ті завдання, що можуть бути формалізованими та перевірятися автоматично);

обмеження при здійсненні зворотного зв’язку (оскільки професори не можуть відповідати кожному студентові, частково завдання перекидається на співтовариства і на рейтингові алгоритми, які дозволяють виявляти найбільш компетентні відповіді, що в жодному разі не можна порівняти з очним спілкуванням);

має проблеми при сертифікації (неможливо перевірити чи дійсно за комп’ютером під час іспиту знаходиться та ж людина, яка проходила відповідний курс та неможливо перевірити чи відповідає студент сам або консультується з іншими. Усе це призводить до розподілення функцій навчання і сертифікації. Роль сертифікації та іспитів в онлайн-курсах все більше зво-

диться виключно до функції перевірки людиною своїх знань, тоді як завдання сертифікації поступово переносяться на незалежні сертифікаційні центри, які іспитують студентів, позбавляючи можливості видати себе за іншого або списати.

Не зважаючи на недоліки, МООС все більше і більше набувають популярності. Отже, пропонуємо короткий огляд найпопулярніших освітянських порталів з усього світу.

**Khan Academy.** Свого часу педагог Салман Хан вирішив створити ресурс, який дозволятиме людям з усього світу займатися самоосвітою, не виходячи з власного будинку. Таким чином, у 2006 році в Інтернеті народився проект Khan Academy, що розпочав новий етап та шалений розвиток освіти в сучасному світі.

Організація поставила собі за мету надати безкоштовний доступ до освітніх матеріалів людям, які мають бажання вчитися, але з якоїсь причини не можуть відвідувати освітні заклади. Khan Academy пропонує онлайн курси та лекції у форматі YouTube відео. Окрім мікролекцій, веб-сторінка організації має практичні заняття та методичні матеріали для педагогів – тож самоосвіта вчителя теж ніким не забута.

Всі матеріали, курси та лекції знаходяться у вільному безкоштовному доступі для будь-якої людини на планеті, яка має можливість користуватися Інтернетом.

Онлайн лекції перекладено на 65 мов, пріоритетну мову користування платформою користувач можете обрати з 7 варіантів, а деякі ресурси проекту перекладені і на українську мову. Навчання тут – безкоштовне, за виключенням можливості добровільно внести пожертву.

**EDX.** В ТРАВНІ 2012 РОКУ НАУКОВЦЯМИ ГАРВАРДСЬКОГО УНІВЕРСИТЕТУ ТА МАССАЧУСЕТСЬКОГО ТЕХНОЛОГІЧНОГО ІНСТИТУТУ БУЛА ЗАСНОВАНА ПЛАТФОРМА МАСОВИХ ВІДКРИТИХ ІНТЕРНЕТ КУРСІВ EDX.

У 2013 році організація розпочала партнерство зі Стенфордом, і в червні 2013 року кількість слухачів edX дійшла до позначки в 1 млн. студентів.

Наразі в світі нараховується 53 школи та некомерційні організації, які запропонували чи мають в своїх намірах запропонувати власні курси на ресурсі edX. Нині платформа налічує більше двох з половиною мільйонів користувачів, які мають доступ до двох сотень курсів в Інтернеті на різноманітну тематику: від біохімії до дизайну та мистецтва.

В цілому, навчання на платформі абсолютно безкоштовне з правом отримати сертифікат. Втім, існує можливість зробити волонтерський внесок за навчання на кожному курсі та по його завершенню слухачу буде видано спеціальний сертифікат, який має свої незначні привілеї.

Вміст платформи перекладений на чотири мови, української серед них, на жаль, немає.

**COURSERA.** РОЗПОЧАЛА СВОЮ ДІЯЛЬНІСТЬ У КВІТНІ 2012 РОКУ. ПЕРШІ УНІВЕРСИТЕТИ, ЩО ПОГОДИЛИСЯ НАДАТИ СВОЇ НАУКОВІ МАТЕРІАЛИ – ВИШІ СТЕНФОРДА, ПРИНСТОНА, МІЧИГАНСЬ-

КИЙ ТА ПЕНСИЛЬВАНСЬКИЙ УНІВЕРСИТЕТИ, ПРОТЕ ВЖЕ З 23 ЖОВТНЯ 2013 РОКУ ОНЛАЙН ОСВІТА З COURSERA – ЦЕ СПІВПРАЦЯ ІЗ 107 ВИШАМИ ТА ІНШИМИ УСТАНОВАМИ.

Як і попередні освітні платформи, Coursera пропонує повністю безкоштовні онлайн курси, проте, щоб отримати верифікований сертифікат, необхідно заплатити 30-40 доларів. Втім, при сильному бажанні, якщо студент зможе довести адміністрації наявність у нього фінансових труднощів або обов'язковість отримання такого сертифікату, Coursera може піти на поступки.

Щотижня студент, підписаний на той чи інший курс, отримує відео лекції та домашні завдання. Їх виконання обов'язкове, для отримання сертифікату про закінчення курсу. Особливістю оцінювання знань і, напевно, одним із найбільших мінусів проекту є той факт, що домашні завдання оцінюють інші студенти. Вони ставлять бали за роботу, а підсумковий результат дорівнюватиме середньому арифметичному всіх поставлених ними оцінок.

Сертифікат про завершення курсу можна отримати, набравши мінімально необхідний загальний бал, встановлений викладачем. Крім того, є можливість отримати сертифікат з відзнакою, в разі, якщо студент покаже високий рівень знань.

Як і в Khan Academy, основну мову користування можна обрати з семи запропонованих. Деякі матеріали перекладені і на українську мову.

**Canvas Network.** Проект відрізняється великою різноманітністю курсів, які проводять абсолютно різні за рівнем підготовки та напрямком діяльності люди: доктори наук, менеджери, письменники. Курси не мають єдиного підходу до викладання. Матеріал можуть пояснювати виключно в коротких відеолекціях, доповнювати можливістю обговорювати прослуханий матеріал на форумі з викладачем та іншими студентами, сертифікат по закінченні курсу можуть видавати чи ні. Особливості конкретного курсу містяться в описі. Крім вищевказаного документа в прев'ю можна дізнатися, для кого розроблена ця програма (доступна для всіх, орієнтована виключно на професіоналів в тій чи іншій галузі). Курси можуть мати вікові обмеження.

Canvas Network пропонує безкоштовні, умовно безкоштовні й платні курси. Умовно безкоштовні передбачають придбання додаткових навчальних матеріалів (посібників, літератури), платні дозволяють заробити кредити в системі безперервної освіти (актуально для професій, де необхідно постійно підтверджувати свою кваліфікацію - вчителів, архітекторів, медичних працівників і т. д.).

Курси тривають 2-3 тижні, анонсуються за місяць і раніше, що дозволяє бажаючим попередньо записатися на них. Оскільки кількість місць на курсі обмежена, в цікавих класах краще реєструватися якомога раніше.

**Udemy.** Сайт MOOC-платформи «Udemy» має російськомовну версію, що робить навігацію по порталу максимально комфортною. Освітні проекти розбиті на шістнадцять категорій, серед яких є комп'ютерні, гуманітарні дисципліни, а також рукоділля, мистецтво і фотозйомка.

Всі матеріали на сайті платні, вартість може варіювати від 10 до 500 доларів. Отримати знижку можна, скориставшись купоном.

Після закінчення курсів студенти отримують сертифікат. Деякі курси пропонують унікальну можливість підтвердити свої знання в спеціальному центрі і отримати сертифікат, завірений великими компаніями - Cisco Systems, Microsoft Corporation, Financial Industry Regulatory Authority та ін.

Компанії і професіонали можуть створювати і продавати на платформі «Udemy» власні курси (середній заробіток лектора може становити близько $ 7000 на рік).

Окрім світових платформ для навчання, останнім часом стали популярними вітчизняні онлайн-платформи, такі як ВУМ, Prometheus, Educational Era.

**ВУМ.** Відкритий університет Майдану розпочав свою роботу як цикл лекцій для людей, які протестували під час Революції Гідності, і з того часу став інтернет-платформою для поширення ідей та розвитку громадянського суспільства.

Онлайн-проект пропонує більше ніж 30 тем для безкоштовного навчання. Курси сформовані з відеолекцій, практичних завдань та контрольних запитань. Наявність форуму надає можливість спілкуватись з іншими студентами та викладачами.

Лекції читають провідні викладачі бізнес-шкіл, громадянського сектору, практики з бізнесу та соціальної сфери, а тому онлайн-курси пов’язані з такими напрямами як персональний розвиток, реалізація потенціалу, підприємництво, формування відкритого суспільства в Україні.

За умови успішного проходження обраного курсу, можна завантажити сертифікат.

**Prometheus.** 15 жовтня 2014 року Іван Примаченко разом зі своєї командою волонтерів запустив проект Prometheus.

«Prometheus» – громадський проект масових відкритих онлайн-курсів. У співпраці з викладачами кращих ВНЗ України команда створює та розміщує МООС на власній онлайн-платформі та надає безкоштовну можливість університетам, організаціям та провідним компаніям публікувати та розповсюджувати курси на цій платформі. А також відкрито безкоштовний онлайн-доступ до найкращих навчальних курсів університетського рівня всім охочим в Україні.

Навчання на порталі абсолютно безкоштовне, складається з перегляду відео лекцій, виконання домашніх завдань, та складання іспитів. Для отримання електронного сертифікату, студенту необхідно набрати необхідний мінімум балів по проходженню того чи іншого курсу. Якщо ж студент готовий здійснити благодійний внесок, Prometheus може запропонувати отримати верифікований сертифікат.

Одним з недоліків порталу можна назвати те, що деякі курси не передбачають отримання безкоштовних сертифікатів.

**Educational Era.** Український освітній проект, що створює повноцінні онлайн-курси у форматі МООС та відповідні матеріали широкого профілю. Команда проекту у зв’язці з викладачем розробляє увесь контент самостійно та розміщує курси на своїй онлайн-платформі.

Проект включає в себе: інтерактивні лекції, високоякісні конспекти, іспити та домашні завдання.

Щотижневі домашні завдання мають deadline – час, до якого потрібно встигнути їх зробити. Також в середині й наприкінці курсу учень повинен скласти іспити. Це може бути тест або проектна робота. Всі результати потрапляють на динамічну сторінку прогресу учня, де формується остаточна оцінка. Щоб отримати сертифікат про успішне проходження курсу, ця оцінка повинна бути вище встановленої межі.

Весь навчальний процес доступний онлайн 24/7. Вчитися можна вдома, в кафе, бібліотеці або вільних просторах. Все, що потрібно, - це інтернет.

Проблемні завдання можна обговорювати з іншими учнями і педагогами, після чого матеріал може доповнюватися в залежності від ваших потреб.

**Онлайн-курс для працівників сервісних центрів МВС.** У рамках співпраці з Консультативною місією ЄС розроблено навчальний онлайн-курс для 150 працівників фронт-офісу центрів, щодо покращення якості послуг та спілкування з клієнтами. Онлайн-курс був розроблений професійною командою компанії Basic Group.

Онлайн-курс – веб-портал для навчання працівників сервісних центрів МВС.

Курс включає в себе матеріали з основних напрямів роботи СЦ МВС, протидії корупції, професійної етики та ефективної комунікації.

Навчальні матеріали подані у вигляді презентацій, текстових файлів, відеофайлів та ілюстрацій.

Рівень знань перевіряється шляхом складання тестів після кожного модуля.

Безумовно, онлайн освіти не вистачить для того, щоб стати повноцінним спеціалістом у тій чи іншій галузі. Але вищеперераховані портали можуть виявитись прекрасними помічниками для загального розвитку.

1. http://tvoemisto.tv/news/7_onlaynplatform_dlya_dystantsiynogo_navchannya_67484.html
2. https://vumonline.ua/
3. https://prometheus.org.ua/
4. https://www.ed-era.com/

**Козлова Анастасія Олександрівна**
к.е.н.,
*(Харківський національний університет міського господарства ім. О.М. Бекетова)*

# КОМПЛЕКСНА СИСТЕМА ЕКОНОМІЧНОЇ БЕЗПЕКИ ЯК ШЛЯХ ПОДОЛАННЯ ЗАГРОЗ УСТАНОВАМ ТУРИСТИЧНОЇ ГАЛУЗІ В СУЧАСНИХ УМОВАХ ЄВРОІНТЕГРАЦІЇ КРАЇНИ

Незважаючи на кризові явища та складну соціально-економічну ситуацію Україна, як одна із найбільших європейських країн європейського континенту, впевнено встала на шлях євроінтеграції. Перевагами євроінтеграції є доступ до великого внутрішнього ринку товарів та послуг Євросоюзу, зростання обсягів інвестицій, удосконалення методів управління та збільшення трансферів для поліпшення інфраструктури, що дуже важливо для майбутнього нашої країни.

Однією з небагатьох галузей економіки України, яка виходить з кризи є туристична галузь. З одного боку динаміка зростання обсягів надання туристичних послуг безпосередньо залежить від зростання рівня життя населення країни, зростання економічних показників і т.ін. З другого, як це не парадоксально, певним позитивним чином на зростання обсягів надання туристичних послуг вплинули події пов'язані із анексією Криму та проведення АТО на сході країни. Тимчасова втрата традиційних туристичних ринків в Криму та певне обмеження туристичних можливостей в районі Азовського моря, призвела до переорієнтування туристичних потоків на західний напрямок країни, в Одеський регіон та збільшення обсягів надання послуг на іноземних напрямках. Запровадження лібералізації візової процедури та процесу пересування країнами не тільки Європейського союзу, а й іншими країнами світу теж позитивно вплинули на розвиток туристичного сектору. Втомленість активної частини населення від обстановки напруги в очікуванні настання негативних наслідків із-за агресії та військових дій на окремих територіях держави, відмова на протязі декількох років від відпочинку та інші морально-психологічні чинники також вплинули на зростання попиту щодо туристичного продукту.

При цьому фінансово-економічна нестабільність та погіршення криміногенної обстановки в країні підштовхнуло споживачів туристичних послуг стати більш вимогливими до питань безпеки. Але, вітчизняні туристичні установи повинні враховувати ризики, які підсилюються не тільки внутрішніми загрозами, а й зовнішніми та більше уваги приділяти економічній та власній безпеці клієнтів.

Економічна безпека в умовах активізації вказаних процесів та прискорення процесів євроінтеграції на даний час є пріоритетним завданням. Як слідство невирішеність проблем у цій сфері не дозволяє забезпечити відповідний рівень і власної безпеки туристів, їх майна, капіталів тощо.

Більшість науковців та фахівців визначають сьогодні економічну безпеку як такий стан національної економіки, який забезпечує стабільне функціонування виробництва, кредитно-фінансової і банківської системи, транспортної інфраструктури, задовольняє матеріальні потреби держави, суспільства і особи, здійснює їх захист від зовнішніх та внутрішніх загроз. До цього слід додати, що сталий та безпечний розвиток національної економіки забезпечують конкретні суб'єкти господарчої діяльності, а саме підприємства, організації, установи. Від їх стабільної діяльності залежить функціонування національної економіки в цілому.

Туристичні установи не тільки надають послуги в середині країни, а й за кордоном держави, дуже чутливо реагують на світові чинники, серед яких коливання курсу валют, конфлікти та техногенні події в туристичних регіонах певних країн, зміни політичного та економічного курсів, релігійні чинники, тощо. Тобто туристичні установи найбільше підвернені впливу як внутрішніх так і зовнішніх загроз, з якими самотужки впоратися вони невзмозі. Для цього і існує держава, яка повинна забезпечити умови для їх стабільної, і насамперед, безпечної роботи.

В той же час, очікувати що держава повністю виконає роботу із забезпечення економічної безпеки суб'єктів господарювання є невірним розумінням. Для того, щоб активно протидіяти сучасним загрозам і ризикам в економічній сфері необхідно створити власні систем безпеки на рівні установ та підприємств. При цьому система економічної безпеки підприємства чи установи повинна носити комплексний системний характер. Нажаль у більшості туристичних установ комплексного підходу до створення власної системи безпеки взагалі не було, а вирішення питань безпеки було зведене до інструктажів туристів, вирішення питань страхування та надання консультацій у разі виникнення форс-мажорних обставин.

Комплексна система економічної безпеки підприємства чи установи – це сукупність взаємозв'язаних організаційних, правових та матеріально – технічних заходів, спрямованих на захист підприємства чи установи від реальних і потенційних загроз та ризиків, які можуть призвести до значних економічних втрат, чи затримати розвиток підприємства чи установи. Комплексна система економічної безпеки буде ефективно працювати тільки в тому випадку, якщо будуть задіяні всі можливості підприємства чи установи для протидії реальним і потенційним небезпекам, загрози і ризикам, а самі власники та співробітники будуть розуміти всю важливість питань безпеки.

Система безпеки підприємства складається наступних складових:

- захист комерційної таємниці та конфіденційної інформації;
- комп'ютерна безпека;
- внутрішня безпека;
- безпека будівель і споруд;
- фізична безпека;
- технічна безпека;
- безпека зв'язку;
- безпека господарсько-договірної діяльності;

- безпека рекламних, культурних, масових заходів, ділових зустрічей і переговорів;
- протипожежна безпека;
- екологічна безпека та радіаційно-хімічна безпека;
- інформаційно-аналітична робота;
- експертна перевірка механізму системи безпеки.

Даний перелік може доповнюватися у разі виникнення нових форм ризиків чи форс-мажорних обставин.

Ще одним шляхом посилення комплексної системи безпеки підприємств та установ є запровадження вже існуючих світових та європейських безпекових стандартів та досвіду їх реалізації в сучасних умовах та з адаптованих до специфіки країни та менталітету населення.

Підсумовуючи вищевикладене можна дійти висновку, що успішна діяльність та розвиток підприємств, як основної туристичної ланки, в значній мірі залежить від ефективності діяльності їх власних систем економічної безпеки. Завданням держави є виявлення внутрішніх та зовнішніх, визначення рівня їх небезпеки, реалізації адекватних заходів щодо запобігання та усунення цих загроз, а також негативних наслідків їхнього впливу.

**Кокарєв Іван Васильович**
к.е.н., доц., доцент кафедри
економічної та інформаційної безпеки

**Тютченко Світлана Миколаївна**
здобувач Дніпропетровського
державного університету
внутрішніх справ

## ФІНАНСОВА БЕЗПЕКА РЕГІОНУ ЯК СКЛАДОВИЙ ЕЛЕМЕНТ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Зростання економічного потенціалу та ефективне функціонування будь-якого підприємства і регіону в цілому значною мірою залежить від створення надійної системи економічної безпеки на різних рівнях. Економічна безпека-це універсальна категорія, що відображає захищеність суб`єктів соціально-економічних відносин на всіх рівнях, починаючи з держави і закінчуючи кожним її громадянином [1, с. 19 ].

Для досягнення економічної безпеки на рівні держави, необхідна підтримка відповідного стану захищеності на рівні регіону, міста, окремих підприємств. Регіональний рівень є ланкою, яка зв`язує між собою державу і суб`єкти господарювання. Кожен регіон має свої особливості в забезпеченні фінансування економічних і соціальних програм розвитку, що є основою для створення системи економічної безпеки регіонів.

На сучасному етапі всесвітньої глобалізації та інтеграції у розвитку

України ключове значення набувають питання регіональної безпеки, пов`язані з ідеєю національної єдності, розвитку і вдосконалення соціальних відносин, реалізації проблеми забезпечення прав і свобод громадян та підвищення рівня правової свідомості. Аналіз соціально-економічної ситуації доводить, що причини багатьох загроз економічній безпеці закладені на регіональному рівні [1, с. 26].

Сутність економічної безпеки регіону полягає в можливості і здатності його економіки поетапно покращувати якість життя населення на рівні загальноприйнятих стандартів, протистояти впливу внутрішніх і зовнішніх загроз при оптимальних витратах всіх видів ресурсів і невиснажливого використання природних факторів , забезпечувати соціально-економічну та суспільно-політичну стабільність регіону.

Фінансова безпека держави є досить складним економічним явищем через свою містку структуру. Така структура включає ряд підсистемних елементів, які саме і визначають її поточний стан. Невідповідність одного зі складових системи до критеріального значення може негативно впливати як на інший елемент системи, так і на всю фінансову безпеку держави в цілому. Фінансова безпека держави за вертикальним рівнем управління включає оцінку окремих показників фінансової безпеки держави, регіону, підприємства та громадянина. За горизонтальним рівнем вона включає сукупність безпеки, поточний рівень якої визначається за допомогою певного переліку критеріїв, що мають граничні значення. Визначення рівня фінансової безпеки держави залежить від належної оцінки існуючого рівня фінансової безпеки регіонів [2,с.12].

Фінансовий розвиток регіону характеризується рівнем стабільності державного фінансування, веденням підприємницької діяльності, інвестиційним кліматом, рівнем життя населення, розвитком банківського сектору (рис. 1).

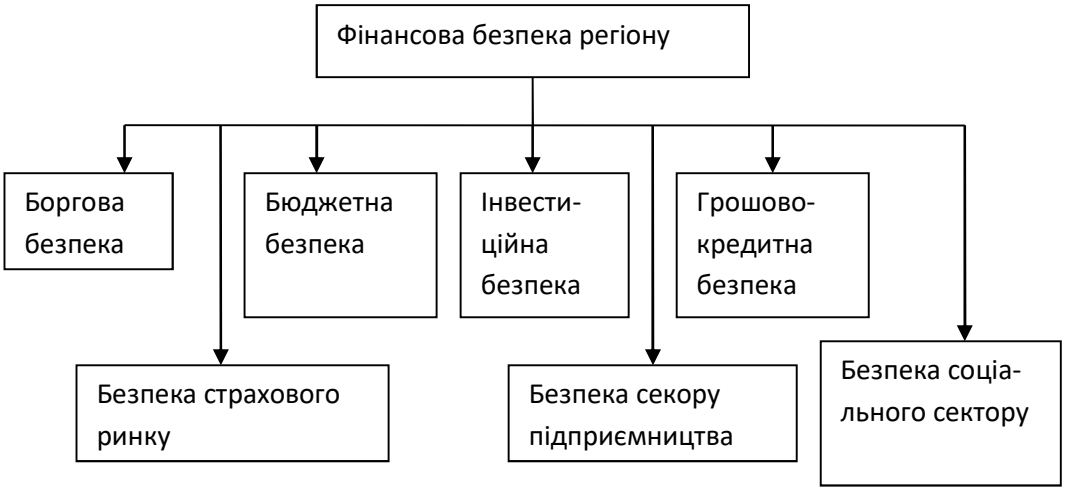



*Рис.1. Складові фінансової системи безпеки регіону [1, с. 24]*

Система показників, що представлена в табл.1, на наш погляд, забезпечить належне оцінювання рівня фінансової безпеки регіону.

Основними загрозами фінансової безпеки регіонів України є наступні:

- дестабілізація фінансового сектору економіки;
- нестача та неефективність використання фінансових ресурсів;
- зростання внутрішнього та зовнішнього боргу держави;
- високий рівень інфляції;
- нестабільний курс національної валюти;
- нерівномірність розміщення виробництв;
- зростання рівня тіньового сектору та корупції;
- воєнні дії та зростання соціальної напруженості в державі.

Подолання таких загроз не є компетенціями органів влади окремого регіону. Тому можна стверджувати, що основним джерелом виникнення загроз є макрорівень. Нажаль, сьогодні державні органи не виконують в повному обсязі свої повноваження щодо забезпечення належного рівня фінансової безпеки регіону, що і викликає за ланцюговим зв'язком поширення небезпеки на інші рівні забезпечення фінансової безпеки.

Таблиця 1

Система показників оцінки фінансової безпеки регіону [1, с. 25]

| Сектор безпеки | № | Показник | Значення, % |
|---|---|---|---|
| Боргова безпека | 1 | Рівень боргу регіону та гарантованого боргу до валового регіонального продукту (ВРП) | <20 |
| | 2 | Рівень зовнішнього боргу регіону до ВРП | <10 |
| | 3 | Обсяг внутрішнього боргу регіону до ВРП | <20 |
| Бюджетна безпека | 4 | Темп зміни ВРП | >100 |
| | 5 | Частка ВРП у ВВП держави | >5 |
| | 6 | Частка доходів місцевих бюджетів у загальнодержавних доходах | >3 |
| | 7 | Частка доходів місцевого бюджету до ВРП | >25 |
| | 8 | Рівень забезпечення видатків доходами | >100 |
| | 9 | Дефіцит (профіцит) бюджету до ВРП | <5 (>3;<5) |
| Інвестиційна безпека | 10 | Темпи зміни прямих іноземних інвестицій у регіон | >100 |
| | 11 | Частка прямих іноземних інвестиції до ВРП | >15 |
| | 12 | Темп зміни інвестицій в основний капітал | >100 |

| | | | |
|---|---|---|---|
| Безпека соціального сектору | 13 | Темп зміни суми заборгованості з виплати заробітної плати | <105 |
| | 14 | Індекс споживчих цін у регіоні | <110 |
| | 15 | Співвідношення витрат до доходів населення | <80 |
| Безпека сектору підприємництва | 16 | Співвідношення сальдо фінансових результатів підприємств до ВРП | >7 |
| | 17 | Рентабельність операційної діяльності підприємств | >10 |
| | 18 | Темпи зміни обсягів промислової продукції в регіоні | >100 |
| Банківська безпека | 19 | Співвідношення кредитів до депозитів банків в регіоні | <100 |

Фінансова безпека регіону є складовим елементом фінансової безпеки держави і займає важливе місце в її структурі. Зведення показників оцінки фінансової безпеки регіонів у комплексну систему надає змогу не тільки оцінити стан фінансової безпеки держави, але і охарактеризувати первинне джерело виникнення ризику порушення фінансової безпеки країни. Підвищення рівня фінансової безпеки кожного регіону надасть змогу забезпечити фінансову стабільність, незалежність від міжбюджетних трансфертів, стимулювання власного виробництва, підвищення рівня життя в регіоні. Забезпечення належного стану фінансової безпеки регіонів є одним із важливих етапів створення сильної та стабільної фінансової безпеки України .

Підвищення безпеки регіону залежить від ступеня державної підтримки й розробки державних програм регіонального розвитку. Особливу роль відіграє паритетна участь центру в значних регіональних інвестиційних проектах та у створенні сприятливого клімату для розвитку економічного середовища в регіоні. З метою забезпечення економічної безпеки територій, економічна регіональна політика держави повинна вирішити подвійне завдання. З одного боку, вона має сприяти розвитку інтеграційних процесів, направлених на зміцнення державності, а з іншого, – забезпечувати регіональну самостійність і належний рівень економічної безпеки регіонів [3]. Існування економічної безпеки регіону неможливе без створення внутрішнього імунітету та зовнішньої захищеності від дистабілізаційних впливів, без конкурентоздатності на світових ринках і стійкості фінансового становища.

1. Криленко В. І. Економічна безпека регіону як складова забезпечення національної економічної безпеки [Текст] / В. І. Криленко // Ефективна економіка. – 2013. – № 2. – С. 17–28.

2. Моделювання економічної безпеки : держава, регіон, підприємство [Текст] : монографія /[В. М. Геєць, М. О. Кизим, Т. С. Клебанова та ін.] ; за ред. В. М. Гейця. – Х. : ІНЖЕК, 2015. – 240 с.

3. Оцінювання конкурентоспроможності регіонів України [Електронний ресурс]. – Режим доступу : http://www.competitiveukraine.org /upload/reports/rozdil5_ukr.pdf

**Колісник Тетяна Петрівна**
к.пед.н., доц., доцент кафедри
інформаційних технологій

**Тулупов Володимир Володимирович**
к.т.н., доц., доцент кафедри
інформаційних технологій
Харківського національного
університету внутрішніх справ

# ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА РОБОТА З БАЗАМИ ДАНИХ ПІД ЧАС ПАТРУЛЮВАННЯ

Післядипломна освіта працівників поліції здійснюється відповідно до Конституції України, законів України, указів Президента України та постанов Верховної Ради України, прийнятих відповідно до Конституції та законів України, актів Кабінету Міністрів України, інших актів законодавства України та Положення про організацію післядипломної освіти працівників Національної поліції. Метою післядипломної освіти є задоволення індивідуальних потреб працівників поліції в особистому професійному зростанні, забезпечення потреб держави у кваліфікованих кадрах високого рівня професіоналізму та культури, здатних компетентно і відповідально виконувати свої функції. Основними завданнями післядипломної освіти є:

- навчання необхідним знанням і спеціальним навичкам для успішного виконання обов'язків із забезпечення публічної безпеки і порядку, охорони прав і свобод людини, а також інтересів суспільства і держави, протидії злочинності та інших службових завдань;
- удосконалення навичок управлінської діяльності, опанування методик навчання та виховання підлеглих, упровадження в практичну діяльність досягнень науки, передових форм і методів роботи, основ наукової організації праці;
- формування професійної самосвідомості працівників поліції, почуття відповідальності за свої дії, розуміння необхідності постійного вдосконалення своєї професійної майстерності з урахуванням специфіки діяльності в конкретних підрозділах поліції;
- навчання прийомам та засобам забезпечення особистої безпеки при виконанні службових обов'язків, під час надзвичайних подій і в екстремальних умовах;
- удосконалення навиків працівників поліції поводження з вогнепальною зброєю, спеціальними засобами і спеціальною технікою, експлуатації транспортних засобів, засобів зв'язку;
- формування високої психологічної стійкості працівників поліції, розвиток у них спостережливості, пильності, пам'яті, мислення та інших професійно-психологічних якостей і навичок.

Зміст післядипломної освіти визначається відповідними планами і про-

грамами з урахуванням сучасних вимог до засобів, форм і методів професійної діяльності [1].

Навчальна дисципліна «Інформаційні технології та робота з базами даних під час патрулювання» є варіативною частиною типового навчально-тематичного плану спеціалізації (перепідготовки) патрульних поліцейських, що здійснюється у Харківському національному університеті внутрішніх справ. Предметом дисципліни «Інформаційні технології та робота з базами даних під час патрулювання» є теорія і практика використання сучасних інформаційних технологій у діяльності патрульної поліції.

Патрульні поліцейські отримують інформацію про систему централізованого управління нарядами поліції «ЦУНАМІ»; навички налаштування планшетного комп'ютера; вміння здійснювати реєстрацію у системі «Цунамі» перед початком патрулювання, проводити процедуру перезміни наряду, проводити необхідні дії на планшетному комп'ютері патрульного у разі отримання завдання від чергового-диспетчера, проводити фіксацію дій патрульного за допомогою планшетного комп'ютера у разі виявлення правопорушення, здійснювати пошук інформації у підсистемах ІІПС за допомогою планшетного комп'ютера патрульного, складати електронну адмін-постанову з використанням планшетного комп'ютера.

Особлива увага приділяється питанням новітніх підходів представлення (візуалізації) криміногенної ситуації в державі та результатів діяльності ОНП. Патрульні поліцейські отримують практичні навички роботи з вебпорталом www.police.kh.ua, розробленого ІТ- фахівцями Харкова спільно з співробітниками Управління інформаційного забезпечення Головного управління Національної поліції в Харківській області, який забезпечує можливість переходу поліції до взаємодії з населенням на абсолютно нових, сучасних, що відповідають європейським вимогам принципах. Портал забезпечує виконання трьох груп функцій :

1. *інформування громадськості про стан злочинності в обслуговуваному регіоні* (в даному випадку - в Харківській області), а саме:

1.1. відображення на географічній карті місцевості всіх реєстрованих поліцією злочинів, включаючи розкриті і нерозкриті, із забезпеченням можливості вибору одного або декількох видів злочинів, необхідного району (або районів) Харкова або Харківській області, необхідного проміжку часу (за останній день, тиждень, місяць та ін.);

1.2. відображення на географічній карті місцевості всіх доступних відеокамер з можливістю перегляду в on-line-режимі ситуації в спостережуваному даною відеокамерою (або декількома відеокамерами одночасно) ділянці місцевості;реалізацію зворотного зв'язку з населенням;

1.3. відображення на географічній карті місцевості розташування всіх дільничних інспекторів з можливістю перегляду їх контактної інформації та зон їх обслуговування (списку будинків);

1.4. можливість перегляду списку всіх злочинців, які перебувають в даний момент в розшуку, а також осіб, зниклих без вести;

2. *реалізацію зворотного зв'язку з населенням*, а саме: можливість будь-

якому громадянину відправити повідомлення про правопорушення, про який-небудь небезпечний предмет і ін. по Інтернету з прикріпленням файлу з фотозображенням або відео описуваної події або предмета;

3. *надання сервісних послуг*, а саме: можливість замовити на порталі довідку про судимість [2].

Патрульним поліцейським надаються теоретичні й практичні навички роботи в системі кримінального аналізу RICAS.

RICAS - WEB орієнтована гео-інформаційна система, яка дозволяє перенести накопичену табличну інформацію про злочини в гео-площину. Функціональними особливостями RICAS є:

- автоматична побудова взаємозв'язків;
- ручне додавання взаємозв'язків;
- ретроспективний аналіз;
- пошук в радіусі;
- інтелектуальний контекстний пошук;
- автоматичне виявлення і візуалізація зон концентрації вуличної злочинності;
- автоматичне створення аналітичних звітів;
- підключення даних із зовнішніх джерел;
- візуалізація пересування патрулів оснащених GPS трекера.

Система виконана як надбудова (оболонка) існуючої ІІПС ОВС України, і, що принципово важливо, дозволяє при її впровадженні не видаляти стару систему або припиняти її функціонування, а просто і безболісно істотно поліпшувати її функціональність і ефективність [3].

Приділяється увага використанню пошуку інформації в довідково-інформаційних базах даних вільного доступу (державних реєстрів) [4].

Моторне (транспортне) страхове бюро України (МТСБУ) є єдиним об'єднанням страховиків, які здійснюють обов'язкове страхування цивільно-правової відповідальності власників наземних транспортних засобів за шкоду, заподіяну третім особам. За допомогою запиту до Централізованої бази даних МТСБУ можна перевірити чинність полісу. Список пошукових запитів: визначити статус полісу внутрішнього страхування за номером транспортного засобу на задану дату; визначити статус полісу внутрішнього страхування за його серією та номером на задану дату; визначити статус «Зеленої картки» за її номером на задану дату; визначити статус «Зеленої картки» за номером транспортного засобу на задану дату; пошук у реєстрі страхових агентів за кодом та найменуванням; поширені питання.

Державне підприємство "Національні інформаційні системи" (надалі - ДП "НАІС") засноване Міністерством юстиції України в травні 2015 року. Організаційна структура ДП "НАІС": головне підприємство та 22 регіональні філії в обласних центрах України. Основною метою діяльності Підприємства є технічне, технологічне забезпечення створення та супроводження програмного забезпечення ведення автоматизованих систем Єдиних та Державних реєстрів, що створюються відповідно до наказів Мін'юсту, а також інших електронних баз даних, що створюються відповідно до законодавства України, на-

дання доступу фізичним та юридичним особам до автоматизованих систем Єдиних та Державних реєстрів, забезпечення збереження та захисту даних, що містяться в автоматизованих системах Єдиних та Державних реєстрів. На сайті nais.gov.ua у розділі «Відкриті дані з реєстрів» можна одержати наступну інформацію: єдиний державний реєстр юридичних осіб, фізичних осіб – підприємців та громадських формувань; реєстр громадських об'єднань; реєстр громадських формувань; єдиний реєстр нотаріусів; державний реєстр атестованих судових експертів; єдиний реєстр спеціальних бланків нотаріальних документів; державний реєстр друкованих засобів масової інформації та інформаційних агентств як суб'єктів інформаційної діяльності; реєстр методик проведення судових експертиз; єдиний державний реєстр осіб, які вчинили корупційні правопорушення; єдиний реєстр підприємств, щодо яких порушено впровадження у справі про банкрутство; єдиний реєстр арбітражних керуючих (розпорядників майна, керуючих санацією, ліквідаторів) України; єдиний державний реєстр нормативно-правових актів; реєстр суб'єктів, які надають послуги, пов'язані з електронним цифровим підписом; електронний реєстр чинних, блокованих та скасованих посилених сертифікатів відкритих ключів засвідчувальних центрів та центрів сертифікації ключів; реєстр адміністративно-територіального устрою; єдиний державний реєстр осіб, щодо яких застосовано положення Закону України «Про очищення влади».

Здійснення пошуку інформації з відкритих джерел мережі Інтернет, офіційного сайту Міністерства внутрішніх справ України (http://mvs.gov.ua/), офіційного сайту Національної поліції України (https://www.npu.gov.ua/) дає можливість слухачам отримати практичні навички пошуку необхідної інформації не тільки у підсистемах ІІПСОНП за допомогою планшетного комп'ютера патрульного, але і у розповсюджених інтернет-ресурсах. Розвиває у них здібності до аналітичної роботи, підвищує якість професійної діяльності.

---

1. Про організацію післядипломної освіти працівників Національної поліції: Положення, затверджене наказом Міністерством внутрішніх справ України від 24.12.2015 № 1625. URL: http://zakon2.rada.gov.ua/laws/show/z0076-16 (дата звернення: 15.04.2018).

2. Узлов Д.Ю., Струков В.М. Инновационный подход к взаимодействию полиции с населением на основе современных информационных технологий. Науковий журнал Право і Безпека. 2016. № 3 (62). С.86-93. URL: http://oaji.net/articles/2016/2258-1481286653.pdf (дата звернення: 15.04.2018).

3. Узлов Д.Ю., Струков В.М. Сучасні інструментальні засоби кримінального аналізу // Проблеми застосування інформаційних технологій правоохоронними структурами України та вищими навчальними закладами зі специфічними умовами навчання: зб. наукових статей за матеріалами доповідей Міжнародної науково-практичної конференції 22 грудня 2017 року / упорядник Т. В. Магеровська / – Львів: ЛьвДУВС, 2018. – 407 с. С.91-94.

4. Краснобрижий І.В., Прокопов С.О., Рижков Е.В. Застосування комп'ютерних технологій в Національній поліції: Навчальний посібник – Дніпро: Дніпропетровський державний університет внутрішніх справ, 2017. – 161 с.

**Коротенко Григорій Михайлович**
к.т.н., доц., професор кафедри
геоінформаційних систем

**Коротенко Леонід Михайлович**
к.т.н., доц., доцент кафедри
програмного забезпечення комп'ютерних систем
ДВНЗ «Національний гірничий університет»

# ЕЛЕМЕНТИ НАВЧАННЯ СТУДЕНТІВ УНІВЕРСИТЕТІВ СТВОРЕННЮ БЕЗПЕЧНИХ ПРОГРАМНИХ КОМПОНЕНТІВ В МЕТОДОЛОГІЇ DEVOPS

В даний час на плечі Університетів лягає все зростаюче навантаження з підготовки студентів, які повинні відповідати сучасному стану ІТ галузі. І це навантаження, на жаль, поступово зростає в умовах існування постійного виклику – необхідності створювати безпечне програмне забезпечення (ПЗ) швидко, якісно і надійно при постійному нарощуванні обсягів так званих *великих даних* (big data) [1]. Для різних галузей цей термін має своє «наповнення», але для правоохоронних органів великі дані включають широкий спектр важливих і необхідних в роботі слідчих органів: відео-, аудіо-, структурованих, графічних, архівних, геопросторових даних і багато інших їх видів [2, 3]. При розробці нових підходів до їх обробки в ІТ-галузі відповіддю на цей виклик стала методологія DevOps [4].

Вперше цей термін ввели Ендрю Шафер і Патрік Дебоіс на конференції Agile в Торонто в 2008 році в процесі обговорення проблем в рубриці «Agile Infrastructure». В цілому – це культура і практика розробки програмного забезпечення, метою якої є уніфікація розробки (Dev) і експлуатації ПЗ (Ops). Головною характеристикою культури DevOps є рішуча підтримка автоматизації та моніторингу на всіх етапах розробки програмного забезпечення: від інтеграції, тестування, до розгортання і управління інфраструктурою. А результатом – значно коротші цикли розробки, підвищена частота розгортання, більш надійні випуски в тісній взаємодії з бізнес-цілями організацій [4-5].

За визначенням, запропонованим Басом, Вебером і Чжу [6]: DevOps – це набір практик, призначених для скорочення часу між внесенням змін до системи і передачі її в нормальному стані у функціонуюче виробництво при забезпеченні високої якості кінцевого продукту.

Феномен DevOps об'єднав під своїми прапорами неймовірний конгломерат існуючих і постійно створюваних організаційних структур, платформ, сервісів, інструментів і т.д. Останнім часом границі цієї методолгії розширені за рахунок додавання компоненти «безпечності» (security), яка додала методології новий рівень – «DevSecOps» [7].

Разом з тим, провідні ІТ-фахівці констатують, що постійний розвиток підходів, практик, інструментів і технологій, що визначають розвиток інфраструктури DevOps зосереджено на її серцевині, яку складає **програмний код**,

що постійно розробляється, накопичується і вдосконалюється. Тому не дивно, що тривають роботи по стандартизації різноманітних характеристик програмних компонентів, які є продуктами кодування. Так, на даний момент, триває розробка серії стандартів під егідою організації Consortium for IT Software Quality (CISQ) [8]. Даний консорціум вирішує завдання підвищення якості програмного забезпечення для широкого кола IT-галузей і є безумовним лідером в області стандартизації процесів розробки ПЗ та об'єднує в своїх рядах системних інтеграторів, постачальників послуг різного призначення, безпосередніх розробників, а також постачальників сервіс-орієнтованих програмних технологій. Основним напрямком діяльності консорціуму є розробка і впровадження різноманітних стандартів на показники, вимоги і норми, які спрямовані на вдосконалення метричних характеристик, що забезпечують високу якість і оптимальні розміри компонентів програмного забезпечення.

Слід зазаничити, що CISQ – це нейтральний відкритий форум, на якому клієнти і постачальники програмного забезпечення для IT-застосунків можуть розробляти загальносистемний порядок денного для вирішення завдань підвищення якості кінцевих програмних продуктів для зниження витрат і ризику. Проведені роботи розосереджені по наступних напрямках:

1. Software Sizing (Розмір програмного забезпечення).
2. Code Quality (Якість коду).
3. Technical Debt (Технічний борг).
4. Additional Measures (Додаткові заходи).

Зокрема, комплекс стандартних показників якості CISQ (або «Показників CISQ»), призначений для забезпечення безпеки, надійності, ефективності і зручності обслуговування ПО різних рівнів застосування та являє собою набір з вісімдесяти шести (86-ти) метрик, які використовуються для оцінки рівнів відповідності необхідним вимогам правил розробки програмного забезпечення, які добре зарекомендували себе на практиці. Запропоновані метрики включені в спеціальні інструментальні засоби статичного аналізу вихідного коду досліджуваних програм і дозволяють виявляти багато критичних недоліки в програмному забезпеченні що розробляється з метою їх подальшого усунення проектувальниками і програмістами (рис. 1)

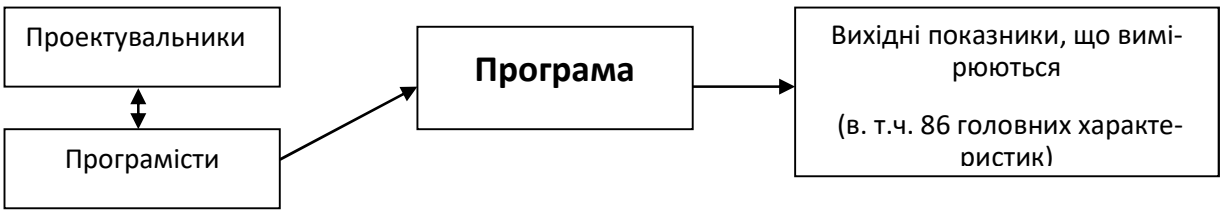



*Рис. 1. Особи, що формують основні показники (характеристики) якості программ*

Розглядаючи будь-який програмний компонент, як об'єкт роботи різних взаємодіючих груп учасників, в першу чергу слід відзначити, що безперечно істотний внесок в його створення вносять, в першу чергу, розробники (програмісти, кодувальники). Саме тому, стандартизація написання вихідних тек-

стів (source code) програм, на думку авторів, повинна істотно спростити всі подальші етапи взаємодії з ними. Дані роботи пропонується вести вже в Університетах, на базі викладання курсів з вивчення мов програмування. Зокрема, в Державному ВНЗ «Національний гірничий університет», на кафедрі програмного забезпечення комп'ютерних систем розроблено «Стандарт кафедри з викладання мови С++ для процедурного програмування» [9], який заснований на документах: «Stanford University CS 106B Style Guide» [10] і «Google C ++ Style Guide» [11].

Зі стандарту Стенфордського університету авторами був використаний т.зв. «ВерблюжійРегістр» (CamelCase) для іменування змінних і рекомендації по опису функцій. В цілому, за основу були прийняті саме основні положення стандарту Google. Природно, що були виключені моменти, пов'язані з ООП. Спираючись на положення структурної теореми Бома і Джакопіні, основну увагу автори приділили базовим структурам мови С++: СЛІДУВАННЯ, РОЗВИЛКА і ЦИКЛ. При цьому враховувалося, що в мові С++ конструкція СЛІДУВАННЯ не відноситься до групи керуючих структур, до якої відносяться оператори if, if / else, switch. for, while, do / while. Тому, коментування функціонального призначення даних структур виділено в окремі підрозділи.

Пропонований підхід був застосований з тією метою, щоб дидактичною «родзинкою» для студента служив психологічний момент, що при коментуванні введеної структури, він повинен задумуватися про її призначення. Також, особлива увага в процесі навчання приділяється освоєнню студентами елементів модульного програмування. У згаданому вище «Стандарті» вказується, що необхідно в описі функції обов'язково коментувати призначення її параметрів, а також писати, по можливості, короткі функції, дотримуватися «Стандарту» при виборі імен функцій, додержуватияс порядку слідування їх параметрів: спочатку йдуть вхідні, потім – вихідні .

На підставі аналізу сучасного стану IT-галузі автори прийшли до висновку, що в цілому в DevOps спостерігається відсутність початкової фази – впровадження в навчання на молодших курсах університетів стандартів програмування для подальшого використання в процесі розробки програм в IT-організаціях. Самі стандарти для різних мов програмування мають базуватися на низхідному проектуванні програм методом покрокової деталізації і структурному програмуванні з використанням основних базових структур мови, щоб студенти зосередилися на проектуванні і конструюванні програм, а не на особливостях мови програмування. Очевидно, що найкращим варіантом було б зведення воєдино кращих практик для якісної підготовки майбутніх професіоналів. Для забезпечення процесу поетапної наступності пропонується розділити стандарти з програмування на Університетські та Професійні.

1. Feng-Sheng. Field Study of Patent Strategies from Patent Map on Big Data: An Empirical Case of Big Data Application Platform in Taiwan. WEB–сайт [Электрон. ресурс] / Режим доступа: URL: https://www.researchgate.net/publication/271838610_Field_Study_of_Patent_Strategies_from_Patent_Map_on_Big_Data_An_Empirical_ Case_of_Big_Data_Application_Platform_in_Taiwan.

2. Саріогло В. Г «Великі дані» як джерело інформації та інструментарій для офіційної статистики: потенціал, проблеми, перспективи / В.Г. Саріогло // Статистика України. – 2016. – № 4. – С. 12-19.

3. Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних: постанова Кабінету Міністрів України від 21 жовтня 2015 р., № 835 / Офіційний сайт Верховної Ради України. – [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/835-2015-%D0%BF

4. DevOps. WEB–сайт [Электрон. ресурс] / Режим доступа: URL: https://en.wikipedia.org/wiki/DevOps.

5. Roger LeBlanc. DevOps and Middleware, common scenarios. WEB–сайт [Электрон. ресурс] / Режим доступа: URL: https://www.ibm.com/developerworks/community/blogs/c914709e-8097-4537-92ef-8982fc416138/entry/DevOps_and_Middleware_common_scenarios?lang=en

6. Философия DevOps. Искусство управления IT / Дэвис Дженнифер, Дэниелс Кэтрин. – СПб.: Питер, 2017. – 416 с.,

7. Secure DevOps: What's in it for dev, sec and ops? https://techbeacon.com/secure-devops-whats-it-dev-sec-ops

8. Consortium for IT Software Quality (CISQ). . WEB–сайт [Электрон. ресурс] / Режим доступа: URL: http://it-cisq.org/

9. Методические рекомендации по разработке программ по курсу «Алгоритмизация и программирование» на языке программирования С++ для бакалавров области знаний 12 «Информационные технологии» / Г.М. Коротенко, Л.М. Коротенко – Д.: ГВУЗ «Национальный горный університет», 2017. – 25 с. (в печати).

10. CS 106B: Programming Abstractions (C++) Summer 2015. WEB–сайт [Электрон. ресурс] / Режим доступа: URL: http://stanford.edu/class/archive/cs/cs106b/cs106b.1158/styleguide.shtml

11. Google C++ Style Guide. WEB–сайт [Электрон. ресурс] / Режим доступа: URL: https://google.github.io/styleguide/cppguide.html

15. DevOps for Dummies, 3rd IBM Limited Edition. / Sanjeev Sharma, Bernie Coyne. – John Wiley & Sons, Inc., 2017. – 62 p.

**Косиченко Олександр Олександрович**
к.т.н., доц., доцент кафедри
економічної та інформаційної безпеки

**Южека Роман Сергійович**
слухач магістратури Дніпропетровського
державного університету внутрішніх справ

## ВИКОРИСТАННЯ МЕНТАЛЬНИХ КАРТ В ДІЯЛЬНОСТІ ПРОКУРОРА

Прокуратура певною мірою покликана виконувати роль гаранта в дотриманні прав та свобод людини й громадянина. Тому, зумовлює інтерес до діяльності прокуратури, викликає неабияку зацікавленість в розгляді особливостей використання засобів візуалізації мислення – ментальних карт (карт мислення, інтелект-карт) в юридичній та правоохоронній діяльності.

Реформування прокуратури в нашій країні, пошук і створення її оптима-

льної моделі, ефективної в реаліях сьогодення, вимагає перегляду змісту основних параметрів прокурорської діяльності, виявлення її потенціалу, який необхідно спрямовувати на підвищення її результативності як на конкретному напрямі, так і прокуратури як державної інституції [1].

Отже, перед дослідженням особливостей використання засобів візуалізації мислення взагалі та ментальних карт особливо, в діяльності прокурора необхідно конкретизувати, що організація та діяльність прокуратури України, статус прокурорів визначаються законами України, чинними міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України. Так, згідно зі ст. 1 Закону України «Про прокуратуру» прокуратура України становить єдину систему, яка в порядку, передбаченому вищенаведеним Законом, здійснює покладені Конституцією України функції з метою захисту прав і свобод людини, загальних інтересів суспільства та держави [2]. Реалізуючи передбачені законодавством функції, прокурор діє з метою захисту прав та свобод людини, загальних інтересів суспільства й держави.

Світ науки і техніки активно розвивається, з кожним днем потік інформації зростає. Отже, зростає і обсяг матеріалу, з яким працює прокурор. Тому, завдання прокурора – максимально оптимізувати і структурувати свою діяльність. Саме ці завдання і покликані вирішувати ментальні.

Отже, карти знань – це схеми, які наочно подають різні поняття, дії, завдання, тези, взаємопов'язані та об'єднані спільною ідеєю. Вважається, що такий метод візуалізації інформації вперше застосував філософ Порфирій Тирський ще в III ст. н.е., намагаючись краще зрозуміти концепції Аристотеля. Схожі малюнки та методи використовував також Леонардо да Вінчі, Ч. Дарвін, С. Далі, Д. Бруно, А. Ейнштейн. Ґрунтовні сучасні розробки в цьому напрямі належать до 60-х років XX ст. [3].

Термін «карта знань» або «інтелектуальна карта» запропонував англійський вчений Тоні Б'юзен (Tony Buzan) [4], який чимало зробив для просування технологій використання таких карт в усіх галузях життя, а також спростив способи їх створення. Б'юзен також запропонував радіальні карти знань, тобто карти, що будуються навколо якоїсь центральної думки або проблеми.

Варто зазначити, що з проблемою необхідності запам'ятовування, засвоєння і логічного структурування інформації знайомо багато людей. Це вміння необхідне в найрізноманітніших областях знань, а також в усіх сферах юридичної діяльності.

Унікальна методика, побудована на використанні ментальних карт, широко відома і використовується у світі. Вона дозволяє, активізуючи природні процеси мозку, отримати значні переваги під час роботи з інформацією будь-якого виду. Ментальні карти використовуються для генерування, відображення, структурування, класифікації ідей, а також у якості допоміжного засобу під час навчання, організації інформації, прийняття рішень, написання статей, лекцій, підручників.

В спеціалізованій літературі термін «ментальна карта» має багато синонімів: інтелект-карта, карта ума, карта пам'яті, карта концепції, асоціативна

карта, діаграма зв'язків. Але кожна назва означає одне й те саме. По-перше, це альтернативний лінійному запису варіант відображення процесу мислення та структуризації інформації у візуальній формі. По-друге, систематизація інформації відбувається шляхом побудови певних значеннєвих блоків та визначення взаємозалежності між ними з відповідним їх логічним та естетичним упорядкуванням. По-третє, ментальна карта є розумовим креативним інструментом, оскільки саме цей варіант упорядкування розумових процесів дозволяє досягти високого рівня генерування нових ідей.

Отже, майндмеппінг (mindmapping) – це зручна й ефективна техніка альтернативного запису аналізу інформації. Її можна застосовувати для створення нових ідей, аналізу і впорядковування інформації, ухвалення рішень тощо. Це не дуже традиційний, але достатньо природний спосіб організації мислення, що має декілька незаперечних переваг над звичайними способами запису.

Ментальні карти – це техніка візуалізації мислення; спосіб запису, за допомогою списків та схем (наприклад, «дерев» або діаграм зав'язків). Головна відмінність ментальних карт від інших способів візуалізації полягає в тому, що ментальні карти активізують асоціативну пам'ять та мислення [4, с. 5].

Сутність методики ментальних карт полягає в тому, що виділяється основне поняття, від якого далі відгалужуються задачі, ідеї, окремі думки та кроки, які необхідні для реалізації конкретного проекту чи задумки. Далі, так само, як і основна, всі більш дрібні гілки можуть ділитись ще на декілька гілок-підпунктів. З цього виходить, що ментальна карта відображає асоціативні зв'язки в мозку її творця. Тут немає ніякого сухого матеріалу, довгих фраз, тому подальша робота з ментальними картами не викликає дискомфорту, а навпаки – з ними буде цікавіше і продуктивніше працювати. Основана ця методика на принципі «радіанного мислення», пов'язаного з асоціативними розумовими процесами. Відправна точка в цьому процесі – центральний об'єкт (думка, ідея, задача). Радіант – це точка небесної сфери, від котрої ніби відходять видимі шляхи тіл, що рухаються з однаково спрямованими швидкостями. З цього можна зробить висновок, що «радіанне мислення» відображає нескінчене різноманіття можливих асоціацій, а ментальні карти дозволяють зафіксувати їх на різноманітних носіях [5].

Для прокурора ментальна карта – суб'єктивне відображення людиною тих самих об'єктів, явищ і процесів, що мають місце у діяльності органів прокуратури. Ментальна карта має такі атрибутивні властивості: будь-який процес, явище, що досліджується, відображається у вигляді певного центрального образу; усі теми, об'єкти і процеси, що пов'язані з цим образом, розходяться від нього у вигляді гілок; кожна гілка позначається ключовими словами чи образами; кожна гілка також може мати свої паростки; гілки об'єднують у зв'язану вузлову систему [6, с. 4].

Ментальні карти сприймаються краще, ніж звичні списки, графіки, таблиці, тексти тому, що вони краще відповідають структурі людського мислення – асоціативного, ієрархічного та візуального. Хоча, зрозуміло, карти не замінюють таблиць і графіків, а органічно доповнюють їх. Звичайний лінійн-

ний спосіб передачі не завжди допомагає при обробці значного обсягу інформації, особливо в екстремальні (типу екзаменаційної сесії) періоди життя студентів. Подана таким чином інформація погано запам'ятовується. Малюнки і символи ж запам'ятовуються легше. Ментальні карти можуть стати зручним способом запису значних обсягів інформації з подальшим її легким відтворенням за рахунок візуалізації.

Ментальні карти можна створювати двома основними способами. Вручну, за допомогою кольорових фломастерів або олівців і за допомогою комп'ютерних програм, як у локальному режимі (наприклад, програма Xmind), так і в режимі онлайн у мережі інтернет (наприклад, онлайн-сервіс на сайті www.mindmeister.com).

Таким чином, ментальні карти в діяльності прокурора – сучасний і компактний спосіб вирішення завдань, які стоять перед прокурором. Застосування інтелект-карт в діяльності прокурора може дати величезні позитивні результати, оскільки ментальні карти дозволяють краще структурувати і запам'ятовувати ключову інформацію, а також відтворювати її в подальшому. Використання ментальних карт в діяльності прокурора дозволяє набути таких умінь: виділяти головну ідею; розпізнавати взаємозв'язки; орієнтуватися у справі; розвивати асоціативне мислення; творчо підходити до вирішення проблем; самостійно знаходити оригінальні ідеї; швидше й ефективніше виконувати покладені на прокурора функції.

1. Представництво прокурором у суді законних інтересів держави: наук.-практ. посіб. / О.П. Натрус, Ю.А. Турлова, О.А. Казак та ін. – К.: Національна академія прокуратури України, 2016. – 262 с.

2. Про прокуратуру : Закон України від 14 жовтня 2014 року (зі змінами і допов.) // Відомості Верховної Ради України. − 2015. − № 2-3. − Ст. 12.

3. Сокол І. М. Веб 2.0. Сайти, блоги, фото сервіси, карти знань / І. М. Сокол. – К. : Шк.світ, 2011. – 128 с.

4. Бьюзен Т. Научите себя думать! / 2-е изд. – М.: ООО "Попурри", 2004. – 192 с.

5. Сиббет Дэвид Визуализируй это! Как использовать графику, стикеры и интеллект-карты для командной работы. / Дэвид Сиббет. – М.: Альпина Паблишер, 2013. – 280 с.

6. Майнд-менеджмент: Решение бизнес-задач с помощью интеллект-карт помощью / Сергей Бехтерев; Под ред. Глеба Архангельского. – 4-е изд. – М.: Альпина Паблишер, 2012. – 308 с.

**Краснобрижий Ігор Володимирович**
к.ю.н., доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

# ВІРОГІДНА РЕАЛІЗАЦІЯ АЛГОРИТМУ ЗБОРУ ТА АНАЛІЗУ ІНФОРМАЦІЇ, ОТРИМАНОЇ В ТОМУ ЧИСЛІ З ВІДКРИТИХ ДЖЕРЕЛ, З МЕТОЮ ПОПЕРЕДЖЕННЯ ТА РОЗКРИТТЯ ПРАВОПОРУШЕНЬ

На теперішній час, у зв’язку з переведенням значної кількості інформаційних масивів у цифрову форму та надання доступу до більшості цієї інформації через глобальну інформаційну мережу (Інтернет), стає можливим отримати цілі пласти логічно зв’язаної інформації, що цікавить різноманітні фізичні чи юридичні особи. За останніми даними сьогодні доступ до Інтернету мають 46 % домогосподарств світу, тоді як у минулому році цей показник був 44 %, а в 2010 році - всього 30 %. В числовому еквіваленті мають доступ до Інтернету 3,2 млрд. людей (43% світового населення). Зафіксовано, що протягом 5 років число користувачів Інтернетом в країнах, що розвиваються, збільшилось в 2 рази. Покриття населення мережами 3G зросла за чотири роки з 45 % до 69 %. Згідно звіту Міжнародного союзу електрозв’язку Україна за показником розвитку інформаційно-телекому¬нікаційних технологій займає 79 місце (в 2010 році - 69) з індексом розвитку 5,23 (в 2010 році - 4,41) [1, с. 2-5]. Збільшення користувачів світовою мережею зумовило значне зростання кількості злочинів, які вчиняються в кіберпросторі, тим більше Україна відноситься до країн, що розвивається в інформаційному просторі, тому збільшується ризики зловживанням інформаційними та комунікаційними технологіями в злочинних або інших цілях. [2, с. 90]. В даній статті ми розглянемо роботу з інформаційними ресурсами, що виконують державні правоохоронні органи з метою попередження та розкриття різноманітних злочинних проявів.

Як вже вказувалось, інформацію в мережі Інтернет на юридичних та фізичних осіб можливо отримати в доволі великих обсягах. Отримання цієї інформації здійснюється за допомогою різноманітних методик [3, с. 111-115] здійснення пошуку, а також засобів [4, с. 110, 111, 114-122], що дозволяє здійснювати пошук в напівавтоматичному, чи навіть в автоматичному режимі. Як приклад програмних засобів для автоматизації пошуку інформації можемо навести такий програмний комплекс як IBM i2 analyst's notebook [5] з підключеними програмними модулями SocialGrabber4i2 2.0 [6]. Основним призначенням SocialGrabber4i2 2.0 є отримання даних із соціальних мереж для аналізу явних і прихованих зв'язків між різними об'єктами дослідження, що дозволяє визначити приховані спільноти, організовані злочинні групи і виявити ключові об'єкти і лідерів груп. Програмний модуль IBM i2 iBase [7]

дозволяє вилучати інформацію з різних баз даних, а також імпортувати ці бази даних гуртом. Інші джерела, які можливо використовувати для пошуку більш-менш достовірної інформації, у цій статті ми приводити не будемо бо вони гідні окремого розгляду.

Але отримання даних це лише початковий етап роботи з інформацією. Наступний етап називається **аналіз**. Аналітичний етап процесу починається з отримання відповідних даних і їх організації у формі, що дозволяє розуміти їх значення. Даний етап, опис даних, сприяє виявленню відсутньої інформації і допомагає направляти подальші заходи по збору даних на отримання відсутніх даних. Їм також утворюється основа для вживання індуктивного висновку з метою розробки однієї або більш гіпотез про ключові аспекти злочинної діяльності. Гіпотези апробовуються повторенням збору, оцінки, впорядковування, опису даних і індуктивного циклу обґрунтовування. Кожного разу при повторенні циклу, він все сильніше націлюється на конкретні види інформації, необхідної для підтвердження або спростування гіпотези, що веде до формування висновку з високим рівнем надійності (рис. 1).

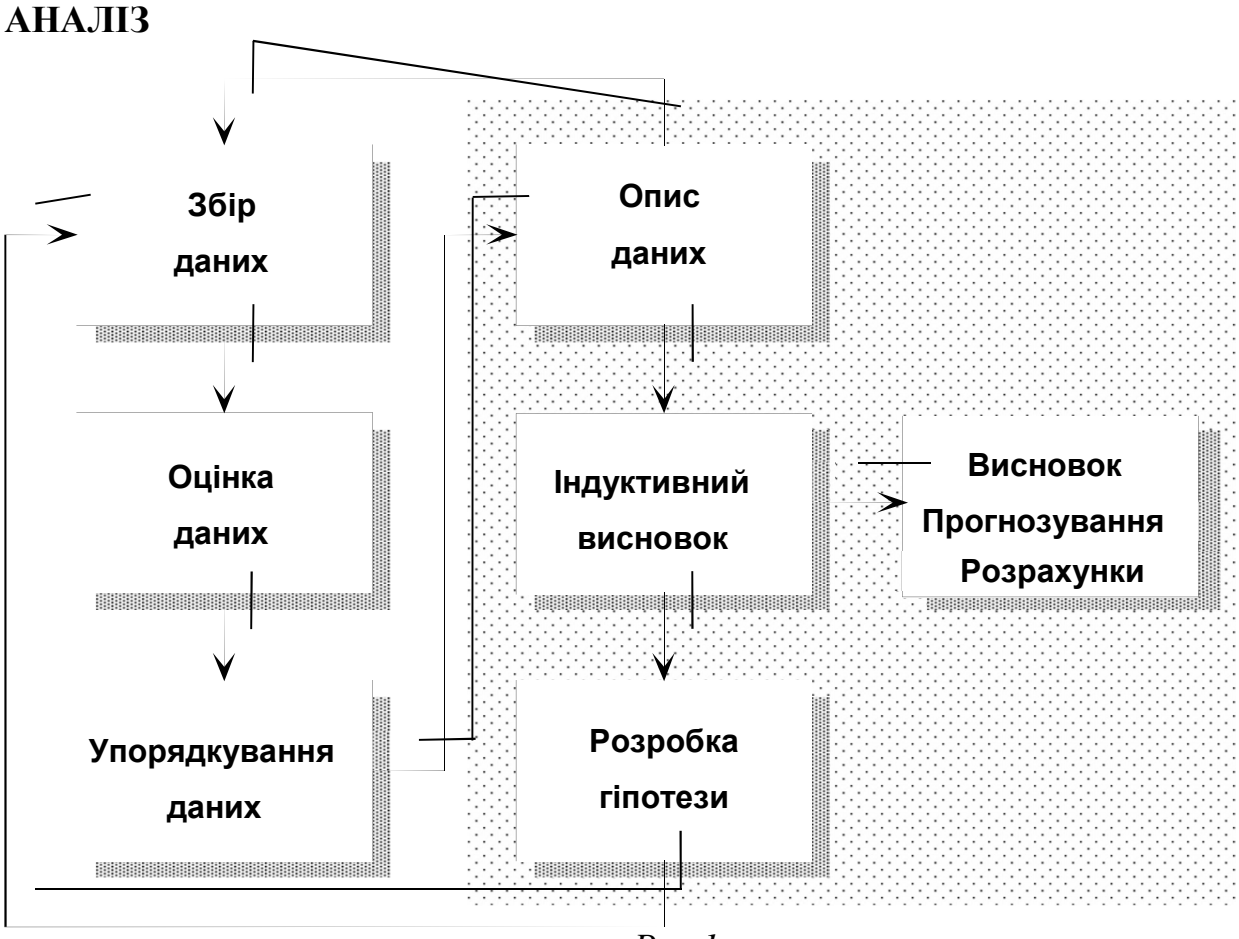



*Рис.1*

Кінцева мета справжнього процесу полягає в забезпеченні даного висновку – висновку, прогнозування або розрахунків, на основі яких можна діяти з упевненістю [8, с. 662, 663].

В якості висновку слід зауважити, що нині проблема не у відсутності потрібних інформаційних даних, а у здатності інформаційних підрозділів навіть фізично обробляти інформаційні потоки, а також знаходити необхідну інформацію в базах даних, тому використовуючи спеціальне програмне забезпечення для отримання та першочергової аналітичної обробки отриманих даних правоохоронні органи набагато покращать ефективність своєї діяльності. Ще я вважаю за необхідне інтенсифікувати підготовку майбутніх поліцейських та провести додаткові практичні курси з практичними працівниками правоохоронних органів в сфері пошуку та аналітичної обробки інформаційних ресурсів з різноманітних джерел.

1. Измерение развития ИКТ: Новые тенденции, новые проблемы II Симпозиум по всемирным показателям в области / ИКТ. - Хиросима, Япония. - 2016. - №1 [Елек-тронний ресурс]. - Режим доступу: http://www.itu.int/ en/itunews/Documents/2016_ITUNews01-ru.pdf

2. Кримінальна розвідка з відкритих джерел як інструмент збирання оперативної інформації / К. Ю. Ісмайлов // Південноукраїнський правничий часопис. - 2016. - № 1. - С. 88-91.

3. Застосування комп'ютерних технологій в Національній поліції : навч. посіб. / І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков – Дніпро : ДДУВС, 2017. – 161 с.

4. Застосування комп'ютерних технологій в Національній поліції : навч. посіб. / І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков – Дніпро : ДДУВС, 2017. – 161 с.

5. https://www.ibm.com/us-en/marketplace/analysts-notebook

6. http://www304.ibm.com/partnerworld/gsd/solutiondetails.do?solution=51450&expand=true&lc=ru

7. https://www.ibm.com/us-en/marketplace/data-management

8. Підвищення кваліфікації слідчих, рамкова програма співробітництва для Вірменії, Азербайджану, Грузії, Республіки Молдова, України й Білорусії, спільний проект Європейського Союзу та Ради Європи «Посилення імплементації європейських стандартів прав людини в Україні», 2017. – 659 с.

**Крикавський Євген Васильович**
д.е.н., проф., завідувач кафедри
маркетингу і логістики
Національного університету
«Львівська політехніка»

**Касян Сергій Якович**
к.е.н., доц., доцент кафедри
економічної теорії та маркетингу
Дніпровського національного
університету імені Олеся Гончара

# МАРКЕТИНГОВІ ІННОВАЦІЙНІ ПРОЦЕДУРИ ІНФОРМАЦІЙНО-ЕКОНОМІЧНОЇ БЕЗПЕКИ У ЛОГІСТИЦІ ДИСТРИБУЦІЇ

Координування міжнародних і регіональних логістичних потоків на засадах їх інтегрування у транспортній сфері потребує урахування комплексних засад економічної та інформаційної безпеки. В умовах темпоральної обмеженості і певної дефіцитності ресурсних потоків доцільним є вдосконалення їх логістичного, інформаційного забезпечення, що полягає у комплексному застосуванні віртуальних логістичних технологій у поєднанні з безпечними Інтернет маркетинговими комунікаціями. Варто моделювати організацію логістичних процесів на підприємствах з урахуванням макро, мезо та мікрорівнів, що інформаційно опосередковує вибір політики логістичного менеджменту та інформаційно-економічного розвитку підприємств.

Гжегож Бієсок і Елеонора Спрінгер (Grzegorz Biesok і Eleonora Springer) надаючи характеристику автомобільного транспорту, визначають основні його цілі, такі як: досягнення високої мобільності товарів та людей, певний внесок у формування національної та глобальної конкурентоспроможності, забезпечення високого рівня якості суспільного й економічного життя. Науковці слушно описують переваги, що надає організація логістики автомобільного транспорту, а саме: висока доступність до основних засобів праці, значна оперативність транспортування, еластичність перевезень стосовно задоволення різноманітних потреб, швидкість перевезень в межах Just in Time, здатність транспортних засобів перевозити більшість видів вантажів, здійснення перевезень типу „door to door" без зайвих операцій з перевантаження [1, с. 57, 58]. Дійсно, варто підкреслити багатофункціональність, доступність, зручність та економічність організації логістики на базі автомобільних маршрутів перевезень в Україні, ЄС та світі. Вартим уваги є комплекс складних питань визначення інформаційно-правових аспектів безпечного координування основних ресурсних потоків у інтегративному маркетинговому просторі. При цьому доцільно оновлювати й підтримувати технологічний парк автомобільного транспорту, застосовуючи найбільш адекватні до рівня його регіонального розвитку транспортні засоби.

Марія Куровска (Maria Kurowska) наголошує на доцільності застосу-

вання інноваційних рішень у сфері технологічної, продуктової, організаційної, маркетингової політики мікро, малих та середніх підприємств для досягнення їх безпечного й успішного функціонування у просторі ринкової взаємодії. Наголошується на значущості отримання додаткових капітальних потоків, що мають надходити із структурних фондів ЄС. Вона справедливо наголошує на ролі ефективного інноваційного процесу, що містить послідовність новаційних змін, пов'язаних із втіленням і комерціалізацією потенційних ідей у площині технічної, технологічної, організаційної і суспільної діяльності підприємств [2, с. 109-110]. Безперечно, такі інноваційні зміни підвищують ступень безпеки економічної і маркетингової діяльності, забезпечуючи необхідний рівень конкурентоспроможності підприємств. В умовах наявного ефекту асиметричної інформації на сучасних висококонцентрованих світових і регіональних ринках доцільно удосконалювати інноваційно-програмні процедури досягнення безпеки економічних трансакцій у регіональній та міжнародній логістиці.

Виокремлюються чотири етапи інноваційного процесу, а саме: пошук можливості здійснення змін, моделювання засад економічного розвитку підприємства, перетворення ідеї у нову товарну або сервісну пропозицію, дисконтування цінностей від запровадження інновації. Такі цінності передусім полягають у підвищенні ринкової частки, зменшенні логістичних і операційних витрат [2, с. 110]. На наш погляд, підтримання позитивної конфігурації таких маркетингових цінностей під час аналітичного розгляду інноваційної діяльності досягається шляхом запровадження ефективного забезпечення інформаційної безпеки. Така безпека є провідною детермінантою процедур економічного і маркетингового розвитку підприємств, регіонів, інформаційного суспільства, що опираються на генерування сучасних інноваційних знань.

Олександр Зозульов (Oleksandr Zozulov) наголошує на існуванні певної розбіжності між науковою оцінкою реального стану економічних процесів та змістовими складовими формування маркетингової теорії. Він справедливо акцентує на взаємозв'язку маркетингової стратегії та стратегічних засад організації бізнесу. Дослідник систематизує та виокремлює такі трактовки маркетингу, як науки: філософська, управлінська, організаційна, функціональна, сутнісна, ціннісна, процесна та інституціональна. Окреслюється значущість маркетингу в формуванні концепції організації бізнесу, що сприяє підвищенню потоків цінностей для споживачів та збільшення ефективності управління капіталом [3, с. 64, 65]. На наш погляд, важливо на інноваційних засадах інтегрувати маркетингову і логістичну теорії і практики стосовно найповнішого відображення сутності логістичних організаційно-часових процесів з перевезення вантажів і людей. Зокрема, логістичні механізми, моделі і процедури постачання, виробництва та дистрибуції мають комплексно узгоджуватися з наявними інноваційними підходами до економіки і організації у транспортній, сервісній галузях країни, формування мереж постачання і дистрибуції. Доцільно застосовувати сучасні інформаційні технології, що мають забезпечувати ефективну взаємодію економічних і соціальних агентів упродовж логістичного ланцюга, спрямованого на створення доданої вартості.

Йоанна Дичковска (Joanna Dyczkowska) досліджує стратегічне управління логістичними послугами, поглиблюючи теоретико-методичні аспекти управління сучасними знаннями. Інформаційне забезпечення під час взаємодії інноваційних логістичних операторів приводять до підвищення рівня логістичного обслуговування, що має відповідати інтересам і вимогам цільових клієнтів. Вона справедливо підкреслює, що наявність комплексу ресурсів та сучасних знань забезпечує своєчасне моніторування змін у навколишньому маркетинговому середовищі, на основі запровадження логістичних систем. При цьому доцільно, щоб сучасне високотехнологічне підприємство було відкритим до змін і нових знань. Така відкритість, безперечно, має підтверджуватися високими стандартами інформаційної безпеки та значними обсягами фінансових внутрішніх і зовнішніх інвестицій [4, с. 28].

Науковець визначає значення організаційних знань при управління знаннями із залученням комплексу людських, матеріальних та інформаційних ресурсів підприємства. Оцінюється комплекс чинників зі сфери системи управління знаннями, що забезпечують успішне формування стратегії підприємства. Комплексом таких чинників передусім є: повна, швидка, актуальна і перевірена інформація; інноваційність технологічних та маркетингових організаційних рішень, гнучкість та динамізм під час впровадження інноваційних рішень і процедур з урахуванням балансування із наявною конфігурацією економічної і маркетингової політики підприємства [4, с. 28, 29]. Ми вважаємо, що маркетингові інноваційні процедури інформаційно-економічної безпеки у логістиці дистрибуції мають ґрунтуватися на формуванні системи генерування та передачі нових знань, які б забезпечували повноту, актуальність, безпечність і прозорість інформаційних потоків, що постійно циркулюють у висококонкурентному логістичному оточенні. Комплексний моніторинг та аналіз таких інформаційних потоків буде забезпечувати розвиток фінансової, економічної та маркетингової безпеки підприємств під час взаємодії на сучасних товарних і сервісних ринках.

Інтеграційні процеси інформаційно-економічного розвитку транспортної галузі здебільшого базуються на впровадженні інноваційних технологій логістичного забезпечення, затвердження високих стандартів інформаційної безпеки. Слід системно впроваджувати маркетингову концепцію до функціонування інтегрованого ланцюга постачання і дистрибуції. Сучасні інноваційні технології та логістична інфраструктура транспорту дозволяють прискорити рух основних ресурсних потоків між економічними агентами в умовах значного розповсюдження креативних знань [5].

Формуванню інноваційного вектору досягнення економічної безпеки у сучасному логістичному просторі сприяє діяльність науково-дослідних установ та ВНЗ. О. Жилінська досліджує обіг інформації на міжнародному ринку в контексті партнерської співпраці на них міжнародних дослідницьких університетів. Вона наголошує на розширенні спектру науково-технічної інформації з урахуванням постійного виникнення мережевих ефектів в інформаційно-економічному просторі комплементарних ринків світу, таких як ринок освітніх послуг і ринок об’єктів промислової власності [6, с. 172].

При цьому аналітичні процедури і функції управління мають бути спрямовані на ресурсне забезпечення кожної ланки створення вартості у логістичному ланцюзі. А модель процесу вибору форм розрахунків за надані логістичні послуги має сприяти фінансово-економічному розвитку транспортної галузі. Таке поєднання логістики постачання, виробництва і дистрибуції має відбуватися на засадах, окреслених в концепції соціально-етичного маркетингу. Завдяки методу абстракції можна мислено уявити генерування потоку маркетингової цінності під час функціонування логістичної системи високотехнологічних підприємств [7]. Безперечно, розвиток продуктивних сил у макрологістичній системі відображає ефективне переміщення логістичних ресурсних потоків.

Отже, задля сталого інформаційно-економічного розвитку транспортної логістики доцільно виокремлювати конкретні інтегративні маркетингові, екологічні та економічні процедури створення додаткової маркетингової цінності у логістичному ланцюзі. При цьому економічна та інформаційна безпека щодо планування і координування проходження основних ресурсних потоків у інтегративному логістичному просторі полягає у страхуванні товарообмінних операцій та прозорому інформаційному супроводі бізнес-трансакцій. Відмітимо, що досягнення безперервного точно пульсуючого ресурсного потоку досягається шляхом узгодження функціональних економічних дій усіх партнерів, що взаємодіють на протязі усіх ланок логістичного ланцюга. Маркетингові інноваційні процедури інформаційно-економічної безпеки мають базуватися на новітніх організаційних рішеннях та використанні конкурентних переваг провідних технологій V і VI рівня у логістиці виробництва та дистрибуції.

1. Biesok Grzegorz Logistyka usług. Springer Eleonora Rozdział 3. Logistyka usług transportu samochodowego rzeczy. – Warszawa : CeDeWu, 2013. – 160 s.

2. Kurowska Maria Wdrażanie innowacji jako czynnik zwiększający konkurencyjność przedsiębiorstw Województwa Łódzkiego / Maria Kurowska. Konsument i przedsiębiorstwo na rynki usług finansowych. Bezpieczeństwo i efyktywność pod redakcją Iwony D. Czechowskiej, Radosława Pastusiaka. Folia Oeconomica 284. Acta Universitatis Lodziensis. – Łódź : Wydawnictwo Uniwersytetu Łódzkiego, 2013. – S. 109–122 (248 s.).

3. Зозульов Олександр Формування концепції ведення бізнесу на маркетингових засадах: сьогодення та майбутнє / Олександр Зозульов // Маркетинг в Україні. – 2017. – №5-6. – С. 64–72.

4. Dyczkowska Joanna Marketing usług logistycznych / Joanna Dyczkowska. – Warszawa : Difin, 2014. – 192 s.

5. Krykavskyy E. V. Implementation of marketing concepts into supply chain management / E. V. Krykavskyy, O. A. /Pokhylchenko // Economics, entrepreneurship, management. – 2014. – Vol. 1, Num. 2. – P. 25–34.

6. Жилінська О. Дослідницькі університети у контексті розвитку міжнародного ринку науково-технічної інформації / О. Жилінська // Формування ринкової економіки в Україні. – 2017. – Вип. 37. – Ч. 1. – С. 172-182.

7. Касян С. Я. Взаємодія е-логістики та маркетингових комунікацій високотехнологічних підприємств у площині дистрибуції цінностей до споживачів / С. Я. Касян // Вісник Національного університету «Львівська політехніка», Серія: Логістика: Збірник наукових праць. Голова Редакційно-видавничої ради д.е.н., проф. Н. І. Чухрай. – Львів: Видав-во Львівської політехніки. – 2017. – №863. – С. 68–76.

**Кудінов Вадим Анатолійович**
к.ф.-м.н., доц., професор кафедри
інформаційних технологій
та кібернетичної безпеки
Національної академії внутрішніх справ

# ПРОБЛЕМИ СТВОРЕННЯ СТАНДАРТНОЇ МОДЕЛІ ЯКОСТІ СПЕЦІАЛЬНОГО МАТЕМАТИЧНОГО І ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ОРГАНІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Повноваження поліції у сфері інформаційно-аналітичного забезпечення передбачені ст. 25 Закону України «Про Національну поліцію» [1] та Положенням про Національну поліцію (далі – НП) [2]. Поліція в рамках інформаційно-аналітичної діяльності формує бази (банки) даних (далі – БД), що входять до Єдиної інформаційної системи (далі – ЄІС) Міністерства внутрішніх справ (далі – МВС) України. При цьому формування інформаційних ресурсів поліцією передбачено ст. 26 Закону України «Про Національну поліцію» [1]. Необхідно відмітити, що поліція наповнює та підтримує в актуальному стані 18 баз (банків) даних, що входять до ЄІС МВС України.

Поліція може створювати також власні БД, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також міжвідомчі інформаційно-аналітичні системи, необхідні для виконання покладених на неї повноважень.

Станом на сьогодні в Національній поліції України здійснюються заходи щодо створення інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» (далі – система ІПНП), яка представляє собою сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції України та її інформаційно-аналітичного забезпечення [3]. Система ІПНП є складовою частиною ЄІС МВС України та містить: а) центральний програмно-технічний комплекс; б) автоматизовані робочі місця (далі – АРМ) користувачів; в) телекомунікаційну мережу доступу; г) комплексну систему захисту інформації.

Інформаційними ресурсами системи ІПНП є інформація, що утворена в процесі діяльності поліції та використовується для формування: 1) тимчасових наборів даних, що створюються в процесі діяльності поліції та використовуються для наповнення та підтримки в актуальному стані БД, які входять до ЄІС МВС; 2) БД у сфері управлінських відносин, необхідних для виконання покладених на поліцію повноважень; 3) БД, необхідних для забезпечення щоденної діяльності поліції, у сфері трудових відносин, фінансового забезпечення, документообігу [3].

В інформаційних ресурсах системи ІПНП обробляється інформація, яка

належить до державних інформаційних ресурсів.

Для роботи з базами даних створюються різноманітні інформаційні системи (далі – ІС). Відповідно до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" «інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів» [4].

Під час створення нових інформаційних підсистем системи ІПНП необхідно враховувати такі принципи [5, 6]: 1) функціонального призначення (інформаційні підсистеми оперативно-розшукового, оперативно-довідкового, організаційно-управлінського призначення, кримінальної статистики, спеціалізовані); 2) нормативно-правової забезпеченості; 3) фактичності даних; 4) доцільності впровадження та експлуатації; 5) нарощення та розвитку.

Розширенню можливостей обчислювальної техніки і збільшенню кількості функціональних задач, покладених на автоматизовані інформаційні системи (далі – АІС) Національної поліції, передує зростання обсягу і складності спеціального математичного і програмного забезпечення (далі – СМПЗ). Необхідність виконання таких функціональних задач АІС НП, як збір, обробка, збереження, видача інформації, автоматизація доведення розпоряджень, контроль за роботою системи, визначає вимоги не тільки до технічних засобів, але і до складу та структури СМПЗ АІС НП. Під *спеціальним математичним і програмним забезпеченням* АІС, як відомо, розуміється сукупність математичних методів, моделей, розрахункових і інформаційних задач, реалізованих програмно.

АІС НП в більшості своїй є системами реального часу, відмовлення чи відступ від заданих обмежень яких може викликати серйозні фатальні наслідки. Залежність цих критичних систем від програмних засобів породжує необхідність надання застосовуваним у них програмним засобам заданих властивостей надійності і здібності протистояти руйнуванню, порушенням функціонування системи при виконанні критичною системою основної своєї цільової функції.

На теперішній час склалася ситуація, коли можливості і стійкість АІС НП визначаються показниками якості програмних засобів у більшому ступені в порівнянні з апаратними засобами. Програмне забезпечення стає джерелом уразливості сучасних спеціалізованих систем НП, а використання програмних засобів у складі систем управління і зв'язку, а також інших критичних систем породжує нову проблему – забезпечення цільової якості програмних засобів.

Якість СМПЗ в загальному випадку визначається сукупністю властивостей (практичність, здатність до супроводу, надійність, здатність до переміщення, ефективність та функціональність), що обумовлюють його придатність задовольняти визначені потреби відповідно до призначення. Причому ці властивості виявляються на всіх стадіях життєвого циклу – від технічного завдання до експлуатації та супроводу.

Математичне моделювання, як засіб прогнозу результатів прийнятих управлінських рішень, сьогодні широко застосовується в практиці роботи

НП.

У той же час застосування моделей стримується відставанням від сучасних вимог методологічних основ моделювання та низькою організацією забезпечення необхідного рівня якості програмного забезпечення. Для розробки та обґрунтування методології створення СМПЗ АІС НП та забезпечення його цільової якості необхідно, перш за все, створити стандартну модель якості СМПЗ АІС НП у вигляді сукупності характеристик і зв'язків між ними. Але існує велика кількість різнорідних класів СМПЗ АІС НП і застосування однієї моделі якості в різних проектах в явному вигляді не уявляється можливим. Для засобів документування, наприклад, більш важливими будуть такі характеристики, як зрозумілість, вивчаємість, зручність інтерфейсу користувача і зовсім некритичними будуть такі важливі характеристики, як гнучкість, коректність, надійність, ефективність та ін. З іншого боку, моделі для вирішення завдань оперативного управління вимагають обов'язкової наявності властивостей несуперечливості, завадостійкості, стійкості функціонування, точності розрахунків та ін.

Тому специфіка спеціального математичного і програмного забезпечення АІС НП вимагає проведення його класифікації та чіткого ранжирування його характеристик якості за важливістю відповідно до класів для гарантування якісного виконання ним завдань за функціональним призначенням.

Насамперед класифікація СМПЗ АІС НП повинна базуватися на аналізі ризику його недостатньої якості і можливих збитків від проявлення прихованих помилок при його функціонуванні.

За мірою відповідальності функцій, що виконуються, СМПЗ АІС НП можливо поділити на три групи [7]: 1) критичне; 2) важливе; 3) ординарне.

*Критичне* – СМПЗ АІС НП, для якого потрібна особливо висока якість функціонування, оскільки помилки можуть призвести до катастрофічних наслідків, псування цінного обладнання або загрожувати життю та здоров'ю людей. *Важливе* – СМПЗ АІС НП, яке повинно мати досить високу якість функціонування. Економічний та моральний збиток від помилок в ньому може бути великим, але катастрофічні наслідки від їх прояву неможливі. *Ординарне* – СМПЗ АІС НП, недоліки в якому не загрожують користувачам великими збитками. Воно є найбільш масовим та поширеним, його якість та області застосування змінюються у широких межах.

Крім того, за призначенням СМПЗ АІС НП можливо поділити на загальне і спеціальне. До *спеціального* відносяться розрахункові задачі і моделі, що реалізують математичні методи забезпечення процесів планування і ухвалення рішення по управлінню об'єктами (процесами). З*агальне* програмне забезпечення призначене для реалізації функціональних задач АІС НП, серед яких можна виділити дві основні: організацію інформаційного процесу і організацію обчислювального процесу.

Нові інформаційні підсистеми системи ІПНП можна класифікувати:

– *за призначенням*: 1) оперативні (облік осіб і їх характеристик; облік подій; облік предметів та речей); 2) експертно-криміналістичні; 3) статистичні та аналітичні; 4) адміністративні (управлінські) та загальні;

– з*а ступенем централізації оброблення інформації*: централізовані та децентралізовані;

– *за ступенем автоматизації процесів управління*: інформаційно-пошукові, інформаційно-довідкові, інформаційно-управляючі системи, інтелектуальні інформаційні системи тощо.

Інформаційні системи можна ще поділити на такі основні класи [8]:

1. *Інформаційно-пошукові системи* – призначені для збору, збереження, обробки і видачі інформації, представленої у виді електронних документів.

2. *Системи електронного документообігу* – використовуються в комп'ютерних мережах і орієнтовані на забезпечення підготовки, оформлення, реєстрації, передачі, прийому електронних документів.

3. *Системи підтримки прийняття рішень* – це інтелектуальні системи, що призначені для видачі експертних рішень щодо окремих виробничих ситуацій, які основані на використанні математичних моделей та алгоритмів і призначені для вирішення задач планування, прогнозування, тощо.

4. *Геоінформаційні системи* – передбачають прив'язку до карти місцевості БД по об'єктам, які розташовані на відповідній території.

5. *Системи обробки інформації* – орієнтовані на накопичення, зберігання, обробку і видачу інформації, що представлена у виді структурованих записів у комп'ютерних базах даних. Це найбільш поширений клас ІС.

Єдину характеристику таких ІС подати неможливо, бо дуже різноманітні системи та об'єкти, де вони використовуються. Але існують два терміни, актуальні для будь-якої предметної галузі, – «корпоративна ІС» та «автоматизоване робоче місце». Загалом можна визначити, що корпоративна інформаційна система – це ІС масштабу підприємства (організації), яка характеризується здатністю працювати в розподіленій структурі (корпорації) із множиною територіально розосереджених філій, а також повнофункціональністю. Її призначення – підвищувати продуктивність праці робітників та попереджувати технічні помилки й невідповідності, які можуть виникати через великий обсяг оброблюваної інформації. Основною ознакою таких систем є прогнозованість запитів на оброблення інформації.

Базовим структурним елементом таких систем є АРМ – це програмно-технічний комплекс, призначений для автоматизації діяльності певного виду. Основною характеристикою АРМ є орієнтація на людину, яка не має професійної підготовки з використання обчислювальної техніки, але професійно обізнана у конкретній предметній галузі. Залежно від категорії працівників організаційного управління, а також відповідно до характеру розв'язуваних задач розглядають три класи типових АРМ:

1. *АРМ керівника*, який складається з підсистем забезпечення ділової діяльності (електронний записник, особистий архів, картотека доручень і т. ін.), прийняття рішень, рутинних робіт та комунікацій.

2. *АРМ спеціаліста*. Основою такого АРМ є підсистема забезпечення професійної діяльності, яка звичайно містить розвинену БД, засоби електронного обчислення форм і ділової графіки, а також набір програмних засобів для проведення математичних розрахунків і моделювання.

3. *АРМ технічного та допоміжного персоналу*. Основні функції, що автоматизуються, – це введення інформації, оформлення документів, ведення картотек і архівів, оброблення вхідної та вихідної документації, контроль виконавчої діяльності. Можливий масовий випуск типових АРМ цієї категорії.

Під час створення нових інформаційних підсистем системи ІПНП необхідно також враховувати таке поняття, як *життєвий цикл ІС* – це період часу, що починається з визначення вимог до неї з боку користувачів і закінчується її експлуатацією, та який складається з наступних стадій:

1. *Формулювання та аналіз вимог користувача* – визначаються й аналізуються вимоги до ІС; виконується дослідження існуючої системи керування об'єкта автоматизації; розробляється техніко-економічне обґрунтування ІС і технічне завдання; визначається перелік функцій ІС.

2. *Проектування* – виконуються розробка структури системи БД, розробляються алгоритми по обробці інформації.

3. *Впровадження і реалізація* – виконується матеріалізація проекту – перенос його на машинні носії; виробляється первісне уведення вихідних даних, виконання контрольних прикладів та опитна експлуатація системи.

4. *Експлуатація і супровід* – з боку розроблювача виконується супровід системи: пошук і виправлення помилок; додавання нових функцій і модифікація існуючих; оптимізація показників продуктивності.

У випадку придбання системи готової програми на робочому місці користувача виконується тільки впровадження системи і її експлуатація.

1. Про Національну поліцію: Закон України від 02 липня 2015 р. № 580-VIII. Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/580-19.

2. Про затвердження Положення про Національну поліцію: Постанова Кабінету Міністрів України від 28 жовтня 2015 р. № 877. Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/877-2015-%D0%BF.

3. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України»: Наказ МВС України від 03 серпня 2017 року № 676.

4. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05 липня 1994 р. № 80/94-ВР. Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

5. Кудінов В. А., Орлов Ю. Ю., Пакриш О. Є. Інформаційні технології в діяльності Національної поліції: навч. посіб. Київ, 2017. 100 с.

6. Кудінов В. А., Смаглюк В. М., Хахановський В. Г. Інформаційне забезпечення ОВС: навч. посіб. Київ, 2015. 108 с.

7. Duke E.L. V&V of flight and mission-critical software // IEEE Software. – 1989. – № 5.

8. Уведення в інформаційні системи [Електронний ресурс]. – Режим доступу: http://shkolniktut.ru/uchitelyam/lektsii-informatsii-ni-sistemi-i-tehnologii-obliku-ukr/?singlepage=1.

**Лаврушина Олена Сергіївна**
студентка юридичного факультету
Дніпропетровського державного
університету внутрішніх справ

Науковий керівник:
**Гавриш Олег Степанович**
викладач кафедри економічної
та інформаційної безпеки

# ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС: ПЕРЕВАГИ ТА НЕДОЛІКИ

З розвитком світових технологій, окрім «живого» підпису, виник і електронний підпис, який став обов'язковий реквізит електронного документа, що дозволяє ідентифікувати його автора.

Електронно-цифровий підпис — це данні, які отримані за допомогою криптографічного перетворення вмісту електронного документа, що дає змогу підтвердити цілісність документа й ідентифікувати особу, котра підписала цей документ.[2] Якщо простіше, то ЕЦП –це певний перелік цифр та знаків, зашифрованих у спеціальному коді.

Метою даної статті є розгляд переваг та недоліків використання та регулювання законодавством України електронного цифрового підпису (ЕЦП).

Питаннями проблем електронного документообігу, юридичної обґрунтованості електронних документів, захисту електронних документів займалися такі вченні, як Бутинець Ф.Ф., Завгородній В.П., Коцупатрий М..М., Кропивко М.Ф., Івахненков С.В. тощо.

Думки стосовно ЕЦП розділяються: прихильники даного підпису, стверджують, що він покликаний узаконити правочини здійснені на відстані, чим значно зекономити час і обсяг паперової документації, інші ж твердо стоять на думці, що власноручний підпис неможливо замінити жодним аналогом.

Перший нормативний акт щодо ЕЦП прийнято в Україні у 2002 р. – це стандарт ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння". Згодом в Україні прийнято закони: "Про електронні документи та електронний документообіг" та "Про електронний цифровий підпис". Згідно з чим, ЕЦП за правовим статусом прирівнюється до власноручного підпису або до «мокрої» печатки у разі, якщо: електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису; під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису; особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті, який виданий в Україні.[2]

Підробка ЕЦП зводиться до нуля, засоби, які використовуються для роботи, проходять експертизу та сертифікацію в Департаменті спеціальних

телекомунікацій системи СБУ, що гарантує неможливість умисного злому та підробки ЕЦП. [1]

Електронний цифровий підпис широко використовується в господарському обороті. На сьогодні банки України ефективно використовують ЕЦП для здійснення операцій шляхом пересилки банківських електронних документів по корпоративних та інших телекомунікаційних мережах. Закони України прирівнюють за юридичною силою електронні документи, підписані ЕЦП, до документів за власноручним підписом або печаткою, це дозволяє здійснювати юридично значущі дії шляхом електронного документообігу. Це одна з переваг впровадження ЕЦП, оскільки даний різновид електронного підпису використовується багатьма розвиненими країнами світу і це значно скорочує об'єм паперової роботи та пришвидшує результат.

Проте є вагомий мінус, законодавство України передбачає декілька умов, за яких ЕЦП може прирівнюватись до власноручного, усі вони вимагають посиленого сертифіката, який міжнародним законодавством не визначений. З цього випливає, що при використанні ЕЦП для здійснення правочинів між юридичними чи фізичними особами, в яких одна сторона знаходиться за межами України, будуть виникати розбіжності, оскільки такий підпис зберігається на окремому носії (наприклад, на флеш-карті), його можна загубити, викрасти та відповідно зробити певні дії на користь третіх осіб без реальної згоди особи, на відміну від підпису, який здійснюється власноручно і є невідокремленим від людини.

Отже, електронний цифровий підпис спрямований на спрощення та прискорення документообігу між суб'єктами господарювання, що, в свою чергу, має зміцнити конкурентоспроможність вітчизняних підприємств. В Україні існує законодавча база ЕЦП, створена Національна система електронного цифрового підпису та функціонують органи, які надають користувачам послуги ЕЦП. Електронний документ має більше переваг, ніж недоліків. У розбудові системи електронних платежів та електронної торгівлі Україна не може обійтися без цього, тому що ця система дозволяє звільнити масу дорогоцінного часу, який працівники різних організацій витрачають на зволікання з паперами. Проте на нашу думку, потрібно узгодити норми українського та міжнародного законодавства щодо надання ЕЦП такої ж юридичної сили, як у власноручного підпису.

---

1. Закон України "Про електронні документи та електронний документообіг" № 851-IV від 22.05.2003 [Електронний ресурс] / Офіційний сайт Верховної ради України. — Режим доступу : http://zakon.rada.gov.ua/ cgibin/laws/main.cgi?nreg=851-15

2. Закон України "Про електронний цифровий підпис" № 852-IV від 22.05.2003 [Електронний ресурс] / Офіційний сайт Верховної ради України. — Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=852-15

**Махницький Олександр Васильович**
старший викладач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

## РОЗПОВСЮДЖЕННЯ НАРКОТИЧНИХ РЕЧОВИН ЗА ДОПОМОГОЮ МЕСЕНДЖЕРІВ

На сучасному етапі розвитку цифрового суспільства нашої країни мабуть складно знайти людину у якої б був відсутній мобільний номер телефону. Технічний прогрес не стоїть на місці і можливості телефонних апаратів все зручніше і за своїми можливостями наближаються до можливостей персонального комп'ютера. Окрему увагу треба приділити так званим месенджерам які можна встановлювати на смартфони. Мова йде про такі месенджери як Viber, WhatsApp та Telegram. Головне призначення будь-якої програми месенджера залишається одне - це передача миттєвих повідомлень, причому формат повідомлень може бути будь-який. Це може бути текст може бути фото, може бути відео чи аудіо файл.

З впровадженням в нашій країні стандарту передачі даних 4G також актуальним стає питання про вчинення відеодзвінків через месенджери, що набагато розширює можливості телефону. Основною особливістю більшості програм месенджерів є те що вся інформація або розмови, що ведуться через месенджер піддаються шифруванню. Тобто забезпечується так званий принцип анонимності. Дуже корисна функція для абонентів у якій на жаль є зворотня сторона. Якщо абонент вирішить чинити протиправні дії, то встановити його особистість практично неможливо. До протиправних дій можна віднести продаж наркотичних речовин через месенджери. А безконтрольне розповсюдження психотропних та наркотичних речовин є чималою проблемою для правоохоронних органів. А тепер про це трохи докладніше.

Сервіс, створений колишнім власником мережі "ВКонтакте" Павлом Дуровим, наразі розташований в Швейцарії. Саме там знаходяться, за інформацією з відкритих джерел, і сервери цієї програми. Доступ до яких в компанії спецслужбам намагаються не давати. Саме тому наразі вуличне розповсюдження наркотиків йде саме через цей сервіс.

Як це працює. Як що хтось вирішив придбати наркотичні речовини, йому не потрібно особисто шукати розповсюджувачів "зілля", виходити з ними на зв'язок, домовлятися про зустріч. Досить зайти на вказаний прямо на стіні анонімний канал Telegram (месенджер для смартфонів) або спеціалізований сайт, зробити замовлення, оплатити на банківську картку або поповнити рахунок телефону. Після цього клієнту надсилають фото "закладки" — місця, де на вулиці захований пакет з наркотиками. Залишається лише підібрати його.

Процес купівлі-продажу відбувається “засекречено” і називається “кла-

дом". Ще до анонсу, "бізнесмени" у різних районах міст закопують у дворах і парках свій «товар» в землю. Далі вони запускають оголошення і інформацію про те, яким чином здійснити оплату. Коли покупець переводить гроші на рахунок, йому надсилають в той самий Telegram координати точки, геолокацію, де саме треба копнути, щоб віднайти свою «покупку». Така собі «гра» для дітей, а водночас - відсутність прямого контакту з покупцем, що дозволяє бути невловимими: як упіймати наркоторговця на місці злочину?

Чому ж правоохоронні органи не вистежать перекази грошей? І тут злочинці перестрахувались! Судячи з групи в Telegram, оплата приймається лише через термінали iBox в криптовалюті — біткойнах. А це, як відомо, найбезпечніший спосіб оплати — хай навіть знайдуть номери електронних гаманців наркодилерів — ідентифікувати їх правоохоронні органи все-одно не зможуть.

Онлайн-торговці ховаються за анонімними ніками. Вирахувати їх важко. Вони активізувалися останнім часом. У 2016 році МВС зафіксувало 1,9 тис. фактів збуту наркотиків, а за 10 місяців 2017-го — 3,6 тис. І якщо раніше наркопродажами в Мережі займалося 26 груп, то нині поліцейські розкрили 108 подібних структур. Багато з них є частиною міжнародних угруповань. Тому що майже всі синтетичні наркотики – так звані солі, спайс та інше – поставляються в Україну з Азії

Отже, як свідчить статистика Нацполіції, наркотична лихоманка поширюється серед дітей катастрофічними темпами. Сучасних підлітків, які виросли у еру нових технологій, важче здивувати, затягнути у наркотичну пастку звичайними методами, тому зловмисники намагаються зіграти на психології підлітка, який прагне пригод, ігор і це, як бачимо, їм вдається. Відтак зараз як ніколи мають бити на сполох соціальні служби, поліція й інші інстанції, а також батьки з педагогами, аби не дати знахабнілим торговцям смертю згубити ще більше дитячих життів.

Правоохоронці, якщо судити за офіційною статистикою, старанно борються з наркодилерами. За минулий рік вони, наприклад, вилучили 15 кг "синтетики", в цьому — ще 3 кг. А в цілому поліція конфіскувала цілих 3,4 т різних наркозасобів.

Саме подібна статистика насторожує. Поліція в основному вилучає марихуану, яка росте повсюдно. При цьому важкі наркотики і "синтетика", як правило, залишаються поза зоною уваги МВС. Так складається тому, що поліція і рада б активніше розробляти тему нових синтезованих речовин, але у неї немає виписаної інструкції про те, хто і як повинен їх визначати і заносити в список заборонених. Зараз відповідний документ лише узгоджують три відомства — МВС, МОЗ та Мін'юст.

За даними незалежних експертів, від наркоманії та пов'язаних з нею хвороб щорічно в країні гине близько 120 тис. осіб. Офіційної статистики по цій темі немає: лікарі в подібних випадках в діагнозі ставлять безпосередню причину смерті — наприклад, зупинку серця.

Управління ООН з наркотиків та злочинності обрало Україну серед 24 країн, що потребують першочергової допомоги через високий рівень вжи-

вання ін'єкційних наркотиків та поширеність ВІЛ серед тих, хто їх вживає.

Роблячи висновок із такої сумної статистики вкрай необхідно якомога швидше розробляти технічні засоби боротьби із розповсюдженням наркотичних речовин. Та на сам перед потрібно отримати міцний юридичний фундамент, спираючись на який працівники кіберполіції зможуть діяти вкрай ефективно в межах своєї компетенції.

_____

1. https://espreso.tv/article/2017/10/23/soli_narkotyky
2. https://www.unian.ua/society/2246464-sil-i-spaysi-na-kojnomu-rozi-v-ukrajini-vse-chastishe-narkotiki-prodayut-cherez-internet.html
3. https://nv.ua/ukr/ukraine/events/soli-u-vilnomu-dostupi-u-velikih-mistah-ukrajini-narkotorgivlja-peremistilasja-v-efiri-2212899.html

**Мельковський Олександр Вікторович**
к.ю.н., доцент кафедри кримінального
права та правосуддя Запорізького
національного університету

## ЗАБЕЗПЕЧЕННЯ ВНУТРІШНЬОЇ БЕЗПЕКИ У СИСТЕМІ МВС УКРАЇНИ. ПРІОРИТЕТИ РОЗВИТКУ

Теоретичні розробки у галузі дослідження проблем внутрішньої безпеки у системі МВС та Національної поліції України на сучасному етапі ведуться не досить активно, через що виникає потреба в їх динамічному розвитку.

На нашу думку на теперішній час залишаються актуальними питання щодо:

- удосконалення нормативного регулювання діяльності підрозділів служби внутрішньої безпеки (далі СВБ) та здійснення ними оперативно-розшукової діяльності (далі ОРД) з метою запобігання злочинам та виявлення корупційних проявів;
- відсутності науково обґрунтованої характеристики злочинів та корупції працівників системи МВС;
- визначення індикаторів проявів корупційної діяльності працівників системи МВС;
- розробки організаційно-тактичної моделі запобіжної діяльності СВБ;
- визначення оперативно-розшукових ознак злочинної діяльності на користь організованих злочинних угрупувань (далі ОЗУ) та розробки методичних рекомендацій щодо здійснення контррозвідувальної діяльності відносно впливу ОЗУ на діяльність конкретних працівників та підрозділів ОВС;
- розробки загальних основ формування агентурної мережі для вирішення завдань підрозділів СВБ;
- розробки методичних рекомендацій щодо використання оперативно-розшукових заходів (далі ОРЗ) з метою запобігання злочинам та корупції

підрозділами СВБ з урахуванням положень новітнього КПК;

- надання науково-обгрунтованих рекомендацій з питань підвищення рівня оперативної готовності персоналу СВБ для вирішення завдань запобіжної діяльності;

- розробки у межах системи правоохоронних органів порядку взаємодії служб внутрішньої та особистої безпеки з метою вирішення завдань запобігання злочинам та фактів корупції серед діючого персоналу.

Ми вважаємо за необхідне визначити пріоритетним напрямком діяльності підрозділів внутрішньої безпеки використання ОРЗ та методів ОРД для вирішення основних завдань служби, якими є запобігання злочинам та правопорушенням в структурі МВС та Національної поліції України.

З метою конкретизації вектору впливу для підрозділів СВБ слід визначити складові елементи оперативно-розшукової характеристики злочинів та корупційної діяльності серед працівників системи МВС України:

1. Причини, умови та особливості оперативно-розшукових ознак злочинів та корупційної діяльності в цілому – причини, умови, особливості типових місць та час учинення злочину, особливості об`єкта посягання та суспільно-небезпечних наслідків, інші ознаки діяння.

2. Особливості оперативно-розшукових ознак способів підготовки, учинення, маскування злочину, типових дій щодо здійснення корупційних діянь на користь конкретних осіб та ОЗУ.

3. Пошукові ознаки предмета злочинних посягань та корупційних проявів.

4. Оперативно-розшукові ознаки особистості та поведінки працівників поліції до і після вчинення злочину і способи протидії запобіжній діяльності підрозділів СВБ.

5. Пошукові ознаки корупційної активності (індикатори корупції) працівників поліції.

Вважаємо, що до основних загроз нормальному функціонуванню системи МВС та Національної поліції України слід віднести:

- протиправну діяльність діючих працівників під час виконання своїх професійних обов’язків;

- здійснення розвідувальної діяльності в підрозділах системи МВС та Національної поліції представниками злочинного середовища з метою протидії діяльності оперативних підрозділів спрямованої на виявлення та припинення протиправних проявів, передусім ОЗУ;

- тиск злочинного середовища на діючих працівників, їх близьких, з метою впливу на їх професійну діяльність в інтересах злочинців;

- корупційні діяння працівників системи МВС та Національної поліції;

- інші негативні фактори зовнішнього впливу які існують у сучасному суспільстві.

Нейтралізація зазначених загроз повинна бути основним напрямком запобіжної діяльності підрозділів СВБ.

У сучасних умовах одним з пріоритетних напрямків діяльності СВБ є забезпечення економічної безпеки системи МВС України. У процесі даної

діяльності необхідно зосередити увагу на обов'язковій перевірці суб'єктів економічної діяльності, порядку, умов та змісту нормативних актів і угод між МВС та іншими державними і комерційними структурами, здійснення їх антикорупційного дослідження і оцінки. Крім того, слід впровадити обов'язкову перевірку як юридичних так і фізичних осіб, які мають договірні економічні відносини та взаємодіють з МВС, надають послуги і благодійну допомогу. Такі перевірки необхідно здійснювати з використанням усіх можливостей ОРД, оперативних та оперативно-технічних підрозділів, а також оперативно-інформаційних обліків як МВС, так і інших правоохоронних органів.

На наш погляд, одним із складових чинників діяльності щодо захисту інтересів системи МВС та Національної поліції зокрема, повинні бути законодавчо закріплені дії підрозділів внутрішньої безпеки із захисту суб'єктів системи (працівників поліції) від негативного впливу кримінальних структур.

Забезпечення внутрішньої безпеки в системі МВС передбачає визначення не тільки характеру (напрямку) діяльності, а й цілі та результатів цієї діяльності, яким має бути об'єктивний стан захищеності інтересів відомства та відповідно правопорядку й законності у суспільстві, а також розуміння працівниками своєї реальної захищеності.

На нашу думку, законодавче закріплення за підрозділами СВБ функції попередження і запобігання можливим протиправним діям з боку діючих працівників є досить перспективним. Цей напрямок є провідним в їх службовій діяльності, оскільки у разі належного виконання цієї функції кадровий потенціал всієї системи якісно покращиться, а це позитивно сприятиме іміджу всієї системи МВС та Національної поліції України.

Під категорією ,,забезпечення внутрішньої безпеки в системі МВС" необхідно розуміти систему правових, організаційних, кадрових, інформаційних та інших заходів які вживаються (реалізуються) спеціальними суб'єктами - підрозділами внутрішньої безпеки.

Ураховуючи зазначене, слід визначити поняття забезпечення внутрішньої безпеки підрозділами СВБ, як засновану на принципах комплексного програмування та планування діяльності спеціальних суб'єктів, які повинні мати за мету досягнення такого рівня захищеності життєво важливих інтересів системи МВС та Національної поліції, який відповідає основним критеріям безпеки в сучасних умовах розвитку правоохоронних органів нашої держави.

На підставі багаторічного практичного досвіду роботи в підрозділах внутрішньої безпеки автор вважає, що в словосполученні ,,внутрішня безпека" провідним (ключовим) та таким, що визначає глибинну сутність діяльності даної служби, має стати слово ,,внутрішня".

Це твердження ґрунтується на специфічних особливостях діяльності такої силової структури, як система МВС, та пов'язано передусім з важливістю завдань, які висуваються перед цією правоохоронною системою та складними умовами у яких ці завдання виконуються.

Слід зазначити, що будь яка система, незалежно від напрямку діяльно-

сті, у процесі свого розвитку завжди прагне до самоочищення та досконалості. У зв'язку з цим, під час розробки та подальшої реалізації відповідних цільових заходів обов'язково слід здійснювати об'єктивний аналіз щодо їх (заходів) доцільності та наявності перспективи отримання позитивного результату для всієї системи взагалі.

Як у побутовому житті, так і у функціонуванні будь-якої системи доречніше вирішувати внутрішні (особисті) проблеми самотужки, спираючись на власний потенціал, оскільки будь-яка проблема, яку суб'єкт (система) вирішує самостійно, додає авторитету, додаткових сил та впевненості самому суб'єкту, чим і сприяє загальному його розвитку.

На підставі аналізу досвіду діяльності правоохоронних органів деяких країн Європейського Союзу (наприклад Німеччина, Англія) вважаємо, що має право на існування ідея щодо відносної інформаційної стриманості при висвітлені деяких особливих проблем системи МВС та Національної поліції. Метою застосування запропонованих нами обмежуючих принципів є формування загального позитивного іміджу всієї системи МВС України шляхом самоочищення силами самої системи. У нашому випадку такі дії повинні виконуватися передусім силами підрозділів СВБ.

Таким чином, головною сутністю діяльності підрозділів СВБ є попередження та усунення будь-яких внутрішніх і зовнішніх загроз як для всієї системи МВС України так і для її суб'єктів. Кінцевою метою цієї діяльності є забезпечення безпеки всієї системи.

**Мирошниченко Володимир Олексійович**
к.т.н., доц., доцент кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

## СТОСОВНО ТЕХНІЧНИХ РІШЕНЬ ДЛЯ АВТОМАТИЧНОЇ ВІДЕОФІКСАЦІЇ ПОРУШЕНЬ ПРАВИЛ ДОРОЖНЬОГО РУХУ

Такі системи діють в європейських країнах і є ефективним засобом в боротьбі за безпеку дорожнього руху, а також попереджають прояви корупції при виписуванні штрафів і підвищують результативність роботи органів контролю за дорожнім рухом. Розглянемо типові завдання, які необхідно вирішувати за допомогою систем відеоаналізу транспортних потоків і існуючі проблеми при їх використанні.

Відеоконтроль дорожнього руху в загальному вигляді, включає пов'язані між собою завдання детектування за допомогою алгоритмів відеоаналізу порушення транспортним засобом правил дорожнього руху і розпізнавання державного реєстраційного знака автомобіля порушника. Попутно корисно

мати і можливість розпізнавання номерів всіх проїжджаючих автомобілів для автоматичного порівняння їх з базою даних викрадених або розшукованих автомобілів. Інша корисна можливість, яка може бути реалізована в системі телеавтоматичного контролю, - аналіз статистики транспортного потоку (підрахунок кількості машин, що проїжджають в одиницю часу, обчислення щільності і середньої швидкості потоку). Крім того, подібні системи відеоспостереження дозволять визначати винуватців та свідків ДТП, а також контролювати швидкісний режим автомобілів, що рухаються у дозволених межах швидкості.

Практично передбачається два основних варіанти застосування камер відеоспостереження, які потребують різних технічних рішень, - на прямому відрізку швидкісної ділянки дороги і на перехрестях. Основне завдання відеоконтролю на прямій ділянці дороги - детектування перевищення швидкості і розпізнавання номера автомобіля. На сьогоднішній день існує практика використання стаціонарних аналогових камер відеоспостереження, які встановлюються на так звану П-образну опору по одній камері на кожну смугу руху. Камери спрямовані фронтально на автомобілі, що наближаються або віддаляються. У такого підходу є дві серйозні проблеми, пов'язані з маленькими розмірами зони контролю традиційних аналогових камер: автомобілі, що рухаються між смуг руху по дорожній розмітці, не потрапляють в поле зору жодної з камер. При цьому зона вимірювання швидкості радаром не збігається з зоною розпізнавання номера, тому якщо машина пересувається з однієї смуги в іншу, то система неправильно визначає номер або взагалі не може визначити номер транспортного засобу порушника. Альтернативой використання аналогових камер може бути застосування цифрових камер, які за своїми технічними характеристиками дозволяють захоплювати кілька смуг руху одночасно і отримувати зображення і номерів автомобілів з вищою в кілька разів роздільною здатністю в порівнянні з аналоговими камерами. Така камера може одночасно захоплювати дві смуги руху і таким чином з'являється можливість використання двох доплеровских радарів. Після появи в поле зору відеокамери автомобіля, система дає команду радару на вимірювання швидкості. Зона, в якій відбуваються захоплення і розпізнавання номера автомобіля, приблизно 25 м. За цих умов максимальна швидкість, при якій система може розпізнати номер транспортного засобу, близько 140 км/год., що при сучасних швидкісних можливостях автомобілів є ще однією технічною проблемою.

Основне завдання системи відеоконтролю на перехресті - фіксація проїзду на червоний сигнал світлофору і розпізнавання номера автомобіля порушника. Кожна проїжджа частина, яка примикає до перехрестя, повинна контролюватися своєю відеокамерою або групою відеокамер. При цьому в деяких випадках, можливо, будуть потрібні окремі камери для розпізнавання номерів на під'їзді автомобілів до перехрестя. Це пов'язано з тим, що для чіткого розпізнавання державного номера граничний кут установки цифрової камери у вертикальній площині не повинен перевищувати 20°, а в горизонтальній - 30°. У той же час для фіксації порушень правил дорожнього руху на

перетині доріг, таких як проїзд на заборонений сигнал світлофора, розворот в недозволеному місці, перетин подвійної суцільної лінії і т.д., потрібна установка камер безпосередньо над перехрестям. Крім того, для контролю проїзду на червоний сигнал світлофора потрібна інтеграція з контролером світлофора.

Певну складність представляє використання системи відеоконтролю в нічний час. У традиційних системах відеоспостереження ця проблема вирішується установкою прожекторів, які працюють у видимому діапазоні. У такого підходу є 2 істотних недоліка: зустрічне світло сліпить водіїв, і система контролю стає потенційним джерелом нових ДТП, і, крім того, прожектори споживають велику потужність, що створює складності при підключенні системи і підвищує вартість її експлуатації. Для забезпечення цілодобового контролю дорожнього руху доцільно використовувати інфрачервоні моделі камер. Для забезпечення роботи в темний час доби доцільно встановлювати спеціалізовані стробовані інфрачервоні прожектори і синхронізувати їх з камерами. Завдяки високій чутливості камер і стробуючого режиму роботи прожекторів істотно знижується споживана електрична потужність, крім того, прожектори працюють в ближньому інфрачервоному діапазоні і не створюють перешкод для водіїв. Якщо крім розпізнавання номера і марки машини потрібно визначати її колір, то на додаток до інфрачервоним камерам ставиться звичайна кольорова аналогова камера високої чутливості. Таку камеру доцільно використовувати як оглядову, зображення з цієї камери може транслюватися в центр спостереження для візуального контролю обстановки і записуватися в архів довготривалого зберігання. Це особливо корисно для розбору спірних ситуацій, так як в цьому випадку крім фотографій, зроблених цифровими камерами високої роздільної здатності, в системі зберігається відеоролик, що дозволяє простежити всю динаміку порушення.

Ще однією проблемою практичного використання системи відеофіксації порушень правил дорожнього руху і відеоконтролю за транспортним потоком є забезпечення надійної і безвідмовної роботи електронної апаратури в жорстких вуличних кліматичних умовах на протязі всього календарного року.

Юридичною проблемою (і технічною також) є ідентифікація самого водія транспортного засобу. Однак розгляд цієї проблеми виходить за рамки даного питання і може вирішуватися використанням відповідних для цієї мети систем біоідентіфікаціі особи.

В якості підсумкової тези хотілося б відзначити, що впровадження подібних систем є вкрай актуальною, але вимагає комплексного вирішення низки технічних проблем і відповідних фінансових вкладень, які помітно перевищують вартість звичайних широко розповсюджених охоронних систем відеоспостереження.

**Момот Тетяна Валеріївна**
д.е.н., проф., завідувач кафедри
фінансово-економічної безпеки,
обліку і аудиту

**Ващенко Олександр Миколайович**
к.е.н., доц., доцент кафедри
фінансово-економічної безпеки,
обліку і аудиту

**Тесленко Роман Юрійович**
аспірант Харківського національного
університету міського господарства
імені О. М. Бекетова

# МІЖНАРОДНІ СТАНДАРТИ І РЕКОМЕНДАЦІЇ З ПРОТИДІЇ КОРУПЦІЇ У ПРИВАТНОМУ СЕКТОРІ ЕКОНОМІКИ

Через два десятиліття глобальних зусиль щодо боротьби з корупцією цілком очевидно, що запобігання та боротьба з корупцією є головною проблемою для будь-якої країни.

У вересні 2015 року в рамках 70-ї сесії Генеральної Асамблеї ООН у Нью-Йорку відбувся Саміт ООН зі сталого розвитку та прийняття Порядку денного розвитку після 2015 року, на якому було затверджено нові орієнтири розвитку. Підсумковим документом Саміту «Перетворення нашого світу: порядок денний у сфері сталого розвитку до 2030 року» було затверджено 17 Цілей Сталого Розвитку (ЦСР) (Sustainable Development Goals (SDG)) та 169 завдань. Відповідно до «Порядку денного у сфері сталого розвитку до 2030 року» (the UN's Agenda 2030 for Sustainable Development) корупція визнана як суттєва перешкода для досягнення ЦСР, які 193 країн зобов'язалися досягти в рамках цієї амбіційної глобальної програми розвитку. Корупція гальмує економічне зростання, збільшує бідність та сприяє політичній та соціальній нестабільності.

Сучасне визначення корупції охоплює будь-яке зловживання довіреними повноваженнями або владою, включаючи корупцію як в державному секторі, так і в приватному. Данна сфера прояву корупції все частіше стає предметом міжнародних дискусій. Численні урядові та неурядові організації займаються розробкою законів, рекомендацій, вказівок, інструкцій та прийняттям практичних заходів з протидії корупції і зміцнення доброчесності ведення бізнесу.

До головних міжнародних стандартів урядових організацій стосовно приватного сектору економіки відносяться наступні:

– Конвенція ООН проти корупції, яка зобов'язує держав-учасниць вжити заходи щодо попередження корупції в приватному секторі, посилити стандарти бухгалтерського обліку і аудиту, встановити ефективні цивільно-

правові, адміністративні та кримінальні санкції за невиконання антикорупційних вимог;

– Конвенція Ради Європи про кримінальну відповідальність за корупцію і Додатковий протокол – документ містить більш жорсткі зобов'язання у сфері криміналізації підкупу в приватному секторі;

– Конвенція Ради Європи про цивільно-правову відповідальність за корупцію, ключовою особливістю якої є можливість особам, які зазнали збитків внаслідок корупційних діянь, вимагати компенсацію за шкоду, визнання недійсності корупційних контрактів, а також захист працівників, які сумлінно повідомляють про підозри на корупцію;

– Конвенція Організації економічного співробітництва та розвитку (ОЕСР) по боротьбі з підкупом іноземних посадових осіб при здійсненні міжнародних комерційних угод, що вимагає встановлення відповідальності юридичних осіб за підкуп посадової особи іноземної держави та вжиття відповідних заходів;

– правові інструменти Європейського Союзу (Конвенція про захист фінансових інтересів європейських співтовариств; Конвенція проти корупції за участю європейських посадовців або посадових осіб держав-членів Європейського Союзу; Директива Європейського Союзу з питань розкриття нефінансової і різноманітної інформації деякими великими підприємствами і групами тощо);

– національні закони деяких країн, які мають екстериторіальну дію: Закон США «Про боротьбу з корупцією закордоном» (1977 рік) та Закон Великобританії «Про хабарництво» (2010 рік);

– рекомендаційні, пояснювальні і допоміжні матеріали ОЕСР та Ради Європи.

Розглянемо основні напрацювання щодо боротьби з корупцією в приватному секторі економіки у розрізі неурядових організацій.

Міжнародна торгова палата (МТП) стала першопроходьцем у встановленні правил з протидії корупції в приватному секторі, видавши у 1977 році першу редакцію «Правил поведінки для боротьби з вимаганням та хабарництвом». Актуальні на даний час документ МТП, окрім самих правил, надає рекомендації з проведення політики, спрямованої на підтримку дотримання правил по боротьбі з корупцією та ефективність програми корпоративного комплаєнсу [1]. Інші керівні стандарти МТП охоплюють розробку політики щодо подарунків та представницьких витрат, вибір і управління третіми сторонами, відповідальний вибір постачальників (відповідальність за ланцюг поставок), а також діяльність викривачів, які повідомляють про порушення тощо.

Іншим важливим недержавним міжнародним стандартом є «Принципи ведення бізнесу для протидії хабарництву» Transparency International (TI), що вперше опубліковані в 2003 році. Її останній переглянутий варіант був виданий в 2013 році [2]. В документі робиться акцент на безперервній оцінці ризиків, де охоплюється більш широке коло питань, ніж просто хабарництво у вузькому сенсі, а саме: конфлікт інтересів, хабарництво; фінансування полі-

тичних партій, благодійні внески та спонсорська допомога, платежі для спрощення процедур, подарунки, представницькі витрати та оплата витрат.

Всесвітній економічний форум є некомерційним фондом і здійснює керівництво Ініціативою з партнерства проти корупції (PACI), яка була запущена в якості платформи з обміну інформацією між рівноправними партнерами в Давосі 2004 року. В рамках PACI у 2004 році розроблені «Принципи бізнесу з протидії хабарництву», які були оновлені і в 2013 році перейменовані в «Принципи PACI щодо боротьби з корупцією» [3]. Дані принципи супроводжуються інструкціями щодо розробки ефективної програми по боротьбі з корупцією.

Протягом 2013-2016 років Міжнародна організація зі стандартизації (ISO) розробила стандарт антикорупційних систем менеджменту ISO 37001 для організацій приватного і державного секторів економіки. Новий стандарт визначає вимоги та надає рекомендації для встановлення, впровадження, підтримки, перегляду та вдосконалення антикорупційної системи менеджменту.

Докладна характеристика та порівняння більшості антикорупційних інструментів для бізнесу містяться в посібнику ОЕСР, ООН і Світового Банку [5].

Таким чином, глобальне антикорупційне співтовариство надає чимало як основних, так і допоміжних матеріалів нормативного та методичного характеру для розробки заходів з протидії корупції та підвищення доброчесності ведення бізнесу, з яких майже всі можна знайти у відкритому доступі.

_____

1. ICC Rules on Combating Corruption [Електронний ресурс]. – Режим доступу : https://iccwbo.org/publication/icc-rules-on-combating-corruption/

2. Business Principles for Countering Bribery [Електронний ресурс]. – Режим доступу : https://www.transparency.org/whatwedo/publication/business_principles_for_countering_bribery

3. WEF PACI Global Principles for Countering Corruption [Електронний ресурс]. – Режим доступу : http://www3.weforum.org/docs/WEF_PACI_Global_Principles_for_Countering_Corruption.pdf

4. ISO 37001:2016. Anti-bribery Management Systems – Requirements with Guidance for Use [Електронний ресурс]. – Режим доступу : https://www.iso.org/standard/65034.html

5. Anti-Corruption Ethics Compliance Handbook for Business [Електронний ресурс]. – Режим доступу : http://www.oecd.org/corruption/Anti-CorruptionEthicsComplianceHandbook.pdf

**Огліх Валентина Валеріївна**
к.ф.-м.н., доц., доцент кафедри економічної кібернетики Дніпропетровського національного університету імені Олеся Гончара

**Шаповалов Олексій Вікторович**
к.т.н., с.н.с., доцент кафедри товарознавства та митної експертизи Університету митної справи та фінансів

**Білова Наталія Анатоліївна**
д.е.н., проф., завідувач кафедри товарознавства та митної експертизи Університету митної справи та фінансів

# ІМПЛЕМЕНТАЦІЯ ЄДИНОГО СПИСКУ ТОВАРІВ ПОДВІЙНОГО ВИКОРИСТАННЯ ЯК ПРОЛОНГАЦІЯ ЄВРОІНТЕГРАЦІЙНИХ ПРОЦЕСІВ В УКРАЇНІ

Вплив євроінтеграційних процесів на суб'єкта міжнародних економічних відносин проявляється я у відкритті перспектив для розвитку національної економіки. Зокрема позитивні наслідки для України можуть проявитися: у збільшенні темпів економічного зростання та рівня життя населення, зменшення рівня безробіття;, припливі інвестицій та підвищенні конкурентоспроможності національних суб'єктів господарювання внаслідок переходу до нових стандартів товарів (Технічних регламентів відповідності), на нові технології виробництва та управління.

Водночас, посилення міжнародного економічного співробітництва, відкриття кордонів та зняття торгових бар'єрів, активізація експортно-імпортних операцій підживлює негативну складову впливу зовнішніх чинників на митну безпеку України, зокрема маємо зростання кількості суб'єктів, які вчиняють порушення митних правил, зростання обсягів контрабандних товарів, зменшення митних ставок і платежів, які стягуються митними органами тощо.

Митна складова державної політики, реалізація якої покладена на фіскальну службу України є вкрай важлива бо не лише стоїть на захисті економічних інтересів, а забезпечує захищеність від внутрішніх та зовнішніх загроз життєво важливих цінностей, потреб й інтересів окремої людини, населення, підприємства, регіону, держави. Неналежна забезпеченість митної безпеки держави, як наслідок постійних змін у податковому та митному законодавстві, складної фінансово-економічної та політичної ситуації, тіньової економіки та високого рівня корупції, негативно впливає на стан соціально-економічного розвитку країни. Акцентуємо увагу на тому, що митна безпека, як складова економічної безпеки країни, знаходиться під загрозою, а питання

пов’язані з її дослідженням є вкрай актуальними.

Окрема увага має бути приділена такому інструменту зовнішньоекономічної політики держави як експортний контроль. Експортний контроль, є за механізмом досить складною управлінською та техніко-економічною процедурою, ґрунтується на складному поєднанні та суперечності економічних інтересів суб’єктів господарювання та держави.

Хоча на перший погляд експортний контроль як інструмент зовнішньоекономічної політики держави стосується лише обмеженої групи товарів, зокрема міжнародних передач товарів військового призначення, подвійного використання та інших товарів, що не внесені до списків товарів, що підлягають державному експортному контролю та щодо яких відповідно до законодавства можуть бути застосовані процедури державного експортного контролю, а втім він здатен суттєво впливати на конкурентну позицію підприємств, динаміку і показники їх економічної діяльності, а суб’єктів господарювання, на міжнародний авторитет держави, показники зовнішньоекономічної діяльності, міжнародної торгівлі, інвестиційної активності. Експортний контроль, як імперативний інструмент економічної політики держави, не передбачає самостійності у зовнішньоекономічної діяльності суб’єктів господарювання. Тому заборона або обмеження постач окремих товарів може суттєво вплинути на функціонування конкретних суб’єктів. Звертаємо увагу, що негативний вплив на національні інтереси держави можуть здійснити, як жорсткі, так і занадто м’які обмеження у сфері експортного контролю, зокрема мова йде про товари подвійного використання. Складності обумовлені тим, що в процесі проходження митного контролю від особи, яка приймає рішення вимагаються поряд зі знаннями в економічній сфері, вкрай необхідні знання в технічній, біологічній, хімічній. Вона має хоча б частково розумітися в ядерних, ракетних, хімічних технологіях, матеріалознавстві та технологічному обладнанні.

Підготовка таких фахівців проходила за участю спеціалістів США (Аргонська Національна Лабораторія Міністерства енергетики США), Державна служба експортного контролю, Інститут ядерних досліджень НАН України, ННЦ "Харківський фізико-технічний інститут" НАН України, Університету митної справи та фінансів згідно з Міжнародної програми з нерозповсюдження та експортного контролю (International Nonproliferation Export Control Program - INECP), заснованої Національною Адміністрацією з Ядерної Безпеки США (National Nuclear Security Administration - NNSA.

За програмою було опрацьовано та апробовано два варіанту курси «Ідентифікація зброї масового знищення, ядерних матеріалів і товарів подвійного використання» (Weapons of Mass Destruction Commodity Identification Training (WMD-CIT)). Курси застосовані для підготовки студентів і перепідготовки митних інспекторів. Матеріали розроблені в рамках цієї програми були використані для підготовки фахівців інших країн.

На заміну чинним на сьогодні п’яти Спискам товарів подвійного використання, що можуть бути використані у створенні:

– звичайних видів озброєнь, військової чи спеціальної техніки.

- ракетної зброї.
- ядерної зброї.
- хімічної зброї.
- бактеріологічної (біологічної) та токсинної зброї,

Постановою Кабінету Міністрів України від 11.01.2018 № 1 "Про внесення змін до Порядку здійснення державного контролю за міжнародними передачами товарів подвійного використання", затверджених постановою Кабінету Міністрів України від 28 січня 2004 р. № 86, прийнято Єдиний список товарів подвійного використання, який складено на підставі Єдиного списку товарів подвійного використання Європейського Союзу (додаток 1 до Регламенту Ради ЄС № 428/2009 від 05.05.2009).

Імплементація в державну законодавчу базу Єдиного списку дозволить покращити позиції України на світовому ринку, більш ефективно захистити інтереси держави у сфері міжнародних передач товарів.

Зазначимо, усунути бар'єри для українського експорту товарів подвійного використання на внутрішній ринок ЄС внаслідок єдиного нормативного поля у сфері експортного контролю та подальшого узгодження процедур і правил державного експортного контролю України з відповідними нормами та стандартами ЄС вдасться не лише у разі створення якісного законодавчого підґрунтя, нормативно-правових актів з питань державного контролю за міжнародними передачами товарів подвійного використання. Вкрай необхідно підготувати фахівців, які забезпечать належний контроль за міжнародними передачами товарів відповідно до міжнародних зобов'язань і керівних принципів, прийнятих Україною у галузі експортного контролю та національної безпеки.

1. Недобєга О. О. Митна безпека як складова економічної безпеки держави [Електронний ресурс] / О. О. Недобега, М. І. Кулєшина. – Режим доступу : *http://archive.nbuv.gov.ua/e-journals/Nvdu/2013_9/ek/13nooebu_ ua.pdf.*

2. Новосад І. В. Митна безпека як важлива складова економічної безпеки держави [Електронний ресурс] / І. В. Новосад. – Режим доступу : *http://dspace.tneu.edu.ua/bitstream/316497/3758/1/%D0%9D%D0%BE%D0%B2%D0%BE%D1%81%D0%B0%D0%B4%20%D0%86..pdf*

3. Вітер Д. В. Митна політика і стратегія митної безпеки ЄС у контексті спільної Європейської політики безпеки / Д. В. Вітер // Митна безпека. – 2013. – № 1 – 2. – С. 164–169.

4. Постанова КМУ від 28.01.2004 р. № 86 зі змінами "Про затвердження Порядку здійснення державного контролю за міжнародними передачами товарів подвійного використання" – Режим доступу : *http://zakon2.rada.gov.ua/laws/show/86-2004-%D0%BF/paran10#n10*

5. Оглих В. В., Шаповалов А. В. Методические аспекты разработки ресурсов для подготовки и переподготовки государственных служащих // службы / В. В. Огліх, О. В. Шаповалов // Бизнес Информ. – 2011. – №6. – С. 187–188.

6. Огліх В. В. Застосування інформаційних технологій як фактор підвищення якості підготовки та перепідготовки фахівців митної служби / В. В. Огліх, О. В. Шаповалов // Бізнес Інформ. – 2012. - № 7. - С. 221-223. - Режим доступу: http://nbuv.gov.ua/UJRN/binf_2012_7_63.

**Огліх Валентина Валеріївна**
к.ф.-м.н., доц., доцент кафедри економічної кібернетики Дніпропетровського національного університету імені Олеся Гончара

**Шаповалов Олексій Вікторович**
к.т.н., с.н.с., доцент кафедри товарознавства та митної експертизи Університету митної справи та фінансів

# ПРОБЛЕМНІ ТА ОРГАНІЗАЦІЙНІ АСПЕКТИ ІДЕНТИФІКАЦІЇ ТОВАРІВ ЕКСПОРТНОГО КОНТРОЛЮ ЯК СКЛАДОВОЇ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ

Складність та проблемний характер, які притаманні економічному та соціально-політичному стану сучасної України суттєво заважають євроінтеграційному руху країни, реалізації її стратегічних національних пріоритетів. Руйнація та корупційна деформація системи державного управління, втрата частини територій, військові дії, недосконаліть правових основ, відсутність ефективної політики в соціальній царині, суттєві прорахунки, які допущені на початкових етапах реформування економічної, військової, правоохоронної сфери, неприйняття суспільством реформ в системах охорони здоров'я та освіти, пенсійного забезпечення – це маркери які характеризують сьогодення держави. Міжнародні рейтинги наочно демонструють, що економічна ситуація в Україні якісно не покращується, попри на деякі ознаки депресивного зростання. Ознаками країни стають корупція, борги, рейдерство.

На тлі активних зусиль деяких держав, спрямованих на послаблення позицій України в політичній, військовій, економічній та гуманітарній сферах, ігнорування її національних інтересів, євроінтеграційні прагнення були й залишаються нашим стратегічним національним пріоритетом, реалізація якого без економічної та політичної взаємодії з іншими державами, яка не обмежуючі суверенітету істотно зміцнює економічну і державну безпеку, неможлива.

Глибинний характер прорахунків призвів до істотного послаблення економічних засад національної безпеки, яке віддзеркалюється через посилення фінансової та технологічної залежності від інших країн, деградації вітчизняних галузей, які займаються випуском кінцевої продукції, руйнування виробничого потенціалу, відтоку кваліфікованих кадрів за кордон, зростання експорту сировини або продуктів з мінімальним рівнем перероблення тощо. Результати аналізу свідчать про загострення усього комплексу проблем забезпечення національної безпеки, зміни характеру загроз, наявності точки біфуркації в сфері зовнішньоекономічних відносин.

Розвиток євроінтеграційних процесів потребує визначення нових пріоритетів державної митної політики спрямованої на заохочення розвитку на-

ціональної економіки, як фактора, який визначає складову, що регулює контакти з іншими державами в системі експортної діяльності. Тобто потрібно сформулювати чітку систему принципів та напрямів діяльності держави у сфері забезпечення безпеки та економічних інтересів шляхом проведення митно-тарифних та нетарифних заходів регулювання зовнішньої торгівлі.

На перші сходинки досліджень виходить пошук адекватних шляхів удосконалення національних механізмів і процедур контролю, які мають надійно убезпечувати інтереси держави й ефективно виконувати функціональні завдання в сфері митної безпеки. Вплив такого вагомого інструменту державної політики, як митний контроль, на розв'язання питань у політичній, економічній та військовій сферах позиціонує його як складову частину політики національної безпеки держави.

Підвищення ефективності митних процедур, зокрема їх спрощення має базуватися на міжнародному співробітництві Тобто, вдосконалення методів експертизи через поширення передового та узагальнення практичного досвіду в царині дотримання Україною міжнародних норм щодо класифікації і кодування товарів. Встановлення реальної вартості є вкрай важливим, суттєво впливає на економічну складову митної діяльності та значною мірою залежить від вірного визначення коду товару. Тобто незаперечним пріоритетом економічної політики має бути експертиза, яка є дуже важливим елементом в системі економічного розвитку держави, підвищенні її конкурентоспроможності, стимулюванні розвитку вітчизняних підприємств.

Захисті національних інтересів, через призначення експертизи полягає не лише у забезпеченні державної підтримки експорту, зростанні доходів від зовнішньоторговельної діяльності, а й у виявлені фальсифікованих та неякісних товарів, захисті споживачів від підробок та товарів невідомого походження й сумнівного виробництва. Звертаємо увагу, що експертиза також спрямована на попередження та виявлення можливих порушень законодавства в галузі експортного контролю українськими підприємствами, які можуть розглядатися світовою спільнотою як недотримання міжнародних зобов'язань взятих на себе Україною. Ідентифікаційна (товарно-партійна, споживацька, асортиментна; якісна; сортова; спеціальна) експертиза товару під час переміщення через митний кордон України дозволяє встановити відповідність самого товару, інформації про нього задекларованій у вантажно-митній декларації, на упаковці та товарі.

Акцентуємо увагу, що формуючі принципи функціонування митної системи, тобто єдиних митної політики, митної території, митного законодавства, тарифного регулювання і поєднуючи їх з засадами економічної політики, яка ставить на перше місце пріоритетність національних інтересів маємо забезпечити дотримання балансу між політичними та економічними інтересами держави та міжнародними зобов'язаннями та принципами.

У цьому контексті слід розрізняти традиційну контрабанду, яку вирізняють протизаконні матеріали або контрабанда, картельні поставки, організована злочинність, приховування та повторювання при постачаннях, мережі розповсюджувачів, продажі на комерційному ринку, «відмивання» грошей

від поставок для розповсюдження.

В частині дотримання міжнародних зобов'язань щодо розповсюдження результативність системи митного контролю має досягатися через поєднання механізмів сприяння українським підприємствам в їх функціонуванні на ринку озброєнь, яке є достатньо вагомим джерелом доходів держави та сприяння діяльності в сфері державного контролю за міжнародними передачами товарів військового призначення та товарів подвійного використання.

Складність полягає у тому, що постачі для розповсюдження проводяться комерційними постачальниками. Мова йде про законні комерційні товари подвійного використання, які зазвичай надсилаються у відкритий спосіб, в рамках нетипових транзакцій в мережах закупівель. Хоча в деякий момент відбувається перемикання з комерційного ринку на підставні брокерські компанії та на «підпільного» кінцевого користувача, які мають бути індикаторами небезпеки незаконної діяльності.

Ефективність зусиль на ідентифікацію товарів подвійного використання, які можна застосовувати як у військовій, так й у цивільних сферах може бути підвищена на засадах удосконалення комплексу заходів, які здійснюються державними органами в частині забезпечення державного контролю за міжнародними передачами товарів, що контролюються, їх використанням юридичними та фізичними особами відповідно до міжнародних зобов'язань України й інтересів національної безпеки.

Складність ідентифікації таких товарів обумовлена: можливостями їх подвійного використання; новими науково-технічними здобутками застосованими у виробах та технологіях; впровадженням в національне законодавство з квітня 2018 року Єдиного списку товарів подвійного використання, створеного на підставі Єдиного списку товарів подвійного використання Європейського Союзу (додаток 1 до Регламенту Ради ЄС № 428/2009 від 05.05.2009). Потрібно як найскоріше здійснити адаптацію до нього положень відповідних нормативно-правових актів з питань державного контролю за міжнародними передачами товарів подвійного використання, узгодити процедури і правила державного експортного контролю України з відповідними нормами і стандартами ЄС. Потрібно якнайскоріше провести навчання з користування Єдиним списком, додати алфавітний покажчик та кореляційну таблицю товарних позицій Єдиного списку з кодами УКТ ЗЕД, пояснити алгоритм знаходження товарів за новою структурою списку.

Підвищення кваліфікації співробітників митниці, прикордонного контролю і спеціальних органів, котрі наглядають за переміщенням таких товарів з акцентом на засвоєння принципів пошуку серед групи постачі товарів включених Єдиного списку товарів подвійного використання, набуття навичок виявлення: невідповідних товарів з нечітким описом та нетрадиційною назвою; у надлишковій або невідповідній кількості; невідповідності задекларованої вартості товару відомим аналогам та ринковій вартості, технічних характеристик, маркування, ваги або об'єму товару традиційним постачанням.

Протидія застосовуванню потенціальної можливості поетапного придбання покупцями роз'єднаними фрагментами у значної кількості постачальни-

ків устаткування, матеріалів, що підпадають під контроль за міжнародними передачами товарів військового призначення та товарами подвійного використання, як на відкритому ринку товарів, так і на ”чорному”, вимагає значної консолідації зусиль на міжнародному рівні та координації дій правоохоронних органів, Державної фіскальної служби, зокрема Департаменту організації митного контролю та Державної служби експортного контролю України.

Несанкціоноване розповсюдження деякими науковцями технологій оборонного та цивільного використання наявних в нематеріалізованій формі є істотною проблемою в контексті майже повного знищення авторитету наукової діяльності та фінансово-соціальних гарантій. Зрівняння рівня оплати праці представників наукових організацій з рівнем мінімальної заробітної плати, скасування наукових пенсій створює середовище для передачі інформації. Лише, всебічна підтримка наукових співробітників різних галузей на національному рівні та запуск механізму взаємодії між носіями інформації (вченими, співробітниками окремих галузей) і правоохоронними органами дозволить звести нанівець вищеозначену загрозу.

Складність полягає у тому, що поставки для розповсюдження проводяться комерційними постачальниками. Мова йде про законні комерційні товари подвійного використання, які зазвичай надсилаються у відкритий спосіб, в рамках нетипових транзакцій в мережах закупівель. Хоча в деякий момент має місце перемикання з комерційного ринку на підставні брокерські компанії та на «підпільного» кінцевого користувача, які мають бути індикаторами небезпеки незаконної діяльності.

1. Неботов П. Г. Експортний контроль як інструмент зовнішньоекономічної політики держави // Економіка та управління національним господарством. – 2017. – №1(7). – С. 29–33.

2. Пашко П. В. Митна складова в системі економічної безпеки держави / П. В. Пашко // Регіональна економіка – 2008, No2. – С. 7–12.

3. Калініченко А. І. Митна безпека як складова національної безпеки України / А. І. Калініченко // Право та інновації. - 2015. - № 2. - С. 14-18. - Режим доступу: http://nbuv.gov.ua/UJRN/apir_2015_2_4.

4. Вітер Д. В. Митна політика і стратегія митної безпеки ЄС у контексті спільної Європейської політики безпеки / Д.В. Вітер // Митна безпека . – 2013. – No 1 – 2. – С. 164–169.

5. Постанова Кабінету Міністрів України від 11.01.2018 № 1 "Про внесення змін до Порядку здійснення державного контролю за міжнародними передачами товарів подвійного використання" прийнято Єдиний список товарів подвійного використання

**Охрименко Сергей Антонович**,
д.э.н., профессор
Лаборатория информационной безопасности
**Бортэ Григорий Русланович,** докторант
*(Молдавская Экономическая Академия)*

## ВЫЗОВЫ ЦИФРОВОЙ ЭКОНОМИКИ

Технологический рывок начала XXI века обусловил глубокую трансформацию всех сфер жизнедеятельности общества и государства. Появление и активное развитие информационно-коммуникационных технологий положило начало формированию информационного общества, под которым понимается переход от производственной к сервисной экономике, где теоретические знания, технологии и информация становятся товаром массового потребления.

Построение цифровой (информационной) экономики связано с решением комплекса задач, направленных на развитие искусственного интеллекта, больших данных, интернета вещей, телемедицины, технологий блокчейна, виртуальной и дополнительной реальности, криптовалюты, уберизации и т.д. К большому сожалению, риски новых технологий замалчиваются или нивелируются, а чаще всего просто не обсуждаются экспертным сообществом.

В частности, в [1], приведен перечень рисков, основными из которых являются такие, как: угроза внешнего управления; массовая и частная слежка; рынки подконтрольные иностранным производителям; исчезновение старых профессий и потеря рабочих мест; вирусы, закладки, уязвимости; юридическая неопределенность, этические проблемы; потеря цифрового суверенитета и цифровая колонизация.

Авторы считают необходимым акцентировать внимание на таком явлении, как теневая цифровая экономика (ТЦЭ). Отправной точкой в данном направлении являются теневые ИТ (Shadow IT), которые описываются следующими определениями: Shadow IT – это сторонние ИТ-решения, в том числе облачные приложения и услуги, неподконтрольные корпоративному ИТ-департаменту [ 2 ]; Shadow IT - это термин, используемый для описания ситуации, когда бизнес-единицы приобретают, владеют и управляют ИТ-ресурсами, без помощи ИТ-подразделения. ИТ-подразделения считают теневые ИТ неэффективными, а также источником риска и видят часть своей задачи как сдерживающую ее распространение [ 3 ]; Термин «теневые информационные системы» (Shadow IS) относится к автономным программным решениям или расширениям существующих решений, которые не разрабатываются и не контролируются центральным ИТ-отделом [4].

В качестве основы для определения ТЦЭ можно использовать следующее [ 5, 6, 7 ]:

- ТЦЭ – специфическая сфера экономической деятельности с присущей ей структурой и системой экономических отношений. Специфичность задается нелегальностью, неофициальностью, а также криминальным характером экономической деятельности и сокрытием доходов;

- С экономической точки зрения – сектор экономических отношений, охватывающих все виды производственно-хозяйственной деятельности, которые по своей направленности, содержанию, характеру и форме противоречат требованиям существующего законодательства и осуществляются вопреки государственному регулированию экономики и в обход контроля над ней;
- С технологической точки зрения – это индивидуальная и коллективная деятельность, являющаяся незаконной, связанная с проектированием, разработкой, распространением, поддержкой и использованием компонент ИКТ, скрываемая от общества.

Таким образом, ТЦЭ – это все незаконные и скрываемые продукты и услуги, использующие и основывающиеся на информационных и коммуникационных технологиях. В качестве наиболее важных экономических элементов данной сферы выделяются: незаконные экономические взаимоотношения, незаконная деятельность, связанная с производством, распространением и использованием продуктов и услуг.

Основу ТЦЭ составляет теневая (незаконная) предпринимательская деятельность, общими чертами которой являются:

- скрытый, латентный (тайный) характер, то есть та деятельность, которая не регистрируется государственными органами и не находит отражение в официальной отчетности;

- охват всех фаз процесса общественного воспроизводства (производство, распределение, обмен и потребление);

- паразитический характер всех процессов, от раскрытия исходного кода программного продукта до монетизации сдачи в аренду бот-нетов.

Следует выделить особенности, характерные для информационной области теневой цифровой экономики. В их числе следующие:

1. Риск быть пойманным и наказанным за преступление, совершенное в сфере теневой цифровой экономики, минимален по сравнению с «классической» теневой экономикой.

2. Начальный порог вхождения низок как с точки зрения материальных, так и временных затрат. Для начала работы необходимо всего лишь иметь компьютер с доступом в сеть Internet. Более того, для начального получения прибыли нет необходимости в углубленном понимании принципов работы как информационных технологий вообще, так и электронной коммерции в частности. Многие инструменты легко или свободно доступны. Интерфейсы управления подобным инструментарием интуитивно понятны и легко осваиваемы. Персональные данные и данные кредитных карт возможно купить, не имея каких-либо технических навыков.

3. В информационной среде куда проще найти клиента или поставщика услуг благодаря процессам глобализации, сети Internet и Darknet.

4. По сравнению с «классическими» денежными переводами, транзакции осуществляются намного быстрей и надежней, могут быть совершены анонимно благодаря криптовалютам.

5. Информационные товары и услуги несут в себе меньшие риски по сравнению с продажей, например, оружия и наркотических веществ, при

этом объем прибыли может быть сопоставим.

6. Минимальные риски, связанные с ответственностью, в том числе уголовной.

Еще одной нерешенной до настоящего времени проблемой является сегментация ТЦЭ и выделение двух направлений деятельности – продукты и услуги. К продуктам в сфере ТЦЭ следует отнести: специализированное программное обеспечение для сокрытия следов присутствия злоумышленника; черви; вирусы; таргетированные кибератаки; вредоносное программное обеспечение, предназначенное для вымогательства; генераторы вредоносного программного обеспечения; программные продукты, нацеленные на автоматизацию процессов совершения кибер-преступлений; троянские программы; программное обеспечение, вводящее пользователя в заблуждение ложными сообщениями; руткиты; упаковщики и др. Следует отметить, что структура вредоносных программ криминального характера постоянно изменяется.

В свою очередь, отдельную группу образуют услуги, в том числе: поиск и анализ уязвимостей программного и аппаратного обеспечения; перехват идентифицированных данных, кредитных карт, логинов и паролей; сдача в аренду вредоносного программного обеспечения; фишинг; фарминг; вымогательство; терроризм; пиратство; сдача в аренду прокси-серверов, а также шифрование и сокрытие интернет-трафика; отмывание денег с помощью информационных технологий; создание и сдача в аренду бот-нетов; организация DOS-атак; распространение спама; изготовление поддельных кредитных карт и многие другие.

Особое внимание следует уделить анализу новых заказных услуг, которые представляются в подпольной сети TOR индивидуальным пользователям и коллективным заказчикам. В их числе такие, как Cybercrime-as-a-Service, Research-as-aService, Crimeware-as-a-Service, Cybercrime Infrastructure-as-a-Service, Hacking-as-a-Service, Rent-a-Hacker.

Следует отметить, что рассмотренный перечень продуктов и услуг не является законченным и полным. Это объясняется динамическим развитием компонент информационных и коммуникационных технологий.

К большому сожалению, в настоящее время отсутствует статистическая информация, характеризующая степень развития и проникновения теневой цифровой экономики. В большинстве источников приводятся данные проводимых опросов, которые не отражают полностью складывающуюся картину. В том числе в Республике Молдова публикуются данные о совершенных информационных преступлениях без должного анализа. В 2015 году Центр по борьбе с компьютерными преступлениями Молдовы (ЦБКП) расследовал 43 случая осуществления интернет-переводов с использованием реквизитов банковских карт, 14 случаев несанкционированного доступа к информационным системам, 6 случаев мошенничества, 42 случая осуществления развратных действий с помощью информационных технологий, 14 случаев перехвата информации и шантажа. По статистике за 2003-2015 гг. на первом месте – изготовление и подлог банковских платежных инструментов, второе – нарушение авторских и смежных прав. На долю нарушения авторских и смежных

прав приходится 256 случаев за указанных период. На третьем месте – нарушение неприкосновенности личной жизни (173 случая), нарушение тайны переписки (55), детская порнография (55). Но все эти данные не отражают полной картины. Например, далеко не все банки предоставляют информацию о попытках взлома их электронных платежных систем [8].

В заключении, считаем возможным предложить разработку целостной стратегии противодействия теневой информационной экономике. Основополагающими принципами этой стратегии могут являться: - совершенствование законодательной базы экономического регулирования, нацеленного на создание условий, при которых сокрытие определенных видов деятельности или их элементов, как и любая незаконная деятельность станут невыгодными;

- развитие сотрудничества на государственном, региональном и международном уровнях с целью понижения уровня теневой цифровой экономики; - создание рабочих мест, реформирование системы налогообложения, с целью ужесточения мер борьбы с отмыванием денег, а также ожесточение борьбы с коррупцией;

- совершенствовать систему подготовки кадров, способных противостоять явлениям теневой цифровой экономики;

- расширить базу теоретических исследований и практических разработок, нацеленных на новые группы угроз, в том числе связанных с интернетом вещей, направленных на медицинское оборудование, криптоманией,

- следует полностью исключить элемент стихийности в процессах выработки стратегии.

1. Касперская Н. Цифровая экономика и риски цифровой колонизации. Санкт-Петербург, 2018.к

2. Орешкина Д. Shadow IT в вашей сети. http://bis- expert.ru/bdi_source /20/files/assets/basic-html/index.html#32 т

3. Every Employee Is a Digital Employee. https://blogs.msdn.microsoft.com/ jmeier/2015/08/23/every-employee-is-a-digital-employee/

4. Fürstenau D., Sandner M., Anapliotis D. Why do Shadow Systems Fail? An Expert Study on Determinants of Discontinuation. https://www.researchgate.net/publication/ 303682057 Why_Do_Shadow_Systems_Fail_An_Expert_Study_on_Determinants_of_Discontinuation –

5. Borta G. The Dark Side of Information Economics. Economica. An. XXIII, nr2. (92), iunie 2015, ISSN 1810-9136, Academia De Studii Economice A Moldovei, Chisinau, Moldova, p. 97-102.

6. Охрименко С., Бортэ Г. Обратная Сторона Информационного общества. Економічна та інформаційна безпека суб'єктів господарювання: сучасний стан і тенденції розвитку: монографія. Авт. кол.: ред. кол.: Т. С. Смовженко, А. Я. Кузнецова, О. І.Барановський, О. М. Тридід, Г. М. Азаренкова та ін., К.: УБС НБУ, 2014, 386 с.

7. Охрименко С., Саркисян А., Бортэ Г. Противостояние в информационной сфере. //Revista militară, №1 (9) 2013, с. 53-61. кт-

8. Волков В. Генпрокуратура Молдовы: Мы предложим руководству страны создать специализированную прокуратуру по борьбе с киберпреступностью. https://digital.report/genprokuratura-moldovyi-predlozhit-rukovodstvu-sozdatspetsprokuraturu-po-borbe-s-kiberprestupnostyu/

**Павлова Наталя Валеріївна**
к.ю.н., старший викладач кафедри
криміналістики, судової медицини
та психіатрії Дніпропетровського
державного університету внутрішніх справ

# ВИКОРИСТАННЯ ТЕХНІЧНИХ ЗАСОБІВ І ТЕХНОЛОГІЙ ПІД ЧАС ПРОВЕДЕННЯ ДОПИТУ У РЕЖИМІ ВІДЕОКОНФЕРЕНЦІЇ

Чинний Кримінальний процесуальний кодекс України передбачає такий вид допиту – як допит у режимі відео конференції. Таке положення законодавства безсумнівно є прогресивним кроком в сторону інновацій. Проте, розмите регламентування даного інституту свідчить про можливі загрози повноцінній реалізації прав учасників процесу та проблемні питання щодо криміналістичного забезпечення проведення допиту у такому форматі.

Згідно ст. 232 КПК України використання відеоконференцзв'язку здійснюється у випадках, коли через поважні причини учасник процесу не має можливості прибути за місцем провадження, якщо мова йде про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві, або дії відбуваються за участю малолітнього або неповнолітнього свідка, потерпілого, а також, якщо необхідно вжити заходів для забезпечення оперативності досудового
розслідування [1]. Однак вказані випадки не є вичерпними, оскільки останнім пунктом їх переліку є «наявність інших підстав, які визначені слідчим, прокурором, слідчим суддею достатніми» для застосування відеоконференції. Як ми бачимо, законодавець віддав визначення поважності причини на власне вирішення особам, які ведуть процес.

З одного боку, використання оціночного поняття дозволяє у кожному випадку особисто підійти до такого питання, з іншого - для несумлінної особи це може стати підставою для зловживання шляхом неправильного тлумачення поважності. У п. 3 статті 232 КПК України мова йдеться, що використання у дистанційному досудовому розслідуванні технічних засобів і технологій повинно забезпечувати належну якість зображення і звуку, а також інформаційну безпеку. Належна якість зображення – це зображення, яке дозволяє однозначно ідентифікувати особу за її зображенням всіма учасниками процесу та зафіксувати зображення технічними засобами з наступною можливістю ідентифікації допитуваного по зображенню. Належна якість звуку – це звук, що дозволяє чітко та розбірливо розрізняти показання допитуваної особи всіма учасниками процесу та зафіксувати його технічними засобами з наступною ідентифікацією допитуваного за голосом [2].

Про обов'язковість належної якості зображення та звуку вказано і в інструкції «Про порядок роботи з технічними засобами відеозапису ходу і результатів процесуальних дій, проведених у режимі відеоконференції під час

судового засідання (кримінального провадження)», затвердженої наказом Державної судової адміністрації України від 15 листопада 2012 року № 155. До того ж, згідно п. 3.2.3. цього нормативного документа, учасникам судового процесу (кримінального провадження) має бути забезпечена можливість чути та бачити хід судового засідання (судового провадження), ставити запитання і отримувати відповіді, реалізовувати інші надані їм процесуальні права та виконувати процесуальні обов'язки, передбачені процесуальним законодавством. Для якісної організації запису всі учасники судового засідання (судового провадження) повинні висловлюватися голосно і виразно [3].

У цьому контексті є сумнівною позиція законодавця, котрий допускає проведення дистанційного допиту (ч. 10 ст. 232 КПК) у режимі відео конференції з аудіо – та відео перешкодами. Так, у п. 3 ст. 232 КПК мова йдеться про необхідне забезпечення належної якості зображення та звуку, як умови допустимості результатів, отриманих внаслідок проведення слідчих дій у режимі відео конференції, а вже у п. 10 цієї ж статті мова йдеться про можливість візуальних перешкод технічного характеру. На нашу думку, це є неприпустимим, оскільки виникає питання щодо достовірності та допустимості результатів проведення дій на досудовому розслідуванні. Крім того, застосування акустичних та візуальних втручань під час дистанційного проведення допиту особи цілком виключає можливість її ідентифікації. Допитувана за таких обставин особа відразу стає анонімним учасником кримінального процесу.

Викликає сумнівів можливість повноцінного використання всього арсеналу тактичних прийомів допиту у такому форматі. За своєю сутністю допит являє собою психологічний процес спілкування між особами, котрі беруть участь у ньому, спрямований на одержання інформації про відомі допитуваному факти, які мають значення для встановлення істини у справі. Аналізуючи визначення, можна побачити, що ключовим моментом є саме встановлення психологічного контакту між допитуваним та особою, яка проводить допит.

Важливе значення мають принциповість і одночасно доброзичливість, зацікавленість особи, яка провадить допит в особі допитуваного, тактовність, витримка, належна культура мови, коректність. Це сприяє створенню і підтриманню протягом слідчої дії спокійної, ділової обстановки, усуненню напруженості. А такого результату за екраном монітора звісно не досягти. Навіть термін «дистанційне розслідування» говорить про певну «дистанцію» між учасниками допиту. Отримати беззаперечні неспростовні фактичні дані можливо тільки за умов спілкування «очі в очі», застосування тактичних прийомів як емоційного, так і логічного впливу, тактичних комбінацій, що полягають у поєднанні прийомів різних видів. За інших умов матиме місце лише технічна фіксація даних. По іншу сторону монітора слідчому або судді складно розпізнати емоційний, вольовий стан допитуваної особи, її жестикуляцію, міміку, манери, звички, неможливо впевнитися, що на неї не здійснюється впливу та тиску з боку присутніх. Крім того, допитувана особа сприймається слідчим та судом більш відчужено, що може викривити сприйняття

інформації та істотно вплинути на прийняття певного рішення.

Втім, ми ніякою мірою не заперечуємо право на існування дистанційного розслідування. Можна сказати, що використання відеоконференції під час допиту може сприяти виключенню маніпулювання щодо затягування процесу досудового розслідування і дозволяє одержати процесуально значущу інформацію у максимально стислі строки. До того ж, використання відеоконференцзв'язку надасть можливість вирішити цілий ряд проблемних питань кримінального судочинства. Проте, дистанційне розслідування не зможе і не повинно повністю замінити традиційну процесуальну форму і повинно застосовуватися лише у виключних випадках.

1. Кримінальний процесуальний кодекс України: - К.: «Центр учбової літератури», 2012. 292 с.

2. Книженко С. О. Особливості допиту в режимі відео конференції під час досудового розслідування // Вісник ХНУ імені В. Н. Каразіна. № 1062, серія «Право». вип.№ 14, 2013р.

3. Про затвердження Інструкції про порядок роботи з технічними засобами відеозапису ходу і результатів процесуальних дій, проведених у режимі відеоконференції під час судового засідання (кримінального провадження) // Наказ Державної судової адміністрації України від 15.11.2012 р. №155 .

**Плетенець Віктор Миколайович**
доцент кафедри криміналістики,
судової медицини та психіатрії
Дніпропетровського державного
університету внутрішніх справ

## МОЖЛИВОСТІ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПОДОЛАННІ ПРОТИДІЇ КРИМІНАЛЬНОМУ СУДОЧИНСТВУ

Розвиток інформаційних технологій накладає свій відбиток на всі сфери нашого життя, у тому числі й діяльність правоохоронних органів у боротьбі зі злочинністю.

Як зазначає В. Є. Ткаліч тенденції динамічного розвитку інформаційних технологій обумовлюють необхідність впроваджувати у практику діяльності ОВС сучасні здобутки науки і техніки, лише завдяки цьому можливий ефективний попереджувальний вплив на всі криміногенні фактори які детермінують злочинність. Роль інформаційних технологій у боротьбі зі злочинністю сама по собі різноманітна. В оперативно-розшуковій діяльності вони можуть успішно використовуватись для виявлення, документування, розкриття, попередження злочинів та припинення злочинної діяльності, у т.ч. на ранніх стадіях їх підготовки, замаху та вчинення [1, с. 211-212]

Розглянувши деякі проблеми використання у діяльності ОВС новітніх інформаційних технологій В.Б. Вишня та В.О. Мирошниченко констатують,

що застосування сучасних способів фіксації інформації та технологій потребує відповідної правової основи, але дозволить суттєво зменшити наступні негативні фактори у діяльності органів внутрішніх справ:

- серйозні недогляди у фіксації матеріальних ознак події злочину як результат недостатньо повного використання всього комплексу технікокриміналістичних засобів і прийомів при виявленні, фіксації, вилученні, збереженні, дослідженні й оцінці слідів й іншої доказової інформації;
- присутність відомих елементів суб'єктивізму при пізнанні істини в ході виконання слідчої або судової дії, у результаті чого протокол, будучи основним процесуальним способом фіксації не дає повного, наочного й, отже, об'єктивного відображення всіх сторін як самої процедури дії, так і тих обставин, із приводу яких воно проводилося;
- відмови свідків, потерпілих, підозрюваних або обвинувачених від раніше даних показань або істотної їх зміни [2, с. 208]
- Це, на нашу думку, повною мірою, може стосуватись випадків формування умов протидії кримінальному судочинству з боку зацікавлених осіб. Так, наявність протоколів слідчих (розшукових) дій, проведення яких супроводжувалось відео-, аудіо записом ускладнює, або нейтралізує спроби зацікавлених осіб вплинути на свідків з метою зміни ними свідчень на користь відповідних учасників.

Скарги на те, що по відношенню до відповідних учасників були застосовані заборонені засоби впливу, при перегляді (прослуховуванні) відповідних записів дозволить переконатись у їх безпідставності.

У той же час відмова від раніше даних, зміна свідчень, відмова від участі у проведенні інших слідчих (розшукових) дій мають аналізуватись із позиції тиску на відповідних учасників, та формування ситуації протидії кримінальному судочинству.

З одного боку використання інформаційних технологій спрямовується на підвищення результативності діяльності правоохоронних органів, що може бути визнано позитивним. З іншого боку захист інформації від несанкціонованого доступу, потребує окремої уваги правоохоронців. Так, , інформація про хід розслідування, здебільшого, зберігається в електронному вигляді на комп'ютерах правоохоронців. Це обумовлює необхідність прийняття заходів з її дублювання на різних носіях, що у разі втрати або пошкодження, наприклад «комп'ютерними вірусами» забезпечить її повноцінне відновлення.

Згідно тлумачення Р.С. Бєлкіна комп'ютерна інформація - інформація на машинному носії, в ЕОМ, системі або мережі ЕОМ - також може бути криміналістично значимою, при розслідуванні і комп'ютерних злочинів, і посягань, де ЕОМ виступає як об'єкт (крадіжка комп'ютера, незаконне використання машинного часу) або засіб скоєння злочину (використання ЕОМ для накопичення інформації, підробки документів і ін.). Програмні продукти теж можуть використовуватися і в якості об'єкту злочину (незаконне копіювання, спричинення збитку застосуванням руйнівних програм - вірусів), і в якості інструменту скоєння злочину (несанкціоноване проник-

нення в комп'ютерну систему, спотворення і підробки інформації) [3, с. 945].

Варто наголосити на тому, що більшість проінтервйованих правоохоронців приділяють належної уваги захисту комп'ютерної інформації щодо ходу розслідування. При цьому всі правоохоронці стикалися із шкідливим програмним забезпеченням та його наслідками. У той же час жоден з правоохоронців не замислювався над тим, що цей вплив може мати цілеспрямований характер протидії кримінальному судочинству.

Наведене дозволяє дійти висновку, що даний напрямок діяльності правоохоронців є важливим та потребує подальших наукових досліджень. Це значно спростить не тільки діяльність відповідних посадовців, а й убезпечить від передчасного витоку інформації за матеріалами кримінальних проваджень, зменшить тиск на зацікавлених осіб. с

1. Ткаліч В. Є. Використання інформаційних технологій та засобів масової інформації при розкритті злочинів : матеріали наукоко-практичн. Конф. [«Сторіччя розшуку: історія, сучасність та перспективи»], Одеса. – 2009. – С.211-212.

2. Вишня В.Б. Пробрлеми застосування інформаційних технологій у слідчій діяльності /В.Б. Вишня та В.О. Мирошниченко// Слідча діяльність: проблеми теорії та практики: Матер. нук.-практ. конф. та круглого столу (м. Дніпропетровськ, ДДУВС, 22 і 26 травня 2008 р.). – Д.: Дніпроп. держ. ун-т внутр.. справ, 2008. – 228 с.

3. Криминалистика: учебник для вузов / Под ред. Р.С. Белкина. – М.: НОРМА, 2001. – 990 с.

**Подворчанський Дмитрий Андреевич**
руководитель интернет-проэкта My Pol,
общественная организация «Ноосфера»

## "MY POL" - МОБИЛЬНОЕ ПРИЛОЖЕНИЕ «МОЯ ПОЛИЦИЯ» НА ВАШЕМ СМАРТФОНЕ

Главная задача нашего приложения «Моя Полиция» - это сделать жизнь безопаснее и ускорить коммуникацию с органами полиции, ведь появление смартфонов в корне изменило нашу жизнь. Проанализировав огромное количество терактов, резонансных и самых частых преступлений, мы поняли простую истину.

Практически во всех странах полиция едет на вызов обладая минимальной информацией о субъекте и происшествии. Вспоминая последние события, можно сказать так - рекламные агентства знают о вас больше чем полицейский когда вы его вызываете, хотя первый предлагает вам новый вкус жвачки а второй должен вас спасти. Поэтому в августе 2016 года приложение «Моя Полиция» начало работать в тестовом режиме в г. Днепр. А уже к концу 2017 года мобильное приложение «Моя Полиция» начало работать в шести областях Украины, включая Винницкую, Днепропетровскую, Закарпатскую, Ивано-Франковскую, Ровенскую и Черновицкую. А кроме основных функций, запуск приложения в в этих областях, на наш взгляд, поможет ре-

шить и проблему вызова спасателей в горную и лесную местность. Здесь ситуативные центры тесно сотрудничают со службой спасения ДСНС. Вызов спасателей через мобильное приложение «Моя Полиция» значительно облегчит и ускорит процесс поиска пострадавших в горах, так как приложение передает сигнал о бедствии и координаты вызова и без наличия мобильного интернета, с помощью GSM-связи. На рис.1-4  Приведен основной интерфейс мобильного приложения "My Pol".


*Рис. 1 Интерфейс мобильного приложения "My Pol"*

"My Pol" позволят быстро и легко получить важные новости. Аналогов такого приложения в стране нет. Функция push-уведомлений может принести много пользы для людей и для полиции.


*Рис. 2 Предусмотрена интерактивная помощь для пользователя*

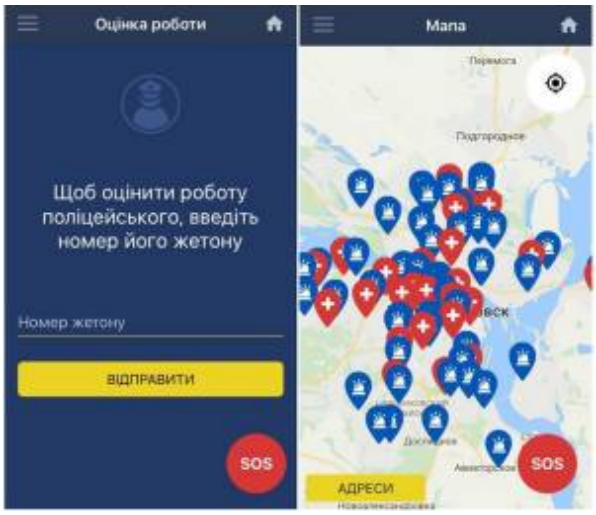



*Рис. 3 Функция оценки работы полицейского по номеру его жетона*

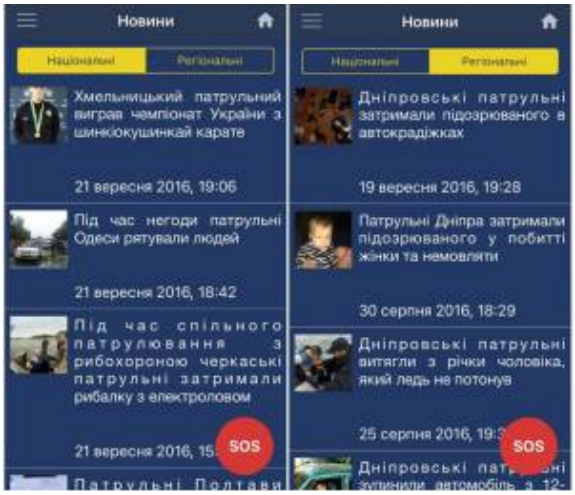



*Рис. 4 На экране высвечиваться информация о происшествиях в городе*

Благодаря сервису удалось ускорить время реагирования полиции почти на 40%. За время тестирования была отработана функция определения координат без включения геолокации на смартфоне пользователя. То есть, даже если пользователь двигается после нажатия кнопки SOS, полиция сможет отследить его перемещения и найти конечное местонахождения.

После запуска приложения впервые в нашей стране стало возможным вызвать полицию со смартфона. Мы добились того, что кнопка SOS (отправка и получение сигнала тревоги) работает как с интернетом, так и без него. Официальное сотрудничество с Национальной Полицией Украины — в первую очередь в сфере технических вопросов, таких как отправка вызовов через приложение сразу на сервер полиции стало еще одним шагом на пути к запуску приложения «Моя Полиция» по всей стране.

Подводя некоторые итоги тестирования мобильного приложения "My Pol", можно резюмировать, что благодаря сервису удалось ускорить время

реагирования полиции почти на 40%. За время тестирования была отработана функция определения координат без включения геолокации на смартфоне пользователя. То есть, даже если пользователь двигается после нажатия кнопки SOS, полиция сможет отследить его перемещения и найти конечное местонахождения.

**Потайчук Ірина Володимирівна**
к.ю.н., доц., доцент кафедри
приватної охоронної діяльності
Інституту управління та права
Запорізького національного
технічного університету

## ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВА

Актуальною світовою проблемою сьогодні є забезпечення суспільної і особистої безпеки. Корупція, зростання злочинності, недобросовісна конкуренція та промислове шпигунство, ріст тіньової економіки сприяють різного роду протиправним посяганням, що викликає необхідність вжиття заходів захисту бізнесу за рахунок власних сил підприємців, створюючи власні служби безпеки.

Успішне функціонування і економічний розвиток українських підприємств багато в чому залежить від вдосконалення їх діяльності у сфері забезпечення економічної безпеки. Економічна безпека підприємства – це складне комплексне явища. Лише беручи до уваги даний факт, слід вирішувати питання пошуку і впровадження в практику нових форм і методів управління, розробки стратегії економічної безпеки підприємств, які дозволили б підготувати і реалізувати заходи по нейтралізації зовнішніх і ліквідації внутрішніх загроз.

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.

Економічна безпека підприємства, в залежності від наукових поглядів, визначається як:

- стан господарюючого суб'єкта, що характеризується високим ступенем захищеності від існуючих небезпек та загроз;
- стан найбільш ефективного використання корпоративних ресурсів для стабільного функціонування підприємства;
- захищеність життєво важливих інтересів підприємства від внутрішніх і зовнішніх загроз, що забезпечується системою заходів спеціального, фінансово-економічного, організаційного й соціального характеру;
- стан виробничих відносин і організаційних зв'язків, при яких забезпечується стабільність функціонування та прогресивний розвиток підприємства;

- забезпечення умов збереження майна та комерційної таємниці. [1]

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.

Діяльність із гарантування безпеки на підприємстві спрямована на конкретні об'єкти і здійснюється особливими засобами і методами. Вона тісно пов'язана з діяльністю всіх функціональних ланок підприємства і має здійснюватися комплексно і з позицій сучасного менеджменту – науки і практики управління персоналом, виробництвом, послугами, збутом, відповідно до умов ринкової економіки.

Система економічної безпеки кожного підприємства є індивідуальною, її дієвість, належна функціональність залежать від нормативно-правової бази, від обсягу матеріально–технічних і фінансових ресурсів, виділених керівниками підприємств, від корпоративної культури (зокрема, розуміння кожним з працівників важливості гарантування безпеки бізнесу), а також від компетентності керівників служб безпеки підприємств.

Усі напрями діяльності підприємства, його життєздатність, залежить від ефективної організації економічної безпеки. В підприємницькій діяльності гарантування безпеки має свою чітку структуру й систему. Перед нею стоїть конкретна мета, якої досягають вирішенням управлінських і специфічних завдань, які часто залежать від роду діяльності підприємства.

Передумовою ефективного захисту сфери економічної діяльності від злочинних посягань є виявлення і вивчення умов та обставин, які передують здійсненню злочинів. Лише багатофункціональний, комплексний підхід до аналізу забезпечення безпеки економічної діяльності як внутрішнього, так і зовнішнього характеру може допомогти виявити і розробити цілеспрямовані заходи щодо запобігання криміналізації системи.

Отже, в підприємницькій діяльності гарантування безпеки – цілісне явище, що має свою чітку структуру й систему. Надійна економічна безпека підприємства можлива лише за комплексного і системного підходу до її організації. Ця система забезпечує умови, за яких можлива оцінка перспектив зростання підприємства, розробка тактики і стратегії його розвитку, зменшення наслідків фінансових криз і негативного впливу нових загроз та небезпек.

1. Гнилицька Л. Основи економічної безпеки підприємства / Лариса Гнилицька. // бухгалтерський облік та аудит. – 2014. – №7. – С. 41–48.

**Прокопов Сергій Олександрович**
старший викладач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

# ПРОБЛЕМИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ПІДГОТОВКИ ПРАЦІВНИКІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ.

Керівництво міністерства внутрішніх справ приділяє багато уваги розвитку інформаційного супроводження діяльності Національної поліції. Вдосконалюються існуючі інформаційні системи МВС як Інтегрована інформаційно-пошукова система Національної поліції, ЦУНАМІ, Арсенал, ОДК, Оріон та інші. Найбільш перспективною та затребуваною працівниками поліції є інформаційно-телекомунікаційна система Національної поліції ЦУНАМІ. Основною перевагою цієї системи є її мобільність. Мобільною складовою системи ЦУНАМІ є програмна оболонка LIS-M, яка використовується вже не тільки патрульною поліцією, а і слідчо-оперативними групами відділів Національної поліції, підрозділами охорони, дільничними та іншими поліцейськими підрозділами. Впроваджена «Електронна система фіксації поліцейськими результатів реагування на події» [1], розроблені типові схеми реагування на різні види подій. Тобто можна констатувати, що інформаційна підтримка практичних підрозділів Національної поліції за останні роки значно покращилась.

Зовсім інша ситуація, нажаль, склалася у навчальних закладах системи Міністерства внутрішніх справ, у яких незважаючи на неодноразові звернення освітян, досі не встановлені оболонки Інтегрованої інформаційно-пошукової система Національної поліції з порожніми базами даних на вже закуплені серверні апарати. У вищих навчальних закладів немає можливості використання системи ЦУНАМІ. Відсутність доступу до двох основних інформаційно-технічних систем Національної поліції, як ЦУНАМІ та Інтегрована інформаційно-пошукова система Національної поліції, негативно впливає на рівень інформаційної практичної підготовки майбутніх правоохоронців [2]. На заняттях у Дніпропетровському державному університеті під час вивчення дисциплін інформаційного напрямку надаються теоретичні відомості про ці системи, вводиться інформація в інформаційні картки, заповнення яких передує введенню інформації в підсистеми ІІПС НП. Викладачі кафедри економічної та інформаційної безпеки ДДУВС розробили для введення інформації картки за допомогою полів форм MS Word, але завдання з пошуку інформації у підсистемах Інтегрованої інформаційно-пошукової система Національної поліції проводити неможливо. Це негативно впливає на рівень інформаційно-аналітичної підготовки поліцейських.

Ознайомлення курсантів з реальними інформаційно-пошуковими системами Національної поліції в Дніпропетровському державному університеті

внутрішніх справ проводиться за допомогою інформаційних обліків, розміщених на офіційному сайті МВС (Рис. 1).

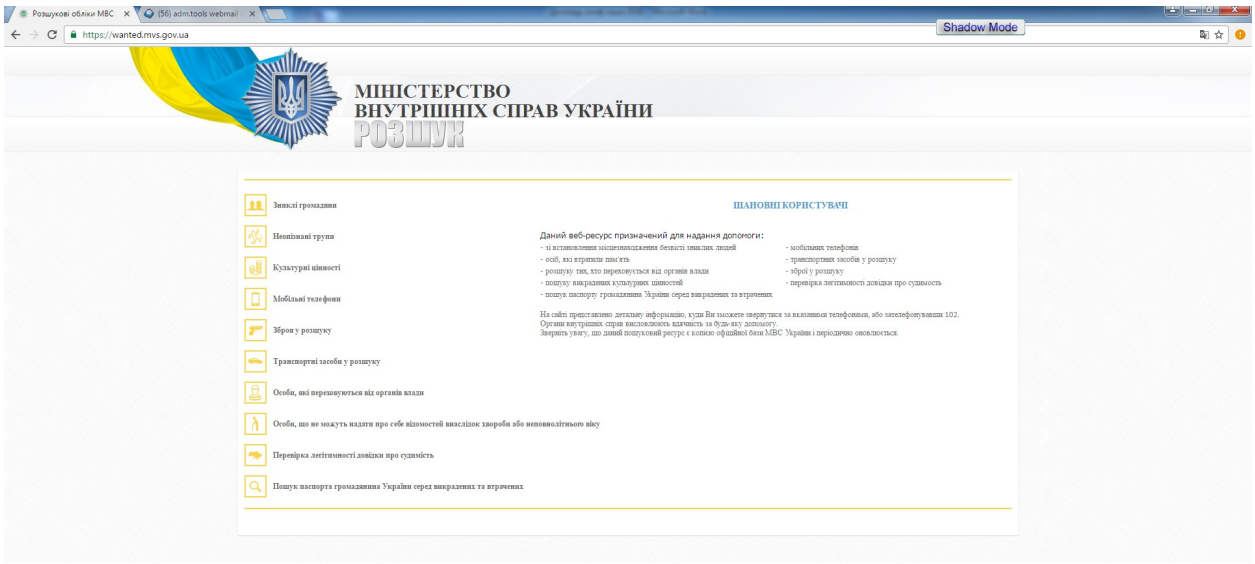



*Рис. 1*

Але ці спрощені бази даних реальної Інтегрованої інформаційно-пошукової система Національної поліції не дають можливості здійснювати складні запити, отримувати групи потенційних підозрюваних, групи номерних речей, без яких неможлива організація навчання аналітичній роботі правоохоронців.

Деякі прогалини з аналітики курсанти закривають вивчаючи тему «Методика організації пошуку інформації у відкритих джерелах мережі Інтернет» [ 3 ]. При вивченні даної теми курсантам надається інформація стосовно особливостей організації простого та розширеного пошуку інформації у пошукових серверах мережі Інтернет, вивчаються логічні та синтаксичні вирази пошукової системи Гугл. Курсанти опановують навички метапошукових серверів глобальної мережі Інтернет та спеціалізованих метапошукових програмних компонентів, таких як:

1. Debriefing (http://www.dogpile.com) Потужна метапошукова система Dogpile використовує для метапошуку не тільки пошукові системи, але і FTP-сервери, а також новинні сайти, котирування фондових бірж і навіть "жовті сторінки" Інтернету.

2. Ixquick (https://www.ixquick.com) - система метапошуку Ixquick працює з десятьма зовнішніми базами. Це пошуковики Bing, Yahoo! Ask, All the Web, Cuil, Entire Web, Gigablast, каталоги Qkport і Open Directory, а також Wikipedia. У списку баз відсутня Google, однак охоплення альтернативних систем варто визнати досить широким. Підтримується пошук на вісімнадцяти мовах, в тому числі російською.

3. SiteSputnik;

4. PDS Поисковик;

5. Info Pilot

Також вивчаються методики пошуку людей в глобальних мережах за допомогою он-лайн сервісів, таких як:

1. Pipl (https://pipl.com): пошук людей в "невидимому" Інтернеті. Запит в пошуковику Pipl допоможе знайти «невидимі» веб-сторінки, які не можна знайти на регулярних пошукових системах. На відміну від типових пошуковиків, Pipl призначений для отримання інформації з Deep Web. Його роботи вміють взаємодіяти з базами даних для пошуку і вилучення фактів, контактних даних та іншої відповідної інформації з особистих профілів, каталогів, наукових публікацій, протоколів судових засідань та інших численних джерел "глибинної" мережі.

2. Yatedo (https://www.yatedo.com) – он-лайн сервіс для пошуку інформації пов'язаних з людьми. Ви можете просто ввести ім'я людини і з'являться всі он-лайнові результати, що мають відношення до введеного Вами імені. Якщо можливо, то будуть показані в результатах резюме і фотографія кожної людини в мініатюрі. При натисканні на результат відкриються публічно доступні дані людини. Ви можете фільтрувати ці деталі для отримання новин, оновлень, документів і книг.

Курсанти навчаються пошуку інформації у соціальних мережах за допомогою наступних оболонок:

1. Webmii (http://webmii.com) – відображає інформацію про людину, отриману з різних соціальних мереж, сайтів і онлайн-документів. Кожна людина також має свій власний PeopleRank (ранг популярності) який є оцінкою його видимості в Інтернеті. WebMii використовує такі різні сайти, як Facebook, Friendster, Google, Twitter і Yahoo для збору інформації. Крім того, сайт містить посилання на Xing і Friendfeed.

2. Snitch.Name (http://snitch.name) – дозволяє шукати людину на сайтах соціальних мереж за його ім'ям і прізвищем та видавати результат пошуку в одному інтерфейсі. Замість того, щоб Ви йшли і окремо шукали когось на Facebook, Twitter, Flickr або MySpace - сервіс надає Вам результати пошуку з цих сайтів в окремих блоках на одній сторінці.

Приділяється увага використанню пошуку інформації в довідково-інформаційних базах даних вільного доступу (державних реєстрів), у посібнику їх близько 80

На кожному з практичних занять курсанти виконують практичні вправи з пошуку наданих викладачами осіб. На занятті використовуються змагальний принцип – курсанти поділяються на команди, оцінка за заняття ставиться відповідно до швидкості та якості представленого звіту.

Підводячи підсумок доповіді хочемо зазначити, що аналітична обробка інформації з відкритих джерел може тільки доповнювати вміння правоохоронцями користуватись інформаційно-пошуковими системами Національної поліції. Впровадження в навчальний процес основних інформаційних систем НП, як Інтегрована інформаційно-пошукова система Національної поліції та ЦУНАМІ, суттєво підвищить можливість отримання курсантами на-

вчальних закладів системи МВС необхідних навичок по пошуку службової інформації, навчити основам аналітичної роботи з отриманою інформацією. Якість підготовки майбутніх правоохоронців стане кращою, вони будуть більш підготовленими в інформаційно-аналітичній сфері діяльності Національної поліції.

1. Методичні рекомендації щодо користування Електронною системою фіксації поліцейськими результатів реагування на подію. Доручення Голови Національної поліції № 6327 від 16.06.2017р.

2. 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.

3. Прокопов С.О. Використання пошуку інформації з відкритих джерел мережі Інтернет у навчальному процесі Дніпропетровського державного університету внутрішніх справ / С.О. Прокопов // Проблеми застосування інформаційних технологій правоохоронними структурами України та ВНЗ зі специфічними умовами навчання. : збірник наукових статей за матеріалами доповідей учасників міжнародної науково-практичної конференції (22 грудня 2017р., м. Львів). – Львівський державний університет внутрішніх справ, 2017. –С.202-204.

**Пушак Ярослав Ярославович**
д.е.н., проф., завідувач кафедри
економіки та економічної безпеки

**Марченко Ольга Михайлівна**
к.е.н., доц., доцент кафедри
економіки та економічної безпеки
Львівського державного
університету внутрішніх справ

## ПРОБЛЕМНІ АСПЕКТИ ЗАПОБІГАННЯ ТА ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Особливістю сучасної економіки є її інформаційний характер, комп'ютеризація господарського обліку та фінансового аналізу, автоматизація систем управління, використання технічних засобів комунікацій і мережі Інтернет, переважаюче оперування даними у цифровій формі. У зв'язку з цим, а також науково-технічним прогресом у сфері інформаційних технологій, зростає небезпека втрати та викрадення інформації через технічні засоби її обробки. А отже, актуальним завданням для держави та суб'єктів господарювання стає їхня інформаційна безпека, захист інформації під час її зберігання, обробки чи передачі. Ця проблема загострюється через поширення кіберзлочинності в Україні і світі.

Всесвітній огляд економічних злочинів PwC за 2016 р. свідчить, що практично кожна третя господарська організація зіштовхнулася з економіч-

ними правопорушеннями, майже третина з яких (32 %) були кіберзлочинами [1]. За даними Всесвітнього огляду стану інформаційної безпеки PwC, кіберзлочинність ще у 2011 р. стала одним із п'яти найпоширеніших економічних злочинів в Україні [2]. Статистика МВС та Генеральної Прокуратури України свідчить про стрімке їхнє зростання протягом останнього десятиріччя. Так, у 2005-2009 рр. спостерігалася загальна тенденція до збільшення кількості злочинів у сфері високих інформаційних технологій: у 2005 р. їх було виявлено 615, а у 2009 р. – 707. З 2010 р. ведеться статистика злочинів у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. У 2010 р. їх було зареєстровано 190, у 2011 р. – 131, а у 2017 р. – вже 2573 [2; 3]. Найбільше таких злочинів реєструють у Дніпропетровські, Донецькій, Запорізькій, Луганській, Миколаївській та Одеській областях [2].

За останні роки найбільша кількість кіберзлочинів у світі діагностується у сфері фінансових послуг, державних структурах, підприємствах роздрібної торгівлі та виробництва споживчих товарів. Зокрема, найбільше постраждали від кіберзлочинності у 2016 р. сфера комунікації та страхових послуг, хімічна та фармацевтична галузі, державні організації та підприємства [1].

Одним з чинників зростання кіберзлочинності є відсутність відповідних фахівців. Тільки у чотирьох з десяти організацій за даними соціологічних досліджень є спеціально підготовлені працівники, готові реагувати на інциденти у сфері кіберпростору [1]. Проблема захисту від кіберзлочинів в українських організаціях ускладнюється відсутністю відповідної політики та розроблених механізмів реагування на кібератаки. Найпоширенішими варіантами їхньої реакції є: залучення власних досвідчених працівників для вирішення проблеми; звернення за допомогою до незалежних експертів; інформування правоохоронних органів. Як правило, зовнішніх консультантів залучають за фактом виникнення інциденту (57% опитаних організацій). І лише 21% організацій в Україні звертається до зовнішніх експертів у попереджувальних цілях [4].

Необхідність запобігання і боротьби з кіберзлочинністю зумовлює, насамперед, потребу в аналіз її правового та організаційного забезпечення.

Донедавна, до головних нормативно-правових актів, які формують правове поле боротьби з кіберзлочинами є: ратифікована Україною Конвенція про кіберзлочинність, Закон України «Про ратифікацію Конвенції про кіберзлочинність», Кримінальний Кодекс України (розділ XVI «Злочини у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку»), Закон України «Про захист інформації в автоматизованих системах». Однак, понятійно-категоріальний апарат кіберзлочинності у них недостатньо визначений та залишається не узгоджений: немає трактування поняття «кіберзлочин», вживаються інші терміни-синоніми.

Оперування значною кількістю термінів-синонімів у цій сфері, що часто не пояснюються та не узгоджуються між собою, спостерігається і в інших нормативно-правових актах. Так у Законі України «Про основи національної

безпеки України», Доктрині інформаційної безпеки України згадуються, але не визначаються такі поняття як «комп'ютерна злочинність» та «комп'ютерний тероризм».

Недостатня ясність понятійного апарату в сфері боротьби з кіберзлочинами не дозволяє: об'єктивно оцінити криміногенну ситуацію у національному сегменті кіберпростору; визначити найбільш ефективні заходи боротьби з кіберзлочинами; чітко сформулювати завдання та функції суб'єктів боротьби з кіберзлочинами; сформувати дієву систему обліку та аналізу інформації щодо боротьби з кіберзлочинністю тощо.

З 5 травня 2018 р. набуде чинності Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII, який визначає, зокрема, правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки. У ньому дається визначення ключових понять у сфері кібербезпеки, зокрема «кібербезпека», «кібератака», «кіберпростір», «кіберзагроза», «кіберзлочин» (комп'ютерний злочин). Очевидно, виникає необхідність узгодити відповідні положення дотичних до цього Закону нормативно-правових актів.

Виходячи з Закону України «Про ратифікацію Конвенції про кіберзлочинність» в Україні органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі, є Міністерство внутрішніх справ України. У грудні 2011 р. був створений Департамент по боротьбі з кіберзлочинністю МВС України, а відповідні територіальні підрозділи почали створюватися лише на початку 2012 р. На наш погляд, однією з проблем у діяльності їхніх співробітників є необхідність володіння інформаційними технологіями, знаннями принципів роботи мереж і пристроїв, які використовуються для скоєння правопорушень, останніх розробок у сфері ІТ-індустрії. З огляду на це, потрібне додаткове навчання і постійне підвищення кваліфікації кадрів.

За оцінками вітчизняних і зарубіжних фахівців вирішення проблем розкриття й розслідування кіберзлочинів є надзвичайно складним завданням для правоохоронних органів як у нашій країні так і за кордоном. Зокрема, сьогодні в Україні рівень латентності комп'ютерних злочинів становить 90 %, із залишку 10 % виявлених комп'ютерних злочинів розкривається тільки 1 %, ще менший відсоток розкритих злочинів закінчується обвинувальним вироком суду [5, с. 76].

Складність розкриття подібних злочинів визначається такими чинниками: латентність; доволі довгий термін приховування факту скоєння злочину, пізнє звернення до правоохоронних органів; відсутність єдиних стандартів у вирішенні даної проблеми; віддаленість злочинця від об'єкту посягань та можливість його скоєння практично з будь-якої точки земної кулі; склад-

ність виявлення, фіксації, вилучення криміналістично-значущої інформації при виконанні слідчих дій для використання її в якості речового доказу; анонімність, неперсоніфікованість злочинців; транснаціональний характер дій кіберзлочинців.

Таким чином, ефективність боротьби з кіберзлочинністю в Україні залежить, насамперед, від вдосконалення її правового та організаційного забезпечення. І в цьому контексті, найважливішим є використання єдиного понятійно-категоріального апарату кіберзлочинності у всіх нормативно-правових актах, підвищення кваліфікації та відповідне навчання правоохоронців, які займаються розкриттям комп'ютерних злочинів, посилення міжнародної співпраці у сфері запобігання та розслідування кіберзлочинів.

1. Всесвітній огляд економічних злочинів за 2016 р. – [Електронний ресурс]. – Доступно з: https://www.pwc.by/ru/publications/other-publications/economic-crime-survey-2016.html

2. Статистика МВС. − [Електронний ресурс]. – Режим доступу: http://mvs.gov.ua

3. Статистична інформація про стан злочинності та результати прокурсько-слідчої діяльності − [Електронний ресурс]. – Режим доступу: https://www.gp.gov.ua/ua/statinfo.html.

4. Україна. Всесвітній огляд економічних злочинів. Кіберзлочинці в центрі уваги. − [Електронний ресурс]. – Режим доступу: https://www.pwc.com/ua/uk/press-room/assets/GECS_Ukraine_ua.pdf

5. Колесник В. А. Розслідування комп'ютерних злочинів: наук.-метод. посіб. / [В.А.Колесник, І.В.Гора, М.І.Костін та ін.]. – К. : Вид-во НА СБ України, 2003. – 124 с.

**Рижков Едуард Володимирович,**
к.ю.н., доцент, завідувач кафедри
економічної та інформаційної
безпеки Дніпропетровського державного
університету внутрішніх справ

## ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЯК ЗАСІБ ПІДГОТОВКИ ФАХІВЦІВ З ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ

У рамках підготовки Всесвітнього огляду економічних злочинів PwC за 2016 рік було опитано більше 6000 учасників із 115 країн. 44 % організацій вважають, що місцеві правоохоронні органи не мають належної підготовки і ресурсів для протидії економічним злочинам. За останні два роки приблизно кожній третій організації (36 %) прийшлось стикнутись із економічними злочинами, приблизно третина (32 %) з яких склали кіберзлочини [1].

Економічна злочинність має пряму залежність від характеру та темпів розвитку інформаційного сектору та трансформується разом з ним як кількі-

сно так і якісно [2]. В зв'язку з цим першочерговим завданням оперативних підрозділів кримінальної поліції за для забезпечення ефективної протидії таким проявам є постійне оновлення тактично-ресурсного забезпечення своєї діяльності, в тому числі в питанні підготовки кадрів [3].

На тлі реформування правоохоронної сфери України це питання не втрачає своєї актуальності з огляду на ступень суспільної небезпеки економічних злочинів та невизначеність термінів реалізації державної стратегії створення нових структур захисту державного і недержавного сектору економіки.

На теперішній час основне навантаження щодо здійснення такої діяльності продовжують нести підрозділи захисту економіки Національної поліції України. Таким чином, відповідальність у питанні підготовки професійних кадрів полягає на відповідні навчальні заклади зі специфічними умовами навчання, до яких належить Дніпропетровський державний університет внутрішніх справ.

Створення факультету економіко-правової безпеки та здійснення набору курсантів покладає на науково-педагогічний колектив зобов'язання щодо використання сучасних, передових форм та методів фахової підготовки майбутніх правоохоронців із базовими знаннями та навичками протидії економічній злочинності.

Необхідно в першу чергу скористатися певними перевагами того, що курсанти 2017 року набору почали вивчати інформаційні технології своєї професійної діяльності не на випускному курсі, як раніше, а з першого. При всіх складнощах розуміння певних аспектів, пов'язаних із юриспруденцією і поліцеїстикою, яку вони поки вивчають у ознайомчому аспекти, у теперішніх першокурсників з самого початку навчання формується інформаційний базис [4] як перший етап наступного оволодіння спеціальними знаннями у сфері протидії економічним злочинам.

З метою максимально ефективного формування професійних знань та навичок у курсантів зазначеної спеціалізації в університеті у 2018 році створено унікальний спеціалізований полігон для відпрацювання в рамках тематичних фабул процедури документування відповідних складів злочинів. Забезпечений найсучаснішою інформаційною технікою та технологіями полігон здатен як автономно так і у складі професійно-орієнтованої ділової гри «Лінія – 102» [5] створити умови для викладачів та курсантів у реалізації сучасних, передових педагогічних методик навчання [6].

Використання в рамках навчального процесу технології кримінального аналізу та започаткування з 2017 року уа кафедрі економічної та інформаційної безпеки університету кіберфакультативу з метою оволодіння додатковими сучасними знаннями та навичками, надає курсантам вказаної спеціалізації додаткових переваг перед їх попередниками, які навчались на відповідних факультетах.

Вважаємо, що запорукою успіху у питанні підготовки фахівців захисту економіки, повинна стати тісна співпраця науково-педагогічних працівників кафедр між собою, зі спорідненими навчальними закладами та педагогічного колективу з практичними працівниками профільних управлінь та департаме-

нтів. Конкретним прикладом такої співпраці є попередня участь у спільних проектах та робота в рамках науково-практичних форумів, подібно цьому.
Таким чином, роль інформаційних технологій у професійній підготовці фахівців з забезпечення економічної безпеки підрозділами Національної поліції є різноплановою та послідовною. На початковому етапі вони виступають як фундамент розуміння формування та функціонування спеціалізованих інформаційних систем та відомчих і не тільки баз даних. На другому етапі – як спеціалізований інструмент банківсько-фінансової діяльності суб'єктів господарювання. На третьому – як засіб аналітичної діяльності суб'єктів правоохоронної діяльності. На четвертому – як засіб оперативно-розшукової та слідчої діяльності в рамках проведення негласних слідчих розшукових дій.

На наш погляд, саме в такій послідовності необхідно організовувати навчальний процес та реалізовувати професійну підготовку фахівців підрозділів кримінальної поліції із захисту економічного сектору держави.

1. Всемирный обзор экономических преступлений в 2016 году. [Електронний ресурс]. – Режим доступу: https://www.pwc.by/ru/publications/other-publications/economic-crime-survey-2016.html.

2. Рижков Е.В. Інформаційно-телекомунікаційні технології як засіб забезпечення економічної безпеки підрозділами кримінальної поліції / Е.В. Рижков // Оперативно-розшукова діяльність Національної поліції: проблеми теорії та практики : матеріали Всеукр. наук.-практ. конф. (Дніпро, 18 листопада 2016 р.). – Дніпро : Дніпроп. держ. ун-т внутр. справ, 2016. – Ч. 1. - С. 163-168.

3. Матвієнко А.О., Рижков Е.В. Попередження злочинності у сфері економіки / А.О. Матвієнко, Е.В. Рижков// 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. – С. 168-170.

4. Рижков Е.В. Отримання підрозділами ОВС по боротьбі з економічною злочинністю інформації про злочини у сфері економіки за допомогою сучасних інфотелекомунікаційних технологій /Е.В. Рижков/ Митна справа. Науково-аналітичний журнал, м. Одеса, № 2 (92). – 2014, частина 2, книга 2. - С. 194- 205.

5. Рижков Е.В. Досвід запровадження проекту «Лінія-102» у Дніпропетровському державному університеті внутрішніх справ /Е.В. Рижков// Проблеми застосування інформаційних технологій правоохоронними структурами України та вищими навчальними закладами зі специфічними умовами навчання : збірник наукових статей за матеріалами доповідей Міжнародної науково-практичної конференції 22 грудня 2017 року / упорядник Т.В. Магеровська / - Львів: ЛьвДУВС, 2018. – 205-211; Система управління нарядами мобільної патрульної служби /Вишня В.Б., Глуховеря В.А., Золотоноша О.В., Рижков Е.В.// Патент України на корисну модель № 118449. Україна. Заявка № u201701677, МПК H04B 1/04. Бюл. №15, 10.08.2017.

6. Рижков Е.В. Інноваційний підхід до вдосконалення практичної складової навчального процесу у вузах МВС на прикладі ДДУВС / О.В. Золотоноша, Е.В. Рижков // Науковий вісник Дніпропетровського державного університету внутрішніх справ : Збірник наукових праць. – 2016. - № 4 (84) . – С. 15-22; Рижков Е.В. Вдосконалення навчального процесу з урахуванням сучасних тенденцій інформатизації структурних підрозділів Національної поліції / Е.В. Рижков // Використання сучасних інформаційних технологій в діяльності Національної поліції: матеріали Всеукраїнського науково-практичного семінару (24 листопада 2017 р., м. Дніпро). – Дніпропетровський державний університет внутрішніх справ, 2018. – С. 8-10.

**Артюшенко Аліна Станіславівна**
старший лаборант кафедри
адміністративного права, процесу
та адміністративної діяльності
Дніпропетровського державного
університету внутрішніх справ

науковий керівник –
**Рижков Едуард Володимирович**
к.ю.н., доцент, завідувач кафедри
економічної та інформаційної безпеки

# ДО ПИТАННЯ ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ ДЛЯ ВИЯВЛЕННЯ, РОЗКРИТТЯ ТА ПОПЕРЕДЖЕННЯ ЗЛОЧИНІВ

В час сучасних технологій кількість Інтернет-аудиторії постійно збільшується, охоплюючи значну кількість населення нашої планети. Зокрема із 7 млрд. жителів планети Земля 2,3 млрд. користуються послугами Інтернет, тобто фактично кожен третій житель. Не залишається осторонь таких глобальних змін і наша держава. Станом на січень 2018 року в Україні налічується 21,8 млн. користувачів Інтернету, інакше кажучи половинна населення України має доступ до мережі, а ще половина з них до соціальних мереж. Поряд із незаперечними позитивними рисами користування, соціальними мережами притаманні також негативні, зокрема: марнування часу, виток конференційної інформації, виникнення психологічної залежності, інтелектуальної деградації, інше. Крім того анонімність користування дає можливість для вчинення злочинів.

Аналізуючи нові загрози для користувачів соціальних мереж, необхідно констатувати, що, такі мережі вже тривалий час активно використовуються злочинцями не тільки як засіб, але й знаряддя чи місце вчинення злочинів. Отже, наразі необхідна розробка засад організаційно-правової протидії Інтернет злочинності. Дослідженням окремих аспектів організаційно-правової протидії вчиненню злочинів з використанням специфічних інформаційних можливостей займались: В.М. Бутузов, В.М. Горовий, А.І. Марущак, О.М. Юрченко, В.П. Шеломанцев, та інші. Однак сьогодні залишаються остаточно невирішеними питання, щодо правової регламентації використання соціальних мереж, для виявлення, розкриття та попередження злочинів.

Інформація стає головним товаром Інтернет-економіки. За прогнозами Boston Consulting, через 8-10 років частка Інтернет-економіки у ВВП Єврозони досягне 8 відсотків, і більша частина буде припадати на збір та аналіз персональних даних, які сьогодні приносять Інтернет-компаніям понад 300 млрд. на рік. Європейські компанії наразі заробляють на кожному користувачу близько 1 тис євро. Ринок цей росте не тільки бурхливо, але й безконтрольно. Єврокомісія, наприклад, вже рік розслідує питання, як саме Google та Facebook використовують особисті данні відвідувачів.[1]

Все швидше набуває обертів спеціальний вид шахрайства, що характеризується використанням Інтернет-магазинів. При цьому злочинці використовують надзвичайно просту технологію, яка за своєю цифровою формою нагадує «спам». Так, вкравши данні користувача, зловмисники заманюють «друзів» користувача, які нічого не підозрюють на сайти Інтернет-магазинів, які спеціалізуються на обмані користувача або клієнта. Варто звернути увагу, що зловмисники із соціальних мереж використовують у своїх цілях найрізноманітнішу інформацію. Наприклад, користувач, повідомляє в мережі, що його не буде певний час вдома, цим можуть скористуватися зловмисники при вчинені квартирної крадіжки, угону автотранспорту.[2; С. 258]

Соціальні мережі нерідко використовуються також при підготовці та вчинені особливо тяжких злочинів корисливо-насильницької спрямованості. Також екстремістські та терористичні організації для здійснення своє деструктивної діяльності активно використовують мережу Інтернет, зокрема соціальні мережі, які виступають засобом зв'язку для вербування, координацією при вчиненні терактів, джерелом отримання інформації, тощо. Варто зазначити, що сьогодні практично вся інформація діяльність терористичних угрупувань перенесена у віртуальних світ. Це пов'язано з тим, що працювати там більш безпечно, ніж у традиційних ЗМІ.

У соціальних мережах люди знаходять один одного, знайомляться, спілкуються, беруть участь у обговореннях – проте інтереси у всіх різні. І один із небезпечних «інтересів» суспільства як наркотики не обійшов мережу Інтернет. Користувачі соціальних мереж активно створюють групи, де радять з приводу придбання наркотичних речовин. В таких групах пропогандують наркотики, радять де їх придбати, виступають за легалізацію наркотичних речовин, вказують ціни та торговців наркотичними препаратами та інше.

Останнім часом усе частіше кіберпростір використовують для цькування опонентів. Занепокоєність викликає кібер-буллінг (кібер-знущання) – це одна з форм залякування, переслідування, насильства, цькування дітей, підлітків з використанням інформаційних ресурсів: електронна пошта, веб-сайти, соціальні мережі та інше. Кібер-буллінг включає в себе цілий спектр форм поведінки, на мінімальному полюсі якого-жарти, які не сприймаються всерйоз, на радикальному ж – психологічний віртуальний терор, який завдає непоправної шкоди, призводить до суїцидів. Прикладом буллінгу може бути випадок, що стався на Закарпатті, де школярі зацькували у соціальній мережі свою однокласницю -14 річну дівчину до самогубства. [3]

За даними фонду Internrt Watch Foundation, Україна посідає 7-ме місце у світі за розповсюдженням дитячої порнографії у всесвітній мережі. За даними Інтерполу, український ринок порнографічної продукції оцінюється у 100 млн дол. на рік. Отже, Інтернет наповнюється протиправним контентом і використовується з метою протиправної діяльності.

У Південній Кореї, де сьогодні найбільша кількість випадків суїциду влада сформувала спеціальну групу експертів з Інтернет, понад 100 осіб, яким належить шукати суїцидально налаштованих користувачів соціальних мереж і сайти, які спонукають людей до таких дій. [4]

В Австралії ще в 2007 році озвучили план установки Інтернет-фільтрів, які повинні були боротися зі сценами жорстокості, детальними інструкціями по вчиненню злочинів або терористичних актів і вживанню наркотиків.

Соціальна мережа Facebook використовує в США автоматичні алгоритми сканування чатів та іншої особистої інформації користувачів з метою пошуку та раннього виявлення злочинів. Головним чином система налаштована на пошук педофілів, але при необхідності її можна перепрограмувати на пошук інших ознак злочинів. Система сканує листування та публікації користувачів Facebook. Цей співробітник, у свою чергу, оцінює ступінь потенційної небезпеки і вразі наявності про злочинця повідомляє про це правоохоронні органи США.

Сьогодні Україна перебуває осторонь цих суспільно-корисних процесів. Це пов'язано з одного боку відсутністю у співробітників поліції спеціальних інформаційно-пошукових систем, особливо контент-моніторингу, контент-аналізу, а з іншого – із відсутністю нормативного закріплення подібних дій. В контексті протиправного використання соціальних мереж, зростання у майбутньому кількості Інтернет-злочинів та суспільної небезпеки необхідно створювати ефективні системи протидії таким деструктивним явищам і локалізації відповідних загроз лише з використанням специфічних можливостей соціальних мереж.

1. Гавловський В.Д. До питання захисту персональних даних у соціальних мережах / В.Д Гавловський // Б-ба з огр. злоч. і корупцією (теорія та практика) : наук.-практ.журнал.- К.: МНДЦ при РНБО України, 2011.-№24. С.252-262.

2. Кількість користувачів інтернету в Україні досягнула 20 млн/ [Електронний ресурс].-Режим доступу: blogosphere.com.ua/

3. На Закарпатье одноклассники убили девочку в Интернете /[Електронний ресурс].- Режим доступу: blogosphere.com.ua/

4.Корея боротиметься із суїцидами через соціальні мережі /[Електронний ресурс].- Режим доступу: blogosphere.com.ua/

**Рудий Тарас Володимирович**
к.т.н., доц., професор кафедри інформатики

**Сеник Володимир Васильович**
к.т.н., доц., завідувач кафедри інформатики

**Кулешник Ярко Федорович**
к.т.н., доц., доцент кафедри інформатики
Львівського державного університету
внутрішніх справ

# ІНФОРМАЦІЙНО-АНАЛІТИЧНА ДІЯЛЬНІСТЬ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ЯК АСПЕКТ КІБЕРБЕЗПЕКИ ДЕРЖАВИ

Сучасні загрози інформаційному та кібернетичному простору держави обумовлені впливом комплексу політичних, соціально-демографічних, економічних, правових, технологічних чинників, які вимагають системного реагування, адекватної трансформації усього сектору безпеки, а також включення цієї системи у сферу політичних пріоритетів держави [1].

Під впливом сучасних глобалізаційних процесів, розвитку інформаційних технологій (ІТ), телекомунікаційних сервісів, цифрової економіки інформаційна та кібербезпека набувають самостійного, трансдержавного характеру.

Розвиток та безпека інформаційного і кіберпростору, запровадження цифровізації процесів управління, гарантування безпеки й сталого функціонування інформаційно-телекомунікаційних систем, державних інформаційних ресурсів мають стати складовими державної політики у сфері розвитку інформаційного простору та становлення інформаційного суспільства в Україні.

Інформаційні відносини уже давно стали об’єктом правового регулювання, але розвиток ІТ та апаратних засобів, систем телекомунікацій відбувається швидше, ніж приймаються нормативно-правові акти, якими вони регулюються, а це призводить до спричинення певних правових колізій [2, 3].

Однак, останнім часом відбувся певний вимушений (зовнішній політичний вплив) поступ у сфері забезпечення інформаційної та кібербезпеки, зокрема, на інституційно-організаційному рівнях:

- у червні 2016 р. Президент України підписав Указ «Про створення Національного координаційного центру кібербезпеки» (першим етапом його роботи є здійснення аналізу та розроблення галузевих індикаторів стану кібербезпеки):
- Указ Президента України №47/2017 про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року ″Про Доктрину інформаційної безпеки України″;
- 5 жовтня 2017 р. Верховна Рада України приймає Закон України ″Про основні засади забезпечення кібербезпеки України″;

- 17 січня 2018 року Кабінет Міністрів України затвердив урядову концепцію розвитку цифрової економіки в державі на 2018-2020 роки.

Такий стан справ зумовлює глибинні зміни у ставленні нашої держави до безпеки власного інформаційного та кіберпростору, а отже, і до посиленого захисту інформації, засобів її оброблення та кіберсередовища, в якому ця інформація циркулює, визначення об'єктів впливу (рис. 1), тобто до вжиття заходів із забезпечення інформаційної та кібербезпеки [4].

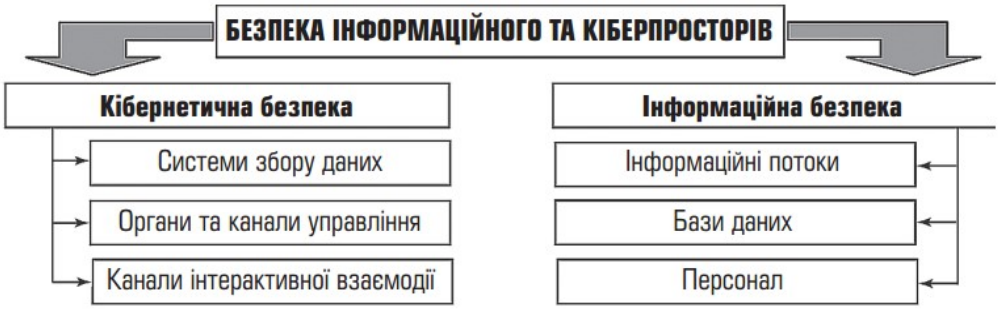



*Рис. 1. Об'єкти впливу в інформаційному та кіберпросторі.*

Невизначеними у нормативно-правовому забезпеченні залишаються питання стосовно методології підходів до проблематики забезпечення інформаційної безпеки. На перше місце слід поставити співвідношення понять ″інформаційна безпека″ та ″кібербезпека″. Українська наука чітко обґрунтувала необхідність розгляду національного сегменту кіберпростору як складової частини інформаційного простору держави [5]. З цього випливає і логічність розгляду питань протидії кіберзагрозам у контексті забезпечення інформаційної безпеки (рис. 2) [4].


*Рис. 2. Структура поняття інформаційна безпека*

Сталі режими функціонування підрозділів Національної поліції України (НПУ) з протидії кіберзлочинності не тільки зумовили збільшення обсягів інформації, які доводиться збирати, накопичувати, обробляти за визначеними алгоритмами, аналізувати і зберігати, а й необхідність забезпечення віддаленого доступу до масивів структурованої інформації та стратегічних інформаційних ресурсів. Застосування технологій інформаційно-аналітичної діяльності (ІАД) та відповідних інформаційно-аналітичних систем (ІАС) дозволить структурувати наявні інформаційні ресурси і використовувати їх як моделі

консолідованої інформації.

Технології ІАД у відповідних структурах НПУ можна визначити як взаємозалежну та сформовану сукупність організаційних, організаційно-правових, інформаційних, методичних, програмно-технічних компонент, які, у першу чергу, повинні забезпечити і супроводжувати прийняття управлінських рішень за рахунок раціонального використання інформаційних ресурсів та ІТ.

ІАД повинна враховувати неоднорідність процесу прийняття управлінських рішень і специфіку діяльності керівників підрозділів НПУ всіх категорій на різних етапах процесу прийняття рішень.

Аналітична інформація повинна відповідати наступним якісним характеристикам: цінність (корисність) – ступінь сприяння досягненню мети ініціатором запиту; точність – допустимий рівень модифікування інформації; достовірність – властивість інформації відтворювати реально існуючі об’єкти з заданою точністю; повнота – необхідний обсяг відомостей для прийняття виваженого та ефективного рішення; оперативність – актуальність, відповідність інформації поточному моменту; коректність – однозначність сприйняття інформації.

За даними [6] ІАД ототожнюють з поняттям аналізу, визначаючи його як дослідницьку функцію в управлінні підрозділами, без якої науково організувати їхню діяльність неможливо. Проте дане твердження є не зовсім правильним. Аналітична робота є діяльністю з дослідження інформації, у той час як аналізом є метод теорії пізнання, коли шляхом розумової діяльності ціле ділиться на частини. Таким чином, аналіз є одним з методів аналітичної роботи, тобто способом дослідження інформації, зокрема, у сфері організаційно-аналітичної роботи у підрозділах НПУ.

Аналітик, спираючись на інформаційні моделі (відбитки в інформаційному просторі подій, фактів, дій, ідей, думок, почуттів людей, природних, політичних, соціальних, соціоінженерних, фінансових, економічних процесів тощо), виявляє об'єктивні закономірності і тенденції, визначає рушійні механізми та, що найголовніше, причинно-наслідкові зв'язки. У цьому змісті аналітик створює нове знання про той фрагмент реальності, який знаходиться в полі його професійного інтересу, виступаючи дослідником своєї предметної області.

Тому, від того, якою мірою аналітичні підрозділи НПУ спроможні якісно аналізувати наявну інформацію і, як результат, надавати аналітичні продукти, які є підтримкою для прийняття адекватних кіберзагрозам управлінських рішень, залежить успіх виконання поставлених завдань.

З огляду на викладене виникла нагальна необхідність у реорганізації та вдосконаленні методів протидії кіберзлочинності. Одним із засадничих підходів стосовно застосування сучасних технологій у сфері протидії кіберзлочинності на якісно новому рівні та прийняття при цьому оптимальних рішень є кримінальний аналіз.

Даючи кримінологічну характеристику кіберзлочинів треба визнати, що більшість виявлених кіберзлочинів розпорошені у звітності різних підрозділів НПУ і це не дає можливості провести комплексний аналіз та характеристику кіберзлочинності. Нещодавно створено Управління кримінального ана-

лізу Національної поліції для консолідації усіх розрізнених джерел оперативної інформації з подальшим глибоким аналізом, що повинно стати вагомим чинником у протидії кіберзлочинності.

Отже, за визначенням керівника Управління кримінального аналізу НПУ кримінальний аналіз – це мисленнєво-аналітична діяльність працівників правоохоронних органів, що полягає у перевірці та оцінці інформації, її інтерпретації, встановленні зв'язків між даними, що отримуються у процесі розслідування та мають значення для кримінального провадження, з метою їх використання правоохоронними органами та судом, подальшого проведення оперативного і стратегічного аналізу (на думку авторів ця дефініція кримінального аналізу притаманна особисто п. В. Єрофеєву).

На основі [7] подамо своє розуміння терміну кримінальний аналіз. Кримінальний аналіз є специфічним видом ІАД, яка полягає в ідентифікуванні та точному визначенні внутрішніх зв'язків між інформаціями (відомостями, даними), що стосуються злочину, і довільними іншими даними, отриманими з різних джерел, їх використанням в інтересах ведення оперативно-розшукової та слідчої діяльності, прийняття адекватних управлінських рішень на основі їх аналітичної підтримки.

Технології кримінального аналізу передбачають впровадження моделі поліцейської діяльності керованої аналітикою ″Intelligence Led Policing″ (ILP) [8], як моделі діяльності, яка спрямована на підтримку, супровід інституційного управління та рішень посадових осіб на основі процесу аналізу інформації і даних.

Основні складові частини розвитку моделі ILP є такими:

- нормативно-правова база для врегулювання;
- інформаційні ресурси;
- система наповнення інформаційних ресурсів;
- система оцінювання джерел та достовірності інформації;
- спеціальне програмне забезпечення;
- інтегрування спеціалізованого програмного забезпечення з інформаційними ресурсами МВС та інших джерел інформації;
- тренінги для аналітиків практичних підрозділів НПУ;
- стандартизовані форми аналітичних продуктів;

Поліцейська діяльність керована аналітикою спрямована на ідентифікування і точне визначення взаємозв'язків між відомостями, які стосуються кіберзлочинів, осіб, пов'язаних з ними, та даними, що походять з різних джерел і їх використання кримінальними підрозділами НПУ

У відповідності до моделі ILP функції підрозділів кримінального аналізу полягають у наступному:

1. Координування діяльності.
2. Адміністрування доступу до інформаційних ресурсів ІАС.
3. Формування аналітичних продуктів.
4. Надання інформації за запитами.
5. Супроводження банків (баз) даних.
6. Адміністрування за територіальним розміщенням підрозділів з вер-

тикальною підпорядкованістю.

7. Взаємодія з підрозділами кримінального аналізу ІПКП ″102″ регіональних органів НП [8].

Кримінальний аналіз передбачає, що результат ІАД повинен гарантувати достатній і сталий рівень забезпеченості аналітичними продуктами ініціаторів, що стосується кожного аспекту діяльності підрозділів кримінальної поліції у режимі реального часу. Також враховуються рамки всіх значущих напрямків і весь реалізований комплекс заходів, здійснюваних у сфері протидії кіберзлочинності.

Базовими елементами та засобами реалізації ІАД виступають ІАС – системи зв'язку та трансмісії даних, інформаційно-телекомунікаційна інфраструктура, бази даних правової інформації, технічні, програмні, лінгвістичні, правові, організаційні засоби. Згадані аспекти відтворені у статтях 25, 26, 27 Закону України ″Про Національну поліцію″ [9]. У сою чергу технологічна платформа ІАС дозволяє здійснювати інтегрування та координування дій між різними підрозділами НПУ.

На останок, як висновок, на думку авторів успішне реалізація та впровадження технологій кримінального аналізу дасть можливість активно використовувати ІАД, що сприятиме підвищенню ефективності протидії кіберзлочинності.

1. Стратегія розвитку системи Міністерства внутрішніх справ України до 2020 року. Електронний ресурс. Шлях доступу: https://www.cyberpolice.gov.ua/strategy-2020/.

2. Рудий Т.В. Принципи організації системи захисту інформаційних систем підрозділів МВС / Т.В. Рудий, О.В. Захарова, О.І. Зачек, А.Т. Рудий / Науковий вісник ЛьвДУВС. Серія юридична / головний редактор М.М. Цимбалюк – Львів: ЛьвДУВС. 2012. – Вип. 2 (2). – С. 309-316.

3. Рудий Т. В. Організаційно-правовий супровід захисту інформаційних систем підрозділів національної поліції України на основі міжнародних стандартів / Т.В. Рудий, О. В. Захарова, В. В. Сеник, С. В. Сеник, М. І. Ізьо // Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична / головний редактор Р. І. Благута. – Львів: ЛьвДУВС, 2017. – Вип. 2. – С. 213-225.

4. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.– К.: ДУТ, 2015. – 288 с.

5. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби з кіберзлочинністю: основні напрями реформування. Аналітична записка. Національний інститут стратегічних досліджень. Електронний ресурс. Шлях доступу: http://www.niss.gov.ua/articles/454/.

6. Єсімов С.С. Юридична природа інформаційно-аналітичної діяльності Національної поліції / Електронний ресурс. Шлях доступу: http://aphd.ua/publication-151/.

7. Заєць О.М. Інститут аналітичного супроводження досудового розслідування кримінального провадження в Україні: сучасний стан і перспективи розвитку / О.М. Заєць // Вісник кримінального судочинства, ТОВ "Правова Єдність". –К: 2016. № 4. – С. 17-25.

8. Кримінальний аналіз у діяльності НПУ / Концепції впровадження в Національній поліції України моделі поліцейської діяльності, керованої аналітикою ″Intelligence Led Policing″ // Електронний ресурс. Шлях доступу: www.slideshare.net/NationalPolice/ss-75925350.

9. Закон України ″Про Національну поліцію″ / Відомості Верховної Ради України, 2015, №40-41. – С. 379 // Електронний ресурс. Шлях доступу: http://zakon3.rada.gov.ua/laws/show/580-19.

**Соломіна Ганна Валеріївна**
к.е.н, доцент кафедри економічної
та інформаційної безпеки

**Шукюров Карім Юсіфович**
студент юридичного факультету
Дніпропетровського державного
університету внутрішніх справ

# ОЦІНКА РІВНЯ ТІНЬОВОЇ ЕКОНОМІКИ УКРАЇНИ ЧЕРЕЗ ФІСКАЛЬНИЙ ЕФЕКТ ЕКОНОМІЧНИХ ЗЛОЧИНІВ В СИСТЕМІ ЕКСПОРТНО - ІМПОРТНИХ ОПЕРАЦІЙ

За розрахунками Мінекономрозвитку у 2017 р., рівень показника тіньової економіки в Україні склав 22 % до обсягу офіційного ВВП, у 2016 р.–25 %. За розрахунками професора економіки Ф. Шнайдера рівень відповідного показника у 2016 - 2017 роках у середньому по країнах ЄС становить 18,6 % від ВВП, Франції – 10,8 %, Німеччині – 12,2 %, Польщі – 23,5 % відповідно [1]. Екстрапольовані дані про рівень тінізації національної економіки, за міжнародно-порівняльним методом з високим рівнем достовірності апроксимації прогностичної лінії тренду станом на кінець 2017 р. становив 40 % ВВП [2].

Найбільші втрати державного бюджету відбуваються через офшорні схеми та сірий імпорт/контрабанду. Загалом через ці схеми держава втрачає до 65 млн грн податків, а через імпорт поза митницею – до 70 млрд грн, що разом складає 17,5% бюджету (771 млрд грн на 2017 рік). На основі статистичних даних державних органів [3,4] найпопулярніші схеми уникнення оподаткування в Україні, які призводять до загальних втрат бюджету у більш ніж 180 млрд грн визначають: офшорні схеми (50-65 млрд грн втрат бюджету); сірий імпорт і контрабанда (25-70 млрд грн); конвертаційні центри (12-15 млрд грн); «скрутки» махінації з відшкодуванням ПДВ (10-12 млрд грн); контрафакт (10 млрд грн).

За даними НБУ [6], лише за три роки рівень переміщення прибутків за кордон збільшився з 9,76 до 14,4 млрд. дол. США, або на 47%. За даними Global Financial Integrity [5], які побудовані на порівнянні національних статистик експорту та імпорту по країнах світу, заниження вартості імпорту (разом із контрабандою і схемами із ввезення фізичними особами товарів, легально експортованих із країни-експортера, але провезених до України без митного оформлення) складало у період 2004-2013 рр. в середньому 13 млрд. дол. на рік (завищення – 4,2 млрд. дол.). Іншими словами, вартість імпорту занижувалася приблизно на 20%, і з урахуванням скорочення імпорту в останні роки відповідна цифра на 2016 р. становить близько 9,6 млрд. дол.

Таким чином, щорічні втрати бюджету від ухилення/уникнення від сплати податків на рівні від 1 до 3% ВВП , при цьому баланс змінився тільки на цьому напрямку на 6 млрд. дол. – тож, зловживання, залишилися в межах

3,6 млрд. Або, якщо правильна гіпотеза щодо зрівняння масштабів завищення та заниження вартості імпорту, то відповідно відкоригована цифра щодо першого виявляється дуже близькою – 3,1 млрд. дол. Отже, зважаючи на приблизність підрахунків, можемо оцінити масштаби заниження митної вартості та контрабанди у 80-100 млрд. грн., з відповідними втратами бюджету у сумі 20-25 млрд. грн. – у разі, якщо зменшення дійсно відбулося.

Використовуючи дані вітчизняної статистики та оперативних заходів (контролю) на митницях України за період 2014-2016 роки, здійснімо оцінку обсягу зловживань, що дозволить перевірити величину несплати податків до державного бюджету та сформулювати фіскальний ефект для економіки України, за використання аналізу вірогідності (за приведеною номенклатурою), який базується на науковому факті: за природних умов будь-які об'єкти, які можуть вільно розвиватися, виявляються розподіленими за принципом Парето.

Методика запропонованої оцінки має наступну структуру:

1. За наявними даними будується лінійна регресія логарифмів обох змінних - величини доходу та кількості правопорушень у відповідному діапазоні. Вона відповідає кривій Парето. Для обчислення параметрів регресії береться «еталонний» відрізок (або кілька відрізків) без видимих аномалій.

2. Точки, що знаходяться вище верхнього довірчого 80-відсоткового інтервалу (перевірялася чутливість методу до вибору величини інтервалу) виділяються окремо і розглядаються як потенційні аномалії. На основі тих, що залишилися, розраховується нова регресія. Якщо потрібно, процес повторюється, допоки не буде отримано достатньо стабільні параметри кривої ($R^2$ покращується не більше, як на 2-3% за одну ітерацію). На практиці для цього знадобилося 1-2 ітерації.

3. На основі розрахованих у такий спосіб параметрів регресії будується рандомізована екстраполяція на решту діапазону: кожному значенню задекларованого доходу співставляється випадкове значення кількості зловживань, розподілене так само, як і справжні значення у межах еталонного відрізку. Точки, що перевищують розраховані у такий спосіб екстрапольовані значення, підлягають подальшому аналізу.

4. Виходячи з отриманих розрахунків, представлених у таблиці 1 коефіцієнт подібності ($R^2$) сягає показника 89-90%, що свідчить про виключення позаринкового фактору, а показники екстраполяції на рівні 8-23% дозволяють врахувати задані параметри в системі природних складових. При цьому симуляція в межах 0.3-10,0% свідчить про наближеність здійсненних розрахувань до системи реальних показників.

Таблиця 1

Результати отриманих розрахунків

| Група тіньових схем | Кількість ітерацій | $R^2$ | Екстраполяція | Симуляція |
|---|---|---|---|---|
| Офшорні операції | 1 | 89% | 23% | 0.5% |
| Сірий імпорт | 2 | 90% | 8% | 9.5% |
| Конвертаційні центри | 2 | 70% | 1.7% | 0.3% |
| Скрутки | 1 | 40% | 1.8% | - |

Підсумки порівняльного аналізу представлено у таблиці 2. Співвідношення між наведеними цифрами підтверджують міркування та існуючу статистику щодо структури втрат бюджету через системи уникнення податків при експорті – імпорті продукції.

Таблиця 2

Аналіз фіскального ефекту схем економічних злочинів для економіки Україні

| Схема | Приблизні обсяги (млрд. грн. на рік) | Приблизні втрати бюджету (млрд. грн. на рік) |
|---|---|---|
| Офшорні схеми | 260-320 | 50-65 |
| «Конвертаційні центри» | 40-50 | 12-15 |
| «Скрутки» | 50-60 | 10-12 |
| Сірий імпорт | 80-230 | 25-70 |
| Загалом втрати ПДВ | **60** | |
| Загалом втрати | **97 - 162** | |

За результатами проведеного дослідження, основні схеми з ухиленням від сплати податків, обов'язкових платежів та мінімізацією податкових зобов'язань, щодо яких нам вдалося знайти дані, припадають на великомасштабні зовнішньоекономічні шахрайства. Загальні обсяги недоотриманих бюджетом коштів внаслідок таких операцій складають мільярди доларів, більше сотні мільярдів гривень. Основні інструменти, які використовуються в схемах – офшорні схеми у відносинах з нерезидентами, сірий імпорт із зниженням митної вартості і споріднені з ними схеми («конвертаційні центри»).

1. Загальні тенденції тіньової економіки в Україні. Режим доступу: file:///D:/down/%D0%A2%D1%96%D0%BD%D1%8C%209%20%D0%BC%D1%96%D1%81.%202017.pdf

2. Звіт про проведення національної оцінки ризиків у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, та фінансуванню тероризму. Режим доступу: http://www.sdfm.gov.ua/content/file/Site_docs/2016/20161013/zvit.pdf

3. Quality report on balance of payments (BOP), international trade in services (ITS) and foreign direct investment statistics (FDI). Режим доступу: http://ec.europa.eu/eurostat/documents/7870049/8566866/KS-FT-17-009-EN-N.pdf/f6fc1365-6286-4faa-8123-14e36fd4ffee

4. Зовнішня торгівля України товарами та послугами у 2016 році// Статистичний збірник.-Режим доступу: http://www.ukrstat.gov.ua/

5. 15 рекомендацій ОЕСР щодо протидії зменшенню податкової бази і переміщенню прибутків за кордон (або BEPS). Режим доступу: https://bank.gov.ua/control/uk/publish/article?art_id=40253803

6. Illicit Financial Flows to and from Developing Countries: 2005-2014. Режим доступу: http://www.gfintegrity.org/wp-content/uploads/2017/05/GFI-IFF-Report-2017_final.pdf

**Сауліна Альона Ігорівна**
студентка юридичного факультету
Дніпропетровського державного
університету внутрішніх справ

Науковий керівник:
**Гавриш Олег Степанович**
викладач кафедри економічної та
інформаційної безпеки

## ПРОБЛЕМАТИКА «ПІРАТСТВА» І МЕТОДИ БОРОТЬБИ З НИМ В ІНТЕРНЕТІ

Очевидно, що Інтернет, або як ще називають Глобальна мережа, Всесвітня павутина, в наш час займає значне місце, як в Україні, так і в інших країнах.

Згідно інтернет-енциклопедії Вікіпедії, «комп'ютерне піратство» - жаргонний термін означає копіювання та розповсюдження творів захищений копірайтом, без відома правовласника.

В даний час піратство у сфері інтелектуальної власності поширюється, головним чином, на книги, музику, фільми, комп'ютерні ігри, програмні забезпечення. Все це перераховане можна швидко, за лічені секунди, знайти в інтернеті. Саме тому, процес отримання даних видів інтелектуальної власно-

сті цим шляхом називається Інтернет-піратством. Причиною такого феномена є, в першу чергу, недосконале і неефективне законодавство, як на рівні всесвітніх організацій, так і на рівні окремих країн. [1]

Сьогодні світова громадськість намагається всіма силами розробити дієвий механізм, який би спростив і прискорив можливість контролю захисту авторського права в Інтернеті. Підтвердженням останнього є:

• Директива ЄС «Про електронний бізнес»;
• HADOPI - закон, прийнятий у Франції в 2009 році;
• Закон DMCA (США);
• Закон ACTA.

Що стосується України, то в нашій країні питання боротьби з піратством до 2014 року не розглядалося системно з подальшою розробкою законодавчої бази і вступом її в силу. Саме через такого недбалого ставлення до всесвітньо значущої проблеми, рівень піратства в Україні набув масштабного характеру.

Безумовно, найголовнішим методом боротьби з Інтернет-піратством є надійний захист продуктів власності. Однак, як показує вітчизняна та світова практика, сьогодні злом захисного ПО виступає, скоріше, окремим видом Інтернет-піратства, ніж методом боротьби з ним.

На сьогодні фахівці виділяють три основні методи боротьби з віртуальним піратством:

— Навчання. Має на увазі проведення семінарів, конференцій, організацію форумів, на яких би лекторами піднімався дане питання більш масштабно. Мета таких заходів - переконати потенційного віртуального «злодія» в негативну сторону присвоєння чужого майна, викладеного в Інтернет без дозволу власника.

— Пропаганда. Її мета - наочна демонстрація переваг ліцензійної продукції та недоліків піратських копій. Одним з ефективних варіантів такої пропаганди є організація PR-кампаній в ЗМІ, загострювати увагу на проблемах присвоєння авторського права, крадіжки інтелектуальної власності шляхом незаконного копіювання, скачування і користування продуктами в мережі Інтернет.

— Силова методика. Передбачає виявлення та притягнення до кримінальної або адміністративної відповідальності виробників (розповсюджувачів) нелегальної продукції в мережі Інтернет. Даний метод боротьби є найбільш дієвий, проте і найбільш складним. [3]

Ефективність боротьби з Інтернет-піратством на своєму досвіді довели вже багато країн. Серед лідерів-борців за права власності в Інтернеті: США, Франція, Нідерланди, Данія, Швеція, Японія. Ефективність їх методик не тільки в правовій нормативній базі, належним чином регулює це питання, але і в особисту відповідальність, яку відчувають самі громадяни, а значить, не ризикують порушувати закон.

Ми пропонуємо розглянути більш детально методи та засоби боротьби з Інтернет-піратством в Україні і в інших країнах.

Найбільш лояльний і в той же час дієвий спосіб боротьби з Інтернет-

піратством розробили у Франції. Hadopi Law - проект «трьох попереджень». Перше попередження про введення санкцій порушник отримує на електронну пошту, друге попередження є офіційним повідомленням про порушення авторського права з боку користувача Інтернету, третє попередження (воно ж і останнє) - привід до дії: уповноважена спеціальне агентство розшукує правопорушника і позбавляє його доступу в Інтернет, на передбачений комісією період часу. Крім того, дане агентство штрафує незаконослухняного громадянина на вельми кругленьку суму.

Самим заплутаним, але в той же час лояльним по відношенню до Інтернет-користувачам, є антипіратський законопроект, розроблений в Нідерландах. Так, наприклад, завантажувати кіно і музику користувачам дозволяється, але тільки, якщо ті не мають на комерційного наміру. Однак завантаження програмного забезпечення виходить за рамки даного права: копіювання і розповсюдження будь-якого неліцензійного ПЗ карається штрафом. Всі діючі раніше торрент-трекери, будь то з літературою, музикою або кіно, визнані незаконними і не мають місця бути у всесвітній павутині, тому поширення будь-якого аудіо-, відео- або літературного матеріалу (спочатку завантаженого в некомерційних цілях) карається чинним законодавством Нідерландів.

Мабуть, більше за всіх до боротьби з Інтернет-піратством поставилася Японія, прийнявши радикальний закон: будь-який Інтернет-користувач, незаконно скачав файл з Інтернету (будь-якого змісту) повинен заплатити штраф у розмірі 25 тисяч доларів. Альтернативою оплати штрафу є відбування покарання в тюремній колонії терміном 2 роки. Якщо ж громадянин Японії не тільки скачав, але ще і завантажив файл зі свого персонального комп'ютера незаконним шляхом, тоді штраф, який йому доведеться заплатити, складе вже 130 тисяч доларів, або ж 10 років в'язниці в разі несплати. [4]

Ще в жовтні 2015 року в рамках реформи системи правоохоронних органів главою МВС Арсеном Аваковим було оголошено про створення кіберполіції, спеціального додаткового органу, що регулює законну діяльність в мережі Інтернет. Головним завданням кіберполіції, де є захист прав власності в віртуальному просторі, боротьба з усіма проявами Інтернет-піратства і допомогу фахівців онлайн.

Головною метою української кіберполіції є протидія кіберзлочинності за допомогою реалізованої державної політики в сферах:

— Платіжних систем;
— Електронної комерції;
— Господарської діяльності;
— Інтелектуальної власності (Інтернет-піратство і кардшаринг);
— Інформаційної безпеки.

Крім того, в компетенцію кіберполіції входить: своєчасне інформування населення з питання відбулися злочинів в мережі Інтернет; аналіз інформації на тему кіберзагроз та можливих кіберзлочинів; співробітництво із зарубіжними колегами в даному питанні; впровадження передових комп'ютерних технологій, що дозволяють виявити порушення в віртуальному просторі; цілодобова робота контактних пунктів, за якими будь-який Інтернет-

користувач зможе повідомити про правопорушення або проконсультуватися по його питанню.

Як би там не було, кількість незаконного контенту, а разом з ним і незаконного скачування в мережі Інтернет, неухильно зростає в усьому світі. Слабкі правові механізми регулювання і відсутність особистої відповідальності користувачів є головними причинами зростання Інтернет-піратства донині. Тим часом, по всьому світу періодично прокочується хвиля протестів та акцій «піратських» партій, які виступають за можливість вільного скачування фільмів, музики і ПО. Їх головним гаслом є свобода і недоторканність особистого життя людини і громадянина. [3]

Інформаційне піратство багато хто розглядає як свого роду спорт. Хакери, часто дуже молоді люди, проявляють дивовижні здібності, зламуючи найскладніші коди доступу. Подібне розвага пов'язане з величезним ризиком. Для забезпечення безпеки інформаційних мереж залучені висококваліфіковані фахівці, і це є як для поліції, так і для банків пріоритетним напрямком роботи.

Зараження мереж вірусами, що знищують файли, є поширеним і ще маловивченим видом вандалізму, який не можна пояснити лише прагненням до знищення. Ринок технологій протидії розвивається одночасно з поширенням цієї небезпеки. Комп'ютерний зв'язок дозволяє кримінальним структурам легко обмінюватися шифрованими посланнями. [5]

1. Столлман Р.М. Интернет и піратство как неотъемленный феномен сети.
2. Л.Н.Чевтаева «Интернет пиратство: вчера и сегодня» - с.284-289.
3. http://mediasat.info/2016/05/11/internet-piratstvo-metody-borby/.
4. https://cyberleninka.ru/article/v/internet-piratstvo-progressiruyuschaya-tendentsiya-xxi-veka.
5. https://keddr.com/2016/11/internet-piratstvo/.

**Соловаров АндрійВалерійович** аспірант
ДВНЗ «Університет
банківської справи», м. Київ

Науковий керівник:
**Барановський Олекандр Іванович**
д.е.н., професор, проректор
з наукової роботи ДВНЗ
«Університет банківської справи», м. Київ

## ПРОБЛЕМНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ БОРГОВОЇ БЕЗПЕКИ БАНКІВСЬКОГО СЕКТОРУ В УКРАЇНІ

Сьогоденний стан забезпечення боргової безпеки вітчизняного банківського сектору характеризується низкою проблемних питань. Так, чинне вітчизняне законодавство не містить чіткого однозначного тлумачення сукуп-

ності боргових зобов'язань банківського сектору, дефолтів комерційних банків як емітентів цінних паперів, прав кредиторів, інституту поручництва.

На заваді підвищенню рівня боргової безпеки банківського сектору й відсутність законодавчих норм про особливості здійснення врегулювання простроченої заборгованості (який би регламентував чіткі правила та обмеження щодо повернення простроченої заборгованості), реструктуризацію боргів фізичної особи або визнання її банкрутом, відповідальність посадових осіб підприємств-боржників (що уможливлює використання ними сумнівних або відверто незаконних методів протидії вимогам кредиторів).

Ст. 75 Закону України «Про банки і банківську діяльність» зобов'язує НБУ приймати рішення про віднесення банку до категорії проблемних за умови, якщо банк не виконав вимогу вкладника або іншого кредитора, строк якої настав п'ять і більше робочих днів тому, ст. 76 – у разі невиконання банком протягом п'яти робочих днів поспіль двох і більше відсотків своїх зобов'язань перед вкладниками та іншими кредиторами після віднесення банку до категорії проблемних. Утім, на практиці є випадки, коли регулятор не виконував такі зобов'язання, мотивуючи це, скажімо, наявністю судового спору між банком та клієнтом, або уявляючи, що йому нічого невідомо про наявність заборгованості. Водночас, оприлюднення інформації про таку заборгованість може спричинити дострокове стягнення з банку заборгованості за зобов'язаннями перед кредиторами, встановлення лімітів по його міжбанківських операціях, відтік коштів тих клієнтів, котрі прискіпливо ставляться до його фінансового стану.

Попри те, що ст.58 Закону України «Про банки і банківську діяльність» зобов'язує власників істотної участі вживати своєчасних заходів для запобігання настання неплатоспроможності банку, приклад банку «Новий», в якому держава через КБ «Південне» була власником істотної участі, свідчить, що на практиці цей обов'язок не виконувався.

Поряд з цим Закон України «Про фінансову реструктуризацію» не стимулює недобросовісних позичальників, насамперед, великі корпорації сплачувати свої борги.

Так і не прийнято закон «Про внесення змін до деяких законодавчих актів України щодо підвищення довіри між банками та їх клієнтами», а відтак неврегульованими належним чином залишилося питання строку дії поручительства.

Ризикованим залишається й механізм визначення відсоткової ставки. Недосконалими є й інструменти позасудового врегулювання боргових відносин, практика відчужування майна, що перебуває в заставі.

На борговій безпеці банківського сектору, безумовно, позначається організація списання банками боргів. Утім, результативність такої практики вкрай низька.

Залишаються і податкові перепони в роботі банків з проблемними кредитами, зумовлені неоднозначним застосуванням податкового законодавства при роботі з необслуговуваними проблемними кредитами, списанні заборгованості, формуванні резервів, повідомленні позичальників про прощен-

ня/анулювання боргів, що спричиняє додаткове податкове навантаження, а, відтак, може спричинити й зростання податкового боргу.

Неоднозначно на рівень боргової безпеки банківського сектору впливає організація роботи банківських установ з кредитними історіями позичальників. Так, функціонування кредитних бюро, з одного боку, позитивно позначається на інформованості банків про кредитну історію клієнтів, підвищуючи тим самим боргову безпеку. Водночас, з другого боку, значна ціна послуг кредитних бюро зумовлює підвищення собівартості кредитів. Крім того, інформація про кредитну історію одного й того ж клієнта може кардинально різнитися в кредитних бюро, що спричиняє різкі коливання кредитних рейтингів позичальників, підвищує кредитні ризики банків, а відтак, не дає їх об'єктивної оцінки. Зазначені недоліки в свою чергу підривають боргову безпеку банківського сектору.

Неоднозначно на боргову безпеку банківського сектору впливають судові рішення.

Не додає обґрунтованості і достовірності визначенню рівня боргової безпеки банківського сектору України і склад і порядок оприлюднення офіційної інформації регулятора та статистичної звітності.

**Стаценко Владимир Иванович**
старший преподаватель, руководитель
Службы информационной
безопасности Днепровского
национального университета
имени Олеся Гончара

## ИСПОЛЬЗОВАНИЕ СИСТЕМНОГО ПОДХОДА ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Процесс подготовки специалистов по информационной безопасности особенно остро сталкивается с проблемой устаревания знаний. На фоне взрывного развития информационных технологий, когда объем знаний в этой отрасли удваивается за очень короткое время, практически невозможно успевать за развитием новых технологий в сфере обработки, накопления, хранения и передачи информации. Особую остроту ситуации придает тот факт, что развитие информационных технологий происходит на фоне активных и драматичных геополитических процессов, слома старых парадигм мышления, переоценки ценностей, возникновении новых внутригосударственных и надгосударственных структур.

Эти процессы происходят одновременно с бурным развитием вычислительной техники, новых средств коммуникации, формировании нового

виртуализированного киберпространства с практически неосязаемыми границами и неконтролируемыми каналами распространения информации, и местами ее хранения и обработки, что ставит новые вызовы информационной безопасности государства [1]. Практически каждый день происходят изменения в области технологии обработки информации, а вместе с ними и создаются новые угрозы информационной безопасности, которые способны нарушить конфиденциальность, целостность и доступность информационных ресурсов. Вместе с техническими изменениями происходят социально-политические изменения, которые также меняют правила информационных отношений в современном обществе, приводят к принятию новых законов и отмене старых. Стремительность этих изменений проявляется в скорости обновления стандартов информационной безопасности [1-3, 6] и в количестве как новых законодательных актов в сфере информационных отношений, так и поправок к существующим, принятых Верховной Радой Украины за последние несколько лет [4].

Возникает системное противоречие. С одной стороны, будущие специалисты по информационной безопасности должны обладать полнотой знаний, знать и уметь применять современные технологии защиты информации и овладеть ими за период обучения, с другой стороны, за время учебы практически невозможно полностью их изучить из-за постоянного обновления технической, технологической и нормативной базы информационной безопасности. Эта проблема стоит перед современным образованием в целом и стимулирует развитие новых подходов. Как отмечают многие авторы, современный образовательный процесс должен быть не фактологическим, а методологическим [8], когда основное внимание уделяется формированию навыков использования эффективных инструментов обработки и анализа информации. Во всех сферах растет спрос на специалистов, умеющих самостоятельно принимать решения, обладающих необходимыми компетенциями для постоянного самообразования и эффективной работы с большими объемами разнообразной информации в условиях усиливающегося «информационного шума».

Разрешение данного противоречия возможно только при применении новых подходов и инструментария в образовании, учитывающих требования современного общества. Одним из эффективных методов формирования системного мышления и необходимых компетенций у студентов является функционально-системный подход, разработанный на основе анализа и дальнейшего развития системного подхода, впервые сформулированный в начале XX века. В середине прошлого века появился функционально-системный анализ (ФСА), применение которого позволяет найти оптимальный баланс между стоимостью продукции и полезностью объекта. Дальнейшее развитие ФСА получило в работах Г. Альтшуллера, основателя ТРИЗ и его последователей. По определению Альтшуллера ФСА – это комплексно-целевая программа, объединяющая три основные составляющие – технико-экономический анализ, организационно-технические мероприятия и научную методологию поиска новых решений, направленная на выявление и использование резервов совершенствования любых объектов [7]. ФСА с успехом

применяется при создании Комплексной системы защиты информации (КСЗИ), которая должна реализовываться при обеспечении принципов системности, комплексности, непрерывности защиты, разумной достаточности, гибкости управления и применения, открытости алгоритмов и механизмов защиты, простоты применения защитных мер и средств [5].

В последние годы, в результате развития ФСА появился Функционально-системный подход (ФСП), как инструмент системного анализа объектов, предметов, явлений [8]. Применение схемы-модели ФСП в учебном процессе помогает структурировать приобретаемые знания на основе переосмысления уже имеющихся знаний и решения учебных задач, как традиционных, так и «открытых». Обучение с применением схемы модели ФСП позволяет вовлечь студентов в исследовательский процесс, когда в процессе обучения формируются новые, неочевидные, на первый взгляд, связи между различными объектами, входящими в технические и нетехнические системы, взаимовлияние систем и подсистем, развивает навык системного мышления. Основой ФСП является системный анализ, в котором основным понятием является «Система» - некоторое множество взаимосвязанных элементов, обладающих свойствами, не сводящимися к свойствам отдельных элементов [7]. Свойства системы определяются не только ее составом, но и связями между элементами. Различают иерархическую связь, при которой четко прослеживаются высшие и низшие элементы и ретикулярную – сетчатую с обратными связями, при которой все подсистемы связаны друг с другом сложными обратными взаимовлияющими связями. При этом четкая иерархия не прослеживается, хотя можно выделить «сильные», «слабые», «системообразующие» и «ключевые» элементы, так или иначе влияющие на информационную безопасность системы в целом.

Для организации системного мышления у обучаемых Г. Альтшуллер предложил модель девятиэкранной схемы, в которой вместе с минимальной 3-х уровневой иерархией (надсистема–система–подсистема) рассматривается развитие свойств системы во времени (прошлое–настоящее–будущее). Такая модель позволяет системно и динамично отразить сложные структурированные системы в их развитии. А знание и использование «Законов развития систем» и накопленных статистических данных, полученных при эксплуатации в прошлом и настоящем, позволяет построить прогнозы развития систем и их отдельных элементов для прогнозирования их изменений и модернизации с целью выполнения новых необходимых требований со стороны надсистем в будущем.

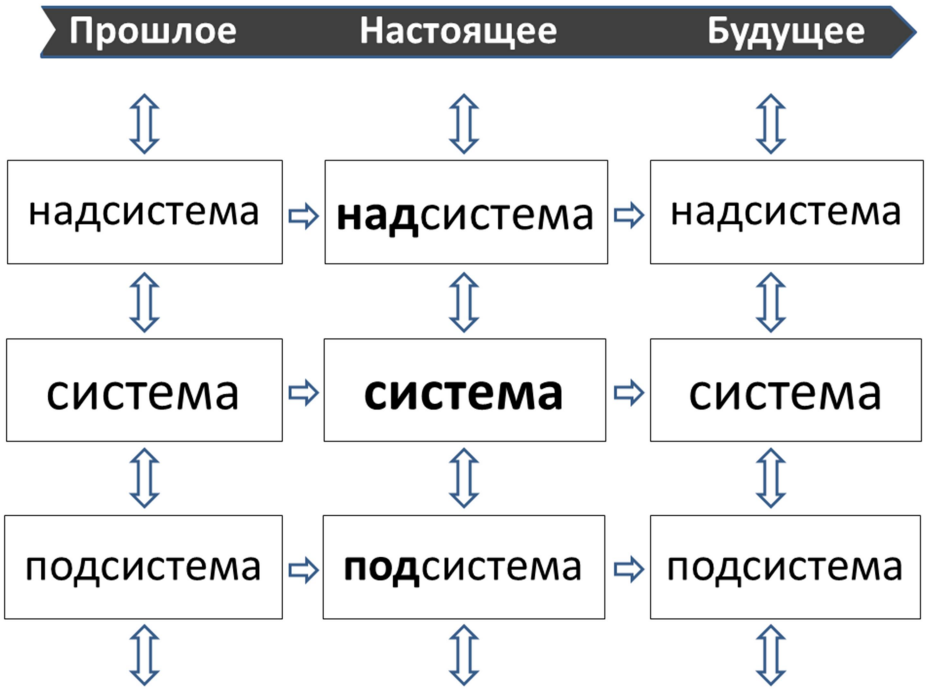



*Рис. 1. Девятиэкранная схема*

Для более глубокого и системного анализа отдельных элементов и компонентов КСЗИ при их изучении целесообразно применять схему-модель функционально-системного подхода (ФСП), разработанную Еленой Гредиаровой как инструмент систематизации знаний и формирования системного и творческого мышления у обучаемых [8]. Применение ФСА в процессе изучения и анализа, в частности Комплексной системы информационной безопасности (КСЗИ), позволяет для каждого компонента и объекта защиты независимо от его типа выделить и закрепить у студентов универсальные понятия, такие как: «Главная функция», «Скрытая функция», «Свойства и признаки», «Различные точки зрения на объект» (систему, компонент), «Местонахождение», «Генетический анализ», «Общие и отличительные признаки», «Оценочные суждения» и эмоциональный компонент со стороны субъектов информационных отношений и персонала. Также схема-модель ФСА позволяет наглядно выделить и проанализировать «Надсистему», в которую входит изучаемый компонент и «Подсистемы», которые входят в его состав, при этом выявляются явные и скрытые связи между компонентами КСЗИ и объектами защиты, что позволяет более полно составить списки угроз и уязвимостей, повысить адекватность моделей безопасности. Заполненная студентами схема-модель ФСА может быть использована ими как основа интеллектуальных карт для составления конспектов при подготовке к текущему и итоговому контролю.

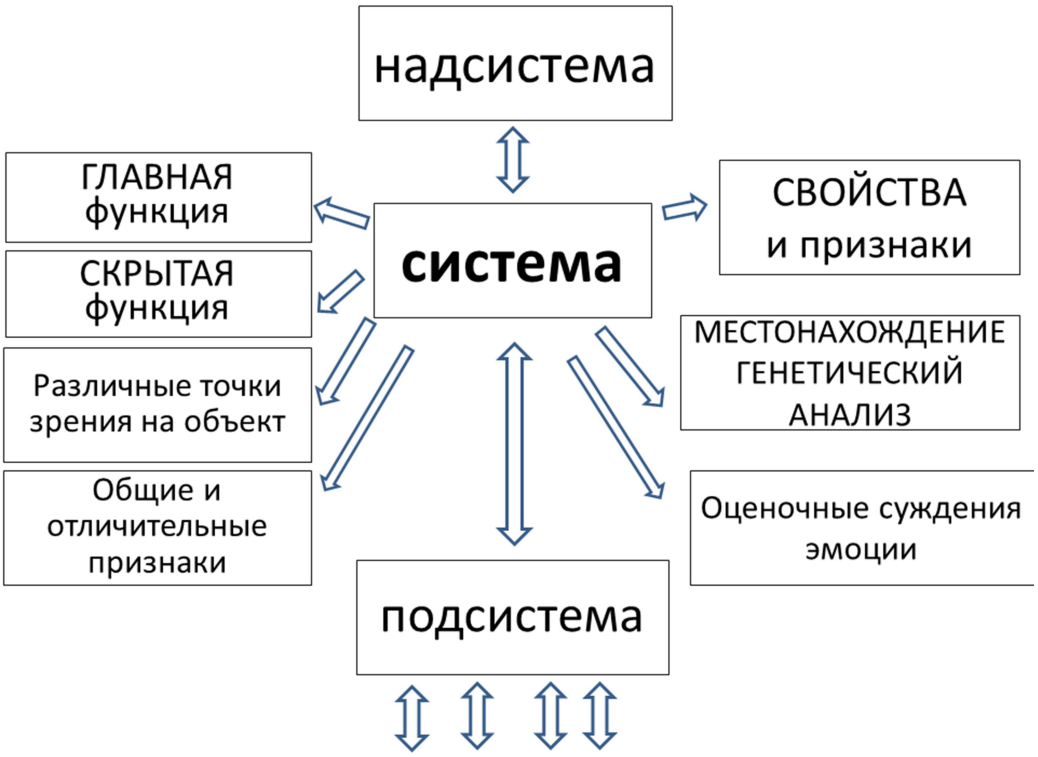



*Рис. 2. Схема-модель ФСА*

Применение современных инструментов системного подхода и анализа при подготовке будущих специалистов в области информационной безопасности дает возможность развить навыки самостоятельного мышления и самообразования, привить и сформировать необходимые компетенции для непрерывного повышения своей квалификации в современных условиях.

1. Юдін О.К., Богуш В.М. Інформаційна безпека держави. — Харків: Консум, 2004. — 508 с.

2. ДСТУ /ISO/IEC 27001:2010 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги.

3. ДСТУ ISO/IEC 27002:2010 Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою.

4. Офіційний портал Верховної Ради України — http://www.rada.gov.ua/

5. Косарев В.М., Петренко А.Н. Информационная безопасность: организация защиты программ и данных: Учебное пособие. Днепропетровск: Изд-во ДУЭП, 2003. – 152с.

6. Зегжда Д.П., Ивашко А.М. Как построить защищенную информационную систему – СПб: Мир и семья-95,1997. – 312с.

7. Альтшуллер Г.С., Злотин Б.Л., Зусман А.В., Филатов В.И. Поиск новых идей: от озарения к технологи (Теория и практика решения изобретательских задач) – Кишинев: Картя Молдовеняскэ, 1989. – 381с.

8. Гредінарова Е.М. Схема-модель функционально-системного подхода как инструмент систематизации знаний учащихся и формирования системного и творческого мышления – Запорожье: Школа «ЭйдоС», 2017. – 60с.

**Струков Владимир Михайлович**
к.т.н., доц., заведующий кафедры
информационных технологий
Харьковского національного
университета внутренних дел

**Узлов Дмитрий Юрьевич**
начальник УИАП ГУ НП Украины
в Харьковской области

**Власов Алексей Вячеславович**
зам. начальника УИАП ГУ НП
Украины в Харьковской области

# ТЕХНОЛОГИИ DATA MINING В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Современное состояние информационного обеспечения деятельности органов внутренних дел Украины отражает общую глобальную тенденцию информатизации человеческой деятельности и ее проблемы. Она состоит в лавинообразном нарастании потоков данных из различных источников и необходимости их хранения и обработки. Так в базах данных интегрированной информационно-поисковой системы (ИИПС) органов внутренних дел только в Харьковской области уже накоплено более десяти миллионов записей о различных объектах. Результаты запросов к этой системе иногда содержат несколько сотен или даже тысяч записей, которые в дальнейшем необходимо обрабатывать вручную. Кроме того, необходимо учитывать следующие особенности массивов данных ИИПС:

1) большое количество признаков, характеризующих объекты (до сотни признаков);

2) различная природа признаков (как правило, нечисловая), измеряемых в различных шкалах;

3) возможность наличия нескольких записей об одном и том же объекте (известная проблема «двойников»);

4) возможность наличия пропусков (отсутствие значений там, где они должны находиться) в массивах данных в силу ряда субъективных и объективных причин.

Кроме перечисленных причин существуют также субъективные причины чисто технического и организационного характера, которые существенно снижают эффективность применения даже тех инструментариев, которые имеются в наличии (к примеру, планшеты у патрульных полицейских с доступом к ИИПС, которые дают некорректные ответы на запросы). Все это не позволяет сопоставлять различные события, лица и объекты, которые казалось бы, явным образом не связаны между собой, но между ними существуют опосредованные либо скрытые

(скрываемые) связи, доказывающие их причастность или участие в определенных расследуемых событиях.

Имеющиеся на данный момент технологические инструменты работы с данными в ОВД Украины с учетом перечисленных особенностей не позволяют в полной мере эффективно обрабатывать накопленные данные и получать из них ту информацию, необходимую для расследования преступлений, которую при наличии соответствующих наукоемких средств (например, аналитических систем типа Palantir) можно было бы получить. В качестве характерного примера, иллюстрирующего описанную проблему, можно привести следующее сообщение: «…в девяностых годах …когда лондонская полиция вела раскопки в архивах дедовскими методами, в колумбийском наркокартеле Кали анализ данных давно был поставлен на широкую ногу. В начале девяностых картель приобрёл мощную компьютерную систему IBM AS/400, стоившую в те времена полтора миллиона долларов, и обзавёлся штатом сисадминов и программистов, разрабатывающих специализированный софт для data mining. Техника была нужна для того, чтобы прочесать краденые базы данных с рабочими и домашними телефонами сотрудников американских спецслужб и дипломатических работников в Колумбии, сопоставить их с полным списком всех телефонных звонков, которые совершаются в стране, и выявить потенциальных информаторов, подлежащих ликвидации. Об эффективности затеи можно судить по тому факту, что, когда эта история всплыла на свет, американское Управление по борьбе с наркотиками предпочло сохранить подробности произошедшего в секрете.» (http://www.computerra.ru/86823/crime-bigdata/)».

Таким образом, безусловным является то, что в сложившихся на данный момент условиях для эффективного использования накопленных и вновь поступающих данных в целях эффективного расследования преступлений единственно возможным путем является использование современных наукоемких инструментов. Примерами таких инструментариев являются такие аналитические системы как I2, Palantir, HOLMS2, RICAS. Математический аппарат, лежащий в основе этих систем, представляет собой технологии Data Mining, Text Mining, Veb Mining [1-5]. Опыт использования инновационных инструментариев в Украине и в странах с аналогичной предысторией позволяет с большой долей вероятности говорить о том, что одной из наиболее эффективных форм наикратчайшей доставки (разработки или закупки) инновационных инструментариев до потребителей (правоохранительных органов) является целевое создание государственного предприятия (либо акционерного с большей долей государства), занимающегося разработкой и приобретением на конкурсной основе готовых технологических решений как отечественных так и зарубежных с последующей их адаптацией и внедрением. Такое предприятие могло бы аккумулировать и распространять наиболее перспективные отечественные наработки на конкурсной основе и приобретать и внедрять передовые зарубежные системы.

1. Aggarwal C.C. Data Mining. – Cham: Springer Ltd. Publ. Switzerland, 2015. – 734p.
2. Westphal C. Data Mining for Intelligence, Fraud and Criminal Detection. Advanced Analytic & Information Sharing Technologies / C. Westphal. – Boca Raton : CRC Press, 2009. – 426p.
3. Mena J. Investigative Data Mining for Security and Criminal Detection. – Amsterdam: Elsevier Science, 2003. – 452p.
4. Бодянский Е.В., Струков В.М., Узлов Д.Ю. Задача оценки близости многомерных объектов анализа данных // УСиМ. – 2016. – № 6. – С. 67-72.
Бодянский Е.В., Струков В.М., Узлов Д.Ю. Обобщенная метрика в задаче анализа многомерных данных с разнотипными признаками // Зб. наук. праць Харк. нац. ун-ту Повітряних Сил. – 2017. – № 3(52). – С. 98-101.

**Свириденко Сергій Володимирович**
начальник Управління
інформаційно-аналітичної підтримки
ГУНП в Дніпропетровській області

**Слісаренко Ігор Вікторович**
заступник начальника Управління
інформаційно-аналітичної підтримки
ГУНП в Дніпропетровській області

**Шевченко Олена Дмитрівна**
начальник відділу супроводження
інтегрованої інформаційно-пошукової
системи Управління інформаційно-
аналітичної підтримки ГУНП
в Дніпропетровській області.

## ПРОБЛЕМНІ ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПІДРОЗДІЛАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ.

До основних проблемних питань інформаційної безпеки підрозділів Національної поліції, на нашу думку, можна віднести:

1. Використання інформаційних технологій в діяльності Національної поліції України.

Запорукою ефективної роботи та функціонування будь-якої державної установи, чи системи державних органів влади в умовах сьогодення є, насамперед, збір, класифікація, аналіз великого обсягу інформації та швидке прийняття рішень за результатами її обробки. Саме це в умовах сучасного, динамічного, високоінформативного світу є одним з найважливіших чинників успіху.

Національна поліція України, як центральний орган виконавчої влади, що служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку, як ніхто інший потребує постійного впровадження сучасних інформаційних технологій, для забезпечення високої ефективності роботи кожного поліцейського, надання швидкого доступу до інформаційних банків даних Національної поліції, сприяння повному збору інформації безпосередньо на місці події, здійснення аналітичної і превентивної діяльність, що має на меті зменшення кількості скоєних кримінальних та адміністративних правопорушень.

2. Проблемні питання інформаційної безпеки відомчої телекомунікаційної мережі Національної поліції України.

У сучасних умовах розвитку інформатизації підрозділів Національної поліції України надзвичайного значення набувають питання забезпечення належної інформаційної безпеки при опрацюванні даних, які, відповідно до Закону України «Про Національну поліцію» збираються та зберігаються у відомчих інформаційних ресурсах.

З одного боку повсякденне виконання службових та функціональних обов'язків поліцейського потребує від нього використання відомчих інформаційних ресурсів, власником яких є держава, та які містять персональні дані громадян і охороняються відповідно до вимог чинного законодавства. З іншого боку, наприклад, слідчі підрозділів Національної поліції обов'язково повинні мати доступ до всесвітньої інформаційної мережі Інтернет для внесення необхідних даних до Єдиного реєстру досудових розслідувань. За аналогічних умов забезпечується доступ поліцейських структурних підрозділів ГУНП до єдиних та державних реєстрів, володільцем яких є Міністерство юстиції України.

3. Аналіз потенційних загроз та впливу вірусного програмного забезпечення на роботу інформаційних ресурсів Національної поліції України.

Минулий 2017 рік, нажаль, був позначений рядом гучних атак на сайти та інші інформаційні ресурси державних установ України, спробами паралізувати деякі органи виконавчої влади та правоохоронні органи держави. Основними типами вірусного забезпечення, до яких є найбільш вразливими інформаційні ресурси державних установ слід визначити:

- Різноманітні програми-шифрувальники (вимагачі) WannaCry, Petya (також відомий як Petya.A, Petya.D, Trojan.Ransom.Petya, PetrWrap, NotPetya, ExPetr, GoldenEye);
- DDos атаки відомчих ресурсів, що розташовані безпосередньо в мережі Інтернет;
- Розширення шкідливого програмного забезпечення у корпоративній обчислювальній мережі та використання її потужностей у Ботнет.

4. Практичні та організаційні засоби боротьби з кіберзагрозами сьогодення.

- Посилення вимог до використання різноманітного програмного забезпечення, використання ліцензійного програмного забезпечення, оновлен-

ня операційних систем та новітнього антивірусного ПЗ в службовій діяльності підрозділів поліції;

- Переведення наявних серверів з інформаційними ресурсами у віртуальне середовище з відповідною організацією резервного копіювання. Використання хмарних технологій.
- Впровадження в службову діяльність НПУ різноманітних методів адміністрування робочого інформаційного середовища поліцейського з можливістю використання групових політик безпеки та користування інформаційними та апаратними ресурсами.

**Тітуніна Катерина Вікторівна**
кандидат юридичних наук,
начальник управління стратегічного
аналізу та прогнозування –
помічник Міністра ДОАР МВС України

**Марценко Валентин Євгенович**
головний спеціаліст відділу
стратегічного аналізу управління
стратегічного аналізу та прогнозування
ДОАР МВС України

## СОЦІАЛЬНІ МЕДІА ЯК ЗАСІБ КОМУНІКАЦІЇ МІЖ ПОЛІЦІЄЮ ТА ГРОМАДОЮ.

15 листопада 2017 року Кабінет Міністрів України на своєму засіданні ухвалив Стратегію розвитку органів системи Міністерства внутрішніх справ на період до 2020 року[1]. Одним із головним пріоритетів якої є тісна співпраця з громадами та інститутами громадянського суспільства. У програмному документі зазначено, що Національна поліція, як орган системи МВС України, буде реалізовувати принцип «community policing». Принцип передбачає тісну взаємодію між поліцією та населенням з метою підвищення рівня безпеки в суспільстві. Тобто функції, які раніше виконувала виключно поліція, в ідеалі можуть стати спільною справою безлічі різних людей.

Залучення громади до взаємодії з поліцією базується на побудові довіри з місцевою громадою. А для цього потрібна прозорість і відкритість діяльності поліції. Люди очікують та мають бути проінформовані про методи роботи поліції, про діяльність та інциденти, а також про повагу і захист прав людини.

Сьогодні, враховуючи вектор розвитку інформатизації суспільства та вдосконалення інтернет-технологій, світ все більше й більше поринає у віртуальну комунікацію. Добитися прозорості, довіри та комунікації між громадянами та поліцією не використовуючи соціальні медіа практично неможливо.

Соціальні медіа – це комп’ютерні технології, які полегшують створен-

ня і обмін інформацією, ідеями, кар'єрними інтересами та іншими формами вираження через віртуальні спільноти та мережі. Різноманітність автономних і вбудованих соціальних медіа-сервісів, доступних на даний час, викликає проблеми з визначенням; однак є деякі загальні особливості [2]:

1. Соціальні медіа – це інтерактивні інтернет-додатки Web 2.0.

2. Призначений для користувача контент: текстові повідомлення (пости) або коментарі, цифрові фотографії, відеоролики або дані, отримані за допомогою всіх онлайнових взаємодій, є життєвою основою соціальних мереж.

3. Користувачі створюють профілі для конкретного веб-сайту або програми, які розробляються і підтримуються організацією соціальних мереж.

4. Соціальні мережі сприяють розвитку онлайн-соціальних мереж шляхом підключення профілю користувача до профілю інших осіб або груп.

Соціальні медіа – потужний інструментарій для роботи поліції, що не тільки надає можливість для безпосереднього та миттєвого спілкування, але й надає можливість комунікації з населенням, допомає змінити деякі негативні стереотипи, які, зазвичай, пов'язані з роботою поліції. Тобто використання соціальних медіа – це ефективний інструмент, який добре підходить для втілення ідеальної моделі зв'язків з громадськістю, за Дж. Грюнігом – двосторонньої симетричної моделі [3].

Двостороння симетрична модель – це налагодження ділових стосунків зі «своєю» громадськістю, які були б прийнятні для обох сторін для досягнення взаєморозуміння між керівництвом організації та громадськістю, яка має вплив на цю організацію. Обидві сторони сприймаються як групи, що дійшли спільної згоди.

Згідно з останнім дослідженням, проведеним We Are Social та Hootsuite, у 2017 році, кількість людей, які використовують соціальні медіа в усьому світі становила більше 3 млрд [4].

Кількість активних користувачів основних соціальних платформ становила: Facebook – понад 2 млрд. (залишається провідною соціальною мережею в 119 зі 149 країн), YouTube – 1,5 млрд. Значно зросло використання додатків WhatsApp – 1,2 млрд., Facebook Messenger – 1,2 млрд. користувачів.

Якщо розглянути міжнародний досвід використання соціальних медіа в роботі поліції то можна виділити декілька напрямків.

Соціальні мережі – один із ключових напрямів роботи з репутаційного менеджменту яка проводиться прес-службою поліції. Особливо використовується Twitter та Facebook. Twitter та Facebook – це швидкий і зручний спосіб поширити меседж серед великої кількості людей. Також, прес-службою періодично проводиться моніторинг соціальних мереж, щоб подивитися, чи не поширюється неточна або неправдива інформація про роботу поліції.

Забезпечення правоохоронної діяльності за допомогою соціальних інтернет-мереж дозволяє силам поліції взаємодіяти з населенням на все більш локальному (місцевому) і особистісному рівні. Наприклад, британські і голландські співробітники поліції використовують Twitter та Facebook для реагування на індивідуальні запити громадян і для безперервного інформаційного обслуговування населення в особі користувачів інтернет. У ряді інших

країн офіцери поліції відкривають свої «офіси» у віртуальному просторі і, таким чином, стають особистими контактерами для користувачів, як в реальному, так і у віртуальному світі.

Відповіді на питання та запити користувачів складають левову частку роботи в соціальних мережах. І є найскладнішим сегментом, оскільки працівникам поліції постійно доводиться вирішувати, на що реагувати, а на що ні. Щоб допомогти в цьому, наприклад, в прес-службі поліції міста Калгарі (Канада) [5] розробляються «гайдлайни» спеціально для соцмедіа. «Гайдлайн» дозволяє розподілити дописи за категоріями: прохання про допомогу, схвальні відгуки, рекомендації, скарги, спам, тролінг, дезінформація. Також для співробітників проводяться навчання та розробляється інструкція по ефективному використанню соціальних мереж.

При роботі в соціальних медіа дуже важливо підібрати правильний тон комунікації. Тон повідомлень поліції зазвичай формальний і безособовий, а самі повідомлення зводяться до передачі фактичної інформації про проведені операції. В певних ситуаціях поліція повинна зберігати в своєму голосі «залізні ноти», але, як показує досвід різних поліцейських служб, більш дружній тон спілкування куди більш ефективний: чим більше «людяними» будуть ваші повідомлення, тим краще на них реагуватимуть люди.

Для залучення більшої кількості підписників на акаунтах поліції в західних країнах проводять вікторини, акції, конкурси або розміщують жартівливі повідомлення. Так поліція Франції пообіцяла подарувати спінер переможцям вікторини [6]. Для участі у вікторині потрібно було підписатися на акаунт поліції в Facebook або Twitter і швидше за всіх правильно відповісти на питання вікторини. Всього п’ять питань – по одному в день. Подарункова іграшка була забарвлена в кольори французького триколора, в її центрі зображено логотип поліції.

Інше популярне завдання поліції в соціальних мережах пов’язана з залученням багатомільйонної аудиторії різних сервісів до розслідувань. Навесні 2014 року детектив Брайан Борг (Brian Borg) з поліції Торонто (Канада) [7] завів твіттер torontocoldcase в надії знайти нові зачіпки в ряді нерозкритих справ про вбивства. Крім деталей злочинів, в своєму акаунті він публікує орієнтування на підозрюваних.

А поліція Меріленда (США) пообіцяла в прямому ефірі провести в твіттері трансляцію захоплення притону, в якому надавали сексуальні послуги. За цим заходом можна було стежити за хештегом #PGPDVice.

Серед переваг використання соціальних мереж можна визначити: можливість легко таргетувати[9] свою аудиторію; інтерактивність, яка дозволяє одразу визначати реакцію суспільства; креативний простір, оскільки немає чітких обмежуючих факторів щодо контенту; постійне оновлення інструментарію просування через те, що соціальні мережі мають тенденцію до створення нових можливостей для підтримання інтересу громадян.

Національна поліція України в соціальних мережах повинна бути гото-

[9] від англ. target – мета – полягає у виборі якоїсь «мішені», на яку треба впливати, щоб досягти певних результатів, поставленої мети.

ва і до позитиву, і до негативу у спілкуванні, повинна бути не просто сміливою, але й готовою до прозорості. Публічна компанія підпадає під контроль суспільства, громадської думки, викликає публічну зацікавленість. Разом з тим прозорість у спілкуванні є запорукою довіри та діалогу з громадянами і зацікавленими особами поліції.

Для цього необхідно щоденно проводити прес-конференції, онлайн-презентації з актуальних питань, відеозапис кожної з них викладати на сервісах соціальних медіа (найпоширенішій серед сервісів YouTube-канал). Оперативне оприлюднення кожного виступу роблять для того, щоб уникнути ситуації, коли окремі фрази вириваються з контексту та подаються викривлено. Однак важливо не лише промотувати свою діяльність та організовувати позитивні кампанії: потрібно вміти давати раду й негативному контенту. Тобто визнавати власні помилки.

Блогінг – ще один інструмент комунікації, який повинен використовуватися у роботі поліції. За останні роки блогінг перетворився в потужний засіб, що становить конкуренцію традиційним засобам масової інформації, в тому числі онлайнових, і дозволяє здійснювати ефективний контроль над ЗМІ. Це надзвичайно гнучка мережева структура, яка допомагає мільйонам користувачів Інтернету співпрацювати, обмінюватися ідеями та координувати свої дії поза мережею. Термін «блогосфера» виник як відображення цієї нової якості комунікаційного середовища.

Блогосфера є важливим середовищем вивчення громадської думки та мемів. Вивчивши думки «блог-експертів» і найбільш читаних блогерів, можна зробити ряд висновків про характерні риси блогів як інструменту комунікації [8]: 1) блоги є неформальним каналом комунікації; 2) основний принцип блогів – наявність зворотного зв'язку; 4) зручність і простота використання; 5) широка аудиторія читачів; 7) використання розмовної мови; 8) виклад інформації в формі оповідань, щирих вражень, версій подій, близьких читачеві; 9) висока ступінь звернення до блогів; 10) великий потік інформації в блогах; 17) найсвіжіша і актуальна інформація доступна через блоги.

За допомогою блогів можна швидко «прощупати» громадську думку з будь-якого питання, відстежити реакцію на публікації, отримати репліки, які можна потім цитувати в своїх матеріалах. З цією метою багато ЗМІ заводять свої блоги спеціально як одну з форм взаємодії з аудиторією і дієвий спосіб її розширення.

На сьогоднішній день Національна поліція України робить перші кроки у освоєнні соціальних медіа. Відповідно до наказу Міністра внутрішніх справ в територіальних підрозділах поліції створені офіційні сторінки в Facebook, Twitter, YouTube, Instagram [9].

Фахівцями Міністерства внутрішніх справ проводяться заняття з відповідальними особами за наповнення контентом офіційних сторінок у соціальних мережах. Підготовлені навчальні матеріали та інструкції по ефективному використанню соціальних мереж.

Треба розуміти що успішна робота з налагодження комунікації в мережі часто залежить від сумлінності співробітників, які створюють і ведуть ін-

тернет-сторінки, безпосередньо контактуючи з підписчиками та онлайн користувачами. Хороша робота в соціальних мережах може бути тільки постійною, креативною і заснованою на знанні специфіки даного інтернет-майданчика та його аудиторії. Тільки недосвідченому користувачу може здатися, що без зайвих зусиль в Інтернеті легко створити собі ім'я і розвинути необхідний майданчик – як часто невмілі дії за таким дилетантським просуванням створило більше шкоди, ніж користі. Мертві (неоновлювані і немодеровані) сторінки можуть завдати істотної шкоди іміджу поліції.

Виходячи з принципу «community policing» та досвіду використання поліцією соціальних медіа в зарубіжних країнах, можна виділити основні напрямки, які обґрунтовують необхідність створення офіційних сторінок та використання ресурсів соціальних медіа підрозділами поліції України:

- По-перше, соціальні медіа стали новинним джерелом для суспільства, особливо для молоді, витіснивши і замінивши собою традиційні ЗМІ. Молоде покоління вважає за краще отримувати інформацію з Інтернету, а робота з молоддю – один з ключових напрямків роботи поліцейських.

- По-друге, зустрічаються і підроблені акаунти, які поширюють інформацію нібито від імені поліції. В цьому випадку створювати свої власні, офіційні акаунти – єдиний спосіб захисту від дезінформації, заснованої на чутках і спекуляціях.

- По-третє, соціальні медіа дають можливість делегувати частину повноважень поліції простим громадянам (за допомогою соціальних мереж користувачі можуть, наприклад, брати участь в пошуку зниклих людей або злочинців).

- По-четверте, варто врахувати, що соціальні медіа тісно пов'язані з повсякденним життям: щодня в мережі з'являються все нові об'єднання, які можуть привернути увагу правоохоронних органів, а моніторинг соціальних мереж дозволяє запобігти спробам тероризму, суїцидам та насильству над дітьми.

1. Розпорядження КМ України від 15.11.2017 № 1023-р «Про схвалення Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року»;

2. Steve Wildman, Jonathan A Obar Social Media Definition and the Governance Challenge: An Introduction to the Special Issue;

3. James E. Gruning and Fred C. Repper Excellance in public relation and Communication Management. Hillsdale, NJ: Lawrence Erlbaum Associates,1992;

4. Number of social media users passes 3 billion with no signs of slowing. URL: https://then-extweb.com/contributors/2017/08/07/number-so-cial-media-users-passes-3-billion-no-signs-slow-ing/#.tnw_pkwOo02Q;

5. Дорош М. Медіа та поліція: точки дотику. URL: http://osvita.mediasapiens.ua/mediaprosvita/master_clas/media_ta_politsiya_tochki_dotiku/;

6. Мурина В. Фрацузкая полиция обещает подарить спиннеры. URL: https://slon.fr/frantsuzskaya-politsiya-obeshhaet-podarit-spinnery/;

7. Сторінка у Twitter @ torontocoldcase. URL: https://twitter.com/search?q=%40%20torontocoldcase&src=typd;

8. Матёкин Н. Практическое использование блоггинга в Интернете в качестве инструмента PR. URL: www.pressclub.host.ru/PR_Lib/pr-papers/legkaya.doc;

9. Наказ МВС України від 27.07.2017 № 648 «Про створення офіційних сторінок у соціальних мережах».

**Тоневицький Андрій Миколайович**
викладач ДУ «Академія патрульної поліції»

## ДЕЯКИ АСПЕКТИ ПРАКТИКИ ПОШУКУ ТА ВИЛУЧЕННЯ ЦИФРОВИХ ДОКАЗІВ (ЗА ДОСВІДОМ ІНШИХ КРАЇН).

Інформатизація всіх сфер життя людини породили не тільки нові види злочинності, а й засоби її здійснення. Комп'ютеризація засобів організації праці перетворилася в знаряддя скоєння злочинів.

На місці події все частіше зустрічаються комп'ютерні засоби, які служили як об'єктами злочинного посягання так і були середовищам скоєння злочину і зберегли сліди злочинної діяльності. Огляд і фіксація таких об'єктів вимагає володіння певним рівнем спеціальних знань поводження з комп'ютером та іншими комп'ютерними засобами.

Як об'єкт цієї слідчої дії комп'ютерна техніка та комп'ютерна інформація виступають як:

a) предмет традиційних злочинних;

b) в якості знаряддя вчинення злочинів, знову ж таки, як традиційних (наприклад, шахрайства), так і злочинів у сфері комп'ютерної інформації. У таких випадках інші комп'ютери є «потерпілими» від проведеної щодо їх атаки і тому також підлягають огляду;

c) як об'єкт, що містить у собі інформацію, що має відношення до розслідуваної злочину.

d) як об'єкт що містить у собі інформацію, що не має безпосереднього відношення до розслідуваної злочину, але використовувався особою, в якості щоденника, телефонної книжки або для ведення переговорів в мережі Інтернет по електронній пошті. Ці відомості часто також представляють інтерес для розслідування.

Слід заначити, що тактика у разі наявності на місці подій специфічна і вимагає чітких і правильних дій.

Першою характерною рисою є обов'язкове залучення до огляду спеціаліста. Слідчий, як правило, не має досить глибокими навичками і знаннями в області комп'ютерної техніки та інформаційних технологій. І тому без допомоги фахівця він може зробити невиправні надалі помилки в ході огляду технічної апаратури, зняття необхідної інформації і (або) її вилучення.

У той же час, залучаючи фахівця, слідчому необхідно переконатися в його компетентності. Справа в тому, що загальне поняття «фахівець з комп'ютерної техніки» є не вірним. Можна говорити лише про те, що є фахівець, компетентний в конкретних комп'ютерних системах. Тому необхідний профіль знань конкретного фахівця слід визначати в залежності від цілей і завдань огляду з урахуванням даних про характер злочину.

Необхідно звернути також увагу, що в якості понятих для участі в огляді

цих об'єктів слід залучати людей, обізнаних у комп'ютерній техніці. Очевидно, що їх участь найбільш необхідно саме при даному слідчій дії, щоб виключити можливі згодом посилання зацікавлених осіб про зміни слідчим під час огляду інформації, що міститься в комп'ютері і на носіях інформації.


*Рисунок 1: заборона доступу це перший крок під час пошуку та вилучення доказів*

Для обмеження доступу зацікавлених осіб необхідно:

1. відсторонити співробітників фірми (підприємства) від комп'ютерних засобів і розмістити їх в приміщенні, що виключає використання будь-яких засобів зв'язку;

2. в процесі огляду не приймати допомоги від співробітників фірми (підприємства);

Серйозною помилкою є допуск до досліджуваного комп'ютера власника для надання допомоги в його експлуатації. Відомо багато випадків з практики, коли підозрюваний на допиті пов'язаному з комп'ютерними доказами, було надано доступ до вилученого комп'ютера. Пізніше вони розповідали своїм знайомим, як шифрували файли "прямо під носом у поліцейських", а ті про це навіть не здогадувалися. Один з варіантів у разі необхідності надати доступ до комп’ютера це зробити попередньо резервну копію комп'ютерної інформації перш, ніж надавати доступ до неї. Під час огляду та вилучення ми не маємо такої копії і надавати доступ категорично заборонено.

3. Ще одна проблема пов'язана з можливістю спростувати в суді ідентичність пред'явленого на процесі програмного забезпечення того, що знаходилося в даному комп'ютері на момент вилучення. Щоб уникнути подібних ситуацій, комп'ютер, слід опечатати в присутності понятих, не включаючи. Якщо працівник правоохоронних органів приймає рішення оглянути комп'ютер на місці, перше, що необхідно зробити, це зняти копію з жорсткого магнітного диска і інших носіїв, які будуть вилучатися як речовий доказ. Це означає, що до проведення будь-яких операцій з комп'ютером, необхідно зафіксувати його стан на момент проведення слідчих дій.

4. вилучити у персоналу, електронні записники, ноутбуки, індивідуальні пристрої відключення сигналізації автомобіля тощо;

5. вимкнути живлення міні-АТС і опечатати її (у разі наявності);

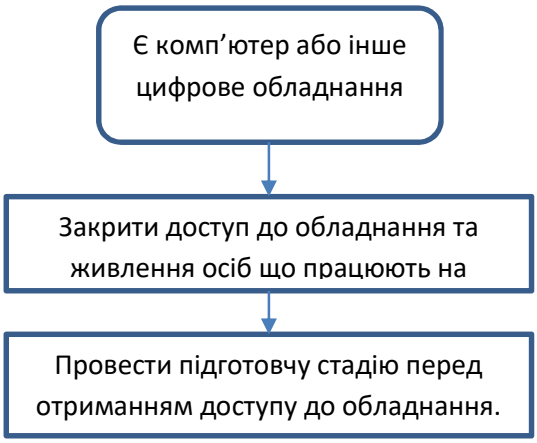



*Рисунок 2: Проведення підготовчих дій це другий крок під час проведення слідчих дій*

**Підготовча стадія** включає в собі кроки які дозволять мінімізувати небезпеку щодо знищення інформації та її спотворення під час проведення слідчих дій. Під час цієї стадії необхідно у керівника або особи, яка відповідає за експлуатацію комп'ютерної техніки відібрати пояснення, а при порушеній кримінальній справі допитати і з'ясувати наступні питання:

1. Як здійснюється допуск до приміщення з технікою:

a. Чи організовано допуск до приміщення, в якому знаходиться техніка, за електронною системою допуску.

b. Чи обладнано приміщення охоронною сигналізацією та які технічні засоби забезпечення використовуються для цього.

c. Отримати документацію і відповідний електронний або фізичний пароль чи додатковий пристрій (електронний ключ) для доступу до об'єктів.

2. Як організовано систему комп'ютерної безпеки в приміщені та безпосередньо на комп'ютерах:

a. які є засоби оповіщення і забезпечення безпеки комп'ютерної інформації при безпосередньому доступі, де знаходиться відповідна документація;

b. чи встановлені спеціальні засоби в комп'ютері для знищення інформації в разі спроби несанкціонованого доступу до неї. Якщо так, то з'ясувати місце хто саме встановив цю систему та отримати відповідну інформацію;

c. пароль чи електронний ключ для доступу до інформації (їх може бути декілька – кожен надає доступ до окремих задач чи масивів інформації. Правила його використання. Чи веде порушення цих правил до псування інформації);

3. з'ясувати інформацію щодо підключення до локальної мережі, з'ясувати її схему та правила використання;

4. з'ясувати інформацію щодо особи відповідальної за резервне копіювання і зберігання протоколів, та отримати від неї інформацію щодо знаходження відповідних документів та копій на носіях;

5. вилучити договір з провайдером у керівника підприємства, зв'язатися з адміністратором провайдера і організувати вилучення і збереження електронної інформації, що надійшла на адресу підприємства або належить йому.

Дуже великою помилкою є включення вимкненого комп’ютера та спроба попрацювати на ньому без створення резервних копій інформації. Це правило допускає, що комп'ютер - насамперед об'єкт дослідження фахівців. Тому до передачі експертам його бажано навіть не включати, оскільки категорично заборонено виконувати будь-які операції на вилученому комп'ютері без вживання необхідних заходів безпеки (наприклад, захисту від модифікації або створення резервної копії). Якщо на комп'ютері встановлена система захисту (наприклад - пароль), то його включення може викликати знищення інформації, яка знаходиться на жорсткому диску. Не допускається завантаження такого комп'ютера з використанням його власної операційної системи.

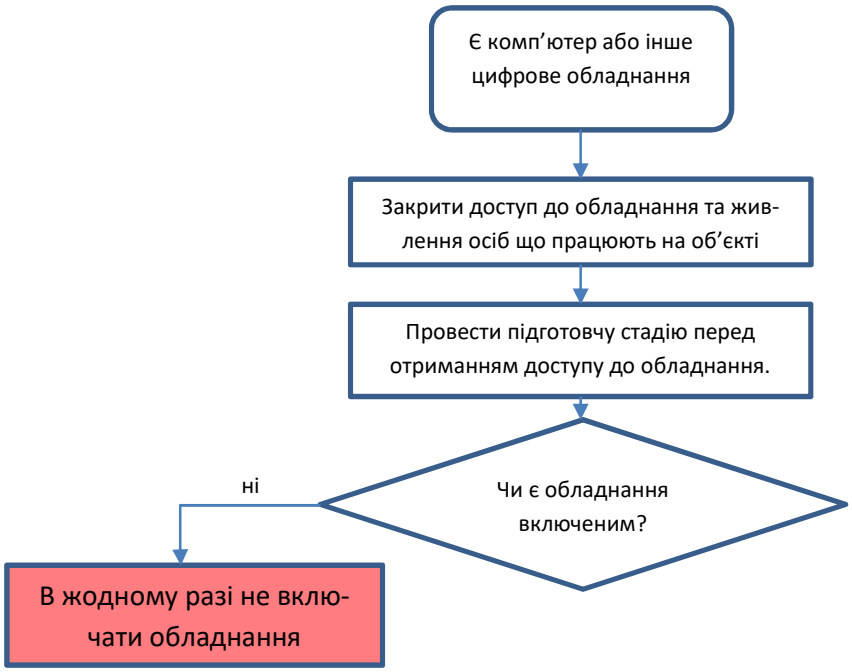



*Рисунок 3: Якщо обладнання вимкнене його включати заборонено.*

Власнику комп’ютера не складає особливих труднощів встановити на своєму комп'ютері програму для знищення інформації на носіях інформації, записавши такі "пастки" через модифікацію операційної системи.

Після того, як дані і сама руйнуюча програма, знищені, ніхто не зможе сказати напевно, чи був "підозрюваний" комп'ютер спеціально оснащений такими програмами, чи це результат недбалості при дослідженні комп'ютерних доказів.

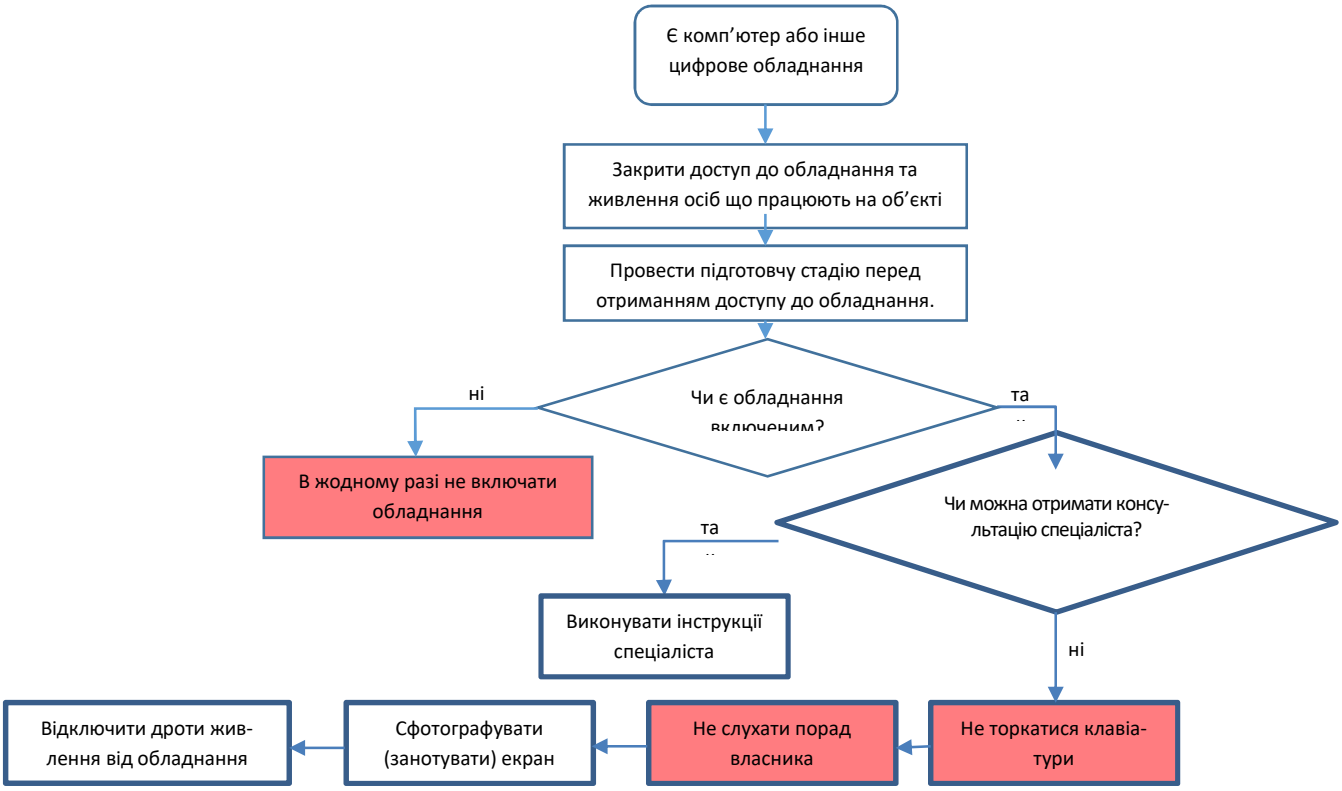



*Рисунок 4: Спрощена схема дій у випадку якщо комп'ютер є включеним.*

Спрощена схема дій може бути застосована у тому випадку, якщо особа яка проводить процедуру вилучення не має знань щодо проведення додаткових дій при огляді включеного комп'ютера, або не має можливості на місці провести такі дії. Питання проведення додаткових дій буде розглянуто у 3 питанні лекції.

Існує декілька методів вимикання комп'ютера, але правильним є саме той що вказано в алгоритмі. Кожен з інших варіантів має суттєві недоліки які можуть призвести до знищення, або спотворення інформації.

a. При відключенні дротів живлення існує можливість наявності UPS, що може призвести до спотворення інформації.

b. При відключенні за допомогою кнопки на блоці живлення комп'ютера також існує можливість наявності UPS, що може призвести до спотворення інформації.

c. При використанні кнопки включення комп'ютера буде знищена певна інформація під час завершення роботи процесів системи.

d. При використанні кнопки пуск буде видалена інформація.

Після того як було завершено процедури щодо приготування комп'ютера до вилучення, можна починати процедуру щодо безпосередньо вилучення комп'ютерної техніки.

По-перше, у разі необхідності, треба вжити заходів до виявлення та вилучення слідів рук, що залишилися на засувках приєднання зовнішніх носіїв

інформації, кнопках включення живлення, ділянках біля гвинтів кріплення кришки корпусу, клавішах клавіатури і миші, роз'ємах портів, а також на кнопках пристроїв друку.

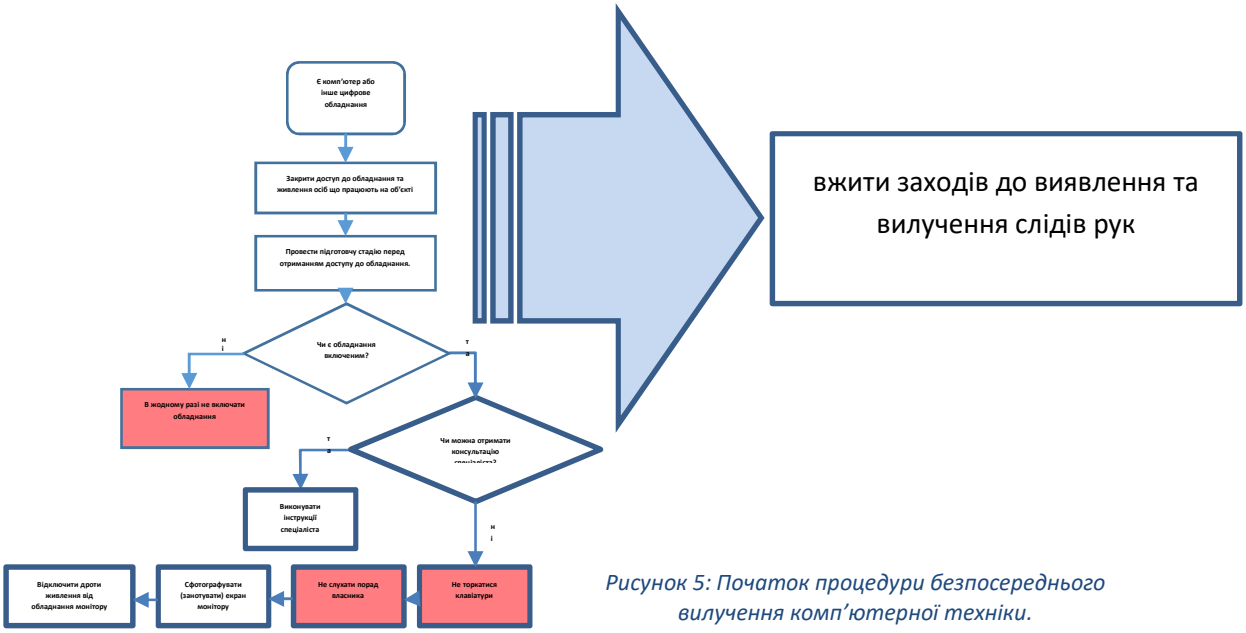



*Рисунок 5: Початок процедури безпосереднього вилучення комп'ютерної техніки.*

**Після вживання заходів щодо виявлення та вилучення проводиться безпосередній огляд комп'ютера. При цьому необхідно звернути увагу та запротоколювати наступну інформацію:**

a. склад комп'ютерного засобу: наявність системного блоку, монітора, клавіатури, принтера, безперебійного джерела живлення, колонок та ін. периферійних пристроїв;

b. по розташуванню пристроїв на передній та задній панелі системного блоку визначається наявність і види пристроїв зберігання інформації, а також пристроїв зчитування кредитних карт, парольних карт, електронного ключа і т.п., звернути увагу на наявність невідомих пристроїв;

c. по розташуванню роз'ємів на задній панелі системного блоку визначається наявність і види вбудованих пристроїв: мережева плата, наявність портів послідовного і паралельного каналів, чи були вони підключені до зовнішніх ліній зв'язку;

**При цьому необхідно встановити і відобразити в протоколі і на схемі, що додається до нього:**

- місцезнаходження комп'ютера та його периферійних пристроїв (принтера, клавіатури, монітора, миші тощо), призначення кожного пристрою, назву, розмір, серійний номер, комплектацію, наявність з'єднання з мережею та стан пристроїв (цілий або із слідами розтину);

• точно описати порядок з'єднання між собою зазначених пристроїв, промаркувати (при необхідності) сполучні кабелі і порти їх підключення, після чого роз'єднати пристрої комп'ютера;

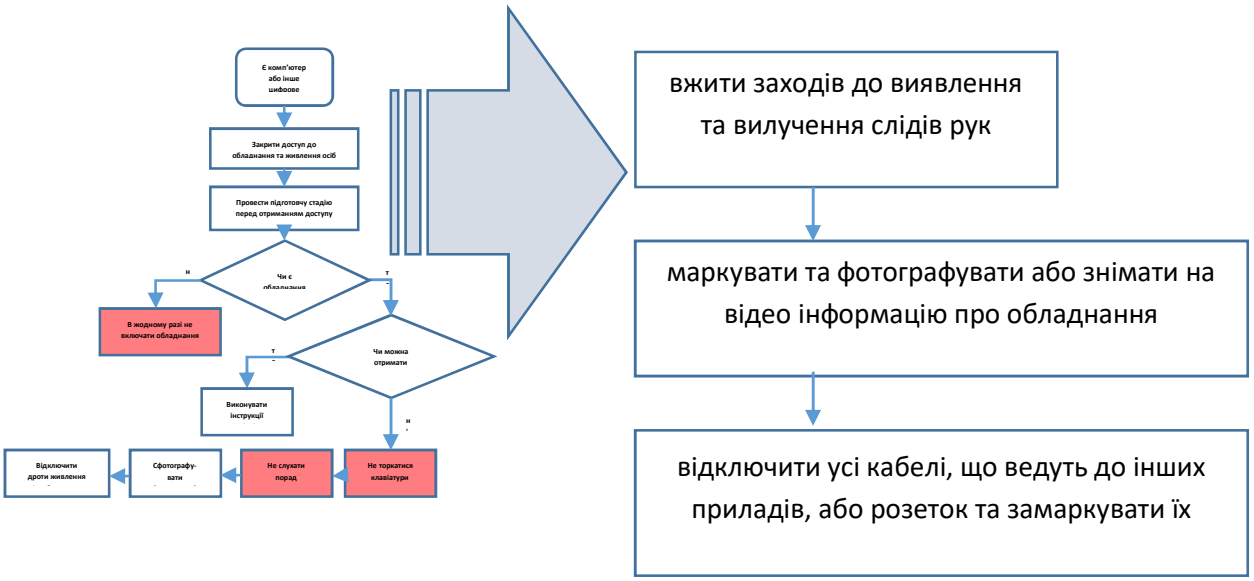



*Рисунок 6: Вимоги щодо огляду комп'ютера.*

У разі проведення вилучення комп'ютера необхідно дотримуватись наступних процедур:

1. перевіряти наявність маркування (закріплення картки доказу) на кожному компоненті який буде вилучено;

2. упакувати (із зазначенням в протоколі місця їх виявлення) носії інформації. Зазначити у протоколі наявність фірмових та саморобних наклейок та написів у разі їх наявності;

3. упакувати кожен пристрій комп'ютера та сполучні кабелі. Вказати в протоколі наявність і стан всіх заміток, пломб, спеціальних знаків і наклейок (інвентарних номерів, записів на пам'ять, контрольних маркерів фірм-продавців і ін.), нанесених на корпуси і пристрої комп'ютерів, наявність забруднень, механічних пошкоджень та їх локалізацію;

4. для виключення доступу сторонніх осіб, необхідно опечатати системний блок - заклеїти захисною стрічкою кнопку включення комп'ютера, гніздо для підключення електрокабелю, а також місця-з'єднання бічних поверхонь з передньої і задньої панелями.

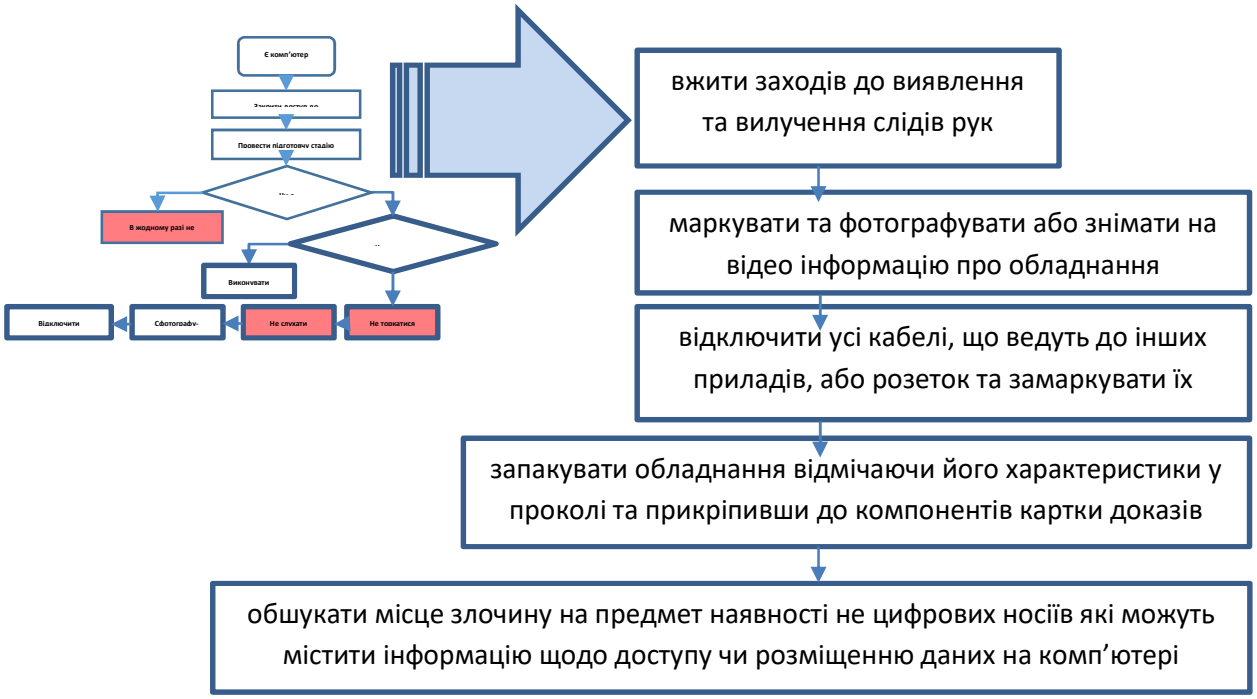



*Рисунок 7: Послідовність дій під час вилучення комп'ютера.*

Також необхідно звернути увагу на наявність на місці події щоденників, записників, стікерів, клаптиків паперу тощо. Вони можуть містити паролі, інформацію щодо місця знаходження даних на комп'ютері тощо.

**Тулупов Володимир Володимирович**
к.т.н., доцент, доцент Харківського
національного університету
внутрішніх справ

**Спориш Євгенія Юріївна**
студент Харківського національного
університету внутрішніх справ

## ЗАХИСТ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ ВІД ВИТОКУ ІНФОРМАЦІЇ

**Актуальність** обраної теми наукової роботи полягає в тому, що в сучасних умовах основна частина атак зловмисників здійснюється через комп'ютерні мережі, постійно ускладнюється їх структура, швидко збільшується кількість комп'ютерів та мережевого обладнання у тому числи систем відеоспостереження. Більш того зловмисники безперервно удосконалюють нові методики, тактики та прийоми для здійснення атак. Тому дуже важливо дослідити комп'ютерну мережу відеоспостереження на наявність слабких місць, ступінь її вразливості, рівень підготовленості ймовірних зловмисників,

можливості засобів мережевої безпеки.

Захист інформації є складовою частиною забезпечення національної безпеки будь-якої держави і забезпечується правовими, організаційними, програмними та інженерно-технічними заходами [ 1 ] .

На державному та регіональних рівнях впроваджуються різні програми та заходи безпеки. Так, наприклад у березні 2018 року на сесії Харківської обласної ради була прийнята «Програма забезпечення публічної безпеки і порядку та протидії злочинності на території Харківської області на 2018-2019 роки», відповідно до якої будуть придбатися системи відеоспостереження, стаціонарні переговорні пристрої для термінового виклику спецслужб, електронні планшети, відеореєстратори, відеотехніка та сучасні засоби зв'язку для груп швидкого реагування та правоохоронців.

Серед завдань програми є:

– удосконалення науково-методичного, матеріально-технічного та інформаційного забезпечення правоохоронних та інших органів, що беруть участь у забезпеченні публічної безпеки та порядку;

– безперервний моніторинг криміногенної ситуації в області, в т.ч. за рахунок соціологічних технологій та забезпечення своєчасного реагування на негативні зміни;

– здійснення посиленого контролю за ситуацією у публічних місцях, передусім при проведення заходів за участю значної кількості громадян;

– запобігання правопорушенням, що вчиняються з використанням телекомунікаційних мереж та мережі Інтернет.

На теперішній час у системі Міністерства внутрішніх справ впроваджено низку аналітичних систем з можливістю проведення глибокого аналізу великих масивів інформації, включаючи відкриті джерела де на першому рівні є система відеомоніторингу наприклад - єдиний аналітичний сервісний центр (UASC) поліції, створений за прикладом системи безпеки Абу-Дабі при ГУНП в Донецькій області.

**Метою даної** роботи є дослідження можливості побудови безпечної мережі відеоспостереження за об'єктами.

**Об'єктом дослідження** в даній роботі є система відеоспостереження за об'єктами.

**Відповідно до поставленої мети визначимо наступні завдання:**

– охарактеризувати стан проблем існуючих систем відеоспостереження та їх використання суб'єктами господарювання;

– дослідити канали витоку інформації та сучасні методи й засоби захисту мереж відеоспостереження;

– проаналізувати технічні завдання на проектування мереж відеоспостереження та існуючи системи на сучасному ринку готового обладнання;

– розглянути рекомендації та виділити нерозкриті проблеми щодо підвищення безпеки при використанні та проектуванні мереж відеоспостереження суб'єктами господарювання.

Системи відеоспостереження - це програмно-апаратний комплекс (відеокамери, об'єктиви, монітори, реєстратори та ін. устаткування), призна-

чений для організації відеоконтролю як на локальних, так і на територіально-розподілених об'єктах. Відеоспостереження є сьогодні невід'ємним елементом будь-якої сучасної системи публічної безпеки та порядку [ 2 ].

На даний момент системи відеоспостереження дозволяють встановлювати відеоконтроль за об'єктами будь-якої складності, а керування ними не вимагає високої кваліфікації від персоналу.

Пристрої фіксації або запису використовують як цифрові відеореєстратори (DVR), так і звичайні комп'ютери з платою відеозахоплення. Серед переваг відеореєстраторів можна виділити функції квадратора (мультиплексора), відеодетектора руху, відеомагнітофону і тому подібне. Також сучасні відео- реєстратори забезпечені мережевим або модемним інтерфейсом, що дозволяє передавати відеодані по IP- протоколу.

На відміну від відеореєстраторів (DVR) системи відеоспостереження які побудовані на базі персональних комп'ютерів (ПК) мають більше функціональних можливостей, високу продуктивність і місткість архівів, а також звичний для користувачів ПК інтерфейс.

Основні завдання, що вирішуються за допомогою систем відеоспостереження:

- можливість організації безперервного online відеозапису на DVR-пристрій, або комп'ютерну систему, що дозволяє документально підтвердити факт порушення та провести оперативний аналіз кожної ситуації;

- візуальний контроль ситуації на об'єкті - надає інформацію на пост спостереження в мультіекранному режимі (у режимі очікування), або в повноекранному режимі (зображення від однієї камери на увесь екран) в режимі реального часу. Це забезпечує можливість прийняття оперативних рішень в конкретній ситуації;

- виконання функцій охоронної сигналізації при використанні детекторів руху відеокамер або зовнішніх охоронних датчиків і інформованість оператора системи про виникнення тривоги в контрольованій зоні за допомогою світлового або звукового сигналу оповіщення.

На теперішній час в умовах створення різних сучасних систем безпеки, у тому числі систем публічної та кібербезпеки конкурентоздатну альтернативу складають системи мережевого або IP - відеоспостереження, основою для яких є IP-камери. Такі системи не вимагають прокладення додаткових ліній зв'язку, передача даних відбувається по мережевій інфраструктурі, побудованій на протоколі IP.

Контроль та адміністрування системи здійснюється з будь-якого комп'ютера , що має доступ до мережі та спеціальне програмне забезпечення .
Зараз IP- камери за ціною набагато перевищують вартість аналогових камер, але зберігаючи такий темп розвитку виробництва, незабаром вони стануть доступнішими.

При створенні технічного завдання для проектування оптимальної системи відеоспостереження слід розглянути типові технології побудови таких систем, їх переваги та недоліки. Так, при використанні аналогових систем відеоспостереження відомі виробники, наприклад компанія BOSH пропонує

спеціальний модуль для конвертації "аналогової" камери в IP –пристрій [3].

Ключовим елементом мережі IP – відеоспостереження є мережева IP-відеокамера яка має об'єктив, оптичний фільтр, ПЗС- матрицю (прилад із зарядним зв'язком), вбудований мікропроцесор для оцифровування/стискування відеозображення, мережевий контролер для підключення в мережу Ethernet та інші елементи. Найголовніше, що кожна мережева відеокамера має свій власний IP-адрес, обчислювальні функції та вбудоване ПЗ, що дозволяє їй функціонувати як повноцінний мережевий пристрій.

На відміну від аналогової відеокамери, IP-камера не потребує прямого підключення до комп'ютера або до будь-яких інших апаратних або програмних засобів. Її підключення може здійснюватися як за допомогою дротяного з'єднання (по міді або оптичному волокну), так і безпровідного (Wi-Fi, GPRS/EDGE, 3G, супутниковому зв'язку та ін.). Таким чином, досягається повна або часткова мобільність користувача, який здатний стежити за видаленими об'єктами практично з будь-якої точки земної кулі.

Тому слід виділити наступні переваги таких систем IP – відеоспостереження, а саме:

1. Оператор системи може здійснювати візуальний контроль як локально, так і віддалено (з ПК, мобільного телефону і так далі), здійснювати функції адміністрування системи відеоспостереження використовуючи переваги веб-технологій.
2. Спрощеність та малі витрати на встановлення й монтаж. Мережеві відеосистеми IP не вимагають прокладення додаткового коаксіального кабелю, як в аналогових системах, а підключаються до існуючої локальної мережі відеоспостереження за об'єктом за допомогою безпровідних технологій.
3. Якість відеозображення. В сучасних IP-системах застосовується формат MPEG-4, який дозволяє ефективніше використовувати ресурси мережі в порівнянні з форматом M-JPEG.
4. Можливість передавати по одній лінії зв’язку не лише відеосигнал, але й звук, а також управляти та адмініструвати IP-камери.
5. Гнучкість й масштабованість систем IP- відеоспостереження полягає в можливості будівництва фізично розподілених мереж відеомоніторингу, контролю і дистанційного керування без прив'язки до відстані.
6. Інтеграція з багатьма існуючими на даний момент системами відеоспостереження.

Критеріями вибору на користь IP – камер при проектуванні таких систем на теперішній час також є:

- наявність каналу зв’язку з високого пропускною спроможністю від 100 Мб/с і вище та вільних портів Ethernet;
- за рахунок вбудованих в камери WEB серверів при рішенні завдань видаленого моніторингу контрольованого об'єкту (без використання архівної інформації) з використання мережі Інтернет;
- завдання вимагають високого розділення, при невисоких вимогах до освітленості, розміру кадру і ін. (З дозволом більш 1 Мпиксель).

Виходячи з проведеного аналізу існуючих на ринку готових систем ві-

деоспостереження, найбільш перспективними технологіями відео- спостереження є IP–відеоспостереження, яке легко розгортається та базується на сучасних комп'ютерних мережах стандарту Ethernet.

Нормальне функціонування комп'ютерних мереж та її складових таких як мережеві екрани, брандмауери, фаєрволи, системи резервного копіювання, антивірусні засоби та інші) неможливо без стандартних засобів захисту, тому існує необхідність використання IDS (СВВ - систем виявлення вторгнень), які є основним засобом боротьби з мережними атаками [4].

Системи виявлення вторгнень починають усе ширше впроваджуватися в практику забезпечення безпеки корпоративних мереж які у свою чергу можуть використовувати системи IP-відеоспостереження.

Системи виявлення вторгнень забезпечують виявлення:

- мережевих атак проти вразливих сервісів;
- атаки спрямовані на підвищення прав користувачів;
- неавторизований доступ до важливих файлів;
- дії шкідливого програмного забезпечення (комп'ютерних вірусів, троянів і черв'яків).

Використання СВВ допомагає досягнути такі цілі:

- виявити вторгнення або мережеві атаки;
- забезпечити належний контроль якості адміністрування, особливо у великих і складних мережах;
- спрогнозувати можливі майбутні атаки і виявити вразливості для запобігання їх подальшого розвитку;
- отримати корисну інформацію про проникнення, для відновлення і налаштування конфігурації мережі;
- визначити розташування джерела атаки по відношенню до локальної мережі (зовнішні або внутрішні атаки) [6. с.122]

Як показала практика при використанні таких систем існує ряд проблем які істотно ускладнюють, а часом і зупиняють процес впровадження СВВ.

Фахівці в галузі інформаційної безпеки виділяють деякі з них, а саме:

- вимогливість до ресурсів і часом незадовільна продуктивність СВВ вже на 100 Мб/с мережах;
- недооцінка ризиків пов'язаних зі здійсненням мережних атак;
- невисока ефективність сучасних СВВ, що характеризується більшим числом помилкових спрацьовувань і неспрацьовувань (false positives and false negatives);
- недооцінка ризиків, пов'язаних зі здійсненням мережних атак;
- відсутність в організації методики аналізу й керування ризиками, що дозволяє адекватно оцінювати величину ризику й обґрунтовувати вартість реалізації контрзаходів для керівництва;
- висока вартість комерційних СВВ;
- висока кваліфікація експертів по виявленню вторгнень, що вимагає для впровадження й розгортання СВВ [5].

На теперішній час для України є відносно невисока залежність підприємств від Інтернет. А також фінансування заходів щодо забезпечення інформаційної безпеки по залишковому принципу, не сприяє придбанню дорогих засобів захисту для протидії мережевим атакам.

1. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки Закон України від 09.01.2007 № 537-V URL: http:// zakon.rada.gov.ua/go/537-16 (дата звернення: 06.04.2018).

2. Системи відеоспостереження (CCTV) URL:https://guard-lviv.com.ua/uk/sistemi-videonablyudeniya/index.html (дата звернення: 06.04.2018).

3. Гібридні системи захисту URL: https://guard-lviv.com.ua/sistemi-videonablyudeniya.html (дата звернення: 07.04.2018).

4. Intrusion Detection System (IDS) URL: https://ru.wikipedia.org/wiki/IDS (дата звернення: 07.04.2018).

5. А. Астахов. IDS как средство управления рисками URL: http://www.globaltrust.ru/security/Pubs/Pub2_part5 (дата звернення: 10.04.2018).

6. Сєвєрінов О.В. Аналіз сучасних систем виявлення вторгнень / О.В. Сєвєрінов, А.Г. Хрєнов // Системи обробки інформації Збірник наукових праць. – Харків: ХУПС. – 2013. – Вип. 6 (122). – С. 122-123.

**Тишлек Дмитро Петрович**
начальник Управління захисту
економіки в Дніпропетровській
області ДЗЕ Національної поліції

## СУЧАСНИЙ СТАН ЗАХИСТУ ЕКОНОМІКИ ДНІПРОПЕТРОВСЬКОЇ ОБЛАСТІ. КОРУПЦІЙНІ ПОРУШЕННЯ ТА ПРАВОПОРУШЕННЯ ПОВ'ЯЗАНІ З КОРУПЦІЄЮ – ПРИЧИНИ ТА УМОВИ ВЧИНЕННЯ

У зв'язку з загальнодержавним курсом, спрямованим на підвищення рівня правової і економічної безпеки України, підготовкою до вступу до Європейського союзу, імплементацію європейських цінностей та вимог до економічної безпеки, Департаментом захисту економіки Національної поліції України вживаються відповідні рішучі заходи з протидії економічній злочинності, встановлення причин та умов, що сприяють вчиненню як окремими громадянами так і організованими групами економічних злочинів та корупційних правопорушень, у різних сферах економіки та суспільного життя нашої держави.

Найбільш актуальними тривалий час та в умовах сьогодення залишаються питання протидії злочинності і порушенням у таких «болючих» напрямках як:

- бюджетна сфера;
- службові злочини та порушення, пов'язані з вимаганням, отриманням, пропозицією, наданням неправомірної вигоди, використанням службового становища для отримання протиправних благ та переваг, перевищення влади

та службових повноважень, ін.;

- корупційні правопорушення та правопорушення, пов'язані з корупцією, за які передбачено кримінальну, адміністративну, дисциплінарну та/або цивільно-правову відповідальність;

- злочини, вчинені організованими злочинними групами та злочинними організаціями.

Так, якщо звернутись до статистичних даних, то управлінням захисту економіки в Дніпропетровській області протягом 2017 та першого кварталу 2018 року досягнуто певних результатів з протидії злочинам та правопорушенням у сфері економіки.

Протягом 2017 року за матеріалами управління захисту економіки в Дніпропетровській області відкрито 395 кримінальних проваджень (163 кримінальні провадження, пов'язані із використанням бюджетних коштів), 42% (167) з них – за тяжкими та особливо тяжкими злочинами, 31 провадження – за злочинами зі збитками понад 100 тис. грн, у т.ч. 9 – із сумою збитків понад 1 млн. гривень, 257 особам повідомлено про підозру у вчиненні кримінальних правопорушень, які виявлені працівниками УЗЕ в Дніпропетровській області, з яких – 97 у вчиненні кримінальних правопорушень у бюджетній сфері. Сума збитків у закінчених провадженнях про злочини у сфері державного бюджету перевищила 49,3 млн. грн., відшкодовано понад 8,4 млн. грн. До суду надіслані кримінальні провадження стосовно 7 організованих злочинних груп (у т.ч. дві – з корупційними зв'язками і одна – у бюджетній сфері) з обвинувальними актами стосовно 34 осіб. За фактами легалізації (відмивання) доходів відкрито 6 кримінальних проваджень, повідомлено про підозру 12 особам, до суду *з* обвинувальними актами надіслано10 кримінальних проваджень. Відкрито 76 кримінальних проваджень фактами вимагання та отримання неправомірної вигоди, реалізовано 39 матеріалів про хабарництво, затримано «на гарячому» 45 осіб. Середня сума хабарів становила 93 040 тис. грн., загальна – 4 млн. 186 тис. 800 гривень. Виявлено 273 правопорушення, пов'язаних з корупцією, за якими складені адміністративні протоколи стосовно 211 осіб (у т.ч. 12 – судді, 4 – посадові особи державної служби найвищої категорії «А», 33 – посадові особи державної служби, які займають відповідальне становище). У судах протягом року розглянуто 168 протоколів, накладено штрафи на загальну суму 231 тис. 540 гривень.

Протягом першого кварталу 2018 року за матеріалами управління вже відкрито 113 кримінальних проваджень (у бюджетній сфері – 48), з яких – 50 (44%) за тяжкими та особливо тяжкими злочинами. Повідомлено про підозру 66 особам, за вчинення тяжких та особливо тяжких злочинів – 31 особі, у т.ч. 14 особам – у вчиненні злочинів у складі організованих злочинних груп. Досудовим розслідуванням закінчено та надіслано до суду з обвинувальним актами матеріали 63 кримінальних проваджень, сума встановлених збитків за якими перевищує 5,3 млн. гривень. На підставі здобутої інформації щодо отримання неправомірної вигоди відкрито 14 кримінальних проваджень, реалізовано 13 матеріалів та «на гарячому» затримано 18 осіб. Загальна сума

хабарів - 1,4 млн. гривень, середня – 86,6 тис. гривень. За злочинні посягання на бюджетні кошти оголошено про підозру 29 особам, до суду надіслано 83 кримінальних провадження, з обвинувальним актом – 79. Збитки у розслідуваних провадженнях про кримінальні правопорушення в сфері державного бюджету склали понад 5,2 млн. гривень, відшкодовано майже 4,7 млн. гривень. Направлено до суду кримінальне провадження стосовно однієї ОЗГ у складі 6 осіб. Працівниками управління складено 116 протоколів про правопорушення, пов'язані з корупцією, у відношенні 96 осіб, серед яких 14 посадових осіб, які займають відповідальне становище, 5 державних службовців центральних органів влади, 3 – судді. У судах протягом кварталу розглянуто 43 протоколи, накладено штрафи на загальну суму 28 тис. 900 гривень.

Наведена статистика свідчить про великий обсяг роботи, яка проводиться не тільки підрозділами захисту економіки, слідчими, оперативно-технічними підрозділами Національної поліції, а й іншими правоохоронними органами, такими як наприклад органи прокуратури, а також представниками судової гілки влади, так як досягнення кінцевого результату у попередженні, виявленні, припиненні, усуненні наслідків та відшкодуванні збитків, спричинених суспільно небезпечними діяннями у сфері економіки можливе лише за тісної злагодженої плідної праці вищевказаних суб'єктів боротьби зі злочинами і правопорушеннями, що посягають на економічну безпеку держави.

З практичної точки зору причинами досить високого рівня порушень у сфері економіки є:

- загальна низька правова, патріотична культура, правосвідомість населення і посадових осіб різного рівня, правовий нігілізм;
- загальний низький (у порівнянні з розвинутими країнами) рівень матеріального забезпечення осіб, уповноважених на виконання функцій держави;
- наявність колізій законодавства, що тягне за собою непоодинокі випадки уникнення від відповідальності за вчинення правопорушень у сфері економіки;
- складний та тривалий у часі порядок притягнення винних осіб до відповідальності.

**Тюря Юлія Іванівна**
к.т.н., доцент,
начальник навчально-методичного
відділу Дніпропетровського державного
університету внутрішніх справ

**Акімова Олена Олександрівна**
заступник начальника
навчально-методичного відділу
Дніпропетровського державного
університету внутрішніх справ

# ЕЛЕМЕНТИ ФОРМУВАННЯ ЕКОНОМІЧНОГО МИСЛЕННЯ У ВИБІРКОВІЙ СКЛАДОВІЙ ПРОГРАМИ ПІДГОТОВКИ ФАХІВЦІВ З ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ

Сучасний ринок освітніх послуг вимагає від закладів вищої освіти Міністерства внутрішніх справ України (далі - ЗВО МВС) враховувати в своїй діяльності зміни глобального зовнішнього середовища та своєчасно реагувати на виклики сьогодення для підтримки сталого розвитку. В останні роки відбувається посилення конкуренції на українському ринку освітніх послуг, що обумовлено необхідністю впровадження стандартів вищої освіти, які затребувані роботодавцями та адаптовані до міжнародного досвіду. ЗВО МВС повинні бути готовими до цієї конкуренції, до орієнтації на споживачів освітніх послуг – здобувачів вищої освіти та роботодавців – і до використання в освітньому процесі інноваційних форм і методів навчання. Освітня політика вишів має бути орієнтована на підвищення адекватності результатів їх освітньої діяльності, наближення рівня підготовки фахівців до потреб роботодавців – підрозділів Національної поліції та Міністерства внутрішніх справ України, організацій, підприємств, установ регіону, тобто зміцнення зв'язків навчання з практикою. Розробка сучасних і прогресивних освітньо-професійних програм, має бути спрямована на підвищення внутрішньої мотивації здобувачів на навчання та гарантувати їм можливість самовдосконалення й отримання інтелектуального задоволення, а також можливості отримати цікаву та високооплачувану роботу.

Метою публікації є аналіз системи підготовки фахівців з фінансово-економічної безпеки та висвітлення особливостей формування економічного мислення у здобувачів вищої освіти, які навчаються за цією спеціалізацією.

Формування економічного мислення є предметом досліджень багатьох науковців в різних сферах суспільних наук. Значна кількість наукових праць присвячена дослідженню його формування у майбутніх фахівців різних не економічних спеціальностей. Дослідники вивчають економічне мислення як різноманітні фактори розвитку потенціалу особистості для різних категорій фахівців, але чіткої системи та показників сформованості цього нововведення

сьогодні конкретно не визначено.

Дослідження Н. Пасічник присвячені аналізу формування економічного мислення майбутніх вчителів [1]. Як влучно зазначено Н. Пасічник, проблеми розвитку мислення вивчалися ще з часів античності. Проводячи аналіз наукових підходів щодо трактування змісту й особливостей економічного мислення авторка дійшла висновку, що економічне мислення – це інтелектуальна властивість особистості, здатність пізнавати сутність економічних процесів, виявляти їх закономірності через мисленеві операції (аналіз, синтез, порівняння, абстрагування, узагальнення) і реалізувати економічні знання, уміння та особистісні якості в економічній діяльності.

Наукові дослідження К.Ю. Тушко присвячені визначенню ролі загальноекономічної освіти у фаховій підготовці майбутніх офіцерів-прикордонників [2]. Слід зауважити, що проблема формування економічного мислення залишилася поза увагою автора. Але дослідниця зазначає, що в системі підготовки майбутніх офіцерів-прикордонників «… сьогодні елементи змісту економічної підготовки все ще носять фрагментарний, недостатньо скоординований характер і не утворюють єдиної системи» [2]. На її думку, необхідно посилити увагу до теоретичних основ загальноекономічної освіти майбутніх фахівців, удосконалення її змісту, запровадження нових форм, методів і прийомів економічної самоосвіти з метою формування високого рівня їх економічної компетентності. Автор стверджує, що при підготовці офіцерів-прикордонників економічна складова професійної освіти не повинна зводитись до накопичення суми необхідних знань та умінь, а передбачати, в першу чергу, формування відповідного рівня економічної компетентності.

Филюк Г.М. зазначає, що розвиток наукового економічного мислення є складовою виховної функції економічної теорії, сутність якої полягає у формуванні в індивідів економічної культури; логіки економічного мислення та розуміння сучасних процесів; аналітичних здібностей, які забезпечують цілісне уявлення про функціонування економіки на національному та світовому рівнях; виховання в індивідів усвідомлення того, що досягти професійних успіхів можна шляхом глибоких знань та наполегливої праці; здатності приймати рішення та відповідати за їх наслідки [3]. Це твердження, на нашу думку, певною мірою відповідає сучасним вимогам, що стоять перед системою підготовки фахівців для потреб Національної поліції та МВС України.

Дослідники С.С. Сливка, О.Д. Несімко та М.Й. Штангрет, проводячи культурологічно-правовий аналіз економічної безпеки, стверджують, що у нинішніх умовах взаємодія економіки і права зумовлена завданнями формування нового економічного мислення та свідомості, оволодіння економічними знаннями та навиками щодо прийняття рішень, необхідних для економічного та соціального будівництва, сприяє плодотворному співробітництву і створює міцну основу для нової галузі знань і практичної діяльності – економічної культури юриста. На думку авторів, механізми, що пов’язують економіку і право, мають загальну культурну основу, що закладена у професіоналізмі людей. І в економічній, і в правовій сферах професіоналізм визначає існування «своєї» сфери так само, як і розвиток у ній окремого індивіда [4].

Не можливо не погодитись із твердженням авторів, що високий ступінь оволодіння економічними знаннями та навиками дає можливість ефективно виконувати практичну юридичну діяльність: попереджати і запобігати недотриманню фінансової дисципліни посадовими особами та окремими громадянами; не допускати фінансово-господарських зловживань у державі; активно сприяти зменшенню обсягів тіньової економіки і перетворення її в легальну; підтримувати чесне підприємництво і ставити перепони злочинним махінаціям тощо, що є необхідним для утвердження економічної безпеки [4].

Сьогодні науковці одностайні у думці, що формування економічного мислення сприяє розвиткові таких компетентностей майбутніх фахівців як здатність до аналізу, синтезу, узагальненню, систематизації, культури передачі інформації, розвиненості образного, репродуктивного, теоретичного та інтуїтивного мислення. Саме ці компетентності виступають базовими в формуванні майбутнього офіцера Національної поліції нової генерації

Ми погоджуємося з твердженням авторів [4], що рівень економічних знань юриста передбачає глибоке знання природних економічних законів, які повинні стати моделлю для законів, що приймаються державою, насамперед тих законодавчих актів, що регулюють матеріально-економічну сферу діяльності, адже недотримання природних економічних законів досить часто призводить до непередбачуваних наслідків. Мікроекономічні явища доволі часто стають причиною правових явищ, де в основному й реалізується службовий обов'язок юриста. Тобто так чи інакше стихійний або активний економічний розвиток суспільства включений у правовий простір.

Їх думки, що у здійсненні юристами-професіоналами державного контролю над економічною сферою життя суспільства і полягає їх внесок щодо захисту економічної безпеки держави не викликають сумніву. Нове економічне мислення юриста формує відповідну економічну свідомість, підґрунтя якої становить правосвідомість. Економічне мислення спрямоване насамперед на виховання у юриста непохитної віри у свою державу, оскільки поєднання економіки і права в їх діалектичному взаємозв'язку допомагає глибше зрозуміти суть економічних реформ ринкового типу, осмислити основні методи саморегулювання господарства та особливості розвитку нових форм господарювання, що зміцнює економічний і науковий потенціал, економічну безпеку нашої держави [4].

Підтримуючи ці твердження можна констатувати, що формування економічного мислення у здобувачів вищої освіти сприятиме підвищенню ефективності їх майбутньої професійної діяльності. І основними ознаками її ефективності, як зазначають С.С. Сливка та інші [4], виступатимуть: здатність проведення економічного аналізу протиправних дій, економічного аналізу їх матеріальних наслідків (завданої шкоди), логіка економічних узагальнень, захист економічних прав вітчизняних виробників тощо.

Суттєвий вплив на необхідність формування системи підготовки фахівців з фінансово-економічної безпеки в системі МВС України має сучасний розвиток ринкових відносин, проявами якого є, зокрема, формування нових видів господарських структур та ускладнення господарсько-договірних взає-

мовідносин, що, в свою чергу, вимагає якісно нових умінь та навичок від фахівців, задіяних в системі юридичного супроводу підготовки і прийняття рішень з попередження та запобігання економічним злочинам.

Не викликає сумніву те, що працівники Національної поліції нової генерації повинні уміти аналізувати соціально-економічні процеси з точки зору їх економічної доцільності, прогнозувати економічні наслідки правових дій, встановлювати причинно-наслідкові зв'язки між економічними та правовими явищами, свідомо використовувати знання про закони ринку та ринкову економіку, сприяючи розвитку цивілізованого підприємницького середовища. З цих позицій, більш глибоке та комплексне вивчення економічних засад функціонування господарських структур є актуальним завданням реформування системи підготовки фахівців для підрозділів Національної поліції, професійна діяльність яких буде спрямована на захист економічних інтересів організацій, підприємств, установ та держави, в цілому.

Сьогодні система підготовки фахівців цього напряму професійної діяльності у Дніпропетровському державному університеті внутрішніх справ (далі – Університет) перебуває на стадії становлення. Вона включає в себе організацію освітнього процесу та науково-виховної роботи зі здобувачами вищої освіти, які обрали саме цю спеціалізацію. Колективом Університету зроблені певні кроки в напрямі розвитку цієї спеціалізації:

– активно проводиться робота щодо модернізації наявної матеріально-технічної бази, яка передбачає створення лабораторій та інтерактивних кімнат, де здобувачі вищої освіти матимуть змогу в умовах максимально наближених до реальної професійної діяльності відпрацьовувати навички аналітичної та оперативно-розшукової діяльності;

– проводяться наукові дослідження з питань запобігання злочинам в економічній та фінансовій сферах, актуальних питань захисту економіки. В діючих курсантських наукових гуртках виокремленні секції з питань цієї тематики;

– науково-педагогічні працівники, які викладають дисципліни економічного спрямування підтримують тісні взаємовигідні зв'язки та проходять стажування в регіональних підрозділах захисту економіки Національної поліції України;

– розроблено і запроваджено освітньо-професійну програму підготовки фахівців в галузі знань «Право» (08) зі спеціальності «Право» (081) за спеціалізацією фінансово-економічна безпека загальним обсягом 240 кредитів ЄКТС.

Дисципліни запропонованої спеціалізації дозволять здобувачам оволодіти навичками та професійними компетентностями щодо реалізації основних завдань Національної поліції з викриття, попередження та розкриття злочинів у сфері економіки. Майбутні офіцери поліції отримають базові знання з економіки, підприємництва, економічного аналізу та фінансової звітності підприємств.

Також майбутнім фахівцям з фінансово-економічної безпеки для набуття компетентностей щодо кваліфікації злочинів у економічній та фінансо-

вій сферах, особливостей їх розслідування та оперативно-розшукової діяльності суб'єктів протидії цим злочинам запропоновані навчальні дисципліни кримінально-процесуального та оперативно-розшукового спрямування (рис. 1).

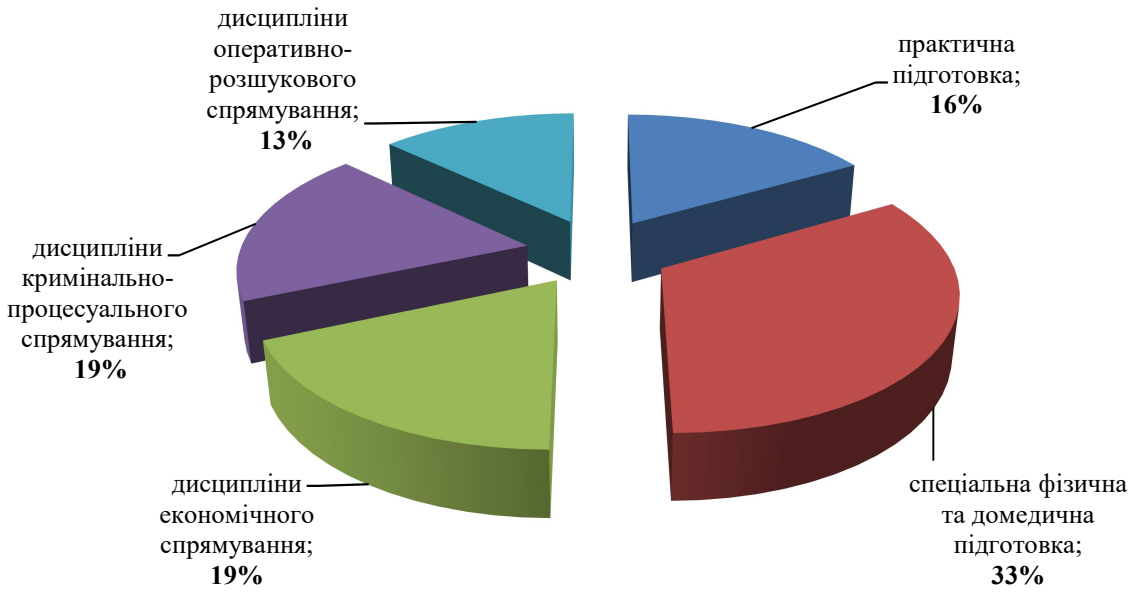



*Рис. 1. Структура вибіркової частини (за вибором здобувачів вищої освіти) навчального плану підготовки фахівців з фінансово-економічної безпеки*

Теоретичні знання та практичні навички, які здобувачі отримують в результаті вивчення базових юридичних дисциплін, впродовж всього періоду навчання доповнюються блоком економічних дисциплін.

Економічна складова Програми традиційно розпочинається викладанням навчальної дисципліни «Основи економічної теорії», яка обґрунтовує економічну політику. Економічна теорія допомагає переосмислити те, що відбувається, й дає можливість передбачити наслідки впливу будь-якого економічного суб'єкта на ті, чи інші економічні параметри [3]. На нашу думку, економічна теорія закладає фундамент економічного мислення, оскільки саме вона, розкриваючи економічні закони і формулюючи принципи, дає можливість визначити цілі, обрати інструменти та способи їх досягнення і таким чином обґрунтувати економічну політику держави, встановлювати сфери та ступінь державного впливу на економіку.

Фундаментальні знання, отримані при опануванні основ економічної теорії, доповнюються прикладними аспектами функціонування економіки та дії економічних законів; економічними та організаційними питаннями підприємництва, які розглядаються в наступній навчальній дисципліні – «Основи економіки та підприємництва». Саме вона аналізує принципи поведінки підприємницьких структур в умовах ринкової економіки. Під час вивчення цієї дисципліни у здобувачів вищої освіти формуються професійні та аналітичні здатності щодо використання найновіших підходів до прийняття господарських рішень, організації планування, управління та здійснення розрахунків. Ця дисципліна виступає черговою ланкою формування економічного мис-

лення, оскільки логічно висвітлює систему економічних відносин суб'єктів господарювання, тобто висвітлює господарський механізм у вигляді відповідних категорій і понять у їхній єдності і взаємозумовленості.

Надалі прикладні аспекти економічної теорії розвиваються в навчальній дисципліні «Основи економічного аналізу», яка формує поряд з економічним мисленням, ще й аналітичні здібності.

Економічний аналіз все ширше застосовується при вивченні різнопланових неринкових інститутів, починаючи від масових заворушень, відвідувань церкви та кількості суїцидів і, завершуючи законодавством про аборти, сімейне життя та розлучення і виступає прикметною ситуацією для економічної безпеки [4]. Старушкевич А.В відводить значну роль методу економічного аналізу, як інструменту одержання криміналістично значимої, насамперед, орієнтуючої інформації, яка важлива при виявленні й розкритті злочину, висуванні й плануванні версій. На думку автора, застосування цього безсумнівно ефективного методу при виявленні ознак розкрадань допомагає у вирішенні завдань, спрямованих як на доказування обставин злочину, так і на встановлення проміжних (допоміжних) фактів його вчинення [5].

Завершується блок економічних дисциплін Програми прикладною дисципліною «Фінансова звітність підприємств», яка формує компетентності щодо здатності «читання» бухгалтерської, податкової та фінансової звітності суб'єктів господарювання існуючими методами економічного аналізу. Ця дисципліна дозволяє правильно зрозуміти природу господарських операцій та відображення їх у фінансовому та податковому обліку й звітності суб'єктів господарювання. Здобувачі отримують навички розрахунку показників фінансового стану суб'єктів господарювання та набувають компетентності щодо визначення суті викривлень внаслідок неправдивої фінансової звітності та визначення їх мети: факти збагачення за рахунок суб'єктів господарювання, маніпулювання економічними рішеннями користувачів звітності тощо.

Вивчення цих дисциплін має сформувати економічне мислення і готовність до розвитку впродовж життя економічних знань, умінь і навичок, а також дає можливість підвищити рівень економічної культури та уміння мислити і діяти в категоріальній системі ринкової економіки. Симбіоз фундаментальних знань з юриспруденції та базових знань дії економічних законів, принципів поведінки суб'єктів господарювання на ринку дасть змогу здобувачам вищої освіти поєднати в майбутній професійній діяльності економічну та правову культуру, які мають спільну природу. Майбутній офіцер поліції матиме розуміння, що будь-яке необґрунтоване правове рішення призводить до економічних наслідків, і навпаки, будь-яке необґрунтоване економічне рішення матиме правові наслідки. Інакше кажучи, розуміння природи і принципів дії економічних законів ринку розвине у випускників уявлення про взаємозв'язок та взаємний вплив права та економіки.

Підсумовуючи, слід додати, що здобувши освіту за спеціалізацією фінансово-економічна безпека, майбутній офіцер поліції матиме глибокі сучасні знання юриспруденції та чітке уявлення про економічні закони функціонування ринку і підприємницьких структур, а також отримає компетентності

щодо стратегічного мислення, володіння навичками інтуїтивного мислення, ухвалення швидких та правильних рішень. Випускник володітиме економічною термінологією, основами економічної та аналітичної діяльності; матиме уявлення про системи прийняття рішень, упорядковування, систематизування, структурування знань й різних даних (інформаційні, статистичні тощо) та використовуватиме для аналізу процесів і явищ бази даних.

Необхідно зауважити, що Програма включає лише базові навчальні дисципліни економічного спрямування і цілком очевидно, що отримати глибокі знання з економіки неможливо. Але її головним завданням, на нашу думку, повинно стати виховання та розвиток у здобувачів вищої освіти вміння та бажання до самоосвіти та самовдосконалення впродовж життя за умов системного підходу до формування економічного мислення.

Системний підхід до формування економічного мислення у здобувачів вищої освіти, на нашу думку, має включати процес гармонійного розвитку його здібностей, що дає можливість ефективно проявляти себе в різних сферах (науково-пізнавальній, професійній, суспільній), а також дасть змогу сформувати певні погляди й інтереси. Основними елементами цього підходу мають стати:

– залучення на навчання до Університету за цією спеціалізацією на етапі прийому мотивованих, цілеспрямованих і більш підготовлених абітурієнтів;

– організація пізнавальної діяльності здобувачів вищої освіти під час освітнього процесу, тобто безпосередньо в аудиторії за участю науково-педагогічного працівника з використанням інноваційних форм навчання (ділові ігри, тренінги, лекції-конференції, лекції-дебати тощо);

– організація самостійної пізнавальної діяльності здобувачів під час самостійної та індивідуальної роботи з дисциплін економічного спрямування з використанням елементів дистанційного навчання;

– організація та проведення постійно-діючих тренінгів для здобувачів вищої освіти з актуальних питань економіки, фінансів, оподаткування тощо;

– організація наукової діяльності здобувачів в гуртках;

– пізнавальна діяльність через навчання інших, тобто активне залучення здобувачів вищої освіти до загальноуніверситетських соціальних проектів з питань правової освіти школярів та молоді.

Поряд з цим, слід зауважити, що одним з головних завдань сучасного розвитку системи вищої освіти в МВС України є підготовка поліцейського нового покоління, але до сих пір в масовій свідомості суспільства зберігається стійке уявлення про «подвійний негативний відбір» – коли зниження престижу цієї професії, недостатня соціальна захищеність поліцейського призводять до того, що далеко не найкраща частина випускників шкіл бажають отримувати цю професію, а відтак, система підготовки поліцейських – це і є сама «слабка» ланка системи української вищої освіти. Ця проблема потребує першочергового вирішення. Без зміни ставлення суспільства до професії поліцейського та істотного підвищення якості підготовки фахівців цього профілю, вирішити стратегічні завдання забезпечення Національної поліції висо-

коквалiфiкованими кадрами неможливо.

1. Пасічник Н. Соціально-психологічні аспекти розвитку економічного мислення майбутнього вчителя. / Наталя Пасічник. // [Електронний ресурс]. – режим доступу: http://dspace.kspu.kr.ua/jspui/bitstream/123456789/2097/1.pdf. Дата доступу: 14.04.2018.

2. Тушко К.Ю. Удосконалення економічної підготовки як один із засобів формування професійно-економічної компетентності майбутніх офіцерів прикордонників у процесі фахової підготовки. / Клавдія Юріївна Тушко. // [Електронний ресурс]. – режим доступу: file:///C:/Users/admin/Desktop/znpnapv_ppn_2014_4_31.pdf. Дата доступу: 14.04.2018.

3. Филюк Г. М. Економічна теорія і економічна політика в Україні: відносна відособленість / Г.М. Филюк. // [Електронний ресурс]. – режим доступу: http://enpuir.npu.edu.ua/bitstream/123456789/17719/1/Filyuk.pdf. Дата доступу: 14.04.2018.

4. С.С., Несімко О.Д., Штангрет М.Й. Економічна безпека: культурологічно-правовий аналіз / С.С. Сливка, Сливка О.Д. Несімко, М.Й. Штангрет // [Електронний ресурс]. – режим доступу: http://www2.lvduvs.edu.ua/documents_pdf/visnyky/nvse/01_2010/ssskpa.pdf. Дата доступу: 15.04.2018.

5. Старушкевич А.В. Метод економічного аналізу злочинної діяльності. / Анатолій Володимирович Старушкевич. // [Електронний ресурс]. – режим доступу: http://www.lexline.com.ua/?language=ua&go=full_article&id=1323. Дата доступу: 15.04.2018.

**Федорова Наталя Євгенівна**
викладач Українського державного
хіміко-технологічного університету,
м. Дніпро

## ШЛЯХИ ПОДОЛАННЯ КІБЕРЗЛОЧИННОСТІ ЯК ФОРМИ ПРОЯВУ ІНФОРМАТИЗАЦІЇ СУСПІЛЬСТВА

На сучасному етапі суспільного розвитку інформаційно-комунікативні технології проникають в усі сфери людської діяльності, а їх ефективне використання перетворюється у основне джерело конкурентних переваг як на рівні фірми, так і на рівні національної економіки.

В той же час, інформатизація як складний та суперечливий процес протікає нелінійно на проявляє себе у формі загострення як позитивних, так і негативних суспільних явищ, підсилює існуючі й створює низку нових специфічних загроз прогресивному соціально-економічному розвитку, серед яких важливе місце займає кіберзлочинність як форма використання інформаційного простору в якості інструмента протиправних дій.

Згідно з даними досліджень компанії «Norton», щодня у світі 1,5 мільйона людей, або 18 осіб у секунду, піддаються атакам кіберзлочинців. За оцінками компанії, 556 мільйонів дорослих жителів світу мають досвід атак кіберзлочинців, серед яких 21% користувачів онлайн-мереж стали жертвами соціальних злочинів чи мобільних технологій, 15% користувачів скаржилися на викрадання коштів з власних рахунків, кожен десятий користувач став же-

ртвою підроблених посилань або шахрайства [1].

Досвід розвинених країн дозволяє виділити серед засобів боротьби з Інтернет-правопорушеннями декілька їх груп: юридичні, інституційні, організаційні і технічні, при цьому міжнародний характер кіберзлочинності вимагає від світової спільноти координації зусиль з її подолання.

До групи юридичних заходів можна віднести:

- конвенцію Ради Європи «Про кіберзлочинність» (2001 р.);
- бангкокську декларацію з попередження злочинності та кримінального правосуддя (2005 р.);
- бухарестську декларацію про міжнародне співробітництво в боротьбі з тероризмом, корупцією і транснаціональною організованою злочинністю (2006 р.);
- спільний проект Європейського союзу і Міжнародного Союзу Електрозв'язку для держав Тихоокеанського регіону (проект ICB4PAC);
- проект ООН з розробки законодавства в області кіберзлочинності для країн Африки (проект ESCWA) тощо [2].

У більшості європейських країн прийняті закони, що дають можливість притягнути до відповідальності провайдерів за розміщення на їхніх сайтах інформації незаконного змісту; мережеві оператори не можуть бути притягнуті до відповідальності за зміст інформації, яка передається мережами, однак вони зобов'язані на умовах виданих ліцензій вжити необхідних заходів щодо користувачів і клієнтів, які використовують мережі для передання інформації незаконного змісту. У зв'язку з цим у Великій Британії, Німеччині та Нідерландах створені незалежні органи, які розробляють етичні стандарти для змісту інформації та класифікації незаконної інформації [3].

До групи інституційно-організаційних заходів можна віднести перш за все створення ефективних управлінських структур та підрозділів, що здійснюють заходи киберзахисту. На сьогодні існують дві великі організації, які готові взяти на себе провідну роль у боротьбі з кіберзлочинністю на міжнародному рівні. Це Підрозділ по боротьбі з тероризмом ОБСЄ та Інтерпол. Крім цього, у ЄС розпочав роботу Центр по боротьбі з кіберзлочинністю (European CyberCrime Centre) [4].

На національному рівні в розвинених країнах також створюються відповідні спеціалізовані організації та підрозділи. Наприклад, у США це U.S. Cyber Command, у Великобританії – Cyber Security Operations Centre, у Німеччині – Internet Crime Unit та Federal Office for Information Security тощо. У січні 2013 року в Гаазі, Нідерланди, почав роботу Європейський центр по боротьбі з кіберзлочинністю [5].

У зв'язку з тим, що основною причиною розвитку злочинів, пов'язаних з інформаційно-комунікативними системами, виступає недостатня обізнаність користувачів у питаннях безпеки інформації, необхідною складовою забезпечення кібербезпеки виступає створення та затвердження інформаційних програм, покликаних прищепити користувачам нові моделі поведінки та роботи, проведення активної роз'яснювальної роботи серед населення щодо небезпек кіберзагроз, а також заснування нової програми освіти, в якій ро-

биться акцент на навчання ІТ-фахівців та професіоналів в області кібербезпеки. Так, нещодавно Великобританія вперше провела разом з Європейськими, американськими і канадськими партнерами захід під назвою GetSafeOnlineWeek для підвищення розуміння загроз кібербезпеки серед населення [6].

Як приклад технічних засобів боротьби з кіберзлочинністю можна назвати такі способи забезпечення безпечного доступу до Інтернету, як блокування сайтів, фільтрацію і класифікацію веб-сайтів, відстеження активності інтернет-користувачів (перлюстрацію повідомлень), введення авторизації користувачів, контроль над ІТ-обладнанням , фільтрацію інтернет-контенту. У якості методів фільтрації контенту використовуються заходи з блокування інтернет-ресурсів за IP-адресою, спотворення DNS-записів, блокування сайтів за URL, пакетної фільтрації, фільтрації через HTTP проксі-сервер, фільтрації результатів пошуку. Так, у Китаї уряд зобов'язав інтернет-компанії перевіряти вміст своїх мереж і видаляти заборонену інформацію. З 2012 року всі блогери зобов'язані реєструватися, вказуючи персональні дані та номери телефонів. Фірма Tencent, власник популярного в Китаї інтернет-месенджера QQ, дає спецслужбам можливість моніторити повідомлення користувачів, здійснюючи пошук за конкретними словами. Китайська версія Skype дозволяє перехоплювати повідомлення, що містять певні слова або надіслані певними користувачами, зберігаючи їх на сервері разом з даними про IP-адреси [7].

Отже, використання світового досвіду боротьби з кіберзлочинами може бути корисним і для України, що характеризується дуже високим рівнем кіберзлочинності.

1. Кобилянська, Л.М. Кіберзлочинність як глобальна загроза економічній безпеці сучасної держави / Л.М. Кобилянська // Науковий вісник Херсонського державного університету. – 2014. – Випуск 8. – Ч. 5. – С. 14-17.

2. Лісайчук, А.А. Проблеми боротьби із кіберзлочинністю на міжнародному рівні [Электронный ресурс]. – Режим доступу: URL: https://internationalconference2014.wordpress.com/2014/10/09/.

3. Федорук, О.В. Концептуальні засади формування системи забезпечення національної інформаційної безпеки / О.В Федорук // Вісник соціально-економічних досліджень – 2013. – Випуск 2 (49). – ч. 1. – С. 182-188.

4. Кібертероризм у складі сучасних проблем національної безпеки [Електронний ресурс] Режим доступу: URL: https://www.nbuv.gov.ua/Portal/soc_gum/bozk/2007/17text/g17_30.htm.

5. European Cybercrime Centre at Europol [Електронний ресурс] Режим доступу: URL: https:// //www.europol.europa.eu/ec3.

6. Садовська, Є.В. Міжнародний досвід у боротьбі із загрозами інформаційній безпеці – уроки для України [Електронний ресурс] Режим доступу: URL: http:// dsaua.org/].

7. Атаманова, Ю.Є. Захист прав інтелектуальної власності у мережі Інтернет / Ю.Є. Атаманова // Право та інновації. – 2014. – № 3 (7). – С. 7-14.

**Федулова Світлана Олександрівна**
к.е.н., доц. завідувач кафедри
теоретичної та прикладної економіки
ДВНЗ «Український державний
хіміко-технологічний університет»

# ПРІОРИТЕТ ВОДНОЇ БЕЗПЕКИ В ЯКОСТІ ГЛОБАЛЬНОГО РИЗИКУВ КОНТЕКСТІ БЕЗПЕКИ ЕКОНОМІЧНОЇ

Сьогодні існує безліч різних визначень терміна «безпека». У більш загальному сенсі цей термін визначається як «безпека людини», що включає соціальні, екологічні та більш ширші аспекти.

Протягом останніх десятиліть широко обговорювалися концепції продовольчої безпеки, енергетичної безпеки і доступу до природних ресурсів. Однак, на сьогоднішній день, все більше число дослідників визнають, що навколишнє середовище та безпека взаємопов'язані.

Зокрема, на прикладі водних ресурсів, можна стверджувати, що дефіцит прісної води представляє як пряму, так і непряму загрозу безпеці, оскільки з одного боку, в результаті цього дефіциту складається небезпечна обстановка, а з іншого боку, він чреватий потенційними конфліктами.

Державна стратегія регіонального розвитку на період до 2020 року, що затверджена постановою Кабінету Міністрів України від 06 серпня 2014 р. № 385, визначає вплив таких світових тенденцій просторового розвитку, яких не уникнути і Україні, а саме [1]:

– урбанізація, депопуляція села, зміна системи розселення;

– загальна відкритість світу щодо руху робочої сили, що впливає на відтік за межі країни як найбільш інтелектуальних, так і найменш кваліфікованих робочих кадрів;

– фінансово-економічна криза, обмеженість ресурсів (насамперед водних), зростання світової потреби у продовольстві, орієнтація на території, які є найбільшими виробниками продовольства.

Доступ до водних ресурсів має вирішальне значення для добробуту людей в усіх сферах життя – особистого, сімейного і суспільного. Вода також важлива для економічної діяльності. Вона – запорука здоров'я природних екологічних і біологічних систем. У багатьох секторах економіки ведеться боротьба за обмежені водні ресурси. Вода є єдиним засобом, за допомогою якого можуть бути в сукупності вирішені основні глобальні проблеми (продовольча, енергетична криза, криза охорони здоров'я і кліматичні зміни, економічна криза). Можливо, для розподілу води між споживачами і максимального збільшення вигоди за цілою низкою секторів розвитку необхідно виробити певні компроміси. Це завдання є дуже важливим для економіки, виконати яке на практиці досить складно [2].

Аналіз глобальних тенденцій на період до 2030 року показує, що попит на водні ресурси істотно зросте через збільшення населення планети. У

зв'язку з цим у науковий обіг, все більшою мірою, вводиться поняття водної безпеки. У 2009 році Всесвітній економічний форум дав пріоритет водної безпеки в якості глобального ризику, заявивши, що «безпека води це нитка, яка з'єднує в павутину продовольство, енергетику, клімат, економічне зростання і виклики безпеки людини, з якими зіткнеться світова економіка протягом наступних десятиліть» [3].

За оцінками Національної розвідувальної ради США попит на продовольство до 2030 року виросте на 35 відсотків, а на воду – на 40. Майже половина населення світу буде жити в районах, що зазнають серйозну нестачу прісної води [4].

Світова наукова спільнота почала використовувати термін «водна безпека» набагато раніше, ніж український науковий світ. На 2-му Всесвітньому водному форумі в 2000 році, Всесвітня Водна Рада представила своє бачення «світу водної безпеки – бачення в ім'я води, життя і навколишнього середовища». Глобальним Водним Партнерством (GWP) було опубліковано працю «На шляху досягнення водної безпеки: платформа для дій».

Отже, технічним комітетом Глобального Водного Партнерства було представлено визначення терміна «водна безпека», а саме: «водна безпека, на будь-якому рівні, від побутового до глобального, означає, що кожна людина має доступ до достатньої кількості безпечної води за доступною ціною для чистого, здорового і продуктивного життя, забезпечуючи при цьому, захист навколишнього середовища» [3].

Проблемами розробки методології безпеки в Україні, в основному, займається Національний інститут стратегічних досліджень. На даний момент розроблена методика розрахунку інтегральної оцінки рівня економічної безпеки України. Дана методика включає 9 складових інтегральної оцінки: демографічна, енергетична, продовольча, соціальна, інноваційна, зовнішньоекономічна, фінансова, інвестиційна та макроекономічна. Вчені даного інституту зазначають, що економічна безпека держави є важливою складовою національної безпеки, але при цьому підкреслюють, що це складна система, яка має свою структуру і внутрішню логіку, що обумовлює необхідність вдосконалення методології інтегральної оцінки рівня економічної безпеки держави з метою забезпечення адекватного реагування на дестабілізуючі чинники.

25 травня 2016 Глобальне водне партнерство України та Інститут водних проблем і меліорації НААН провели Другий національний політичний діалог, присвячений обговоренню зацікавленими сторонами питань досягнення водної безпеки в аграрному секторі країни та управління засухами як важливих складових продовольчої безпеки держави в умовах змін клімату.

Можна зазначити, що і в Україні починає зароджуватися нове наукове поняття «водна безпека», яке тісно пов'язане як з економічною безпекою регіональних систем держави, так і з національною безпекою.

Найсерйозніша загроза безпеці, пов'язана з дефіцитом води, – не війни за водні ресурси, а скоріше аспект безпеки людини, який може поставити під загрозу як безпеку держави, так і міжнародну безпеку.

Однак, потрібно враховувати, що не тільки дефіцит води може заронн-

ти зерна конфлікту, а й сам конфлікт може привести до нестачі води. Конфлікти мають прямі наслідки для водних ресурсів, наприклад, у вигляді забруднення води. Так, води Дунаю були забруднені під час конфлікту в колишній Югославії – в Боснії і в ще більшому ступені під час війни за Косово. Також, греблі і дамби, насосні станції і каналізації можуть постраждати під час військових дій. В сьогоднішніх умовах необхідно не змагатися один з одним, намагаючись забезпечити себе водними ресурсами, а співпрацювати.

З ростом водного дефіциту в ряді країн, останнім часом у зв'язку з глобальним потеплінням, виникла ціла низка стратегій його подолання, які включають економію на споживанні води, знесолення солонуватою або солоною морської води. Ще одна альтернатива полягає в мінімізації споживання води шляхом імпорту водоємної продукції – як сільськогосподарської, так і промислової, включаючи енергетику. З'явилася концепція віртуальної води. Творцем концепції «віртуальної води», пов'язаної з вимірюванням об'єму води, втіленої в продукцію і торгівлю продовольчими та іншими споживчими товарами, є професор Лондонського університету Джон Антонії Алан [5]. Дана концепція допомагає зрозуміти, скільки води потрібно для того щоб зробити різні товари і послуги.

Концепція «віртуальної води» дозволила по-новому поглянути на питання ефективного водокористування та водної політики.

Як зазначає професор Хвесик М. («Віртуальна вода: міф чи реальність?»), зберігаючись в товарі та її вартості, вода переміщається по ланцюжку від місця виробництва до кінцевого споживача. В умовах глобальної економіки відстані, які долають товари, становлять тисячі кілометрів. Якщо врахувати товарообіг між країнами і континентами, то показники торгових операцій дуже високі. Не менш значними є і обсяги водних складових, а також їх грошове вираження.

Потоки віртуальної води формуються на основі експортно-імпортних операцій. Необхідно відзначити, що за тематикою водних ресурсів в Україні публікується велика безліч доповідей про стан навколишнього середовища та оцінки стану водних ресурсів, які містять різноманітні матеріали і багату статистичну інформацію. У той же час аналіз всіх національних і регіональних публікацій, які висвітлюють ефективність використання водних ресурсів, показує, що сьогодні не вистачає великого обсягу інформації, а її актуальність для ефективних політичних рішень як і раніше залишається низькою.

Даний науковий напрям, звичайно ж, вимагає постановки завдань дослідження, розробки методик аналізу та оцінки, а також пов'язаних з цим визначенням порогових значень, механізму реалізації концепції водної безпеки з метою забезпечення адекватного реагування на дестабілізуючі чинники і збереження економічного розвитку держави.

---

1. Про затвердження Державної стратегії регіонального розвитку на період до 2020 року: Постанова Кабінету Міністрів України від 6 серп. 2014р. № 385. URL : http://zakon2.rada.gov.ua/laws/show/385-2014-%D0%BF (дата звернення : 21.02.2017).

2. Управление водными ресурсами в условиях неопределенности и риска // Обзор важных сообщений 4-го доклада об освоении водных ресурсов мира (WWDR4) / Доку-

мент опубликован в рамках Программы оценки водных ресурсов ООН. UNESCO-WWAP, 2012. 16 с.

3. Водная безопасность: Применение концепции на практике / Илко ван Бик, Воутер Линклаен Арриенс. Перевод: Е. Абдраманова, под редакцией к.г.н. В. Соколова // Тематическая публикация Технического комитета № 20. Глобальное Водное Партнерство (GWP). Ташкент : Секретариат GWP Центральная Азия и Кавказ, 2014. 48 с.

4. Глобальные будущие тенденции 2030: альтернативные миры. Публикация Национального разведывательного совета США / перевод: Усманова О.К. Ташкент : Научно-Информационный Центр МКВК, 2013. 32 с.

5. Allan, J.A., 1998. Virtual water: a strategic resource. Global solutions to regional deficits. Groundwater, 36(4):545-546.

**Фісуненко Надія Олександрівна**
аспірант кафедри міжнародних
економічних відносин
Університет митної справи та фінансів

## ВАЖЛИВІСТЬ ІНВЕСТИЦІЙНИХ РЕСУРСІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ КРАЇНИ

В сучасних кризових умовах стан економічної безпеки держави визначає можливості соціально-економічного розвитку та темпів зростання національної економіки. Для практичного забезпечення економічної безпеки об'єктивно необхідно сприяти активізації інвестиційного процесу, його спрямування на забезпечення потенціалу позитивних економічних та соціальних змін в умовах загострення соціально-економічних суперечностей, виникнення загроз здатності до економічного розвитку та підтримки економічного суверенітету держави [1, с. 460]. Свою реалізацію це знаходить у посиленні спрямованості інвестиційних процесів на забезпечення сталого економічного зростання досягнення реальних структурних зрушень у національному господарстві, технічному переозброєнні, підвищенні якісних показників господарської діяльності і, головне, якості і рівня життя населення.

Однією з найважливіших складових економічної безпеки є інвестиційна безпека. Інвестиційна безпека держави забезпечується за умов дотримання граничної норми інвестування, що дає можливість: відтворювати науково-технічний та інтелектуальний потенціал нації; здійснювати розширене відтворення основного капіталу; підтримувати конкурентоспроможність економіки; гарантувати стійке зростання ВВП на рівні завдань соціально-економічного розвитку і міжнародного співробітництва; створювати стратегічні резерви; долати депресивні явища у регіонах країни; зберігати і відновлювати природні ресурси; утримувати на безпечному рівні екологічні параметри [2, с. 36-58].

Інвестиційна безпека є сукупністю нормативно-правових, соціальних і економічних та політичних чинників, що визначають тип і динаміку відтворювального процесу і забезпечують надійність відшкодування та ефективність використання вкладеного капіталу (інвестиційних ресурсів).

Економіка України тривалий період перебуває в умовах гострого дефіциту інвестиційних ресурсів. Тому підвищення інвестиційної привабливості та забезпечення сприятливого інвестиційного клімату в Україні залишаються питаннями стратегічної важливості, від реалізації яких залежать соціально-економічна динаміка, перспективність залучення у світові ланцюги створення вартості та виробничі мережі, можливості модернізації на цій основі національної економіки.

Досліджуючи інвестиційні ресурси національної економіки, було встановлено, що їх доцільно групувати на наступними видами:

- матеріально-речові інвестиційні ресурси;
- трудові інвестиційні ресурси;
- наукові та інноваційні інвестиційні ресурси;
- фінансові інвестиційні ресурси.

Дане групування дає можливість дослідити інвестиційні ресурси за показниками та виділити основні загрози для інвестиційної безпеки. При цьому потрібно досліджувати як внутрішні загрози (стан фінансових ринків, банківської системи, технологічний рівень виробництва основних галузей економіки, ступінь зносу основних виробничих фондів, неготовність будівельного комплексу забезпечити необхідний рівень обсягів будівництва тощо), так і зовнішні загрози, спричинені умовами зовнішніх.

Пропонуємо до показників, що характеризують матеріально-речові ресурси, віднести: обсяг основних засобів в економіці України, введення в дію основних засобів, обсяги реалізованої продукції та послуг; ступінь зносу основних засобів, інвестиції в основний капітал та обсяг виконаних будівельних робіт.

Наявність основних фондів, що виступають як основний капітал (матеріально-речовий ресурс) та як вагомий потенціал економіки, станом на сьогодні та необхідністю (в новому будівництві, реконструкції, реставрації, капітальному ремонті, впорядкуванні об’єктів містобудування, розширенні та технічному переоснащенні підприємств та їх модернізація) у майбутньому, визначає економічні передумови подальшого розвитку національної економіки.

Аналізуючи динаміку обсягу основних засобів (далі - ООЗ) в економіці України та ступінь зносу основних засобів на рис. 1, встановлено, що у період з 2015 року спостерігається стрімке зниження ООЗ на 44,4 % від показників 2014 року, що пов’язано в першу чергу з тимчасово окупованою територією Крим та воєнними подіями на сході країни.

Ступінь зносу основних засобів за цей же період також зростає, але всього на 1,8%, що при загальному обсязі основних засобів є сприятливим. Втім, незважаючи на незначне збільшується ООЗ у 2016 та 2017 рр., ступінь зносу основних засобів стрімко зростає, і у 2017 становить 58,9%.

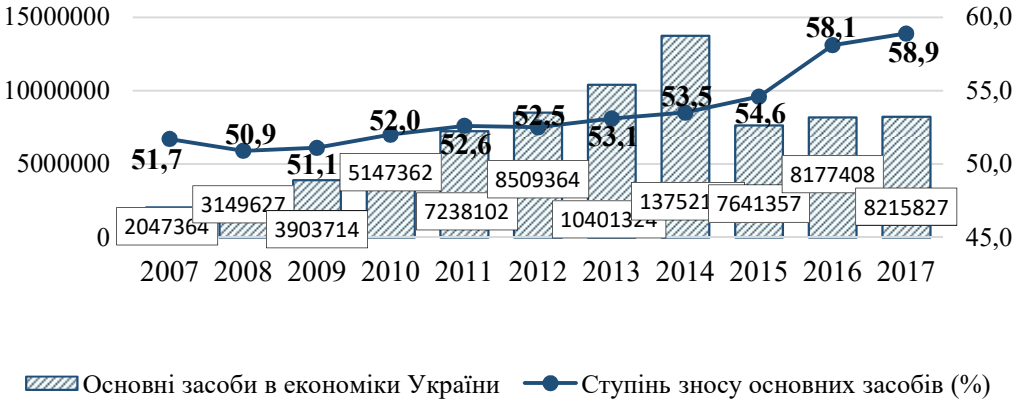



*Рис. 1. Співвідношення обсягів основних засобів в економіку України та ступеня зносу основних засобів у період 2007 - 2017 рр.**

*Джерело: побудовано автором на основі даних [4, с. 246]

Як засвідчує проведене дослідження, зниження обсягів основних засобів та високий ступінь їх зносу є загрозою для національної економіки.

До дослідження трудових інвестиційних ресурсів, які мають також велике значення для економічної безпеки країни та національної економіки, запропоновано віднести показники: кількість підприємств (суб'єктів господарювання), потреба роботодавців у працівниках, кількість найманих працівників загалом по країні, рівень зареєстрованих безробітних та загальних рівень безробіття.

Розглядаючи та порівняючи кількість зареєстрованих підприємств та кількість найманих працівників загалом по країні (рис. 2), встановлено, що при збільшення кількості суб'єктів господарювання знижується чисельність найманих працівників. При цьому за період з 2007-2017 рр., середня кількість працівників починаючи з 2012 року поступово зростає.

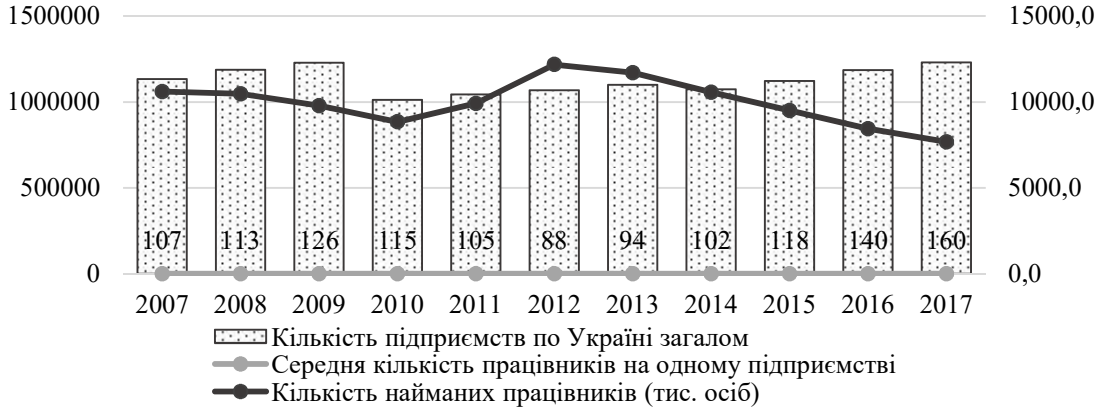



*Рис. 2. Показники кількості зареєстрованих підприємств та кількість найманих працівників за період 2007-2017 рр.**

*Джерело: побудовано на основі даних [4, с. 126-128]

Досліджуючи загальний рівень безробіття по Україні (у %) за останні десять років, з'ясовано, що показник збільшився з 6,4% у 2007 рік до 9,7% у 2017 році.

Отже, зниження кількості найманих працівників та високий рівень без-

робітних впливає на стан інвестиційної безпеки України.

Досліджувати наукові та інноваційні інвестиційні ресурси (нематеріальні інвестиційні ресурси) запропоновано за показниками: обсяг витрат фінансування наукових та науково-технічних робіт, обсяг фінансування інноваційної діяльності та обсяг витрат на фінансування наукових розробок організацій власними силами.

Досліджуючи обсяги фінансування наукових та науково-технічних робіт та обсяг витрат на фінансування наукових розробок організацій власними силами, можна стверджувати, що за період з 2007-2017 рр. показники зростають (рис. 3).


*Рис. 3. Динаміка обсягів фінансування наукових та науково-технічних робіт та обсяг витрат на фінансування наукових розробок організацій власними силами за період 2007-2017 рр.**

*Джерело: сформовано на основі статистичних даних [3, с. 57-63]

Отже, зростання показника обсягів фінансування наукових та науково-технічних робіт характеризує активацію науково-технічних розробок. А зниження обсяг витрат на фінансування наукових розробок організацій власними силами навпаки свідчить про скорочення попиту на інвестиційні ресурси зовні.

Тобто, науковий потенціал країни затребуваний, посідає важливе місце і належить до важливих індикаторів сталого розвитку національної економіки та інвестиційної безпеки країни.

Що ж стосується фінансових інвестиційних ресурсів, то вони відіграють визначальну роль у підтримці стабільності економіки, забезпеченні пропорційного та збалансованого функціонування різних галузей, підвищенні рівня життя населення держави.

Для аналізу фінансові інвестиційні ресурси до яких запропоновано використовуються показники: капітальні інвестиції загалом в економіці країни, фінансовий результат до оподаткування підприємств, рівень рентабельності діяльності підприємств, обсяги кредитів та відсоткова ставка по кредитам, доходи, витрати, заощадження населення, середньомісячна номінальна заробітна плата, індекс споживчих цін, обсяги депозитів, ставка по депозитам, офіційний курс гривні по відношенню до долара США, ставка НБУ та обсяги прямих іноземних інвестицій в економіку країни.

Розглядаючи показники доходів, витрат та заощадження населення, що характеризують обсяг вільних фінансових ресурсів домогосподарств, зроби-

мо висновок, що доходи населення починаючи з 2007 по 2016 роки поступово зростають, витрати також зростають (зростає купівельна спроможність), але незважаючи на позитивну динаміку росту доходів, заощадження населення кожного року зменшуються (табл. 1) і у 2016 році взагалі мають від'ємне значення у вигляді -0,5%, тобто витрати населення склали 100,5% при загальному доході населення у 100%, отже знижується купівельна спроможність населення.

Таблиця 1

Співвідношення доходів, витрат та заощадження населення у (%)

| Показники | Роки | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 |
| Доходи населення | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| Витрати населення | 93,9 | 97,3 | 92,2 | 87,1 | 88,3 | 89,7 | 92,8 | 98,2 | 99,1 | 100,5 |
| Заощадження населення | 6,1 | 2,7 | 7,8 | 12,9 | 11,7 | 10,3 | 7,2 | 1,8 | 0,9 | -0,5 |

Про зниження купівельної спроможності свідчить і динаміка індексу споживчих цін – показник, що характеризує динаміку загального рівня цін на товари та послуги, які купує населення для невиробничого споживання, тобто показник загального рівня інфляції в економіці, за допомогою якого вимірюється цінова стабільність в країні і неконтрольоване знецінення національної валюти. Фактично відбулась «консервація» рівня реальних фінансових доходів громадян. Зважаючи на сталу динаміку реального сектору економіки і заробітних плат, найближчим часом не слід очікувати зростання депозитних вкладень. Низький рівень життя населення визначатиме рівень споживчого попиту, який може стимулювати економічне і інвестиційне відновлення.

Вивчаючи динаміку фінансового результату діяльності підприємств до оподаткування (показник прибутковості підприємств) та рівень рентабельності (показник, який характеризує інвестиційну привабливість), встановлено, що у період 2014-2015 рр. підприємства мають збиток -348471,7 млн. грн., та рівень рентабельності у 2016 році становить -0,2.

Аналізуючи динаміку показників та співвідношення обсягів капітальних інвестицій в економіці країни та обсягів прямих іноземних інвестицій, виявлено, що обсяги іноземних інвестицій кожного року зменшуються і це свідчить про недовіру іноземних інвесторів і становить велику інвестиційну загрозу.

Світова економіка історично сформувала вагомість інвестиційних ресурсів для забезпечення економічної безпеки країн. Нажаль в Україні інвестиційна безпека досить хитка, що суттєво погіршило готовність іноземних інвесторів вкладати кошти у розвиток вітчизняної економіки, наслідком чого стало «вимивання інвестиційного» потенціалу.

На сьогоднішній день нема чинників, за рахунок яких вдалося б помітно посилити інвестиційну безпеку України. Основні інвестиційні ресурси українські підприємства отримують, в основному, з власних джерел, власних нагромаджень. Але економічний розвиток держави в сучасних умовах має обов'язково підпорядковуватися національній ідеї, національним інтересам, що є спільною ознакою для всіх розвинених країн, рушійною силою і найвагомішим фактором мобілізації суспільства, основою консенсусу, засобом реалізації його інвестиційного потенціалу.

1. Економічний суверенітет України : монографія / А.А. Мазаракі, Т.М. Мельник, В.В. Юхименко, В.М. Костюченко та ін. ; за ред. А.А. Мазаракі та Т.М. Мельник. – К.: Київ. нац. торг.-екон. ун-т, 2015. – 700 с.
2. Кулицький С. Проблеми розвитку української економіки у контексті загрози дестабілізації міжнародних фінансових ринків [Електронний ресурс] / С. Кулицький // Україна: події, факти, коментарі. – 2015. – № 21. – С. 36–58. – Режим доступу: http://nbuviap.gov.ua/images/ukraine/2015/ukr21.pdf
3. Науково-технічний комплекс статистичних досліджень. – К.: ІЦВ Держстату України, 2017. – 223 с., с. 57-63
4. Статистичний щорічник України за 2016 рік / за редакцією І. Є. Вернера. Київ: Державна служба статистики України, 2017. – 611с.

**Харазішвілі Юрій Михайлович**
д.е.н., с.н.с., головний науковий співробітник Інституту економіки промисловості НАН України

**Ляшенко В'ячеслав Іванович**
д.е.н., проф., завідуючий відділом Інституту економіки промисловості НАН України, м. Київ

## СУЧАСНА КОНЦЕПЦІЯ СТАЛОГО РОЗВИТКУ З ПОЗИЦІЙ ЕКОНОМІЧНОЇ БЕЗПЕКИ

Важлива роль науково-технологічного прогресу та інноваціям у промисловості приділяється у звіті ООН, без яких процес індустріалізації є неможливим, що, у свою чергу, стримує розвиток [1]. З одного боку, завдяки технологіям процес виробництва стає більш ефективним, підвищуючи, тим самим, конкурентоспроможність країн і знижуючи їх уразливість через коливань на ринках. З іншого боку, економічне зростання тягне за собою збільшення обсягу використаних ресурсів, матеріалів і викопного палива, що призводить до забруднення і деградації навколишнього середовища, особливо в країнах з низьким рівнем доходу. Тому, якщо країни не будуть робити кроків за всіма трьома напрямками – підтримувати економічне зростання, сприяти соціальному розвитку та прагнути до екологічної стійкості – і по досягненню комп-

ромісних рішень між ними, то малоймовірно, що такі країни далеко просунуться на шляху до сталого промислового розвитку, незалежно від рівня їх розвитку. Така концепція безпосередньо узгоджується з трактуванням економічної безпеки.

Отже, головний висновок звіту ООН полягає в тому, що технології можуть служити досягненню цілей у всіх трьох вимірах сталого розвитку, збалансованість яких займає одне з провідних місць серед проблем сталого розвитку країн або регіонів. У цілому відсутня збалансованість економічного, соціального та екологічного розвитку як у промислових регіонах, так і в регіонах України в цілому, яка трансформується на державний рівень [2].

Дослідженням проблем сталого розвитку України та промисловості присвячені праці як зарубіжних, так і вітчизняних вчених. Серед них варто виділити праці Б.Є. Патона, М.З. Згуровського, Н.Д. Панкратової, О.Ф. Новикової і О.І. Амоши, Е.М. Лібанової і М.А. Хвесика, О.І. Амоши і В.П. Вишневського та інших.

Незважаючи на об'ємність та важливість виконаних досліджень, слід зауважити, що недостатньо уваги приділяється визначенню існуючого стану сталого розвитку – методології інтегрального оцінювання рівня сталого розвитку країни (регіонів, основних видів економічної діяльності - ВЕД). У першу чергу це стосується обґрунтуванню переліку складових та їх індикаторів для відображення соціального, екологічного та економічного стану країни. У більшості формулювань стратегії спостерігається обов'язкова наявність в визначеннях певних цільових орієнтирів, на досягнення яких повинна бути спрямована стратегія. Тому, наукове обґрунтування кількісних орієнтирів індикаторів стратегій розвитку є необхідним та актуальним. На жаль, більшість стратегій, які пропонувались в Україні до цього часу, визначали основні напрями та пріоритети реалізації стратегії через декларування необхідних заходів на кшталт: *забезпечення*, *підвищення*, *створення*, *формування*, *оновлення*, *упровадження*, *удосконалення*, *залучення* та *розроблення*. На нашу думку визначення напрямів та пріоритетів модернізації є умовою необхідною, але недостатньою.

Отже, у таких Стратегіях відсутні зрозумілі критерії досягнення сталого розвитку як в цілому, так і на рівні складових. Таким чином, вони носить переважно декларативний характер, якій не дає чіткого уявлення щодо результатів дії – науково обґрунтованих кількісних орієнтирів складових та індикаторів по кожному року, моніторинг яких дозволив би контролювати процес розвитку визначених напрямків. Висновки, які робляться за таких досліджень, можуть призвести до реалізації "не тих заходів" і "не в тому місці".

Враховуючи важливість збалансованого розвитку економіки, можемо стверджувати, що ефективна концепція сталого розвитку (країни, регіонів або видів економічної діяльності) повинна ґрунтуватись на поєднанні збалансованого розвитку економічної, соціальної, екологічної та інституційної складових з позицій безпеки кожної складової. Тобто, *концепція* повинна містити найбільш пріоритетні напрямки та стратегічні орієнтири розвитку об'єкту управління на визначену перспективу та є, по суті, сценарієм досяг-

нення цілей. Крім того, в концепції визначаються шляхи переходу від поточного положення об'єкта управління до бажаного у відповідності з цілями, поставленими суб'єктом управління. Отже, *концепція* – це управлінська конструкція, що містить загальне системне уявлення шляхів переходу від поточного положення об'єкта управління до бажаного. Зазвичай, концепція містить:

1. Методологію дослідження, тобто систему принципів дослідження, яка базується на діалектичному методі та системному підході.

2. Набор методів проведення дослідження, які являють собою способи збору, обробки та аналізу даних.

3. Принципи організації дослідження.

Стратегічне бачення сталого розвитку передбачає спочатку визначення: на якій відстані від сталого розвитку знаходяться його соціальна, економічна та екологічна складові. Тобто бажано визначити відправну точку для кожної складової сталого (соціо-еколого-економічного – СЕЕ) розвитку, від якої і залежить стратегічне бачення сталого розвитку, а потім – застосовувати теоретичні підходи до обґрунтування стратегічних орієнтирів досягнення сталого розвитку.

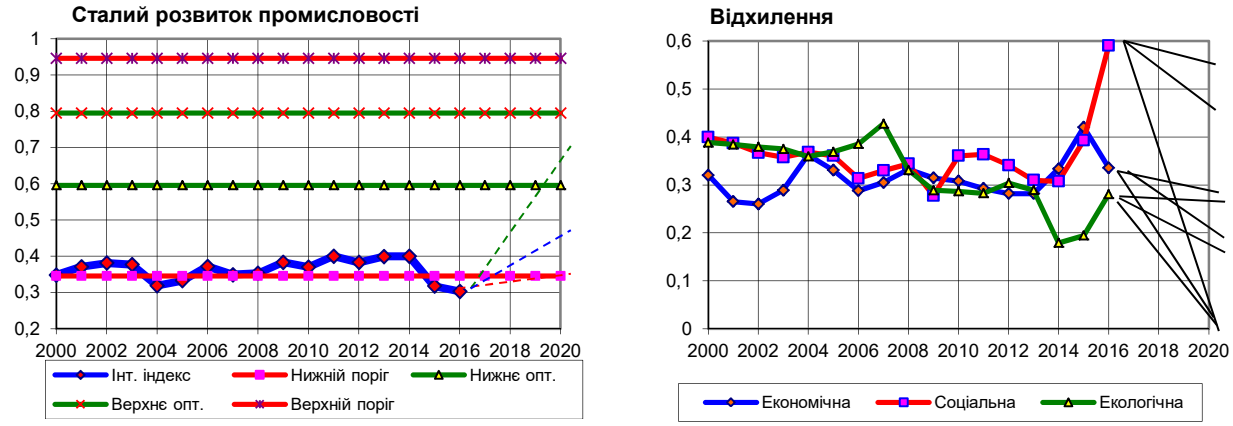
З урахуванням викладеного, можна запропонувати *концепцію сталого розвитку економіки* (країни, регіонів, основних ВЕД) з позицій економічної безпеки, яка включає наступні етапи:

1. *Визначення структури сталого розвитку*. Цей етап передбачає деталізацію складових та їх індикаторів, формування динаміки індикаторів та їх приналежність до стимуляторів (збільшення яких бажано), або де стимуляторів (зменшення яких бажано).

2. *Визначення меж безпечного існування*. Системне дослідження проблеми модернізації економіки повинно включати визначення меж безпечного існування системи, тому важливим етапом моніторингу стану системи є визначення вектору порогових значень індикаторів, якій передбачає визначення: нижнього та верхнього критичного, нижнього та верхнього порогового, нижнього та верхнього оптимального. Без знання границь безпечних умов функціонування економічної системи є неможливим захист її життєво важливих інтересів. Тому головне завдання забезпечення сталого розвитку – не максимізація рівня (інтегрального індексу) розвитку, а забезпечення його знаходження в межах порогових, а краще оптимальних, значень (у границях "*гомеостатичного плато*") [3]. З кожного боку "*гомеостатичного плато*" розташовані області з нейтральним та додатнім зворотнім зв'язком, перебування в яких є небезпечним або взагалі загрожує існуванню системи. Отже, визначення порогових значень досить тісно пов'язане з поняттям динамічної стійкості економічної системи та окремих її складників, або з механізмом гомеостазу.

3. *Ідентифікація рівня сталого розвитку*. Передбачає інтегральне оцінювання рівня сталого розвитку у порівнянні з інтегральними пороговими значеннями та включає: вибір форми інтегрального індексу (мультиплікативна), нормування індикаторів та порогових значень (комбінований метод), ви-

значення динамічних вагових коефіцієнтів (за методом "*Головних компонент*" та методом "*Ковзної матриці*")(рис. 1, *а*) [4]. Таким чином, визначення інтегральних індексів економічної системи та їх порівняння з інтегральними пороговими значеннями переводить поняття "*розвиток*" в поняття "*безпека*".




*а* *б*

*Рис. 1. Динаміка інтегральних індексів (а) та їх відхилень від критеріїв сталого розвитку (б)*

4. *Визначення дисбалансів сталого розвитку*. Використовуючи отриману динаміку інтегральних індексів складових сталого розвитку та інтегральні порогові значення, можна обчислити відхилення інтегральних індексів від їх середніх оптимальних значень, які можна вважати критеріями досягнення сталого розвитку, що засвідчує диспропорційність їхнього розвитку (рис.1, *б*).

5. *Визначення впливу загроз*. Для визначення впливу загроз обчислюються коефіцієнти еластичності кожної складової та індикаторів, які пояснюють міру впливу окремих складових та індикаторів на рівень сталого розвитку та є необхідною інформацією для розроблення пріоритетних заходів впливу.

6. *Обґрунтування стратегічних орієнтирів* передбачає вирішення задачі послідовної декомпозиції інтегральних індексів, тобто завдання синтезу необхідних значень складових та їх індикаторів для знаходження інтегрального індексу у заданих межах шляхом вирішення зворотної задачи. Вирішення такої задачі для кожної складової сталого розвитку, коли відомо (або задано) його необхідне значення, дозволяє з урахуванням чутливості складових або індикаторів, вагових коефіцієнтів впливу та адаптивних методів регулювання з теорії управління (рис. 2) визначити необхідні значення складових та їх індикаторів впродовж періоду прогнозування у кожному році, які задовольняють визначеним цілям [5]. Така процедура виконується спочатку на рівні складових (табл. 1), а потім на рівні індикаторів сталого розвитку.

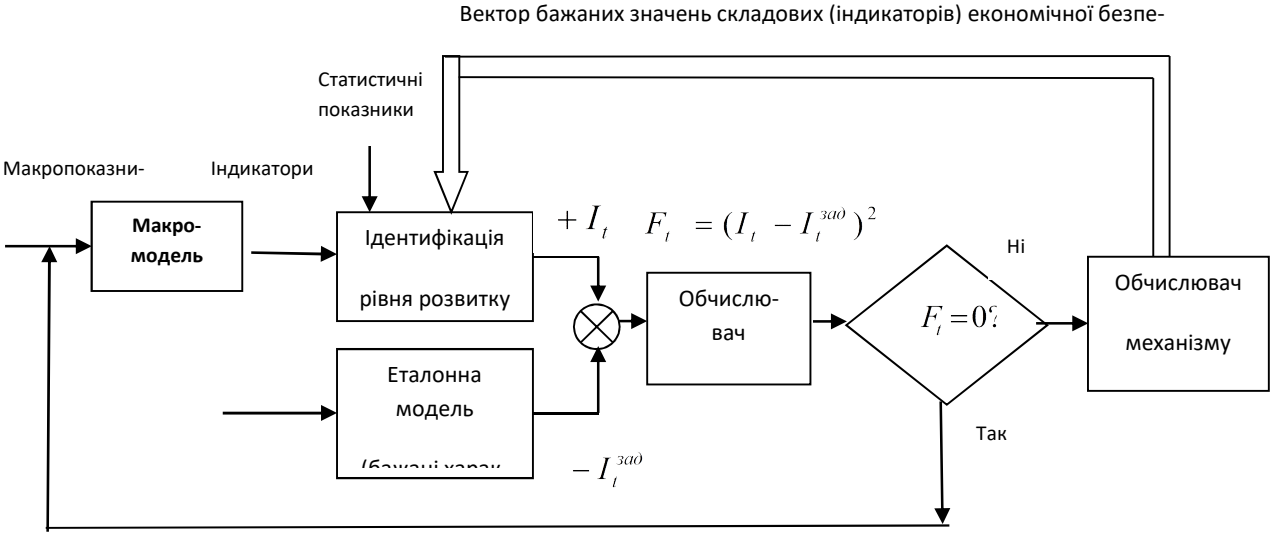



*Рис. 2. Узагальнена схема адаптивної системи регулювання*

*Таблиця 1*

**Стратегічні орієнтири інтегральних індексів сталого розвитку промисловості України**

| Складові розвитку | Рік | | | | |
|---|---|---|---|---|---|
| | 2016 | 2017 | 2018 | 2019 | 2020 |
| *Повноцінний сценарій (збалансований) – сталий розвиток* | | | | | |
| **Сталий розвиток** | **0,3033** | **0,4391** | **0,5238** | **0,6085** | **0,6422** |
| Соціальна | 0,1394 | 0,2629 | 0,3855 | 0,5080 | 0,6295 |
| Екологічна | 0,4575 | 0,5011 | 0,5439 | 0,5868 | 0,6291 |
| Економічна | 0,3087 | 0,3983 | 0,4883 | 0,5783 | 0,6688 |

*Джерело: розраховано авторами.*

Використовуючи відповідні формули обчислення індикаторів кожної складової сталого розвитку та формули нормування у зворотному порядку, можна отримати стратегічні орієнтири ключових макропоказників, які поряд із стратегічними значення,245ми індикаторів є кінцевою метою регулювання сталого розвитку (табл. 2).

*Таблиця 2*

**Зміна найважливіших макропоказників сталого розвитку промисловості України за період 2016-2020 рр.**[*]

| ***Показник*** | ***Сценарії Стратегії*** | | |
|---|---|---|---|
| | *Реаліс-тичний* | *Опти-міс-тичний* | *Повноцінний сталий роз-виток* |
| 1.Збільшення ном. ВДВ промисловості, *разів* | 1,29 | 2,85 | 3,05 |
| 2. Збільшення реальної ВДВ, % (*річна зміна*) | -42,7 | 2,7-28,3 | 10,0-37,5 |
| 3. Зменшення зайнятості, *разів* | 0,79 | 0,75 | 0,74 |
| 4. Збільшення тіньової ВДВ, *разів* | 1,26 | 2,48 | 1,54 |
| 5. Зменшення рівня тінізації ВДВ, *разів* | 0,97 | 0,87 | 0,5 |
| 5. Збільшення тіньового ПС., *разів* | 1,26 | 2,3 | 0,68 |
| 6. Зменшення рівня тінізації ПС, *разів* | 0,98 | 0,9 | 0,5 |
| 6. Збільшення капітальних інвестиції, *разів* | 1,48 | 4,53 | 4,01 |
| 7. Збільшення фінансування НТР, *разів* | 1,76 | 7,52 | 7,24 |
| 8. Збільшення фінанс. інов. діяль-сті, *разів* | 1,39 | 4,05 | 3,53 |
| 9. Збільшення ном. заробітної плати, *разів* | 1,68 | 3,84 | 6,32 |
| 10. Збільшення прожиткового мінімуму, *разів* | 1,68 | 3,74 | 4,2 |
| 11. Зменшення обсягу викидів забруднюючих речовин в атмосферне повітря, *разів* | 1,05 | 1,35 | 3,31 |
| 12. Зменшення обсягу скидання забруднених зворотних вод у поверхневі водні об'єкти, *разів* | 1,05 | 1,28 | 2,21 |

[*] *Розрахунки авторів*

7. *Розроблення інституційних заходів*. Цей етап передбачає розроблення та врахування індикаторів інституційних аспектів сталого розвитку: програмування і планування політики, наукові розробки, міжнародні правові інструменти, інформаційне забезпечення, посилення ролі основних груп населення та ін.

1. *Организация* Объединенных Наций по промышленному развитию, 2015. Отчет о промышленном развитии – 2016. Роль технологий и инноваций во всеохватывающем и устойчивом промышленном развитии. Обзор. Вена. – 77 с.

2. *Згуровский, М.З*. Сталий розвиток у глобальному і регіональному вимірах: аналіз за даними 2005. / *М.З. Згуровский*. – К. : НТУУ «КПІ», ВПІ ВПК «Політехніка», 2006. – 84 с.

3. Промисловість України – 2016: стан та перспективи розвитку: наук.-аналіт. доп. /

*О.І. Амоша, І.П. Булєєв, А.І. Землянкін, Л.О. Збаразська, Ю.М. Харазішвілі* та ін.; НАН України, Ін-т економіки пром- сті. – Київ, 2017. – 120 с.

4. *Харазішвілі Ю.М.* Проблеми інтегрального оцінювання рівня економічної безпеки держави / *Ю.М. Харазішвілі, Є.В. Дронь //* Банківська справа. – 2015. – № 1 (133). – С. 3–21.

5. *Харазішвілі Ю.М.* Модернізація економіки Донецької області: стратегічні сценарії реалізації з позицій сталого розвитку до 2020 року: наук. доп. / *Ю.М. Харазішвілі, В.І. Ляшенко, Л.Л. Шамілева, Ю.І. Жихарева*; НАН України, Ін-т економіки пром-ті. – Київ, 2016. – 119 с.

**Христов Олександр Леонідович**
к.ю.н., доцент кафедри
кримі-налістики, судової медицини
та психіатрії Дніпропетровського
державного університету внутрішніх справ,

**Бакало Вікторія Олександрівна**
курсант Дніпропетровського державного
університету внутрішніх справ

# ОСОБЛИВОСТІ ЗАЛУЧЕННЯ ПОНЯТИХ ДО ОГЛЯДУ ВІДКРИТИХ ДЖЕРЕЛ ІНФОРМАЦІЇ, ЩО РОЗМІЩЕНІ НА ІНТЕРНЕТ-РЕСУРСАХ, МЕТОЮ СТВОРЕННЯ ЯКИХ Є СПРИЯННЯ НЕЗАКОННІЙ ДІЯЛЬНОСТІ

Організаційно-правові аспекти забезпечення участі незалежних осіб під час досудового розслідування до сьогодні ще не знайшли повного вирішення.

Сьогодні чисельна плеяда правників визначає важливість і необхідність існування інституту понятих у кримінальному провадженні, оскільки поняті є незалежними джерелами і відіграють вагоме значення під час визнання доказами тих чи інших фактичних даних [1].

Слід зазначити, що огляд житла чи іншого володіння особи здійснюються з обов'язковою участю не менше двох понятих незалежно від застосування технічних засобів фіксування відповідної СРД [2], однак, залишається неврегульоване на законодавчому рівні питання участі понятих у проведенні огляду джерел інформації, що розміщені на Інтернет-ресурсах, метою створення яких є сприяння незаконній діяльності.

Працівникам правоохоронних органів часто доводиться мати справу із технічними засобами, які використовуються злочинцями у якості знарядь та засобів вчинення злочинів. Серед таких засобів найчастіше зустрічаються: 1) стаціонарні персональні комп'ютери (робочі станції або сервери); 2) ноутбуки та нетбуки; 3) планшети; 4) бортові комп'ютери автомобілів; 5) телевізори із функцією SMART; 6) GPS-навігатори; 7) носії цифрової ін-

формації (диски, дискети, флеш-носії тощо); 8) периферійне обладнання (принтери, сканери тощо); 9) мобільні комп'ютерні пристрої із функцією телефону та ін.

Специфіка проведення такого огляду полягає у тому, що докази із цифрових джерел інформації мають низку унікальних характеристик, зокрема, нестійкість. Особливо це стосується енергозалежних даних, які є дуже нестійкими у часі, і якщо їх не зберегти правильно і швидко, то вони можуть бути втрачені. В сучасних комп'ютерних системах дані часто зберігаються і обробляються не на самому пристрої а в інших місцях (наприклад, хмарні сховища), доступ до яких регулюється законодавством тієї країни, де вони фізично розташовані [3].

Тому особливу роль у цьому випадку відіграють пошук і вилучення комп'ютерних даних в режимі реального часу з фіксацією часу здійснення своїх дій.

Окремо слід зазначити, що інформація, яку сприймають поняті під час проведення огляду джерел інформації, що розміщені на Інтернет-ресурсах (в режимі реального часу) з часом стирається у пам'яті і може викривлятися, що негативно впливає на встановлення істини під час наступних стадій кримінального провадження.

Крім того, існування в КПК вимоги щодо обов'язкової участі понятих породило ситуацію, коли одні і ті ж особи постійно (або періодично) приймають участь у проведенні СРД (так звані «чергові» поняті), більшість із яких не мають відповідних знань з ІТ-технологій та особливостей функціонування програмних продуктів.

У зв'язку з цим, усвідомлення понятими операційних процесів, які здійснюються відповідним спеціалістом, залученим до огляду джерел інформації в режимі реального часу буде ускладнено, і як наслідок поставить під сумнів об'єктивність і достовірність показань понятих під час судового провадження.

У зв'язку з цим, можна дійти висновку, що для проведення огляду відкритих джерел інформації, що розміщені на Інтернет-ресурсах, метою створення яких є сприяння незаконній діяльності необхідно залучати понятих, які володіють відповідними знаннями.

Такі висновки підтверджує й напрацьована практика залучення понятих зі спеціальними знаннями до огляду Інтернет-ресурсів працівниками Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми Національної поліції, яка дає позитивні результати у подальшому розгляді кримінальних проваджень на судових стадіях. Одним із прикладів участі у якості понятих громадян зі спеціальними знаннями з ІТ-технологій є залучення студентів технічних ВНЗ.

---

1. Христов О. Л. Організаційно-правові аспекти залучення понятих при проведенні слідчих (розшукових) дій / О. Л. Христов, А. О. Панасенко // Оперативно-розшукова дія-

льність Національної поліції: проблеми теорії та практики : матеріали Всеукр. наук.-практ. конф. (Дніпро, 18 листоп. 2016 р.) : у 2-х ч. – Дніпро : Дніпроп. держ. ун-т внутр. справ, 2016. – Ч. 1. – С. 192-195.

2. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI в редакції від 12.04.2018 [Електронний ресурс] / Офіційний Сайт Верховної Ради України. – Режим доступу до код. http://zakon3.rada.gov.ua/laws/show/4651-17.

3. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій: навчальний курс / [А. Вінаков, В Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манджай, В. Марков, В. Носов, О. Соловйов]. – К., 2017. – 148 с.

**Чередниченко Олександр Юрійович**
к.е.н., доцент, професор спеціальної
кафедри «Правове забезпечення
оперативно-службової діяльності
Служби безпеки України» Інституту
підготовки юридичних кадрів для СБУ
Національного юридичного
університету імені Ярослава Мудрого,

## ОКРЕМІ ПРОБЛЕМНІ ПИТАННЯ ПРАКТИЧНОГО ВТІЛЕННЯ ПЕРСОНАЛЬНОГО «ОНЛАЙН-,КАБІНЕТУ» В КРИМІНАЛЬНОМУ ПРОЦЕСІ УКРАЇНИ

Прискорення євроінтеграційних процесів в Україні, зміни в громадянському та соціально-економічному середовищі країни, обумовили необхідність впровадження сучасних світових стандартів в галузі економіки та права. З цього приводу в середовищі як законодавців так і практичних фахівців розгорнута серйозна дискусія, яка стосується реформування системи кримінального процесу, що підштовхує вітчизняного законодавця до внесення змін до кримінально-процесуального законодавства.

Як результат, до відповідних комітетів Верховної Ради України подано декілька нових законопроектів, що стосуються змін чи прийняття нових кримінально-процесуальних кодексів в яких пропонується введення такого поняття як «персональний онлайн-, кабінет». Законодавець вважає, що таким чином буде надана можливість доступу судей, адвокатів та самих звинувачених до матеріалів кримінального провадження в електронному вигляді. Мова йде про відеозапис засідань, фото- відео-докази, скановані копії документів процесуальних записів тощо. Досить прогресивне нововведення, але без детального опрацювання механізму його втілення це може призвести до серйозних проблем.

Так, законодавцем пропонується введення електронних версій процесу-

альних документів в спеціально створений банк даних, при цьому цю роботу пропонується покласти на технічних співробітників судів. В результаті, виникає декілька проблемних питань, які можуть призвести не тільки до збоїв у роботі судів, а й до порушень вимог діючого законодавства, в тому числі, про захист інформації з обмеженим доступом (закони України: «Про державну таємницю», «Про захист персональних даних», «Про інформацію» та ін.).

Наприклад, досить дискусійним є питання щодо механізму надання доступу до «онлайн-, кабінет» для осіб, які утримуються в слідчих ізоляторах за санкцією судів. Ця норма міститься в одному із законопроектів, а для її реалізації необхідно буде технічно обладнати всі слідчі ізолятори одночасно комп'ютерною технікою, створити електронно-інформаційні системи та мережі.

Але, на нашу думку, головною проблемою в реалізації вищевказаного нововведення є неможливість запровадження надійної системи протидії несанкціонованим втручанням ззовні, а саме протидії так званим хакерським атакам. Це в свою чергу може погрожувати не тільки витоком інформації з обмеженим доступом, а й оприлюдненням інформації особистого характеру, наприклад, з метою компрометації як посадових осіб учасників кримінального процесу так і осіб які ще не є засудженими, інших суб'єктів кримінального судочинства, правоохоронців тощо. Тобто виникає проблема не тільки технічного характеру, а й проблема правового гарантованого діючим законами захисту персональних даних, приватної інформації, банківської таємниці, медичної таємниці тощо.

Крім того, залишається невирішеним питання яким чином будуть долатися чисельні вимоги, що стосуються технічного захисту обладнання (насамперед комп'ютерів, інформаційно-комп'ютерних мереж), приміщень, інформаційних ресурсів (баз даних), допуску технічного персоналу до роботи з документами з грифами обмеженого доступу і т. ін. Негативним прикладом вирішення проблеми технічного захисту інформаційних ресурсів є введення в дію восени 2016 року Національним агентством запобігання корупції (НАЗК) системи, так званого «е-декларування», яка працювала певний час з перебоями, а дієвість її системи захисту від несанкціонованих втручань у фахівців викликає сумніви.

Також, виникає і ще одна проблема організаційно-штатного (кадрового) характеру, а саме необхідність збільшення кількості секретоносіїв. По-перше в судах з числа штатних посадовців технічного персоналу, а це спеціалісти, які повинні вводити інформацію в систему, фахівці з її захисту, ремонту, експлуатації. По-друге також й в середовищі сторін захисту. Це призведе не тільки до додаткових обов'язкових процедур з персональної перевірки на предмет можливого допуску до роботи з інформацією з обмеженим доступом, а й до додаткового фінансового навантаження (наприклад, доплат за секретність тощо).

Неможливо ігнорувати і думку окремих правників, які вбачають в реа-

лізації цієї ідеї ще й спробу збільшення судового сбіру, інших сплат до бюджету (наприклад, пропонується брати такого роду платежі із нерозглянутих справ, кількість яких дуже велика).

Повертаючись до фінансової сторони треба враховувати що до додаткових фінансових витрат безперечно призведе придбання додаткового сучасного сумісного між собою комп'ютерного обладнання, сканерів, апаратури передачі даних, засобів захисту, захищених ліній передачі даних (наприклад, для кримінальних проваджень, що стосуються державної зради чи розголошення державної або військової таємниці) і т. ін. Це ціла низка проблемних питань, які буде необхідно вирішувати в умовах недостатнього фінансування правоохоронної та судової сфер.

Таким чином, не ставлячи під сумнів необхідність «осучаснення кримінального процесу», впровадження європейських стандартів поспішне, недостатньо опрацьоване прийняття рішення щодо впровадження системи «персональний онлайн-, кабінет» може призвести не до покращення, а навпаки до погіршення ситуації та виникнення передумов до низки порушень норм діючого законодавства, прав і свобод громадян. Тому, на нашу думку, важливо не тільки внести нові зміни в кримінальний процес, а й ретельно, із залученням відповідних фахівців, напрацювати механізм їх реалізації з обов'язковою його апробацією на практиці.

**Шеломенцев Володимир Петрович**
кандидат юридичних наук,
Заслужений юрист України,
головний спеціаліст відділу
впровадження реформ МВС України

## КІБЕРЗАГРОЗИ У ЗАКОНОДАВСТВІ УКРАЇНИ

У травні поточного року набирає чинності Закон України «Про основні засади забезпечення кібербезпеки України». Вперше на законодавчому рівні закріплено визначення основних термінів сфери кібербезпеки.

Відповідно статті 1 вказаного Закону кіберзагроза визначається як наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів;

Водночас, у тексті Закону використовуються такі терміни, як:

– «загроза безпеці систем електронних комунікацій, систем управління технологічними процесами»; «загроза безпеці (захищеності) електронних ін-

формаційних ресурсів» – у визначенні поняття інциденту кібербезпеки (ст. 1);

– «загрози національній безпеці України у кіберпросторі» – у визначенні поняття кібербезпеки (ст. 1), при визначенні основних завдань розвідувальних органів України (ст. 8); при визначенні шляхів забезпечення функціонування національної системи кібербезпеки (ст. 8);

– «загрози з використанням кіберпростору»; «зовнішні і внутрішні загрози безпеці України з використанням кіберпростору» – при визначенні шляхів забезпечення функціонування національної системи кібербезпеки (ст. 8);

– «загрози національній безпеці з використанням кіберпростору» – при визначенні змісту сприяння суб'єктам забезпечення кібербезпеки (ст. 11).

При цьому, законодавець не надав ані визначення цих термінів, ані їх співвідношення з терміном «кіберзагроза».

Як вбачається, загрози безпеці систем електронних комунікацій, систем управління технологічними процесами та безпеці електронних інформаційних ресурсів є окремими видами кіберзагроз.

Загрози національній безпеці України у кіберпросторі також можна віднести до окремого виду кіберзагроз відповідно наданої характерної риси – створення небезпеки життєво важливим національним інтересам України у кіберпросторі.

А ось загрози з використанням кіберпростору, загрози безпеці України (національній безпеці) з використанням кіберпростору необхідно тлумачити як окремий вид кіберзагроз відповідно до іншої характерної риси – справляння негативного впливу на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів.

Законом України «Про Державну програму авіаційної безпеки цивільної авіації» визначено кіберзагрози цивільній авіації – наявні та потенційно можливі явища і чинники, що становлять загрозу кібербезпеці та можуть призвести до актів незаконного втручання в діяльність цивільної авіації.

Розглядати певне явище (обставини, події) як кіберзагрозу можливо лише у зв'язку з об'єктом, якому це явище може заподіяти шкоди. З іншого боку, виникнення кіберзагроз пов'язане з наявністю джерел таких загроз. Також, при розгляді феномену кібербезпеки доцільно звертатися й до її антитези – кібернебезпеки, під якою слід розуміти певний стан, при якому існує можливість реалізації об'єктивно існуючих кіберзагроз, що у свою чергу, призведе до завдання шкоди (збитків) об'єктам кібербезпеки.

Хоча у статті 4 Закону і визначено об'єкти кібербезпеки, проте не надано переліку основних кіберзагроз цим об'єктам, що є першим етапом у процесі розбудови системи кібербезпеки держави.

На думку автора, до основних елементів характеристики кіберзагроз слід віднести:

– джерела кіберзагроз;

– уразливості комп'ютерних систем, існування яких обумовлюють наявність відповідних кіберзагроз;

– імовірність реалізації кіберзагрози;

– імовірний обсяг шкоди, що може завдати реалізація кіберзагрози.

Аналіз наукових праць дозволяє розглядати джерела кіберзагроз як фактори, здатні призвести до реалізації кіберзагрози та завдання шкоди. Джерелом таких кіберзагроз є люди, що мають відповідні знання та можливість використання цих систем (оператори систем, користувачі їх ресурсів тощо). При цьому у якості джерел загроз кіберпростору слід розглядати його користувачів та персонал, що забезпечує його функціонування.

Під уразливістю комп’ютерної системи дослідники розуміють певну характеристику цієї системи: яка робить можливим виникнення загрози; використання якої може призвести до реалізації загрози. Лише об'єктивна оцінка наявних уразливостей певної комп’ютерної системи дозволяє правильно визначити відповідні кіберзагрози для цієї системи та оцінити імовірність їх реалізації.

Для кожної комп’ютерної системи можуть існувати різноманітні кіберзагрози, але ступінь вірогідності реалізації таких загроз та величина завданої шкоди для певної комп’ютерної системи є індивідуальним. При цьому, прогнозовану величину шкоди, що може бути завдана виникати внаслідок реалізації кіберзагрози слід розглядати як відповідний ризик.

Водночас, слід вказати на необхідність розгляду поняття кіберзагроз:

– у широкому розумінні, як загроз, пов’язаних з неналежним використанням будь-яких комп’ютерних систем (локальних, виробничих, глобальних);

– у вузькому розумінні, як загроз, пов’язаних з використанням кіберпростору.

Кіберзагрози у вузькому розумінні це загрози:

– належному функціонуванню комп’ютерних систем кіберпростору;

– безперешкодному доступу до ресурсів кіберпростору;

– вільному користуванню ресурсами кіберпростору (їх споживанню);

– безпечній інформаційній та операційній взаємодії користувачів кіберпростору.

Шляхом тлумачення термінів, наведених у статті 1, можна виділити такі кіберзагрози:

– кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпе-

ки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту;

– кіберзлочин (комп’ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

– кіберзлочинність – сукупність кіберзлочинів;

– кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням;

– кібершпигунство – шпигунство, що здійснюється у кіберпросторі або з його використанням.

Поняття кіберзагроз як явищ перебуває на межі правових та технічних дисциплін і тому є надзвичайно складним для визначення. Проте, всі наведені загрози визначаються шляхом використання терміну «кіберпростір», який у Законі України «Про основні засади забезпечення кібербезпеки України» має досить спірне визначення і більше ніде у законодавстві не використовується (в першу чергу у Законі України «Про основи національної безпеки України» та Кримінальному кодексі України).

Відповідно до положень Конвенції про кіберзлочинність кіберзагрози кримінального характеру пов'язані з протиправними посяганнями всередині комп’ютерних систем чи мереж, проти комп’ютерних систем чи мереж, за допомогою комп’ютерних систем чи мереж. Розглядати кримінальні кіберзагрози кримінального характеру  необхідно з урахуванням його технічної та соціальної складових.

Так, кіберзагрози кримінального характеру технічній складовій кіберпростору, не пов'язані з інформаційної взаємодії (спілкування) користувачів у кіберпросторі, і полягають у протиправному посяганні на: конфіденційність (порушення режиму доступу) та цілісність комп'ютерних даних (знищення, перекручення); нормальну роботу комп'ютерних систем і мереж – перешкоджання їх роботі, порушення порядку доступу до них, правил їх експлуатації.

Кіберзагрози кримінального характеру соціальній складовій кіберпростору, пов'язані з інформаційною взаємодією (спілкуванням) користувачів у кіберпросторі, і полягають у: протиправному посяганні на конфіденційність (розголошення) та доступність (блокування, обмеженням свободи слова та доступу) комп'ютерних даних; протиправному використанні комп'ютерних даних (поширення недостовірної, неповної або упередженої інформації, а також культу насильства, жорстокості, порнографії, матеріалів расистського та ксенофобного характеру); протиправним використанням комп'ютерних систем і мереж при посяганні на суспільні відносини в інших галузях людської діяльності, не пов'язаних з інформаційною діяльністю (шахрайство, вимагання, терористичний акт тощо).

Хоча Законом і визначено термін «індикатори кіберзагроз» як показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози, проте характеристик кіберзагроз не наведено, а впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту лише передбачається.

Функціонування кіберпростору пов'язане не тільки із забезпеченням користувачам доступу до обчислювальних та інформаційних ресурсів кібернетичних комп'ютерних систем, виробленням електронних інформаційних продуктів, обміном електронними повідомленнями, а також у наданні користувачам можливості за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання інформаційних послуг, ведення електронної комерції тощо).

До найбільш значимих чинників, що впливають на формування кіберзагроз, можна віднести:

– наддержавний характер глобальних мереж, що територіально охоплюють різні країни та призводять до рознесення елементів складу злочинів у правовому просторі різних країн;

– децентралізовану структуру глобальних мереж, відсутність єдиної організації, що координує та контролює функціонування кіберпростору;

– неврегульованість переважної більшості соціальних відносин у кіберпросторі відповідними нормативно-правовими актами, що впливає на структуру злочинності та породжує невідомі для фізичного середовища форми протиправної поведінки.

– відсутність у кіберпросторі стійких ідентифікаційних ознак інформації та достовірних ідентифікаторів особи користувача;

– електронний характер інформаційних об'єктів кіберпростору, що потребує застосування спеціальних програмно-технічних засобів при здійсненні пошуку і фіксації фактичних даних;

– підвищену складність та мінливість інфраструктур сучасних мереж і мережних процесів, надзвичайну розгалуженість комунікацій, постійно зростаючий обсяг інформаційних ресурсів.

При цьому, слід враховувати, що користувачі (особи, громадські організації, державні органи тощо) проявляються у кіберпросторі як певні інформаційні об'єкти. Тому, забезпечення кібербезпеки можна розглядати й як забезпечення безпечного існування відповідних інформаційних об'єктів кіберпростору, їх діяльності щодо використання його ресурсів та взаємодії з іншими об'єктами у віртуальному середовищі кіберпростору.

Підсумовуючи викладено, можна зазначити, що знання характеристики кіберзагроз дозволить вжити найбільш ефективних заходів щодо їх виявлення та нейтралізації.

При визначенні характеристик кіберзагроз пропонується надавати їх у більш широкому розумінні, враховуючи вже наявні напрацювання у таких

галузях науки як кібернетика, інформатика, безпекознавство, кримінальне право, кримінологія тощо.

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 року № 2163-VIII [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/2163-19.

2. Про основи національної безпеки України: Закон України від 19 червня 2003 року // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.

3. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05 липня 1994 року № 80/94-ВР [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/80/94-вр.

4. Про кіберзлочинність : Конвенція Ради Європи // Офіційний вісник України від 10.09.2007 – 2007 р. – № 65. – Стор. 107. – Ст. 2535. – Код акту 40846/2007.

**Шнейдерова Дарья Игоревна**
преподаватель Могилевского института
Министерства внутренних дел
Республики Беларусь

## ОСОБЕННОСТИ ЛЕГАЛИЗАЦИИ КРИПТОВАЛЮТЫ В РЕСПУБЛИКЕ БЕЛАРУСЬ

За последние несколько лет особую популярность на мировом финансовом рынке приобрела цифровая валюта, именуемая «криптовалютой», и, в частности, один из ее ярких представителей «биткойн». В начале 2017 года стоимость биткойна на биржевых рынках цифровой валюты возросла более чем в 6 раз, чем и привлекла внимание общественности.

На просторах сети Интернет с каждым днем появляется все больше и больше рекламных роликов, заметок, статей, раскрывающих сущность и привлекательность криптовалюты, описывается, как кажется с первого взгляда, достаточно простой и прозрачный механизм работы такого актива. Однако следует отметить, что на сегодняшний день ни мировые финансовые аналитики, ни правоведы не могут прийти к одному единому мнению о том, что же представляет собой криптовалюта. Так ее можно рассматривать как средство платежа, как своеобразный товар, как имущество и как выгодный инвестиционный проект. Однако каждое из этих понятий имеет свои положительные и отрицательные аспекты в отношении цифровой валюты.

Для того чтобы являться полноценным универсальным средством платежа, криптовалюта должна быть признана таковой во всех странах мира, что позволит ей заменить стандартное и привычное для нас денежное обращение в наличном и безналичном виде. И тут следует отметить, что далеко не все

мировые державы активно поддерживают идею мирового прогресса о введении в действие цифровых денег. Официально криптовалюта была признана в таких странах как США, Канада, Великобритания, Япония и другие [1, с. 64].

В 2018 году и Республика Беларусь сделала первый шаг к легализации криптовалюты и сделок с ней. Так, с марта 2018 года начал свое действие подписанный Президентом Республики Беларусь 21 декабря 2017 г. Декрет № 8 «О развитии цифровой экономики» (далее – Декрет), который определяет криптовалюту как биткойн, иной цифровой знак (токен), используемый в международном обороте в качестве универсального средства обмена. То есть, если проанализировать данное определение, то можно сделать вывод о том, что криптовалюта как средство платежа на белорусском рынке может иметь место только в виде биткойна  или токена, несмотря на то, что в рамках мирового рынка действует более 20 видов различных криптовалют.

Также белорусский законодатель дает нормативное определение цифрового знака, так называемого токена, представляющего собой запись в блокчейне, иной распределенной информационной системе, которая удостоверяет наличие у владельца цифрового знака (токена) прав на объекты гражданских прав и (или) является криптовалютой. Исходя из данного определения можно говорить о том, что криптовалюта, являясь цифровым знаком, приравнивается к токену, что в действительности не совсем так.

Если криптовалюта подразумевается как расчетная единица, являющаяся криптографическим цифровым кодом, фиксируемым в децентрализованной базе данных в виде блока (блокчейне), то токен представляет собой скорее долговое обязательство на оказание услуги или предоставление товара. Иными словами криптовалюта это своеобразный аналог денег, а токен – цифровой актив, имеющий конкретное предназначение (например, как акция).

Чтобы увидеть отличия токена от криптовалюты (на примере биткойна), рассмотрим механизмы их работы. В основе работы биткойна лежит криптографический принцип, который включает в себя определенный набор уникальных криптознаков, генерирующихся за счет составления всевозможных комбинаций нулей и единиц в единую формулу – код. Процесс совершения операций с криптовалютой базируется на методе «блокчейн», то есть построение последовательной непрерывной цепочки блоков, каждый из которых содержит информацию о группе совершенных транзакций в общей системе. Все блоки цепочки связаны между собой, так как каждый из них содержит информацию о предыдущем, таким образом, цепочка содержит информацию обо всех транзакциях, совершенных когда-либо в системе. При этом транзакция считается совершенной, только если она была подтверждена и объединена в блок.

Следует добавить, что сегодня существует множество направлений, использующих ключевую технологию «блокчейн», но каждое из них имеет свои собственные правила и особенности. Многие выступают в роли открытых фи-

нансовых платформ, позволяя появляться новым продуктам и сервисам, которые ранее были невозможны или слишком дороги в создании [2, с. 27].

Особенность системы «блокчейн» заключается в ее децентрализации, то есть отсутствии управляющего лица. Все участники системы равноправны и имеют общий доступ ко всей информации, находящейся в системе. Иначе говоря, на компьютере каждого участника криптоплатформы храниться вся информационная база о совершенных в системе транзакциях. И чем больше участников у криптоплатформы, тем выше уровень контроля над совершаемыми транзакциями, так как для того, чтобы транзакция имела место быть, она должна быть удостоверена (подтверждена) всеми участниками платформы, и информация о такой операции храниться у всех без исключения участников.

Получить криптовалюту можно несколькими способами: путем майнинга или покупки на криптобирже. Майнинг представляет собой процесс «добычи» биткойнов путем использования вычислительных мощностей компьютера майнера. Суть данного процесса заключается в том, что компьютер за определенный временной интервал решает математические задачи (генерирует уникальный код), и когда решение будет найдено, то есть, сформирован новый блок в системе, майнер получит вознаграждение в виде определенного количества биткойнов. С одной стороны данный путь сложный и требует больших затрат времени и мощности вычислительной машину, а с другой стороны наиболее прибыльный, так как за каждый блок майнер получает по 25 биткойнов. При этом майнером может стать любой человек в мире, имеющий мощный по производительности компьютер.

Другой путь приобретения биткойнов – это их покупка у самих владельцев биткойнов (которыми могут являться те же майнеры), или на криптобирже биткойнов как за вполне реальные деньги, так и за электронные деньги. Минус данного способа заключается в больших затратах времени и реальных денежных ресурсов.

Следует отметить, что первоначально в основе системы «блокчейн» лежали принципы равноправия участников и независимости от какого-либо одного участника, органа или государства. Стоимость данного вида валюты не зависит от курса валюты какого-либо государства, цен на нефть, размера золотовалютного подкрепления или любого другого фактора. Стоимость криптовалюты увеличивается или уменьшается пропорционально росту или спаду спроса на нее. Чем больше людей захотят приобрести биткойн, тем выше будет его стоимость на бирже, а, следовательно, будут расти и доходы владельцев криптовалюты. Однако в данном случае прослеживается наличие ничем неподкрепленного риска, в случае если спрос на биткойн упадет, то и его стоимость будет минимально, а, значит, владелец потеряет уже вполне реальные деньги.

Таким образом, среди особенностей криптовалюты можно выделить следующие:

1) криптовалюта не имеет определенного центра эмиссии и она не под-

вержена инфляции;

2) при помощи мощностей своего компьютера любой человек может самостоятельно производить такую валюту (майнинг), покупать ее на биржах (онлайн-сервисах) или получать в результате совершения сделок в сети Интернет;

3) надежность защиты: в основе криптовалюты лежит криптографический код, обладающий высокой степенью цифрового шифрования, взломать который практически невозможно;

4) стоимость криптовалюты определяется уровнем спроса и предложения на нее на специальных биржах;

5) отсутствие контроля с третьей стороны (банка, налоговых или правоохранительных органов), что способствует защите от блокирования, оспаривания или принудительного совершения транзакций.

В свою очередь токены имеют свои, противоречащие указанным ранее для криптовалюты, особенности. Так, согласно Декрету, владельцами токенов могут быть как физические, так и юридические лица. При этом юридические лица могут создавать и размещать собственные токены в Республике Беларусь и за рубежом, хранить их в виртуальных кошельках только через резидента Парка высоких технологий, осуществляющего соответствующий вид деятельности. Также через операторов криптоплатформ или операторов обмена криптовалют юридические лица могут приобретать, отчуждать токены, совершать с ними иные сделки (операции), с учетом того, что указанные операторы также должны являться резидентами Парка высоких технологий.

Физические лица вправе владеть и совершать следующие операции: майнинг, хранение токенов в виртуальных кошельках, обмен токенов на иные токены, их приобретение, отчуждение за белорусские рубли, иностранную валюту, электронные деньги, а также дарить и завещать токены.

Из выше представленного следует, что принципы децентрализации и самостоятельности, характерные для криптовалюты, в процессе совершения сделок с токенами, исключаются, так как в данном случае в любой операции всегда присутствует посредник, который контролирует весь процесс. С одной стороны наличие контроля и организации процесса осуществления операций с токенами служит способом защиты субъектов таких сделок не только от преступных посягательств, но и от возможности самими субъектами использовать токены для легализации доходов, полученных преступным, или как средство в теневых финансовых системах. С другой стороны, данное положение исключает анонимность и независимость, заложенные в основе действия криптовалют.

Кроме того, деятельность оператора криптоплатформы и оператора обмена криптоплатформы должна быть обеспечена реальными денежными средствами на счетах в банках Республики Беларусь, что позволит установить определенную финансовую ответственность данных субъектов перед своими клиентами, чего не предусматривает деятельность с криптовалютой.

Еще одна отличительная особенность – это субъектный состав. Если физическое лицо может без особого труда купить криптовалюту при наличии у него денег, то юридическое лицо столкнется с трудностями перевода денежных средств со своего расчетного счета, так как любая операция со счетом должна быть обоснована, а основание «покупка биткойна» может быть непризнанно банком, ввиду отсутствия легализации криптовалюты в большинстве стран мира.

Белорусский же законодатель не только обозначил субъектный состав, который может участвовать в сделках с токенами, но и предоставил определенный набор льгот и преференций. Так, вплоть до 1 января 2023 г. не признаются объектами налогообложения налогом на добавленную стоимость, подоходным налогом с физических лиц, налогом на прибыль обороты по отчуждению токенов, в том числе иностранными организациями, прибыль и выручка от обмена токенов на другие, доходы физических лиц от осуществления разрешенных операций с токенами. Также впервые на законодательном уровне предусмотрено отражение сделок с токинами в бухгалтерском учете и отчетности юридических лиц, операторов криптоплатформ и операторов обмена криптовалют. Анализируя изложенное, прослеживается еще одно отличие токена от представителей криптовалюты – учет в бухгалтерских документах и возможность государства на правовой основе в будущем взимать налоги от совершения подобных сделок или с доходов субъектов.

Кроме того, токены более централизованы, чем криптовалюта, так как выпуск и размещение токенов на территории Республики Беларусь при использовании специальных платформ может осуществляться только юридическими лицами резидентами Парка высоких технологий. Следовательно, и стоимость токена будет зависеть не от уровня спроса, как в случае с криптовалютой, а от субъекта, осуществляющего эмиссию.

Таким образом, нельзя не отметить позитивность самого факта создания в Республике Беларусь правовой базы, регулирующей сделки юридических и физических лиц с цифровой валютой, что, несомненно, говорит о стремлении страны развиваться в рамках тенденций мировой экономики будущего и готовности к восприятию новых позитивных IT-технологий. Следует отметить, что Декрет № 8 «О развитии цифровой экономики» не только предоставил белорусским гражданам и субъектам хозяйствования право на законном основании заниматься практически всеми видами деятельности с цифровой валютой, но и в будущем может послужить основанием для привлечения иностранных компаний в Республику Беларусь, так как во многих других мировых державах подобного рода деятельность законодательно не урегулирована, а более того, запрещена.

---

1. Лясковик, Я. Bitcoin – электронная валюта нового поколения / Яна Лясковик, Сергей Локтев // Предпринимательство. – 2014. – № 3. – С. 63–71.

2. Разумов, А. Технология Блокчейн и белорусская МСИ уже завтра изменят наш подход к бизнесу / Андрей Разумов // Финансовый директор. – 2016. – № 12. – С. 27–30.

**Шраго Альона Олексіївна**
ад'юнкт
Дніпропетровського державного
університету внутрішніх справ

# ПРОТИДІЯ ПОРНОГРАФІЇ ЯК ЗАСІБ ЗАБЕЗПЕЧЕННЯ І НФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

В Україні, як і в інших державах світу, невпинно розвиваються нові галузі економіки, що ґрунтуються передусім на використанні сучасних інформаційних технологій, локальних та глобальних комп'ютерних мереж, зокрема Інтернету.

Кіберзлочинність не обмежується рамками злочинів вчинених у глобальній інформаційній мережі Інтернет, вона поширюється на всі види злочинів вчинених в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть виступати предметом злочинних посягань, середовищем, в якому відбуваються правопорушення і засобом або знаряддям злочину. Це і порнографія, шахрайства, виготовлення та поширення шкідливих програм, викрадення ідентифікаційних даних осіб та інші.

23 листопада 2001 року в Будапешті підписана Конвенція Ради Європи про кіберзлочинність (далі – Конвенція), яка була прийнята для протидії комп'ютерним злочинам та для співробітництва й координації діяльності правоохоронних органів різних держав. На сьогодні ратифікована 18 країнами та підписана 25 країнами, у т.ч. й Україною (2005) [1].

У новій редакції Стратегії національної безпеки, затвердженій Указом Президента України від 8 червня 2012 року № 389/2012, вживаються терміни «кіберзлочинність», «кіберзагроза», «кібербезпека» [2]. Слід зазначити, що в «Доктрині інформаційної безпеки України» згадувалися поняття «комп'ютерна злочинність» та «комп'ютерний тероризм», а також питання захисту інформації від «кібернетичних атак» [3].

Механізми контролю, запобігання та розслідування злочинів у кіберпросторі дуже обмежені соціально і технологічно. Анонімність мережі Інтернет, вразливість бездротового доступу і використання проксі-серверів істотно ускладнюють виявлення злочинців: для вчинення злочину може використовуватися «ланцюжок» серверів, злочини можуть бути вчинені шляхом виходу в Інтернет через точки загального доступу, такі, як Інтернет-кафе, технології дозволяють також «зламати» доступ в чужу бездротову мережу Wi-Fi. Отже, існує достатньо способів ускладнити припинення і розслідування злочинів.

Боротьба з кіберзлочинністю неможлива без глибокого розуміння і правових проблем регулювання інформаційних мереж. Саме аналіз взаємозв'язку між технічними характеристиками мережі і зумовленими цими характеристиками правовими і соціальними труднощами, з якими стикаються

законодавці та правоохоронні органи, є першим кроком до можливого вироблення механізмів адекватного реагування на розвиток і зростання кіберзлочинності.

Теоретичні та практичні основи використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій, розроблені недостатньо. Аналіз спеціальної літератури та практики розслідування комп'ютерних злочинів свідчить, що існує низка проблем, пов'язаних із використанням спеціальних знань з метою пошуку, виявлення, фіксації, вилучення та дослідження слідів даної категорії злочинів у відповідності до способів їх утворення, стадії порушення кримінального провадження, при проведенні слідчих дій, розробкою спеціальних методів, засобів збирання та дослідження комп'ютерних слідів, не точно визначається предмет злочину та обставини, що підлягають доказуванню, особливо під час розслідування збуту та розповсюдження порнографії мережею Інтернет.

Проте, у практичній діяльності науково-методичні розробки не завжди схвально сприймаються. У межах проведеного нами опитування працівників кіберполіції НП України, 23 % респондентів вказали на те, що вони взагалі не звертаються до наукових рекомендацій у протидії порнографії, 43 % не використовують їх, бо вважають їх застарілими, 15 % – не ознайомлені з такими рекомендаціями, 19 % – звикли покладатися на власний досвід, з них 7 % вказали, що такі рекомендації обмежують творчий підхід до розслідування.

Однією із причин низької ефективності припинення і розслідування незаконного збуту та розповсюдження порнографії у мережі Інтернет є те, що працівники слідчих та оперативних підрозділів досі не готові до ефективного виявлення та розслідування подібних злочинів, недостатньо використовують спеціальні знання.

Серед причин високої латентності злочинів, передбачених 263н.. 301 КК України, виділяємо такі: 1) недостатня розробка понятійного апарату, що використовується в текстах відповідних статей, зокрема, відсутність чіткого визначення предмета злочинів; 2) особливий стан громадської думки, який в сучасних умовах характеризується неприйняттям названих діянь як злочинів; 3) прихований характер злочинної діяльності, відсутність очевидних її наслідків; 4) недостатня професійна підготовка працівників правоохоронних органів по виявленню і розслідуванню цих злочинів; 5) відсутність зорієнтованості правоохоронних органів на виявлення цих злочинів, які на фоні складної криміногенної ситуації (вбивства, бандитизм, розбій, зґвалтування тощо) розглядаються як другорядні і їм не приділяється належної уваги.

Закон України «Про ОРД» надає можливість використовувати права лише для виконання завдань ОРД. На законодавчому рівні не передбачено у переліку завдань профілактики злочинів, попередження та запобігання злочинам, зазначено лише припинення, про що свідчить 263н.. 1 Закону. Тобто, у Законі України «Про ОРД» наводяться два поняття, які містять суперечності, створюючи колізію правових норм: з одного боку – обов'язок оперативно-

го підрозділу здійснювати профілактику правопорушень (п. 1 ч. 1 ст. 7 Закону), з іншого – перспектива користуватися своїми правами лише для виконання завдань оперативно-розшукової діяльності (ч. 1 ст. 8 Закону), у змісті яких немає профілактики, попередження, запобігання. Відповідно, нормативно-правова регламентація профілактичної та попереджувальної діяльності оперативних підрозділів НП України має декларативний характер.

Стрімко розвивається використання Інтернету, як для вербування жертви, так і для реклами послуг. Зустрічі між жертвами та клієнтами організовуються за допомогою спеціальних веб-сайтів. Жертви швидко змінюються, залишаючись в одному місті не більше ніж на 1-2 дні. Ілюзія анонімності і масова кількість онлайн-послуг збільшує і обережність, і рентабельність цих послуг, що робить надскладною ідентифікацію злочинців із використанням лише традиційних методів поліції [4, с. 179].

Правоохоронним органам часто доводиться здійснювати первинний пошук інформації про певні об’єкти в мережі. Найбільш проблемним питанням залишається встановлення особи та визначення її місцезнаходження за тими обліковими даними, що особа лишила в мережі. Як правило, такими ідентифікаторами є адреса електронної пошти, нікнейм у форумі, профіль соціальної мережі тощо. Вказана проблема часто обумовлена підвищеним рівнем анонімності, що реалізується за допомогою різного роду розподілених ресурсів (проксі-сервери, шели) та використанням спеціалізованих захищених мереж (TOR, I2P) [5, с. 256].

Важливими правовими основами діяльності оперативних та слідчих підрозділів НП України є також норми кримінального процесуального кодексу, які, на нашу думку, сьогодні ускладнюють ефективність роботи оперативних підрозділів НП України. Так, положення 264н.. 41 КПК України забороняють співробітникам оперативних підрозділів (крім підрозділу детективів, підрозділу внутрішнього контролю НАБУ) здійснювати процесуальні дії у кримінальному провадженні за власною ініціативою або звертатися з клопотаннями до слідчого судді чи прокурора.

Пошукові заходи можуть здійснюватися і гласно, і негласно. Виходячи з того, що ефективність правоохоронного моніторингу соціальних мереж буде вищою за умови непоінформованості про нього суб’єктів деструктивних діянь, особливого значення набувають саме негласні заходи. Такі заходи в тому числі можуть здійснюватися оперативними підрозділами НП України.

З одного боку КПК містить прямі вказівки на необхідність проведення відповідних гласних та негласних слідчих (розшукових) дій, а з іншого – забороняє співробітникам оперативних підрозділів здійснювати процесуальні дії за власною ініціативою та звертатись з клопотанням до слідчого судді або прокурора, що, в свою чергу, знижує ефективність боротьби зі злочинами у сфері суспільної моралі, яким властива висока латентність. А тому, виникає сумнів щодо ефективності процесуалізації деяких ОРЗ у НСРД. Фактично, майже весь процес досудового розслідування сьогодні побудовано не лише

на законодавчій базі, а більшою мірою на особистих стосунках, що ставить під сумнів ефективність роботи загалом.

Із введенням в дію КПК України значно ускладнилася процедура отримання інформації від провайдерів телекомунікаційних послуг. Якщо раніше отримання такої інформації здійснювалося на підставі положень про «Конвенцію про кіберзлочинність» і Закону України «Про міліцію», то зараз така інформація віднесена до категорії документів, що містять охоронювану законом таємницю. А в розумінні статті 505 Цивільного кодексу України така 265н.формація становить комерційну таємницю, яка є одним із об'єктів інтелектуальної власності. Тому, суб'єкти протидії позбавлені можливості оперативно і своєчасно отримувати необхідну інформацію через запити правоохоронних органів. Сьогодні рівень і темпи зростання кіберзлочинності вимагають адекватного реагування, у тому числі і на законодавчому рівні. А тому, потребують змін положення законодавства про порядок і підстави виконання запитів, отриманих від правоохоронних органів у рамках виконання зобов'язань України, узятих у зв'язку з ратифікацією «Конвенції про кіберзлочинність». Як наслідок, одним із пріоритетних напрямків є організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою. Сьогодні жодна держава не може ефективно протистояти кіберзлочинності самостійно. Нагальною є необхідність активізації міжнародної співпраці в цій сфері.

В умовах сьогодення постає необхідність в налагодженні на відповідній правовій основі ефективної взаємодії з міжбанківськими інституціями, телекомунікаційними компаніями, зацікавленими центральними державними органами та правоохоронними органами інших країн з метою документування злочинних груп з міжнародними зв'язками.

Інформаційно-аналітичне забезпечення є важливим і необхідним елементом організації оперативного пошуку ознак злочинів, пов'язаних з незаконним контентом, оскільки воно сприяє прийняттю найбільш доцільних управлінських рішень на всіх рівнях, що є однією з головних умов підвищення ефективності діяльності оперативних підрозділів НП України.

Отже, сьогодні для суб'єктів ОРД необхідною є розробка організаційно-тактичних основ проведення оперативно-розшукової діяльності у кіберпросторі та введення в дію відповідних правових механізмів їх здійснення. Окрім того, у контексті проведеного дослідження, необхідним є: 1) розробка актуального спеціалізованого програмного та апаратного забезпечення для провадження оперативно-розшукової діяльності в кіберпросторі; 2) удосконалення системи інформаційно-аналітичного забезпечення (створення Єдиної інформаційно-аналітичної системи правоохоронних органів із підсистемами за напрямами, у тому числі з окремим блоком для підрозділів боротьби з кіберзлочинністю); 3) гармонізація кримінального законодавства про кіберзлочини на державному рівні; 4) розробка на міжнародному рівні та імплементація в національне законодавство процесуальних стандартів, що

дозволяють ефективно розслідувати злочини в глобальних інформаційних мережах, отримувати, досліджувати і представляти електронні докази з урахуванням транскордонної проблеми; 5) налагоджене співробітництво правоохоронних органів при розслідуванні кіберзлочинів на оперативному рівні; 6) створення швидких та дієвих механізмів вирішення юрисдикційних питань у кіберпросторі; 7) удосконалення механізмів обробки електронних доказів за цією категорією кримінальних проваджень; 8) зобов'язання компаній зберігати резервні копії електронних даних для підвищення ефективності розслідування таких злочинів; 9) полегшення доступу правоохоронних органів до електронних банків даних; 10) удосконалення системи оперативного супроводження підприємств, установ та організацій, основна діяльність яких пов'язана з використанням комп'ютерних технологій або наданням інформаційних послуг; 11) забезпечення заходів безпеки на об'єктах, що призначені для передачі інформації; 12) підвищення рівня обізнаності щодо торгівлі дітьми (дитячою порнографією тощо) серед батьків та осіб, які їх замінюють, осіб, які постійно контактують з дітьми у сферах освіти, охорони здоров'я, культури, фізичної культури та спорту, судовій та правоохоронній сферах; 13) підвищення ефективності правоохоронних заходів щодо профілактики злочинів та переслідування осіб, які вчиняють цей злочин або сприяють його вчиненню; 14) створення та координування «гарячих ліній», призначених для повідомлення про факти сексуального насильства та експлуатації дітей в Інтернеті.

Розв'язання окреслених питань сприятиме підвищенню ефективності діяльності оперативних та слідчих підрозділів НП України, спрямованої на протидію загрозам інформаційного простору в цілому, та кіберзлочинам у сфері суспільної моралі зокрема, а відтак, вказані напрямки потребують подальшого поглибленого науково-методичного дослідження.

---

1. Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : Закон України від 21 липня 2006 р. № 23-V // Відомості Верховної Ради України. – 2006. – № 39. – С. 1384. – Ст. 328.

2. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України : Указ Президента України Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. // Офіційний вісник Президента України. – 2014. – № 16. – С. 6. – Ст. 982.

3. Про рішення Ради національної безпеки і оборони України від 8 червня 2012 р. «Про нову редакцію Стратегії національної безпеки України» : Указ Президента України // Урядовий кур'єр. – 2012. – № 113.

4. Справочное руководство ОБСЕ по обучению полиции: Торговля людьми / серия публикаций ДТУ/ОВСВПД. Том 12. 2013. – 210 с.

5. Бандурка О.М. Оперативно-розшукова компаративістика: монографія / О.М. Бандурка, М.М. Перепелиця, О.В. Манжай та ін. – Х.: Золота миля, 2013. – 352 с.

**Юнацький Олександр Володимирович**
К.ю.н., доц., доцент кафедри
приватної охоронної діяльності
Запорізького національного
технічного університету

# ОРГАНІЗАЦІЙНІ АСПЕКТИ УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

За сучасних умов ринкових відносин для ефективного господарювання підприємства необхідно, насамперед, визначити цілі його створення та функціонування. Крім того, виникає потреба у постійному дотриманні економічної безпеки підприємства як запоруки його стабільного й максимально ефективного функціонування.

У цьому аспекті забезпечення економічної безпеки являє собою системний процес, в якому поєднуються три основних компоненти: по-перше, діагностика та оцінка фінансово-економічних, операційних та організаційних критеріїв для завчасної ідентифікації джерел виникнення небезпечних для діяльності підприємства проявів; по-друге, своєчасне застосування релевантного каталогу антикризових (стабілізаційних) заходів нейтралізації внутрішніх і зовнішніх факторів; по-третє, формування системи рекомендацій і заходів щодо створення конкурентної переваги і забезпечення розвитку підприємства на усіх етапах його життєвого та операційного циклів [1, с. 18].

Слід зазначити, що не всі компоненти забезпечення економічної безпеки 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.

Тому питання організації забезпечення економічної безпеки суб'єктів господарювання залишається актуальним як з теоретичної точки зору, так і з прикладної.

Серед фахівців, що вивчали такі проблеми [2, 3, 4, 5, 6, 7], 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.

У такому контексті організаційне забезпечення управління економічною безпекою підприємства виступає як підфункція управління економічною

безпекою підприємства, яка охоплює комплекс організаційних заходів і методичних прийомів щодо упорядкування дій, спрямованих на досягнення мети і вирішення завдань управління економічною безпекою підприємства. Варто зазначити, що організаційне забезпечення, хоча й виділене в окрему складову, неявно присутнє в різних компонентах управління економічною безпекою підприємства, адже специфіка такого управління вимагає постійних високопрофесійних оцінювань, чого неможливо досягти без відповідної організаційної підтримки [4, с. 289-290].

Виділимо окремі напрями організаційного забезпечення управління економічною безпекою підприємства.

Перший з них – це сканування зовнішнього та внутрішнього середовища підприємства. До даного напряму належать перевірка майбутніх учасників коаліції або групи зацікавлених осіб. Залежно від глибини запланованої співпраці встановлюються: фінансовий і майновий їх стан, наявність у особи, яка укладатиме угоду, прав на її здійснення, наявність і дійсність ліцензії (якщо його діяльність ліцензована), відсутність відносно майна, що набуває, суперечки або прав на нього третіх осіб, встановлення афілійованих осіб, визначення справжніх власників бізнесу тощо.

Сканування зовнішнього середовища підприємства також включає: пошуки боржників, що ховаються, здійснення комплексу заходів щодо стягнення прострочених боргів, реалізацію заходів щодо розшуку викраденого майна; роботу з правоохоронними органами по питаннях розслідування злочинів і правопорушень, що заподіяли збиток організації; інформаційно-аналітичну діяльність (відстеження матеріалів в пресі, що містять згадки про організацію); інформаційно-пропагандистське забезпечення (створення в суспільній свідомості позитивного іміджу організації); інформаційний захист (створення в організації системи захисту комерційної таємниці і забезпечення її функціонування, зокрема через роботу з персоналом, створення максимально захищених від зламування комп’ютерних мереж, дотримання режиму роботи з конфіденційною інформацією).

До найважливіших складових сканування внутрішнього середовища підприємства належать: правова і психологічна робота із співробітниками, що порушують дисципліну і правила внутрішнього розпорядку; охорона об'єктів від проникнення третіх осіб; забезпечення особистої безпеки керівника і перших осіб підприємства, охорона життя і здоров’я працівників та ін.

Другим напрямом організаційного забезпечення управління економічною безпекою підприємства є побудова захисту на умовах об’єднання внутрішніх і зовнішніх ресурсів. Дана політика, безумовно, є виправданою. Залучення сторонніх організацій, що спеціалізуються на кваліфікованій, професіональній діяльності, дозволяє отримати максимальний результат з оптимальними витратами в порівнянні із створенням своєї системи економічної безпеки з нуля. Проте потрібно розуміти, що повна передача аналітичних функцій сторонній організації може виявитися небезпечною. Така передача функцій

потребує повної упевненості не тільки у високому рівні професіоналізму фахівців, але і у високому ступені їх лояльності.

Отже, забезпечення економічної безпеки вітчизняних підприємств потребує суттєвої організаційної підтримки. В умовах сьогодення така підтримка має охоплювати, перш за все, площину управлінських, фінансово-економічних, правових відносин та інтересів, що вимагає від фахівців певної сукупності знань з менеджменту, економіки, права тощо.

Основне завдання створення організаційної підтримки полягає у координації дій щодо забезпечення економічної безпеки підприємства, тобто у здійсненні управлінської діяльності, яка забезпечує узгодженість роботи різних функціональних підрозділів в процесі виконання завдань і досягнення встановлених на підприємстві цілей, орієнтованих на забезпечення взаємоузгодження внутрішніх та зовнішніх інтересів підприємства.

За цих умов ефективною є модель організаційної підтримки економічної безпеки підприємств з використанням системного та ситуаційного підходів, які враховують два види ресурсів: знання, що є невичерпними й такими, що постійно оновлюються й накопичуються; час, який є невідновлюваним ресурсом, і тому його врахування є особливо важливим в умовах швидких змін при впровадженні інформаційних технологій.

Торкаючись першого виду ресурсів – знань, слід зазначити, що в умовах сьогодення на перший план виступає забезпечення підприємств висококваліфікованими фахівцями, що вимагає від них наявності певної сукупності знань з управління, економіки, права, організації інформаційно-аналітичного забезпечення безпеки, конкурентної розвідки, корпоративних конфліктів (рейдерства) та методів їх подолання, сучасних методів забезпечення надійності персоналу, управління захистом комерційної таємниці тощо. Всі ці питання формують площину організаційно-кадрової безпеки, яку слід визнати соціальним підґрунтям управління економічною безпекою підприємства.

Отже, третій напрям організаційного забезпечення – організаційно-кадрове забезпечення є одним з головних компонентів економічної безпеки підприємства. Він, в свою чергу, потребує вирішення таких завдань:

– аналіз і оцінка організаційних чинників, що загрожують безпеці підприємства;

– збір та аналіз відомостей про співробітників щодо прийняття рішень про допуск до конфіденційних документів або участь у важливих проектах;

– виявлення й знешкодження загроз, спричинених діями персоналу (кримінальна діяльність, розголошення комерційної таємниці, співробітництво з конкурентами, нанесення збитку інтересам бізнесу, негативні психолого-фізіологічні і моральні прояви; збір відомостей про кандидатів на роботу для прийняття керівництвом рішень про прийом або відмовлення);

– участь у службових розслідуваннях по фактах поведінки співробітників, що наносять шкоду економічній безпеці підприємства;

– навчання і підготовка персоналу з питань дотримання заходів безпеки і

правил поводження з конфіденційною інформацією і т. ін.

Крім того, формування організаційно-кадрового забезпечення економічної безпеки підприємств нерозривно пов'язано із інформаційним забезпеченням та інформаційною безпекою підприємства і тому, безперечно, потребує значних витрат.

1. Шкарлет С.М. Формування економічної безпеки підприємств засобами активізації їх інноваційного розвитку : автореф. дис. д-ра екон. наук: 08.00.04 / С.М. Шкарлет. – К., 2007. – 24 с.
2. Донець Л.І. Економічна безпека підприємства : навч. посібник / Л.І. Донець, Н.В. Ващенко. – К. :Центр навчальної літератури, 2008. – 240 с.
3. 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.
4. Ляшенко О.М. Концептуалізація управління економічною безпекою підприємства : монографія / О.М. Ляшенко. – 2-ге вид., переробл. – К. : НІСД, 2015. – 348 с.
5. Фоміна М.В. Проблеми економічно-безпечного розвитку підприємств: теорія і практика : монографія / М.В. Фоміна. – Донецьк : ДонДУЕТ, 2005. – 141 с.
6. 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.
7. Шемаєва Л.Г. Економічна безпека у стратегічній взаємодії з суб'єктами зовнішнього середовища : автореф. дис. д-ра екон. наук: 21.04.02 / Л.Г. Шемаєва. – К., 2010. – 39 с.

**Юрків Надія Ярославівна**
д.е.н., професор, головний науковий співробітник відділу фінансової безпеки Національного інституту стратегічних досліджень, м. Київ.

**Дубровін Віталій Олександрович**
здобувач
ДВНЗ «Університет банківської справи», м. Київ

## ПРОБЛЕМА РЕФОРМУВАННЯ СИСТЕМИ ГАРАНТУВАННЯ ВКЛАДІВ НАСЕЛЕННЯ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ ДЕРЖАВИ

Відповідно до «Стратегії національної безпеки України», затвердженої Указом Президента України від 26 травня 2015 року №287-2015 серед актуальних загроз національній безпеці України визначено:

- агресивні дії Росії, що здійснюються для виснаження української економіки і підриву суспільно-політичної стабільності з метою знищення су-

веренітету держави та захоплення її території;

- неефективність системи забезпечення національної безпеки і оборони України;
- корупція та неефективна система державного управління;
- економічна криза, виснаження фінансових ресурсів держави, зниження рівня життя населення [1].

Подолання економічної кризи, відновлення фінансових ресурсів держави та підвищення оптимального рівня життя населення можливе лише за умови економічного зростання національної економіки та забезпечення фінансової безпеки держави. Досягнути цього можливо при виконанні цілого комплексу заходів та формування відповідних умов в економічній політиці Уряду, серед яких визначено необхідність *стабілізації банківської системи, забезпечення прозорості грошово-кредитної політики та відновлення довіри до вітчизняних фінансових інститутів.* Отже, актуальності набуває необхідність вирішення проблеми забезпечення фінансової безпеки держави через стабілізацію її банківської системи. Розглянемо тенденції у банківській системі України та визначимо шляхи подолання негативних явищ у контексті забезпечення фінансової безпеки держави.

Криза банківської системи, яка була викликана як політичною, так і макроекономічною нестабільністю в 2014 – 2015 - 2016рр. була зумовлена в першу чергу з*начним відпливом банківського капіталу.*

За даними НБУ, оприлюдненими в повідомленні «Основні тенденції грошово-кредитного ринку України» [2], загальний обсяг депозитів в Україні на 1.09.2014 р. становив 680,0 млрд. грн.., з них: депозити фізичних осіб: 433,9 млрд. грн.. (64 %); депозити юридичних осіб: 246,2 млрд. грн.. (36 %). У 2014 році обсяг коштів фізичних осіб у банківській системі порівняно з початком року скоротився на 126 млрд. грн., або на 29 %, у т.ч. у національній валюті – на 57 млрд. грн., в іноземній валюті – на 9 млрд. дол. США.

*Обсяг депозитів в іноземній валюті* за 2015р. зменшився з 13,8 млрд. дол. США до 8,8 млрд. дол. США , або на 36,3% , у національній валюті – на 2 млрд. грн., або на 1%.

Негативна тенденція скорочення депозитів зупинилась протягом 2016 р. і вклади населення у гривні зросли майже на 11 млрд. грн., у валюті зменшились лише на 189 млн. дол. США. , або на 2,1% (практично не змінились). Протягом 2017 р. динаміка вкладів населення відповідала тенденції повільного зростання, сформованій у минулому році: депозити у гривні зросли на 4 млрд. грн., обсяг валютних вкладів майже не змінився. Основними чинниками, що забезпечили позитивну динаміку вкладів фізичних осіб, були: відносна курсова стабільність та довгостроковий ефект від законодавчого *скасування можливості дострокового зняття депозитів населення.*

Законом України «Про внесення змін до деяких законодавчих актів України щодо умов повернення строкових депозитів» № 424-VIII від 14.05.2015р. встановлено часткову стабільність банківської системи через

врегулювання механізму створення ресурсної бази діяльності банківської системи [3]. Цей Закон спрямований на підвищення надійності банківської системи та повернення довіри до неї з боку клієнтів.

Для досягнення цієї мети внесено зміни до статей 1060, 1065 Цивільного кодексу України та статті 13 Закону України «Про цінні папери та фондовий ринок» відповідно до яких клієнти банку матимуть право отримати вклади та нараховані по ним відсотки за строковим банківським договором по закінченню терміну дії договору на відміну від чинного у даний час правила, за яким, зокрема, фізичні особи – вкладники можуть отримати власний вклад або його частину на першу вимогу. Дострокове повернення даного вкладу та нарахованих процентів за цим вкладом можливе виключно у випадку, коли це передбачено умовами договору банківського строкового вкладу. Вплив цих законодавчих змін на банківську систему є позитивним, адже унеможливлює одночасне зняття нових депозитів вкладниками і дозволяє банкам більш достовірно планувати свою діяльність. Аналогічно, він є позитивним і для вкладників банку, оскільки даний Закон не дозволяє банкам автоматично продовжувати строки депозитних вкладів.

Станом на 01.01.2018 року вклади населення становили разом – 495,3 млрд. грн. в т.ч. у національній валюті – 252,4 млрд. грн., в іноземній валюті – 8,6 млрд. дол. США., за два місяці 2018 року депозитні вклади населення зменшилися на 4,3% до початку року і станом на 01.03.2018р. становили уже 474,2 млрд. грн.

Одним із найбільш *ефективних інструментів стабілізації банківської системи,* забезпечення прозорості грошово-кредитної політики та відновлення довіри до вітчизняних фінансових інститутів є реформування системи гарантування вкладів населення.

Для стимулювання повернення коштів у банківську систему та поступове відновлення довіри до банківської системи є підвищення гарантованої державою суми відшкодування вкладів фізичних осіб. Поточні можливості держави не дають змоги підвищити суму гарантованого відшкодування вкладів фізичних осіб до європейського рівня у 100 тис. євро. Проте, після остаточного очищення банківської системи, необхідною умовою відновлення депозитного ринку в Україні є зростання суми гарантованого відшкодування вкладів фізичних осіб до рівня 500тис.грн., що становить приблизно 20 тис. дол. США, що у валютному еквіваленті є меншою за суму відшкодування до девальвації гривні (25 тис. дол. США при курсі 8 грн. за 1 дол. США).

Відповідно до інформації заступника директора – розпорядника ФГВФО (А.Оленчика) про перспективи підвищення суми виплат з Фонду, запровадження гарантій для юридичних осіб і судах з екс- власниками банків — банкрутів зазначено, за минулі 4 роки через вихід банків з ринку, включаючи націоналізацію Приватбанку, було виплачено вкладникам майже 90 млрд. грн. В умовах банківської кризи активів Фонду, що формуються з регулярних відрахувань банків-учасників, не вистачає на своєчасне відшкодування

вкладів найбільших банків, що були виведені з ринку. Уряд регулярно надає Фонду кредити для своєчасного і повного відшкодування їх вкладів, було залучено кошти НБУ і кошти державного бюджету, з яких залишок за кредитом НБУ становить – 5млрд.грн. і кредит МФУ 60 млрд. грн [4].

Якщо із залишком кредиту НБУ все зрозуміло і Фонд планує повернути йому в поточному році, то з поверненням коштів в бюджет виникає складність через випуск ОВДП, які мають свій цикл обігу. Тому дострокове погашення кредиту не буде співпадати з тими строками ОВДП, за якими має зобов'язання Міністерство фінансів України. Консультації з цього приводу уже ведуться з МВФ, Світовим банком та US Treasury, які виконують функцію медіаторів. Однак, погашення цих кредитів дуже важливе із-за умов їх надання. При погашенні цієї позики, до 2031 року сума виплати процентів становитиме 85 млрд. грн. Це у фінансовому плані – дуже складно, адже ФГВФО не заробляє кошти, і в даній ситуації, держава мала б запропонувати Фонду безпроцентні позики.

Якщо у 2018-2019рр. вимоги кредиторів будуть погашатися через продаж активів банків, то не пізніше 2020 року виникне проблема нестачі коштів. Відповідно до ситуації, яка склалася, ФГВФО було прийнято рішення з 2018 року запровадити систему диференційованих зборів для банків. Тепер ФГВФО самостійно (за своєю методикою) буде оцінювати фінансовий стан банку і відповідно розраховувати його внесок. Для різних банківських установ сума внеску буде відрізнятися залежно від ступеню ризикованості їхньої політики, яку вони проводять, гірший стан банку, то будуть більші відрахування у Фонд [5].

На думку фахівців, це правильний метод реформування наявної системи, однак, виникають питання щодо запропонованих Фондом показників. Зокрема: *показники щодо нормативу достатності капіталу (Н2), якщо він (*Н2) становить менше -10 (значить банк вимоги НБУ не виконує), то банк справедливо має нуль балів, якщо значення Н2 у банку становить від 10 до 20 –банк має 5 балів, а при значенні більше 20 - банк отримає 10 балів. Різниця між 10 і 20 значна, і фінансовий стан двох таких банків буде відрізнятися, але кількість балів однакова. Виходить, що оцінка банків буде умовною. У світі аналогічний показник (capital adequacy ratio) є нормальним, якщо він перебуває в діапазоні 12–14. В національній банківській системі існує інколи штучна ситуація, коли у деяких банків цей норматив достатності капіталу - Н2 перевищує 20, 30, і 60, що свідчить про те, що наша банківська система досі переживає кризу.

*Інший показник - щодо співвідношення статутного капіталу до регулятивного*. Так як, банки зазнали суттєвих збитків після кризи 2008 – 2009 рр., їхні прибутки минулих років стали збитками минулих років, то ці збитки були компенсовані збільшенням статутного капіталу, а регулятивний капітал залишився без змін. Наступна (сучасна) криза цей розрив лише збільшила. Тому, до нової методики виникає питання: головне її мета полягає в оцінці

реального фінансового стану банку, чи просто збільшити внески до ФГВФО, яких катастрофічно не вистачає ?

Виникають питання також до *індикаторів, які оцінюють якість банківських активів,* адже від суми балів, набраних у цьому блоці, буде залежати кінцева сума внеску. Сучасна банківська криза сприяла великим втратам та зниженню якості кредитних портфелів банківських установ. Так, резерви під ці втрати формувалися, акціонери вносили кошти, капітал на покриття збитків збільшено, проте ФГВФО для оцінки якості кредитів банку пропонує брати всі наявні (недоходні) кредити й ділити на активи банку, і не враховувати резерви.

Всі вище описані проблеми з новою методикою відрахувань, ще раз доводять закономірний наслідок того, що банківський сектор порівну розділений на державні банки й банки з іноземним капіталом. Проте, всі вони перебувають у нерівних конкурентних умовах. Аналіз конкурентних умов державних банків й банків з іноземним капіталом в Україні є напрямом подальших досліджень.

1. «Стратегія національної безпеки України», затвердженої Указом Президента України від 26 травня 2015року №287-2015, [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/287/2015

2. «Основні тенденції грошово-кредитного ринку України». - Офіційний сайт Національного банку України – [Електронний ресурс]. –Режим доступу http://www.bank.gov.ua/control/uk/publish/article?art_id=1471 6152&cat_id=580385

3. Закон № 424-VIII «Про внесення змін до деяких законодавчих актів України щодо умов повернення строкових депозитів» від 14.05.2015р. [Електронний ресурс], режим доступу: http://golovbukh.ua/regulations/8186/8187/460612/.

4. Крадіжки в банках носять характер стихійного лиха національного масштабу. Заступник голови ФГВФО (А.Оленчик) [Електронний ресурс]. – Режим доступу: https://ua.112.ua/interview/kradizhky-v-bankakh-nosiat-kharakter-stykhiinoho-lykha-natsionalnoho-masshtabu-434992.html

5. Ю. Самаєва. За себе й за того хлопця. Дисбаланси в банківському секторі посилюються // Зеркало тижня. 15 грудня, 2017.- [Електронний ресурс]. – Режим доступу: https://dt.ua/finances/za-sebe-y-togo-hlopcya-disbalansi-v-bankivskomu-sektori-posilyuyutsya-263549_.html)

Наукове видання

# ЕКОНОМІЧНА ТА ІНФОРМАЦІЙНА БЕЗПЕКА: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

***Матеріали***
***Міжнародної науково-практичної конференції***
*(м. Дніпро, 27 квітня 2018 р.)*

**Українською, англійською,**
**польською та російською мовами**

Редактор, оригінал-макет – *А.В. Самотуга*

Підп. до друку 23.04.2018. Формат 60х84/16. Друк – трафаретний. Папір офісний.
Гарнітура – Times. Ум.-друк. арк. 16,50. Обл.-вид. арк. 17,25. Тираж – 500 прим.
Зам. № 03/18-зб

Надруковано у Дніпропетровському державному університеті внутрішніх справ
49005, м. Дніпро, просп. Гагаріна, 26, тел. (056) 370-96-59
Свідоцтво суб'єкта видавничої справи ДК № 6054 від 28.02.2018