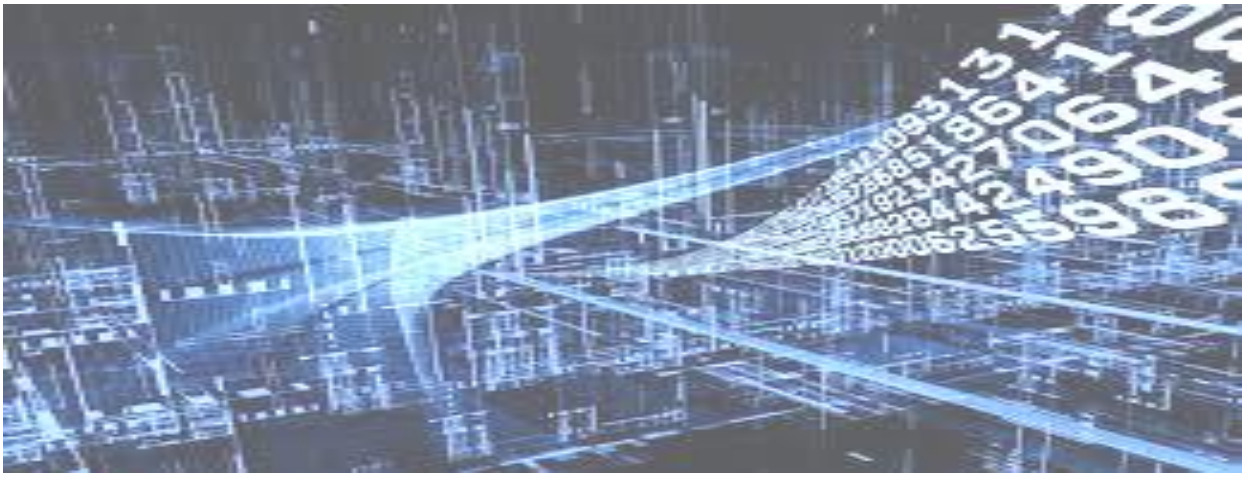
МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КАФЕДРА ЕКОНОМІЧНОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ



Матеріали Всеукраїнського науково-практичного семінару
(м. Дніпро, 23 листопада 2018 р.)

Дніпро – 2018

ББК 67.9(4УКР)305
П 685
УДК 347.23 (477)

Рекомендовано до друку Науково-методичною радою Дніпропетровського державного університету внутрішніх справ.
(протокол № 4 від 18.12 2018)

П 685 **ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ**: матеріали Всеукраїнського науково-практичного семінару (23 листопада 2018 р., м. Дніпро). – Дніпро: Дніпропетровський державний університет внутрішніх справ, 2018. – 150 с. *(в авторській редакції)*

СКЛАД ОРГАНІЗАЦІЙНОГО КОМІТЕТУ

Фоменко А.Е. - кандидат юридичних наук, заслужений юрист України, ректор (голова оргкомітету)
Наливайко Л.Р. – доктор юридичних наук, професор, заслужений юрист України, проректор
Рижков Е.В. - кандидат юридичних наук, доцент, завідувач кафедри економічної та інформаційної безпеки (заступник голови оргкомітету);
Косиченко О.О. - кандидат технічних наук, доцент кафедри економічної та інформаційної безпеки (відповідальний секретар оргкомітету).

ЧЛЕНИ ОРГКОМІТЕТУ

Марченко О.В. – доктор філософських наук, начальник відділу організації наукової роботи
Краснобрижий І.В. – доцент кафедри економічної та інформаційної безпеки, кандидат юридичних наук;
Махницький О.В. - старший викладач кафедри економічної та інформаційної безпеки;
Гавриш О.С. - викладач кафедри економічної та інформаційної безпеки.

ББК 67.9(4УКР)305

ЗМІСТ

ТЕЗИ ВИСТУПІВ

Вишня В.Б. - професор кафедри Дніпропетровського державного університету внутрішніх справ, доктор технічних наук, професор;
Гавриш О.С. - викладач Дніпропетровського державного університету внутрішніх справ

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

При розгляді питання про інформаційно-аналітичне забезпечення безпеки підприємства ми можемо зустрітися з двома підходами до її організації. Відповідно до першого вважається, що інформаційно-аналітичним забезпеченням безпеки діяльності фірми повинна займатися безпосередньо сама фірма. Інформаційний підрозділ при цьому є структурним підрозділом організації, має прямий вихід на директора (власника) і сам будує стосунки з іншими структурними підрозділами, у тому числі і його службою безпеки.

Міжнародний досвід показує, що такий підхід характерний для великих корпорацій, тих, хто займається виробництвом і реалізацією продукції. Така організація інформаційно-аналітичного забезпечення виробничої діяльності пов'язана з тим, що основні ризики і погрози породжуються комерційною діяльністю конкурентів, виходять із змін стану ринків і тому подібних обставин.

В даному випадку таку інформаційно-аналітичну роботу ведуть конкретні фахівці. Взаємодія інформаційно-аналітичного підрозділу із службою безпеки у такому разі полягає в тому, що служба повідомляє аналітиків про можливість загрози з боку кримінальних структур та ін. Аналітики ж орієнтують службу безпеки про характер змін в ризиках бізнесу, виникненні нових викликів, певних погрозах і їх суб'єктах, орієнтують підрозділи, які зайняті пошуками інформації відносно напрямів її пошуків, розвідувальних і контррозвідувальних заходів [1]. Подібна організація інформаційно-аналітичної роботи використовується в великих брендових корпораціях.

Відповідно до іншого підходу – інформаційно-аналітичний підрозділ (група або окремий аналітик) мають бути включені до складу служби безпеки організації. В цьому випадку аналітики структурно входять в службу безпеки і підкоряються безпосередньо начальникові служби безпеки, який, як правило, виконує і роль головного аналітика. Безпосередній вихід на керівництво фірми має тільки керівник служби безпеки.

Така організація інформаційно-аналітичного забезпечення безпеки підприємства характерна для більшості вітчизняних кредитно-фінансових

установ, торговельних і посередницьких підприємств регіональних і міжрегіональних рівнів. Зусилля при цьому концентруються на необхідності протистояти неправомірним погрозам з боку дій конкурентів, і значним погрозам з боку кримінальних структур, а останнім часом необхідності протистояти можливим рейдерським атакам.

Аналітична робота в цьому випадку покладається на досвідчених фахівців у сфері недержавної безпеки, які повинні мати професійні знання у сфері діяльності підприємства. До сьогодення таких фахівців готували з працівників структур, які виявили інтерес і здібності до аналітичної роботи. Зараз все частіше на такі посади приходять фахівці, які здобули вищу освіту у ВНЗ, що готують фахівців з безпеки. Окрім фахівців сфери діяльності підприємств для проведення конкурентних аналітичних розробок і експертиз іноді притягуються вузькі фахівці: психологи, інженери і технологи, соціологи, прикладні математики і програмісти, криміналісти і т.ін. Подібна організація інформаційно-аналітичного забезпечення безпеки недержавних структур зараз використовується практично в усіх банках, страхових компаніях.

При будь-якій діяльності необхідно враховувати, що інформаційно-аналітичне забезпечення безпеки підприємства повинне вестися однією структурою. Паралельно аналітична робота служби безпеки і власне підприємства практично не допустима. Це зв'язано з тим, що інформаційне поле дійсно буває істотно обмеженим, тому робота декількох структурних підрозділів в одному і тому ж напрямі може бути легко виявлена, прорахована (конкурентами, або злочинними угрупуваннями) і припинена або паралізована.

В той же час, не виключається варіант такої організації інформаційно-аналітичного забезпечення безпеки виробничій діяльності, коли аналітична група діє на правах самостійного структурного підрозділу підприємства, підкоряється паралельно директорові і начальникові служби безпеки. Як правило, при цьому назва групи зашифровується: група вивчення ринку, відділ маркетингу, інформаційно-довідкова служба і так далі.

Декілька слів про функції інформаційно-аналітичного підрозділу, що забезпечує безпеку підприємства. Вони можуть бути досить великими, але на практиці вони зведені до тих цілей і завдань, які зараз стоять перед організацією.

У будь-якому випадку сьогодні аналітики повинні:

- вивчати кон'юнктуру ринку;
- вести збір, накопичення, обробку і переробку інформації (про можливих клієнтів, партнерів, перспективи співпраці, конкурентів, рейдерські структури і їх діяльність), її видачу на запит правоохоронних підрозділів і керівництва фірми;
- збирати і обробляти інформацію про процеси, що відбуваються в кримінальних структурах, про кримінальну обстановку в районі (регіоні), її впливі на діяльність підприємства;
- розробляти рекомендації і ефективні заходи протистояння

злочинним посяганням, спрямованим проти інтересів фірми, її співробітників, її активів, землі і, загалом, власності;

- сприяти кадровому відділу у вивченні кандидатів, підборі співробітників, постійному моніторингу їх діяльності за межами організації;
- контролювати діяльність партнерів і клієнтів, з'ясовувати питання їх надійності, платоспроможності, майнового і фінансового положення, визначати їх дійсні наміри;
- брати участь в діяльності служби безпеки фірми в справах повернення боргів, кредитів і вирішеннях інших проблемних питань, що виникають в повсякденній діяльності організації;
- надійно забезпечувати діяльність захисту інформації з обмеженим доступом.

Якщо у Вашій організації буде можливість мати декілька співробітників, які займатимуться інформаційно-аналітичній забезпеченням безпеці підприємства, то виникне можливість деякої спеціалізації аналітиків. Частина з них орієнтується на збір інформації, це так звані збирачі. А частина – займається узагальненням, класифікацією, аналізом, збереженням і видачею інформації, аналітичних матеріалів – інформаційних документів. Саме ці співробітники орієнтують збирачів про те яку інформацію треба збирати, де її можна знайти і тому подібне. Значна частина роботи по збору інформації кладеться на плечі збирачів. Саме вони використовуючи свої можливості, можливості інших категорій співробітників фірми, можливості, які відкриваються всесвітньою мережею Інтернет. Вони збирають інформацію про платоспроможність клієнтів, стан справ у партнерів, дані про можливі зв'язки контрагентів з мафіозними структурами, намірах конкурентів і про багато що інше.

Іноді для отримання додаткової важливої інформації доводиться користуватися послугами різних інформаційних систем і інформаційно-аналітичних агентств. За такі послуги, як правило, доводиться платити і платити немало. У крузі фахівців з безпеки вже склався своєрідний «крилатий вислів» – «За інформацію треба платити, за її відсутність доводиться розплачуватися» [2].

Рішення задачі інформаційного забезпечення безпеки власними зусиллями організації має відмінність від забезпечення її зовнішніми структурами. Власними силами відбувається рішення завдань інформаційного забезпечення конкретних проектів, що визначає наявність і конкретні підстави для збору і аналізу загальної інформації. Інформація, що добувається, повинна мати цільову спрямованість та:

- визначати ознаки виникнення і розвитку кризових ситуацій;
- давати характеристику сильним і слабким сторонам конкурентів;
- розкривати дійсні наміри потенційних і діючих партнерів відносно нашої організації;
- бути ефективною в цілях здійснення впливу на позицію зацікавлених осіб в ході переговорного процесу;

- своєчасно виявляти моменти виникнення нових викликів, і їх переростання в погрози підприємству;
- забезпечити контроль виконання партнерами досягнутих домовленостей;
- забезпечити також виявлення каналів витоку і втрати інформації з організації через вивчення змін в діяльності партнерів і конкурентів;
- стати основою для ухвалення рішення;
- орієнтувати керівництво підприємства про виникнення небезпек і сприяти організації ефективної діяльності по ліквідації наслідку негативного впливу.

І це далеко не усі питання, що повинні підніматися і відпрацьовуватися працівниками аналітичного підрозділу підприємства [3]. Треба обов'язково враховувати, що в країнах з ринковою економікою, а Україна поступово просувається в їх число, відомості про клієнтів, партнерів інші відомості прийнято вважати капіталом фірми. Списки клієнтів фірми, її партнерів і конкурентів, банки відомостей про них складаються в першу чергу зусиллями власників фірми і у будь-якому випадку – за їх рахунок. Значна частина цієї інформації надається менеджерами відділу продажів, відділу закупівель і відділу маркетингу. Аналітики повинні добре зорієнтувати персонал цих відділів, давати чіткі інструкції за яким принципом вони повинні поставляти інформацію аналітичному підрозділу.

Аналітичній групі підприємства разом з цими службами треба регулярно поповнювати спеціальний банк даних. При цьому окремим завданням аналітиків має бути строгий облік відомостей: де, як і коли отримані ці відомості, як вони були використані. Систематичне накопичення даних в належному виді з можливостями оперативного зіставлення відомостей даних з різних джерел забезпечує перевірку достовірності останніх, а також своєчасне збудження підозри про наявність дезінформації.

У нормально працюючому інформаційно-аналітичному підрозділі на кожного партнера, клієнта, конкурента накопичуються відомості про нього: – потреби і бажання, звички, стан, договори про надання йому раніше привілеїв, а також примітки, за що вони надавалися і багато інших даних.

Відносно вимог клієнта: фіксуються дані про кількість товарів і послуг, то якими способами і з використанням яких режимів відбулася доставка товарів; яка періодичність постачань, чим вони повинні доповняться, інформації про оплати, а також інші специфічні особливості контрактів з цим клієнтом. Також накопичуються дані, які визначають прибутковість усієї операції з конкретним клієнтом (об'єми трансакції, що очікуються, частота постачань, зміна цін, розпродажі, які плануються).

У завдання аналітичного підрозділу входить орієнтація продавців послуг і товарів, які випускаються фірмою, на надання письмових звітів конкретним клієнтам по кожному факту продажів. У таких звітах можуть бути відображені перспективи майбутніх продажів.

Відповідна інформація має бути впорядкована, сконцентрована у керівництва організації, а також мати конфіденційний характер (навіть

характер комерційної таємниці).

Завдання аналітиків певним чином орієнтувати працівників відділу маркетингу своєї фірми. Вивчаючи клієнтів, вони зобов'язані збирати і аналізувати дані про конкурентів. Саме аналітики повинні пропонувати їм план такої діяльності: – які відомості необхідно збирати, де і як ці дані добуваються і відображуються, які дії персоналу організації для цього потрібні, як вирішуються проблеми при отриманні необхідних відомостей. Разом з цим необхідно враховувати: час, місце, спосіб отримання, їх стосунки до об'єктів, які вивчаються, до дій, що прогнозуються і які обумовлюються змістом інформації.

Якщо ми обізнані про найбільш прибуткових клієнтів конкурента, то у нас з'явиться шанс перемогти останнього, переманивши його клієнтуру. Значення має особиста інформація про клієнтів: а саме, дані про їх прив'язаності, дружні і інші зв'язки в середовищі підприємців і конкурентів, особливо такі, які впливають на процес ухвалення рішень про підтримку ділових стосунків з організацією або про їх припинення.

У літературі є різні варіанти списків основних напрямів збору інформації, які охоплюють практично усі аспекти діяльності підприємства-партнера і підприємства-конкурента [4].

Приведемо узагальнений список:

1. Інформація про ринок:
   - ціна, умови угод, специфіка продукту, знижки;
   - об'єм, тенденція і прогноз збуту конкурентного продукту;
   - частина ринку і тенденції його зміни;
   - ринкова політика і плани;
   - стосунки із споживачами і репутація;
   - чисельність і розставляння торговельних агентів;
   - канали, політика і методи збуту;
   - постановка реклами.
2. Інформація про виробництво продукції:
   - оцінка якості і ефективності;
   - номенклатура виробу;
   - технологія і устаткування;
   - рівень витрат;
   - виробничі потужності;
   - спосіб упаковки;
   - доставка;
   - розміщення і розмір виробничих підрозділів і складів;
   - можливості проведення науково-дослідних робіт.
3. Інформація про організаційні особливості і фінанси:
   - виявлення осіб, які приймають ключові рішення;
   - філософія осіб, які приймають ключові рішення;
   - програми розширення і придбань;
   - головні проблеми і можливості їх рішення;

- програми проведення науково-дослідних робіт.

Звичайно, заведений перелік не є повним, він тільки орієнтує відносно напрямів отримання, накопичення, обробки і перетворення інформації необхідної для надійного інформаційно-аналітичного забезпечення безпеки підприємства.

Використані джерела:

1. Герасимчук А., Тимошенко О., Шашкевич Я. Етика і етикет сучасного бізнесу – запорука економічної безпеки підприємств: навч. посіб / за заг. Ред.. З.І. Тимошенко - К.: Вид-во Європ. ун-ту, 2007. - 285 с.
2. Позднишев Є.В. Інформаційно-аналітичне забезпечення безпеки підприємництва «Методи та їх застосування»: Навч. посібник. Книга 1.-К.: Видавець Позднишев, 2007 р. - 76 с.
3. Романчев Н.Р., Нежданов И.Ю. Конкурентная разведка. Практический курс – М.: «Ось - 89», 2007. – 272 с.
4. Чергенець Е.В., Зайцев А.В., Позднишев Є.В. Інформаційно-аналітичне забезпечення безпеки підприємництва «Збір та пошук інформації»: Навч. посібник. Книга 2. – К.: Видавець Позднишев 2007. – 74 с.

Воронов І.О. – доктор юридичних наук, старший науковий співробітник, адвокат АО "Саенко Харенко (м. Київ)

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ

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, підвищується швидкість передачі даних, з'являються нові види каналів зв'язку, виникають раніше невідомі або недосяжні послуги.

Інформатизація суспільства надала кожному її члену можливість користуватися такими здобутками для повноцінної життєдіяльності та функціонування у сучасних умовах. Неможливість здійснення вибірковості у розповсюдженні й впровадженні здобутків високих інформаційних технологій призвела до того, що кримінальні структури стали їх активним необмеженим споживачем. Таким чином вони отримали гнучку структуру управління, високу пластичність індивідуальної й організованої кримінальної діяльності, специфічну інфраструктуру. Це також призвело до виникнення нових видів кримінальних діянь і певного поширення числа потенційних потерпілих. Аналіз законодавства, опублікованих точок зору, матеріалів практичної діяльності вітчизняних правоохоронних підрозділів, а також правоохоронних органів зарубіжних країн свідчить про те, що в сучасних умовах ефективне забезпечення кібербезпеки України неможливе без врахування специфіки та системного підходу.

Незважаючи на численні публікації, на даний час й досі бракує

ґрунтовних методологічних положень, присвячених:

- принципам забезпечення кібербезпеки, правовим та організаційним основам забезпечення захисту життєво важливих інтересів суспільства та держави, національних інтересів України у кіберпросторі, повноваженням і обов'язкам державних органів;
- основним об'єктам кіберзахисту, які створюють критичну інфраструктуру держави;
- методики формування та визначення основних показників ефективності реалізації Стратегії кібербезпеки України з урахуванням досвіду європейських і світових практик;
- розмежуванню підслідності органів, що здійснюють досудове розслідування кримінальних правопорушень у сфері високих інформаційних технологій;
- протидії інформаційним впливам («кібервійнам»).

Окремо слід відзначити, що незважаючи на позитивні зміни, продовжують існувати численні проблемні питання підготовки спеціалістів правоохоронних органів.

Аналіз офіційної статистики та практичних матеріалів свідчить, що створення шкідливих програмних засобів і несанкціоноване втручання в роботу комп'ютерів та їх мереж стає об'єднуючим фактором широкого спектра кримінальних дій. Одна з основних причин такого становища полягає у тому, що шкідливі програмні засоби, на відміну від попередніх етапів злочинної діяльності, все більше застосовуються не для знищення даних, а для отримання прибутків.

Не повинен залишатися поза увагою й такий принцип кримінальної діяльності, згідно з яким можливості одного програмно-апаратного комплексу помножуються на їх кількість. Спочатку необхідна кількість комп'ютерів досягалася за рахунок засобів, які належали членам злочинного угруповання. Виникнення та вдосконалення телекомунікаційних програмних засобів надали можливість одному користувачу встановлювати контроль над великою кількістю комп'ютерів і керувати ними особисто.

Аналіз зарубіжних джерел свідчить, що для позначення мережі комп'ютерів, над якими встановлено контроль, використовується термін "Ботнет". Наводиться авторське визначення поняття Ботнет, під яким слід розуміти субмережу, що функціонує за двоканальним принципом і виникає внаслідок латентної мобілізації ресурсів. Гостро постає необхідність застосовувати новий підхід щодо постійного спостереження за станом, тенденціями, чинниками оперативної обстановки та створення прогностичної моделі її розвитку з метою визначення ефективної моделі використання сил і засобів у протидії кіберзлочинності. Єдність потенціалів та можливостей підрозділів органів внутрішніх справ істотно підвищує ефективність протидії злочинності. Як свідчать результати практики, необхідною складовою розкриття і розслідування злочинів є постійне підвищення ефективності взаємодії. Очевидною є неспроможність держав індивідуально ефективно протидіяти злочинам у сфері високих інформаційних технологій, яким

притаманний міжнародний характер.

Найважливішою умовою ефективності кібербезпеки держави та профілактики правопорушень є організація взаємодії. Проблема взаємодії є загальною, і залежно від того, яким змістом воно буде наповнене, вирішуватиметься питання про принципи, класифікацію, етапи, нормативно-правове регулювання взаємодії правоохоронних підрозділів між собою, а також з правоохоронними відомствами і державними органами України та інших держав. Першочерговою стадією будь-якого процесу виявлення та аналізу є пошук. Його здійснення являє собою організаційно-тактичну форму Криміналізація сфери високих інформаційних технологій визначає необхідність постійного здійснення оперативно-розшукових, оперативно-технічних, організаційних і тактичних заходів. Тактика оперативного пошуку визначається особливостями індексації ресурсів певного сегменту мережі Інтернет.

Система пошукових ознак є структурованою сукупністю даних об'єктів пошуку, яка може бути побудована на базі предмета документування кримінальної діяльності у сфері високих інформаційних технологій. Інформація, отримана за допомогою програмних засобів, у тому числі спеціальних, характеризується існуванням у нематеріальному вигляді, оскільки зберігатиметься на відповідному носії. Дослідження проблеми використання цифрових даних як доказів у кримінальному судочинстві дозволило стверджувати, що головною причиною виникнення сумнівів у відсутності їх модифікації, є об'єктивна неможливість повного контролю за процесами фіксації та обробки.

Основним засобом забезпечення допустимості таких доказів є підтвердження факту відсутності їх модифікації внаслідок використання стандартизованого спеціального сертифікованого програмного забезпечення іноземного і вітчизняного виробництва та типів матеріальних носіїв, які унеможливлюють внесення змін у зафіксовану на них інформацію.

Головною причиною виникнення сумнівів у відсутності модифікації цифрових даних є об'єктивна неможливість повного контролю за процесами створення і обробки. Основним засобом забезпечення допустимості таких даних як докази є підтвердження факту відсутності їх модифікації внаслідок використання спеціального сертифікованого програмного забезпечення та матеріальних носіїв, що унеможливлюють внесення змін у зафіксовану на них інформацію.

Інформаційне суспільство – це об'єктивно виникаюча історична стадія суспільного розвитку. При переході від індустріального до інформаційного суспільства послідовно усувалися обмеження щодо нагромадження і використання інформаційних ресурсів, розповсюдження апаратних та програмних засобів. У свою чергу, інформатизація призвела до побічного виникнення негативних наслідків, оскільки інтегруючи, синтезуючи й акумулюючи в собі низку соціальних інститутів, вийшла за межі технологічної проблематики. Таким чином, інтенсивна розробка, впровадження та широке використання високих інформаційних технологій

практично в усіх видах соціальної діяльності поетапно призвели до вдосконалення конвенціональної (традиційної) кримінальної діяльності, виникнення принципово нових видів злочинів, розширення сфери кримінальної діяльності.

Високі інформаційні технології необхідно розглядати як наукову категорію, що має широку сферу застосування. Вони здатні викликати ланцюгові реакції нововведень, оскільки забезпечують більш оптимальне, у порівнянні з попередніми технологіями, співвідношення витрат та результатів, а також можуть справляти як позитивний, так і негативний вплив на соціальну сферу. Орієнтування кримінальних структур на використання високих інформаційних технологій пояснюються доступністю та рентабельністю останніх. Кримінальні структури використовують або швидко пристосовують для власних цілей можливості, що створюються державою для правового суспільства. Вони є частиною суспільства, і тому не вдається реалізувати вибірковість у використанні й поширенні продуктів високих інформаційних технологій. Наслідки впровадження високих інформаційних технологій створюють сприятливі умови для кримінальної діяльності. Динаміка постійного розвитку призводить до скорочення часу на раціональний аналіз програмних та апаратних новацій, що створюються. Кримінальні структури таку ситуацію обертають на свою користь, оскільки правоохоронні органи не встигають приймати своєчасні рішення і організовувати свою діяльність відповідним чином.

В європейських країнах упроваджується комплексний (інтеграційний) підхід, який поєднує запобіжні й репресивні заходи, що позначаються терміном «протидія». Протидія злочинам у сфері високих інформаційних технологій – це система правових, організаційних і тактичних заходів, спрямованих на безпосереднє запобігання, розкриття й розслідування злочинів, а також діяльність, спрямована на виявлення, усунення або нейтралізацію причин, умов, явищ і процесів, які їм сприяють.

Протидія злочинам у сфері високих інформаційних технологій безпосередньо впливає на рівень захищеності інформаційної безпеки, яка, у свою чергу, є складовою національної безпеки країни. Доведено, що криміналізації сфери високих інформаційних технологій сприяє деперсоналізація, можливість анонімного доступу до ресурсів мережі Інтернет, її міжнародний характер, а також можливість отримання надприбутків шляхом здійснення масштабних проектів, які не вимагають значних капіталовкладень.

Специфічною ознакою сучасної організованої злочинності є те, що спільноти злочинців взаємодіють переважно у рамках вільних злочинних мереж, які не мають сталої, чітко визначеної організаційної будови. Вони досить часто швидко змінюють напрями діяльності заради більш раціонального й оптимального досягнення поставленої мети.

У переважній більшості проаналізованих наукових праць відчувається проблема адекватного визначення понятійно-термінологічного апарату. Ідеться про значний перелік понять і термінів, що вимагає їх уніфікації

трактування та використання. Залучення нових понять і термінів для криміналістики та теорії й практики оперативно-розшукової діяльності повинно забезпечити сучасні методологічні підходи. При цьому, новизна підходів має визначатися з позиції їх первинності для юридичних наук.

Вітчизняна наука в аспекті забезпечення практичними рекомендаціями оперативно-розшукової протидії злочинам у сфері високих інформаційних технологій перебуває на початку формування своїх регіональних шкіл. Ключове значення набуває правильність вибору пріоритетів – стратегічних напрямів, на яких необхідно зосередити увесь наявний науковий та практичний потенціал, забезпечити їх належне фінансування. Логічним та виправданим слід вважати розмежування напрямів правоохоронної діяльності.

З метою підвищення ефективності інформаційно-аналітичного забезпечення також необхідно розробити й запровадити децентралізовану схему накопичення і зберігання даних всіма суб'єктами боротьби з кіберзлочинністю на основі сумісного програмного забезпечення, а також централізовану комунікаційну мережу з їх обміну.

Використання аналітичних програмних засобів допоможе розкрити природу і масштаб проблем, прийняти обґрунтоване рішення, розробити відповідні плани дій і використовувати наявні засоби найбільш ефективним чином в оперативно-розшуковій протидії злочинам у сфері високих інформаційних технологій. Не слід залишати поза увагою сучасні прийоми ведення інформаційної війни. У зв'язку з чим розроблювати системи протидії та безпеки інформаційної системи із залученням кращих практик країн Східної Європи. За останні роки кожен член суспільства став свідком посилення загроз для національної безпеки України, що пов'язані з активізацією агресії в інформаційному просторі. Отже, питання правового забезпечення кібербезпеки в умовах європейської інтеграції, комплексна протидія кіберзлочинам та кібервійнам з урахуванням останніх тенденцій потребують постійної уваги.

Воскобойник В.О. – доцент кафедри захисту інформації, кандидат технічних наук; **Слива О.М., Єфіменко М.М.** – студенти (Запорізький національний технічний університет)

ЗАСТОСУВАННЯ ГРАФОАНАЛІТИЧНИХ МЕТОДІВ ПРИ ОЦІНЮВАННІ ЗВУКОІЗОЛЯЦІЇ ВИДІЛЕНИХ ПРИМІЩЕНЬ

На сьогоднішній день налічується декілька десятків методів розрахунку і виміру розбірливості мови , що застосовуються для оцінки захищеності мовної інформації шляхом визначення якості акустики приміщень, ліній зв'язку тощо.

Такими являються об'єктивні методи: формантні - зарубіжні (AI, SII),

вітчизняні (Покровського, Бикова, Сапожкова, Калінцева); модуляційні (STI, RASTI, STITEL, STIPA); емпіричні (Alcons, C50).

За версією Покровського, оцінюючи формантну (артикуляційну) розбірливість мови, усю аналізовану область частот розбивають на K суміжних частотних смуг з центральними частотами f_{ok} і граничними частотами $f_{нk}$ і $f_{вk}$, в межах кожної з яких спектри мови і шуму та густину ймовірностей формант, можна вважати практично незмінними.

Формантний метод за версією Бикова Ю.С. відрізняється від методики Покровського двома моментами:

- спектр формант λ визначається як спектр такого шуму, який, будучи підсумованим з мовним сигналом, призведе до повної втрати розбірливості мови;
- враховується залежність коефіцієнта сприйняття від частоти.

Принципова особливість версії Сапожкова М.А. – це фактичне ототожнення спектра формант зі спектром мови: «...потужність формант в діапазоні вище 300 Гц по відношенню до потужності мови в цьому ж діапазоні складає 98%...» .

Версія формантного методу, відома як індекс артикуляції (AI). В рамках даної версії вважається, що розбірливість мови пропорційна середній різниці між піковим рівнем мови і ефективним рівнем маскувального шуму.

При використанні методу STI можливість одночасного врахування шумової та реверберaційної завад забезпечується спеціальним вибором тестового сигналу у вигляді шуму зі спектром, ідентичним спектру довготривалої мови. Цей шум в кожній октавній смузі частот модулюється періодичним сигналом таким чином, щоб огинаюча миттєвої потужності сигналу мала форму синусоїди.

Метод RASTI є скороченою версією методу STI. Як і метод STI, метод RASTI дозволяє врахувати реверберaційну заваду. Випробувальний сигнал спрощений: кількість октавних смуг скорочено до двох, з центральними частотами 500 Гц та 2 кГц. При такому підході смуга пропускання обмежена і, отже, фоновий шум з нерегулярним спектром і нелінійні спотворення не враховуються коректно. Проте, метод RASTI може використовуватися для приблизної діагностики приміщень.

Метод STIPA - модифікація методу STI для систем звукопідсилення (public address systems), яка дозволяє враховувати не тільки реверберацію, а й нелінійні спотворення звуку в приміщеннях. Випробувальний сигнал спрощений в тому сенсі, що в кожній з семи октавних смуг використовують тільки дві частоти модуляції, стосовно іншого – метод STIPA ідентичний методу STI.

У методі STITEL застосовується тільки одна частота модуляції в кожній з семи 1/1 октавних смуг. Несучий шум для кожної 1/1 октавної смуги має ширину спектра 1/2 октави, щоб уникнути впливу на суміжні смуги. Метод STITEL не дозволяє враховувати реверберaційну заваду і нелінійні спотворення.

Серед емпіричних методів найбільш популярний метод Alcons – метод

вимірювання величини втрати артикуляції приголосних вираженою у відсотках. Метод Alcons широко використовується, особливо в США, для наближеної оцінки розбірливості мови і відображає втрату вокалізованих приголосних, викликану реверберацією і поглинанням звуку в приміщенні.

Використані джерела

1. Покровский Н.Б. Расчет и измерение разборчивости речи. – М.: Связьиздат, 1962. – 390 с.
2. Железняк В.К., Макаров Ю.К., Хорев А.А. Некоторые методические подходы к оценке эффективности защиты речевой информации // Специальная техника. – М.: 2000, № 4.
3. К оценке эффективности защиты акустической (речевой) информации. [Електронний ресурс]: - Режим доступу: http://st.ess.ru/publications/articles/tspi/tspi.htm.

Дворецький О.О. - інспектор ВПДО УІАП в Дніпропетровській області;
Калюга Р.І. - інспектор СІП Новомосковського ВП ГУНП в Дніпропетровській області;
Паштета О.М. - старший інспектор СІП Новомосковського ВП ГУНП в Дніпропетровській області;
Рижков Е. В. - завідувач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету, кандидат юридичних наук, доцент

ОПТИМІЗАЦІЯ ДЕЯКИХ ПІДСИСТЕМ ІІПС ОВС ТА ІТС НПУ ТА ІНШІ ПИТАННЯ В ДІЯЛЬНОСТІ ПРАЦІВНИКІВ ІАП ГУНП

В процесі реформування діяльності органів Національної поліції Департаментом інформаційно-аналітичної підтримки поступово реалізується запровадження нової концепції діяльності структурних підрозділів. Централізація та оптимізація доступу до баз даних, питання безпеки - є пріоритетними. Саме тому, проблемні питання діяльності інформаційно-аналітичних підрозділів, які існують на сьогодні, повинні бути враховані при вдосконаленні цього виду діяльності в Національній поліції.

Традиційно, працівник ІАП працює з кількома службовими базами, які різняться процедурами ідентифікації. Тому не було б зайвим створення комплексу програмного забезпечення типу автоматизованого робочого місця з єдиним протоколом ідентифікації що б об’єднував та здійснював одночасний вхід до систем. Це б також позитивно позначилось на можливому подальшому електронному документообігу з УІАП в областях та їх структурними підрозділами (зокрема за допомогою включених засобів обміну інформацією).

Актуальним є також питання матеріально-технічного та програмного забезпечення підрозділів ІАП. Однією з проблем роботи є незадовільне забезпечення комп’ютерним обладнанням, багатьом комп’ютерам у

відділеннях по 10-15 років, що унеможливлює встановити на них відповідні програми, тому як операційна система не відповідає вимогам оновлених програм.

Наступною проблемою є незадовільний доступ до всесвітньої мережі «Інтернет», це виявляється у низькій швидкості, обмеженому доступі ,що в свою чергу не надає можливості коректно та швидко переглядати та вводити інформацію в системах ІІПС «Армор» та ІТС «Цунамі».

Критичною також залишається ситуація зі штатною чисельність ІАП. СІП за штатним розписом передбачені лише у відділах поліції, які включають в себе 4-5 відділень. Разом з тим у відділеннях поліції здебільшого є можливість закріплення лише по одному працівнику СІП, а це в свою чергу унеможливлює якісну роботу по всім напрямкам службової діяльності, зокрема під час перебування даного працівника у відпустці, відрядженні тощо.

Практичний досвід роботи з ІІПС ОВС «Армор» (далі ІІПС), ІТС НПУ «Цунамі» (далі ІТС НПУ) дозволив виявити низку проблемних питань, які потребують свого потенційного вирішення. Тому автори висловлюють ряд порад, побажань, спрямованих на оптимізацію роботи їх підсистем.

Інформаційна підсистема «Єдиний облік» ІТС НПУ. Одна з найголовніших підсистем ІТС НПУ. Суть її роботи полягає у реєстрації заяви (повідомлення), введення інформації щодо суті події, місця, дати, часу, заявника чи потерпілого, кваліфікації тощо. На інформацію, введену до ІП «ЄО» спирається безліч інших підсистем, тому від своєчасного, повного та об'єктивного внесення даних до електронних контурів – запорука розкриття злочину. Так, ІП «ЄО» містить вкладку «Речі», для заповнення в т.ч. на випадок крадіжки, добровільної здачі, знахідки тощо речей, які можна ідентифікувати за зовнішніми ознаками (як правило номером). Разом з тим ІТС НПУ містить ряд окремих підсистем, для роботи з окремими їхніми групами (ІП «Номерна річ», «ТЗ, що розшукується», «Кримінальна зброя», «Добровільно здана, знайдена зброя» і т.д.). Їх функціонування мотивується також і необхідністю співпраці з іншими, в т.ч. зовнішніми базами та системами (наприклад, ІП «ТЗ, що розшукуються»). Джерелом для заповнення підсистем є, як правило, інформація, внесена до вкладки «Речі» ІТС НПУ. Тобто, на сьогоднішній день ми маємо проблему дублювання інформації у вкладці «Речі» ІП «ЄО» та у відповідній підсистемі (введення чи корегування однієї і тієї ж інформації до двох підсистем), що призводить до виникнення розбіжностей та, найголовніше, втрачається дорогоцінний час, знижується оперативність розкриття злочинів. Як приклад: інспектор-черговий ОНП реєструє крадіжку мобільного телефону та вносить інформацію щодо нього до вкладки «Речі» ІП «ЄО». Відповідальним за введенням інформації до ІП «Номерна річ» начальником ОНП визначено оперуповноваженого СКП (по аналогії з Інструкцією ІІПС ОВС). У випадку подібної організації роботи в ОНП втрачається час для розкриття злочину, знижується оперативність, нераціонально використовуються ресурси (в т.ч. шляхом визначення окремого працівника, надання чи корегування йому

відповідного доступу тощо). На теперішній час більш-менш нормативно врегульоване питання роботи з ІП «Транспортні засоби, що розшукується», так як в методичних рекомендаціях 2018 року обов'язок введення до неї інформації та підтримання її в актуальному стані належить до компетенції інспектора-чергового органу поліції.

ШЛЯХИ ВИРІШЕННЯ. 1. Програмний – внесення змін до ІТС НПУ при яких у випадках коли об'єктом злочину виступає предмет щодо якого передбачена окрема підсистема – дані з вкладки «Речі» ІП «ЄО» автоматично експортувалися до відповідної підсистеми. Також необхідно передбачити можливість перевірки актуальності даних та автоматичного оновлення стану (наприклад, знаття з обліку в обох підсистемах одночасно). У даному випадку відсутня також необхідність надання (корегування) доступу до цих підсистем наприклад, працівникам чергової служби ОНП. В разі ж виникнення необхідності введення інформації про певний об'єкт джерелом якого виступає не реєстрація у ІП «ЄО» - дані вносяться до підсистеми окремо працівником СІП. 2. Нормативний – на рівні ДІАП (УІАП) розпорядчим документом визначити окремі служби, працівники яких будуть відповідальними за формування певних підсистем (по аналогії з ІІПС).

Пропонуємо також надати старшому інспектору–черговому територіального підрозділу поліції більше можливостей по корегуванню карток, які надходять по даній лінії, в т.ч. їх об'єднання. Наприклад, може одна людина по одному і тому ж факту дзвонити на лінію «102» по декілька раз в окремих випадках - до 10-ти) і весь час приходять нові картки, що в свою чергу призводить до збільшення кількості реєстрацій. Також, на нашу думку, було б доцільним не реєстрація або одночасне списання до справи повідомлень, які не містять ознак кримінального чи адміністративного правопорушення та виключають випадки необхідності надання поліцейських послуг без направлення картки «102» до територіального підрозділу (наприклад, щодо надання контактних телефонів працівників, служб, «інформація незрозумілого змісту», коли заявник «верзе нісенітницю» та ін). Це в свою чергу сприятиме зменшенню кількості реєстрацій та виключення випадків висміювання фабул подій в т.ч. в мережі Інтернет.

Вкладка «Рішення» ІП «ЄО» унеможливлює складання висновку про списання матеріалів «до справи» деякими працівниками в т.ч. працівниками ДС, заступником начальника тощо. Хоча ці працівники досить часто складають подібні висновки, наприклад, при добровільній здачі зброї чи після проведення перевірки по факту несвоєчасного прибуття ГРПП чи СОГ.

ШЛЯХИ ВИРІШЕННЯ. 1. Внесення змін до програмного коду ІТС НПУ. У випадку проставлення у ІП «ЄО» рішення «внесено до ЄРДР» доцільно б було експортувати наявну інформацію до ІП «Кримінальна статистика» (далі ІП «КС»), а саме: орган, місце скоєння, кваліфікація, заявник і т.д. Внесення ж іншої інформації – проводилась би працівником СІП після отримання від слідчого картки Ф. 1. Разом з тим актуальним залишається питання кваліфікації злочинів, а саме відповідність інформації в ІП «ЄО», ІП «КС» та ЄРДР. Саме тому необхідно передбачити автоматичну

зміну кваліфікації після корегування відповідного поля в одній з систем. Це б у свою чергу підтримувало статистичні дані в актуальному стані та значно зменшило б час на внесення інформації до електронних контурів.

Значно б полегшало роботу працівників ІАП і інтегрування ЄРДР до ІП «КС», чи хоча б можливість доступу до ЄРДР через відомчу мережу НПУ.

Інформаційна підсистема «Особа» ІТС НПУ. На сьогоднішній день маємо проблемну ситуацію в вигляді наявності в даній підсистемі електронних карток фактично однієї і тієї ж особи проте з незначними розбіжностями (наприклад, у вигляді місця народження – населеного пункту чи району, дати тощо), які розпізнаються підсистемою як різні. Це пов'язано зокрема із значною кількістю структурних підсистем, багатьма користувачами з можливістю введення відповідної інформації. Як приклад, інспектор-черговий (помічник чергового) отримавши повідомлення вносить до ІП «ЄО» першочергові дані щодо особи заявника з його слів, крім того нерідко трапляються випадки відсутності чи неповідомлення такої інформації. Цей факт негативно впливає зокрема на час обробки інформації, адже необхідно переглянути інформацію всіх карток, часто виникають помилки кваліфікації адміністративних правопорушень, як наслідок повернення судом матеріалів адміністративних правопорушень на доопрацювання, закриття адміністративних правопорушень, уникнення потенційного правопорушника від відповідальності.

ШЛЯХИ ВИРІШЕННЯ. 1. Надання окремій особі територіального підрозділу поліції (наприклад, працівникові ІАП) право на об'єднання карток осіб за наявності обґрунтованих підстав (наприклад, при внесення даних до ІП «Адмінпрактика» маються дані про документ, що посвідчує особу).

У зв'язку зі службовою діяльністю досить часто виникає необхідність прикріплення фото особи до її електронної картки ІП «Особа». Проте програмно це можливо лише, наприклад, у випадах перебування особи на відповідних профілактичних обліках, доставляння чи затримання особи тощо та при наявності чітко визначених законодавчих підстав, які не відповідають потребам служби. Адже існує категорія громадян, які представляють чи можуть представляти оперативний чи службовий інтерес (особи ромської національності, без постійного місця проживання, особи, які часто залишають місце постійного проживання чи навчання (підпадають під категорію безвісно зниклих), психічно хворі, правопорушники тощо). Наявність фотокартки осіб даних категорій значно полегшив би процес ідентифікації, позитивно сприяв би оперативності здійснення розшукових заходів тощо.

ШЛЯХИ ВИРІШЕННЯ. 1. Законодавчий – на нормативному рівні розширення кола підстав для здійснення фотографування особи. 2. Програмний – поповнення інших підсистем ІТС НПУ можливістю прикріплення фотокартки особи.

Інформаційна підсистема «Адмінпрактика». Дана інформаційна підсистема ІТС НПУ призначена для введення інформації щодо складених поліцейськими протоколів про адміністративні правопорушення, накладення

та виконання стягнень. Згідно КУпАП підставою для визначення повторності є «вчинені повторно протягом року після застосування заходів адміністративного стягнення» як і ст. 39 КУпАП: «якщо особа, піддана адміністративному стягненню, протягом року з дня закінчення виконання стягнення не вчинила нового адміністративного правопорушення, то ця особа вважається такою, що не була піддана адміністративному стягненню». Ключовим моментом у цій ситуації виступає необхідність висвітлення у відомчих підсистемах (ІП «Адмінпрактика») виду накладення адміністративного стягнення та, що найголовніше, відмітку його виконання та дату виконання. Проте КУпАП передбачено кілька суб'єктів розгляду та прийняття рішення за адміністративними матеріалами, проте КУпАП не містить жодних законодавчо визначених підстав надання цими суб'єктами інформації до поліції для її внесення до підсистеми. Надсилання відповідних запитів з метою отримання такої інформації як правило займає досить багато часу чи взагалі безрезультатно. Як наслідок – неправильна кваліфікація дій правопорушника з подальшим поверненням матеріалів чи закриття провадження та уникнення особи від відповідальності.

ШЛЯХИ ВИРІШЕННЯ. 1. Законодавчий – визначення у нормативній базі (наприклад, КУПАП) обов'язку суб'єкта прийняття рішення повідомити про це до орган, посадова особа якого склала протокол протягом певного строку (наприклад, 1 робочого дня). 2. Програмний – на сьогоднішній день маємо Інтернет-ресурс судових рішень, в т.ч. за адміністративними матеріалами. Саме тому було б доцільно інтегрувати автоматичний експорт цих рішень до відомчих підсистем та, зокрема, до вкладки про прийняте рішення кожної електронної картки протоколу. 3. Глобальний – створення єдиної об'єднаної системи на базі Інтернет-ресурсів, що об'єднувала б інформацію з усіх суб'єктів розгляду адміністративних матеріалів, ДВС, секторів пробації Міністерства дстиції з подальшим інтегруванням її до ІП ІТС НПУ (для ідентифікації можливе використання ЕЦП, так як його отримують більшість посадовий осіб даних установ і які являються суб'єктами декларування). Крім того у ІП «Адмінпрактика» передбачена можливість автоматичного експорту інформації щодо сплати штрафу правопорушниками проте лише по лінії безпеки дорожнього руху. Цей факт потребує оптимізації в вигляді застосування подібного експорту і до інших адміністративних протоколів. Це в свою чергу значно зменшить паперовий документообіг, забезпечить отримання інформації про сплату без повторного візиту до органу поліції та надання підтверджуючих документів (квитанції, чеку тощо).

На прикладі зазначених проблемних питань маємо ситуацію, яка потребує свого вирішення як мінімум адміністративно-нормативним шляхом, особливо в умовах, коли керівництвом Департаменту інформаційно-аналітичної підтримки та керівництвом Національної поліції у найближчий час буде реалізовуватися стратегія On-line інформаційно-аналітичного супроводу діяльності органів Національної поліції, в т.ч. оперативних підрозділів, слідства, патрульної поліції тощо, що, у сою чергу, є безумовно

перспективним форматом діяльності сучасного правоохоронного органу держави.

Демидов З.Г. - науковий співробітник;
Ницюк С.П. - старший науковий співробітник (Науково-дослідна лабораторія захисту інформації та кібербезпеки Харківського національного університету внутрішніх справ)

КОМП'ЮТЕРНІ ВІРУСИ, ЯК ЗАСІБ ЗАРОБІТКУ

Найскладніше в специфіці хакеру не зламати чийсь комп'ютер або сервер, а залишитися непоміченим або анонімним при цьому. На призначених для користувача (домашніх) машинах, немає нормального захисту від вірусів. Ні військових суперпотужних серверів з хардварними фаєрволами, як в Пентагоні, які, до речі, теж зламуються хакерами. Ні відділу безпеки або навіть системного адміністратора, який хоч щось може протиставити злому. Від провайдера ми максимум отримуємо ізоляційну стрічку на кабелі))), основна наша надія на антивіруси з того ж інтернету, звідки до нас приходять віруси. Багато хто вважає, що віруси в їх комп'ютерах тільки гальмують систему і витрачають нерви користувача. Насправді хтось заробляє на них величезні гроші без вашого відома. Все, що відбувається в цьому світі, кому-то вигідно. З вірусами та ж історія [1].

Є 5 основних методів заробітку на вірусах:

1) Шантаж

Найпростіший метод, в нього потрапляють віруси-шифратори і "вінлокери". Суть проста - вірус при попаданні на комп'ютер шифрує всі дані на ньому або повністю блокує роботу комп'ютера. Для відновлення роботи зловмисник вимагає гроші за антивірус або програму-дешифратор. Звичайно ж, після отримання "викупу" ніхто нічого не надсилає і не розблокує. Вирішити проблему в принципі можна в сервісному центрі, або якщо є знайомий сисадмін. А в разі вірусу-шифратора можна сподіватися тільки на те, що дешифратор вже написаний. В іншому випадку доведеться відформатувати жорсткий диск і позбутися всієї інформації, яка там була ...

2) Прямий злом

Тут мова йде про крадіжку особистих даних. Користувач може і не здогадуватися, що зламаний, поки не спливе факт використання його особистих даних деінде. Вірус потрапляє на комп'ютер і знімає всю особисту інформацію користувача, висилаючи її на сервер зловмисника. Це інформація про паролі, логіни, номери банківських карток, рахунків і т.п. Зазвичай це робиться вірусом класу "кейлоггер".

3) Прихований злом

Тут зовсім інша система ... Користувач взагалі не повинен здогадатися

про те, що його комп'ютер заражений. Існує кілька подальших шляхів розвитку. В інтернеті можна знайти замовлення на DDos-атаки якихось серверів або розповсюдження реклами "нового крему для п'ят" величезної кількості користувачів. В цьому випадку потрібно велику кількість машин, з яких відбуватимуться запити або розсилки. Тому хакер створює собі базу, з якої він надалі буде розсилати спам, або бомбити запитами який-небудь сервер, щоб той ліг. Або ж він може майнити на ваших потужностях - завантажувати повністю ваш процесор і заробляти таким чином гроші. Існує два основних типи майнінгу з використанням чужих комп'ютерів, якими користуються хакери:

1. Браузерний майнінг.

Вам достатньо перейти за посиланням на ресурс, в скрипті якого прописаний потрібний код, і, поки ви будете перебувати на сайті, ваш комп'ютер стане частиною мережі з генерування криптовалюти.

2. Віруси-майнеи.

Підчепити цей вірус можна, перейшовши за посиланням з листа або встановивши сумнівну програму [2]. У зону ризику потрапляють всі комп'ютери з сильними технічними характеристиками. Віруси завдають більшої шкоди комп'ютерам, ніж браузерні майнінги, тому що більш активно використовують потужності комп'ютера. Це дуже популярна останнім часом тема.

4) Антивірус на продаж

Якщо в мережі з'являються віруси, то хтось їх створює. Значить розуміє питання зсередини, отже може створити антивірус ... Ось вам і схема - написав вірус і антивірус. Заразив - продав антивірус))) Звичайно, цей теорія, ніхто нічого не доводив і за руку лабораторії, типу Касперського, ніхто не хапав. Але думка прямо-таки витає в повітрі))

5) Білий злом.

Хакери зламують сервера великих компаній, щоб показати уразливості. Сама компанія зазвичай призначає ціну і конкурс для хакерів, щоб ті навмисно атакували їх і надсилали потім звіти вразливостей. Хакери заробляють гроші, не порушуючи закони, а компанії отримують інформацію про свої прогалини і покращують систему безпеки.

Використані джерела

1. Расследование: Как хакеры зарабатывают на компьютерных вирусах [Електрон. ресурс] / Режим доступу: https://www.youtube.com/watch?v=CLLPWY1SvNI

2. Чёрный майнинг: как зарабатывают деньги через чужие компьютеры [Електрон. ресурс] / Режим доступу: https://lifehacker.ru/chernyj-majning/

Дисковський О.А. – професор кафедри економічної та інформаційної безпеки, доктор технічних наук, доцент;
Косиченко О.О. – доцент кафедри економічної та інформаційної безпеки, кандидат технічних наук, доцент (Дніпропетровський державний університет внутрішніх справ)

ВИКОРИСТАННЯ МЕТОДІВ ВІЗУАЛІЗАЦІЇ В ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ

Візуалізація процесу мислення застосовується людьми не одну сотню (а може бути й тисячу) років. Як ще писав Леонардо да Вінчі "З початку всіх часів повітря наповнене незліченними зображеннями, яки для очей є магнітом". Більша частина проблем століття, що настало, буде вирішуватися на рівні розвитку здатностей людей створювати, накопичувати та використовувати знання. Роль аналітичної складової в обробці інформації буде неухильно зростати. Існуючі зараз проблеми в правоохоронній діяльності і юриспруденції існують через невміння та небажання аналізувати наявну інформацію. Існує багато аналітичних технологій, найбільш важливими є структурування, класифікація та систематизація.

Однієї із сучасних аналітичних технологій є використання так званих інтелект-карт [1–4]. Інтелект-карта (mind map, відома також як майнд-карта, карта думок і ментальна карта) – це аналітичний інструмент, який використовують, якщо необхідно знайти максимально ефективне рішення проблеми. Застосовувати інтелект-карти можна із самими різними цілями: щоб генерувати ідеї, готуватися до презентацій, організовувати й проводити різні заходи, конспектувати лекції, запам'ятовувати більші обсяги інформації, планувати робочий день, контролювати хід роботи над проектом або планувати вільний час і багато чого іншого. В основі ідеї інтелект-карт лежить принцип «радіантного мислення» (від "радіанта" – точка небесної сфери, з якої ніби виходять видимі шляхи тіл з однаково направленими швидкостями, наприклад, метеоритів одного потоку) [1, 2].

Головна перевага ментальних карт – це можливість охопити картину в цілому. Будучи, по суті, одним зі способів когнітивної візуалізації, ментальні карти мають ряд особливостей. Зокрема, істотну відмінність ментальних карт від різного роду логіко-структурних схем полягає у вільній візуалізації розумового процесу. Описуючи технологію майндмепінгу (англ. mindmapping – застосування ментальних карт), Т. Бьюзен радить використовувати не лінійну, а радіальну структуру, віддаючи перевагу не логіко-ієрархічним, а асоціативним зв'язкам.

Узагальнюючи специфіку ментальних карт, можна виділити їхні

особливості. Ментальні карти – це спосіб вільної візуалізації думок. Результат може бути як схожим на звичайні логічні схеми, так і являти собою досить мудрі барвисті малюнки – кому як зручніше. При створенні ментальних карт рекомендується не використовувати готові традиційні форми таблиць і схем, оскільки вони провокують підганяти по них розумовий процес, тим самим обмежуючи його, заганяючи нашу думку в початкові задані стандартні рамки. Зображувані зв'язки можуть бути не тільки логічними, але й асоціативними, а записи – не тільки термінологічними, але і образними, приблизними.

В Інтернеті багато матеріалів про ментальні карти і переважна більшість публікацій присвячена застосуванню ментальних карт в економіці, у менеджменті, у бізнесі, у винахідництві, у навчанні. На жаль використання інтелект-карт практично не зустрічається серед вітчизняних юристів. У мережі Інтернет можна знайти тільки окремі приклади [5]. Практично не використовуються інтелект-карти при викладанні правових дисциплін у юридичні та правоохоронних ВНЗ України. Але, як ні сумно, у середніх навчальних закладах використання інтелект-карт для викладання різних дисциплін значно випереджає використання у вищій школі, навіть випускаються методичні посібники для вчителів, наприклад [6]. В англомовних країнах використанню інтелект-карт приділяється величезна увага, наприклад [7].

Використання технології інтелект-карт може бути дуже ефективно використано при візуалізації процесу розслідування злочинів, для виявлення й аналізу зв'язків між фігурантами злочинних угруповань і т.п.

Існує два основні способи створення інтелект-карт: перший спосіб - створення вручну (лист паперу та набор фломастерів) з використанням технології, яка вже добре відпрацьована [1-5] і другий спосіб – використання спеціально розроблених програм (в основному для операційних систем Windows, ios і Android). При комп'ютерному створенні інтелект-карт існує кілька варіантів: програми для локального використання й програми в мережі Інтернет у режимі он-лайн. В останньому варіанті дуже перспективним є реалізація спільного створення групою фахівців інтелект-карт для інформаційного супроводу оперативної діяльності з використанням хмарних технологій, що може бути використано в правоохоронній діяльності, у судовій діяльності, в експертній роботі і т.п. [8]

Слід також зазначити, що інтелект-карти є не єдиним засобом візуалізації в аналітиці, існує ще багато різних методів, наприклад, причинно-наслідкові діаграми Ісікави [9] які використовуються фахівцями в різних галузях (економісти, психологи і т.п.) для з'ясування причин виникнення яких-небудь проблем (наприклад, з'ясування мотивації злочинця й т.п.)

Використані джерела

1. Бьюзен Т. и Бьюзен Б. Супермышление / Пер. с англ. Е. А. Самсонов; Худ. обл. М. В. Драко.— 2-е изд.— Мн.: ООО «Попурри», 2003.— 304 с. (Серия «Живите с умом»).

2. Тони Бьюзен. Интеллект-карты. Полное руководство по мощному инструменту мышления = Mind Map Mastery. — М.: Манн, Иванов и Фербер, 2018. — 208 с.

3. Бехтерев С. Майнд-менеджмент: Решение бизнес-задач с помощью интеллект-карт /Сергей Бехтерев; Под ред. Г. Архангельского. – М.: Альпина Паблишерз, 2009. – 3-8 с.
4. Мюллер Х. Составление ментальных карт. Метод генерации и структурирования идей [Текст]. – М. : Омега-Л, 2007. – 126 с.
5. Креативная юриспруденция. Блог Абакшина Алексея об эффективной правовой работе – [Електрон. ресурс] / Режим доступу: http://blog.abakshin.com/archives/2202
6. Найдьонова А.В. Посібник по складанню інтелект-карт для педагогів та учнів. ДНЗ "Дніпропетровський центр професійно-технічної освіти туристичного сервісу". [Електрон. ресурс] / Режим доступу: https://en.calameo.com/read/004373434dec4e2bf2b83
7. Mapping Law School - [Електрон. ресурс] / Режим доступу: https://lawmindmaps.com/
8. Холопов А.В. Использование научно-технических средств для обеспечения наглядности представляемой информации в государственном обвинении. – КриминалистЪ, 2013, №1(12), с.60-66 - [Електрон. ресурс] / Режим доступу: http://www.procuror.spb.ru/k1213.html
9. Центр креативних технологий - [Електрон. ресурс] / Режим доступу: https://www.inventech.ru/pub/methods/metod-0019/

Ісмайлов К.Ю. - кандидат юридичних наук,
завідувач кафедри кібербезпеки та інформаційного забезпечення;
Бедрій Т.А. курсант факультету №2
(Одеський державний університет внутрішніх справ

ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН У ЗЛОЧИННІЙ ДІЯЛЬНОСТІ

Сьогодні фінансові системи країн, як й інші сторони економіки, удосконалюються і прогресують у контексті розвитку глобалізації, поширення ІТ-технологій та загальної інформатизації. Це сприяє появі нових фінансових інститутів, інструментів та форм взаємодії між людьми і зрозуміло, що злочинна діяльність також змінюється в зазначеному напрямку, тому співробітниками правоохоронних органів необхідно адаптувати свою тактику та методи боротьби зі злочинністю.

Перед тим як розглянути питання застосування злочинними елементами технології блокчейн у своїй протиправній діяльності необхідно з'ясувати перш за все, що саме таке блокчейн та чому він так швидко поширюється в кримінальному середовищі. По-перше технологія «блокчейн» або «розподіленого реєстру» (DLT) вводить принципово іншу структуру децентралізованих платіжних систем, з криптографічними методами шифрування інформації. В основі криптовалют лежить технологія блокчейн – це ланцюжок блоків транзакцій (англ. Blockchain, Block chain від block - блок, chain - ланцюг) – розподілена база даних, яка підтримує перелік записів, так званих блоків, що постійно зростає [1]. По-друге технологія блокчейн являє собою платформою віртуальної платіжної системи біткоін. Тобто збудована база захищена до будь-якої підробки та переробки. Кожен блок містить часову мітку та посилання на попередній

блок хеш дерева [2].

Згідно з результатами дослідження, в 2017 році 15% фінансових установ використовували блокчейн в практичній діяльності. Саме ці банки є новаторами, які вважають, що технологія допоможе їм створити нові бізнесмоделі і запуститися на нових ринках [3].

Унікальність методу блокчейн у:

1. **Децентралізації системи.** Інформація про блоки зберігається на всіх вузлах в мережі. Це видаляє необхідність наявності єдиного централізованого управління транзакціями. Інформацію про транзакції може перевірити будь-хто: жодної комерційної таємниці, всі операції видно всім, перевірка відправлення коштів не становить проблем.

2. Анонімність транзакції. *Справжність транзакції і її виконання можна побачити завжди, а самого відправника ні. Можна бачити лише адресу з якого виробляється транзакція або адресу кому вона призначена.*

3. Неможливість підробки блоку. *За рахунок самого принципу роботи мережі це неймовірно складно зробити. Для того щоб блок вважався справжнім з ним повинні погодитися 51% всіх існуючих вузлів.*

4. Виключається подвійна витрата коштів. *При відправленні коштів відразу можна побачити, що вони відіслані, але ці кошти не будуть зараховані на рахунок до тих пір, поки транзакція не потрапить в блок і не буде підтверджена. Приблизно в цей час зловмисник може ще раз відправити ці ж кошти до іншої людині, але Блокчейн не дозволить цього зробити. В нього присутні такий запобіжник, як мітки часу і транзакція, яка була відправлена раніше потрапить до блоку, а всі наступні, маючи інформацію про те, що гроші вже витрачені будуть відкинуті мережею.*

Тобто всі транзакції відбуваються напряму між користувачами. Ніякого головного сервера, який можна підключити, немає, а є лише мережа блокчейн, що складається з окремих суб'єктів. А спроби встановити анкетні данні власника криптогаманця через мережу досі не існує, тому інкогніто користувачів забезпечено, тобто всі ці параметри технічно дуже ускладнюють виявлення злочину не тільки правоохоронними органами України, а всього світу.

Слід відмітити, що вивчення технології блокчейн на науковому рівні проводиться в основному в технічному напрямку, а щодо впливу її на виникнення нових способів злочинної діяльності, або ще більш удосконалення існуючої злочинної діяльності не представлено ширико в юриспруденції. Вивчення блокчейна з боку фахівців у кримінології, кримінальному праві, кримінального процесу, криміналістики, економічної безпеки практично не проводиться. Щодо законодавства України, то досі невизначений статус криптовалюти, як і основні поняття, що пов’язані з нею (блокчейн, токен, криптавалюта, майнінг та інші).

6 жовтня 2017 року Верховна Рада зареєструвала законопроект №7183 «Про обіг криптовалют в Україні». Цей документ вперше визначає поняття криптовалюти, майнерів, і наділяє НБУ статусом органу, який буде здійснювати управління в сфері обігу віртуальних валют. Крім того, проект

закону встановлює для майнерів вимоги платити податки і позбавляє 25 криптовалют ключової переваги для інвесторів – анонімності [4].

Повинні пам'ятати за існування терористичної загрози в Україні використання криптовалют надає додаткові можливості криміналітету та нашим ворогам. Згідно звіту міжурядової організації FATF, яка займається розробкою світових стандартів у сфері протидії відмивання злочинних коштів та фінансуванню тероризму, відсутність правових регуляторів впливу на біткоін дозволяє використання їх у злочинних цілях, зокрема спрямовувати на купівлю зброї.

Експерти Центру соціально-економічних досліджень «CASE Україна» підтвердили, що криптовалюта можна розглядатись як один із способів приховування доходів і ухилення від податків. Так один з розробників клієнта мережі Bitcoin Гевін Андріс висловив занепокоєння тим, що деякі криптовалюти можуть бути шахрайськими [5].

За інформацією НБУ, СБУ та НПУ, відсутність контролю за обігом криптовалют та анонімність розрахунків створює потенційні передумови для їхнього використання з метою легалізації коштів, отриманих злочинним шляхом, оплати заборонених до вільного обігу товарів (наркотиків, зброї), дають можливість фінансування тероризму, зокрема на окупованих територіях України.

Таким чином, технологія блокчейн широко використовується в злочинній діяльності, а саме:

1. **В якості грошових коштів** при купівлі зброї, наркотичних засобів, порнографії та інших заборонених предметів, легалізація злочинних доходів, фінансування тероризму та ін.); створенні власної платіжної системи для злочинних цілей; у незаконній мережевій торгівлі отримана криптовалюта обмінюється на товарних біржах, потім перекладається на карти і знімається в банкоматі; використанні гаманця, на якій не знайомі один з одним люди переводять віртуальні гроші, потім та ж сума чужих BTC частинами повертається відправнику. Зв’язок між зловмисником і злочинними грошима таким чином розривається; фальшиві інтернет магазини імітують операційну діяльність

2. **Криптовалюта як предмет злочинного посягання**: розкрадання криптовалюти з рахунків, інтернет-шахрайство, вимагання викупу у криптовалюті, шантаж у вигляді викупу у криптовалюті за розблокування державних сайтів, зараження шкідливим програмним забезпеченням ransomware (шифрує данні на усіх носіях в мережі та вимагає криптовалюту для відновлення доступу до даних;

3. Добича криптовалют шляхом зараження шкідливим програмним забезпеченням користувача, самовільне використання електроенергії на державних підприємствах.

Також дуже важлива проблема на сьогодні щодо ефективної протидії злочинності в сфері застосування блокчейна - це не включення в навчальні плани підготовки кадрів правоохоронних органів навчальних дисциплін, які включають питання пов’язані з використанням криптовалют, блокчейна,

юридичної практики та цифрової економіки.

Список використаних джерел:

1. Блокчейн [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Блокчейн
2. Blockchain. Investopedia. Процитовано 19 March 2016. «Based on the Bitcoin protocol, the blockchain database is shared by all nodes participating in a system.»
3. Blockchain Luxembourg S.A.R.L. [Електронний ресурс]. – Режим доступу:https://blockchain.info/charts/blockssize?timespan=all&showDataPoints=true
4. Розвиток банківського сектору завдяки новітнім технологіям в Україні [Електронний ресурс]. – Режим доступу: https://www.segodnya.ua/economics/finance/v-ukraine-zapustyat-elektronnuyugrivnyu-na-blokcheyne-1096367.html
5. Here's why Bitcoin is the future of money / Molly Wood // Cnet. — 2013. — 29 April.
6. Н. Хак Сіддікі, Р.О. Мовчан Криптовалюти та blockchain-технології у сучасній противоправній діяльності / Вісник студентського наукового товариства ДонНУ імені Василя Стуса. Том 1. – Вінниця: ДонНУ імені Василя Стуса, 2018. – С. 81-82.

Каблуков А.О. - доцент кафедри медичної та фармацевтичної інформатики і новітніх технологій, кандидат технічних наук, доцент; **Страхова О. П. -** викладач кафедри медичної та фармацевтичної інформатики і новітніх технологій (Запорізький державний медичний університет)

УДОСКОНАЛЕННЯ МЕТОДИКИ ПІДГОТОВКИ ФАХІВЦІВ В ВУЗАХ МВС

Сучасне суспільство, висуває нові вимоги до вищої освіти. Тому виникає необхідність у використанні нових більш ефективних форм, засобів і технологій навчання, які забезпечать підготовку фахівця МВС з рівнем знань, достатнім для його самостійної роботи після закінчення вузу. В той же час потрібні такі фахівці, які вміють вчитися, самостійно працювати з інформацією - тільки вони зможуть розраховувати на успіх в інформаційному суспільстві.

В теперішній час з’явились нові методики навчання, пов’язані з використанням інформаційних технологій. Однією з таких новітніх технологій навчання є дистанційне навчання (ДН). Дистанційне навчання визнано перспективним напрямком розвитку сучасної системи освіти, здатним вирішити цілий ряд актуальних проблем вищої освіти. ДН не заперечує існуючі освітні тенденції і технології, форми навчання; воно покликане інтегруватися в ці системи, доповнюючи і розвиваючи їх.

Ефективність дистанційної освіти залежить від ряду факторів, основними з яких є підготовка контенту дисципліни, а також професіоналізм викладача (т'ютор) супроводжуючого дисципліну. Викладач є ключовою

фігурою яка безпосередньо впливає на якість дистанційного навчання.

Система дистанційної освіти висуває особливі вимоги до рівня професійної підготовки і кваліфікації фахівців, задіяних в організації та проведенні різних курсів дистанційного навчання (ДН). Викладачі дистанційного навчання повинні не тільки добре розбиратися в предметі навчання, а й володіти необхідними навичками організації навчальної діяльності в умовах сучасної високотехнологічної оснащеності освітнього середовища. Основним завданням т'ютора є активізація процесу навчання. Т'ютор, як функціональна одиниця в навчальному процесі, надає учневі комплексний взаємозв'язок навчальних матеріалів з практикою їх застосування [1].

Головними проблемами при застосуванні дистанційних освітніх технологій викладачі називають недостатню інформаційну компетентність в технічних аспектах розробки дистанційного навчального курсу і значні витрати часу на розробку дистанційного навчального курсу. Таким чином, найбільшою складність для викладачів становить процес розробки дистанційного навчального курсу.

В зв’язку з вище викладеним проблема підготовка викладачів для системи дистанційного навчання є актуальною проблемою в системі вищої освіти. В Запорізькому державному медичному університеті дистанційне навчання на платформі EDX використовується для вивчення курсу за вибором на денній формі навчання.

Для підготовки викладачів-т'юторів, які супроводжують дистанційний курс навчання, в ЗДМУ використовувались лекції, підготовлені викладачами кафедри медичної і фармацевтичної інформатики та новітніх технологій. Також викладачами кафедри надаються консультації з технічних питань по створенню навчально-методичних матеріалів для дистанційного курсу.

Підготовка викладачів(т'юторів) для системи дистанційного навчання в вузах МВС України прогнозовано підвищить якість знань і професійну готовність фахівця до роботи за обраною професією.

Використані джерела

1. Основы деятельности тьютора в системе дистанционного образования: Программа специализированного учебного курса / Моисеева М. В., Троян Г. М. — М.: Изд. дом «Обучение-Сервис», 2006.

Клімушин П. С. - доцент кафедри інформаційних технологій, кандидат технічних наук, доцент;
Білобров А. В. – курсант (Харківськй національний університет внутрішніх справ)

БАЗОВІ ПРИНЦИПИ ТА ІНСТРУМЕНТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ Е-ІДЕНТИФІКАЦІЇ ГРОМАДЯН

Застосування інструментів е-ідентифікації громадян необхідно вести на основі таких базових принципів, сформованих на базі найкращих світових практик [1]:

– *адекватність вимог,* тобто використання методу ідентифікації має відповідати меті його застосування (чим менше значущість трансакції з погляду зміни прав громадянина або організації, тим простіші ідентифікатори слід застосовувати);

– *децентралізація та диверсифікація* – системи ідентифікації мають передбачати можливість застосування різних способів виконання операції та не повинні бути прив'язаними до єдиного рішення (наприклад, до універсальної е-картки) або до якоїсь централізованої бази ідентифікаторів;

– *індивідуальний вибір* – система ідентифікації повинна пропонувати користувачеві засоби вибору й контролю тих ідентифікаційних даних, які він надає для різних трансакцій, взаємодіючи з різними відомствами;

– *роз'яснення наслідків* – користувачів необхідно попереджати про те, які їхні ідентифікаційні дані і для чого буде використано в інформаційних системах е-уряду;

– *контроль розповсюдження* – доступ державних відомств до трансакцій в недержавних інформаційних системах (наприклад, платіжних), розроблених на основі загальних ідентифікаційних даних, можливий тільки за рішенням суду або в інших законодавчо встановлюваних випадках.

З урахуванням цих принципів і найкращих світових практик е-ідентифікації громадян повинні передбачати підтримку декількох незалежних варіантів ідентифікації з можливістю вибору користувачем найбільш зручного варіанта. Тобто єдина е-картка повинна розглядатися тільки як один із інструментів ідентифікації. Система ідентифікації повинна передбачати можливість поділу трансакції на кілька асинхронних сесій, у яких можуть використовуватись різні засоби ідентифікації.

Е-картка повинна бути захищеною від зміни носія інформації, на якому розміщено довірені облікові дані, спеціалізоване програмне забезпечення, прикладне програмне забезпечення (додатки), а також графічні (візуальні) дані, що розміщуються на поверхні картки.

Розширення сфери застосування картки до універсального посвідчення особистості стримується у світі двома факторами: недостатньою

поширеністю інфраструктури прийому таких карток; ризиками, що пов'язані з інформаційною безпекою і недостатньою надійністю захисту персональних даних.

Щоб зняти ці ризики, у світі використовують кілька способів. Одним із них є зберігання персональної інформації безпосередньо на картках без створення централізованих регістрів громадян. Державні установи надають послуги, щоразу дізнаючись персональних даних від самого громадянина, і не мають доступу до даних, контроль над якими міг би становити загрозу для свободи громадян. Персональні дані записуються на картку з використанням криптометодів, що забезпечують виключення несанкціонованого читання і збирання даних.

Зазначені вище ризики об’єднуються, якщо в одній картці поєднуються функції посвідчення особистості з функціями доступу до транзакцій. Така картка в разі її втрати відкриває для зловмисника можливості "крадіжки особистості", а також відкриває перед непідконтрольними користувачами можливості з втручання в життя громадян. У випадках, коли доступ до картки отримує особа, пов'язана з іноземними державами, такі картки можуть становити загрозу і для національної безпеки.

Держави – члени ЄС мають широкий спектр заходів політики щодо ідентифікаційних е-карток. Такі документи є обов'язковими у восьми державах – членах ЄС. При цьому вони використовуються як засоби е-ідентифікації для отримання онлайн-сервісів від держави [2]. На сьогодні загальний принцип необов'язковості отримання цифрового посвідчення особи є загальноприйнятим. Важливо відзначити, що всі країни, що реалізували проекти упровадження універсальних е-карток, які суміщують функції посвідчення особи і доступу до транзакцій, мають внутрішньополітичну стабільність, відносно невелике населення і є компактними в територіальному плані.

Більшість держав – членів ЄС використовують засоби е-ідентифікації, специфічні для бізнес-установ. Більшість із цих засобів є апаратними ключами, що містять кваліфікований сертифікат для е-підпису. Ці засоби е-ідентифікації можуть використовуватися не тільки для автентифікації, а й для підписання документів від імені компанії. Слід зауважити, що, хоча ці засоби е-ідентифікації можуть використовуватись виключно для представлення компанії, вони є номінативними, тобто містять ідентифікаційні дані представників.

Використані джерела

1. Клімушин П. С. Стратегії та механізми електронного урядування в інформаційному суспільстві: монографія. Харків. Вид-во ХарРІ НАДУ «Магістр», 2016. 524с.
2. Національна стратегія електронної ідентифікації України. Біла книга з електронного урядування / під редакцією О. Потія та Ю. Козлова. URL : http://dknii.gov.ua/sites/default/files/wb_eid_20_03_0.pdf.

Кокарєв І.В. - доцент кафедри економічної та інформаційної безпеки, кандидат економічних наук, доцент;
Повстін І.В. - курсант факультету економіко-правової безпеки (Дніпропетровський державний університет внутрішніх справ)

ПЕРСПЕКТИВИ РОЗВИТКУ РИНКУ КРИПТОВАЛЮТ

З неспинним розвитком сучасних технологій постійно змінюються певні сфери суспільного життя людей. Ці зміни не оминули і сферу економіки, а саме товарно-грошові відносини. Люба життєздатна валюта - будь це традиційна паперова валюта або ж створена комп'ютерною програмою криптовалюта – повинна завоювати довіру суспільства в якому вона знаходиться. Без цього не можна сподіватись на продуктивний ріст валютного курсу та на змогу валюти закріпитись на ринку. З появою криптовалют, з'являється нова модель завоювання суспільної довіри, що з часом може змінити всі консервативні тенденції щодо валюти, а також вплинути на всі сфери життя людини.

Всі користувачі криптовалют виділяють основні переваги нової електронної валюти – біткоїна. Біткоїн пропонує систему платежів, в котрій в отримувача більше немає потреби довіряти "третій стороні" (різним банківським установам або державі) перевірку платоспроможності відправника в межах обумовленої заздалегідь суми. Рішення цієї проблеми покладають на комп'ютерну програму, яку неможливо зруйнувати, яка має розгалужену систему та котра неспроможна обманювати людей. Однак це не позбавляє криптовалюту цілі завоювати довіру суспільства. Їй доведеться зробити це, задля того щоб отримати можливість виконувати свої функції в повному обсязі. Довіра- фундаментальна основа кожної валютної системи. Для того, щоб вона працювала, в людей повинна бути впевненість, що їй можуть довіряти і інші.

Суть біткоїна як технології полягає в тому, що він являє собою системний протокол - широко поширене поняття в програмуванні, що позначає базовий набір програмних інструкцій, який дозволяє комп'ютерам встановлювати між собою зв'язок. Протокол біткоїна працює в мережі комп'ютерів, що належать безлічі людей в різних куточках світу котрі підтримують його, блокчейн і систему грошових розрахунків.

Блокчейн – найголовніший регістр, виконуючий роль центральної нервової системи біткоїна. Цей регістр, а точніше інноваційна технологія (так званого Сатоши Накамото – невідомого творця цієї електронної валюти), яка зламала звичну логіку, і необхідність в посередниках відпадає. Це досягається завдяки особливій формі зберігання інформації об транзакціях зразу на всіх комп'ютерах системи – в розгалужених реєстрах або базах даних. Кожна транзакція відбувається в онлайні і являє собою лише

повідомлення про те, що якийсь користувач переводить іншому користувачеві певну кількість біткоїнів. Як тільки транзакція проведена, вона стає видно майнерам (так званим добувачам криптовалюти). Збереження історії операцій з біткоїном гарантує, що користувач не переведе комусь суму, якої у нього немає. Блокчейн-технологія дозволяє уникнути і подвійного витрачання - ситуації, коли людина двічі намагається витратити одну і ту ж суму. Запорукою цього є велика кількість користувачів і економічна мотивація майнерів.

Добування біткоїна давно перетворилося на повноцінний бізнес. Згідно з дослідженням Кембриджського університету, з моменту появи біткоїна майнери заробили понад $ 2 млрд. за рахунок обчислень і $ 14 млрд. - на комісіях з транзакцій. Виробники обладнання для майнінга відчули сильне зростання попиту. Раніше майнити біткоїни можна було на домашніх комп'ютерах, а до 2017 року цей процес здійснюється на «фермах»: у величезних ангарах, заповнених процесорами. Справа в тому, що створення кожного блоку - вкрай складний процес. Майнер в своїх обчисленнях повинен враховувати певні правила. Найпопулярніше пристрій для майнінга біткоїнів - ASIC-чіпи. Сьогодні їх масово виробляють в Китаї і США.

В 2013 році розвиток блокчейн-технологій вступив на новий рівень, інші молоді винахідники зрозуміли, що на платформі блокчейн можна створити нові валюти аналогічні біткоїну, так з'явились Ethereum (ефіріум), Litecoin (літкоїн), Ripple (ріпл), Neo (нео) і т.д.

Світова тенденція зростання популярності криптовалюта і її частковий успіх в плані визнання в якості економічної одиниці в ряді країн з сильною економікою може свідчити про те, що криптовалюта чекає велике майбутнє, і, можливо, через кілька десятиліть криптовалюта замінить всюдисущий долар і євро.

А поки що ситуація з криптовалютами залишається неоднозначною, і різні торгові операції з її участю містять високу частку ризику.

Хоча вже на сьогодні є кілька банків і платіжних систем, які дозволяють відкриття банківських рахунків під такі види діяльності, як наприклад ICO.

Однак же, варто зауважити, що щось нове, що приходить на зміну традиційному, - це завжди ризик, але ж саме в цих змінах і є суть еволюції, якої схильне все живе на нашій планеті, в тому числі і економіка. Для більшої інформації звертайтеся в нашу компанію. У той час як багато ЗМІ називають криптовалюту наступною «бульбашкою», ніхто з них не усвідомлює, що ця сама «бульбашка» може допомогти вирішити нагальні проблеми світової економіки.

Зрозуміло, що блокчейн має відмінний потенціал для консолідації і, можливо, навіть стандартизації фінансових ринків по всьому світу. Різні приватні підприємства и регулюючі органи вже почали інтегрувати технологію блокчейна в свої бізнес-моделі.

Щодо економічних злочинів, зростає кількість нових економічних махінацій пов'язаних з новою валютою – біткоїном. Злодії як завжди збагачують себе за допомогою крадіжок, розбою, обману та шантажу. Але в

цьому випадку в них з'являються більше можливостей для тіньових схем, завдяки повній анонімності та безпосередності операцій з біткоїном, вони можуть переводити звичайні гроші в біткоїни та фактично виводити їх в офшори.

Збільшуються ризики для чесних добувачів біткоїна, з'являються випадки грабежів націлених на крадіжку обладнання, яке видобуває біткоїни. Збільшення хакерських атак на біржи біткоїну, їх подальше банкрутсво, слідство – зменшення курсу біткоїну.

На даний момент в Україні не існує законодавчих нормативно-правових актів, які регламентують відношення до криптовалют, покарання за махінації з ними та інші установчі акти. Тому, необхідність про ведення таких нормативно-правових актів є більш як актуальна та оправдана, та підлягає якісній реалізації.

Використані джерела

1. Натаниел Поппер : "Цифрове золото - невимовна історія біткоїна".
2. Поль Винья, Майкл Кейси : "Епоха криптовалют. Як біткоїн та блокчейн міняють світовий економічний порядок" .
3. Андреас Антонополююс : "Інтернет грошей".
4. Дон Тепскотт, Алекс Тепскотт: "Еволюція блокчейна: як технології за Біткойн змінює гроші, бізнес і світ" .

Корнейко О.В. - завідувач кафедри інформаційних технологій та кібербезпеки кандидат технічних наук, професор;
Кудінов В.А. - професор кафедри інформаційних технологій та кібербезпеки, кандидат фізико-математичних наук, доцент (Національна академія внутрішніх справ)

УДОСКОНАЛЕННЯ ПІДГОТОВКИ В НАЦІОНАЛЬНІЙ АКАДЕМІЇ ВНУТРІШНІХ СПРАВ ФАХІВЦІВ ДЛЯ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ З ПИТАНЬ ЗАСТОСУВАННЯ НОВІТНІХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Сьогодні проблема впровадження новітніх інформаційних технологій та забезпечення протидії кіберзлочинності є вельми актуальною для Національної поліції України, а, отже, вимагає якісної підготовки фахівців-правоохоронців в закладах вищої освіти Міністерства внутрішніх справ (надалі – МВС) України.

Національна академія внутрішніх справ (надалі – академія) має практичний досвід підготовки таких фахівців. Протягом 2011-2014 років в ній було підготовлено понад 80 фахівців (4 навчальні групи) у сфері протидії

кіберзлочинності [1, 2]. Станом на сьогодні більшість з них працює за фахом.

Після незначної перерви, що пов'язана з деякими питаннями реформування вишу у відповідності до вимог сьогодення, за ініціативою ректора академії генерала поліції другого рангу В.Чернєя у 2017/2018 навчальному році була відновлена підготовка фахівців з поглибленим вивченням сучасних інформаційно-комунікаційних технологій, питань кібербезпеки та протидії кіберзлочинності. Так, зокрема, відповідно до рішення Вченої ради академії від 31 жовтня 2017 року (протокол № 26/1), за підтримки керівництва МВС України та Національної поліції в академії був впроваджений, у якості експерименту, тренінговий курс «Сучасні інформаційні технології» (306 годин / 8,5 кредитів ECTS) для спеціально відібраних 45 курсантів (2 навчальні групи) 4-го курсу вишу, які навчались за бакалаврською програмою спеціальності 6.030401 «Правознавство» [3-5].

Метою тренінгового курсу було розширення фахових компетентностей курсантів щодо застосування інформаційних технологій в діяльності органів та підрозділів Національної поліції України за рахунок отримання ними відповідних додаткових теоретичних знань та надбання необхідних практичних умінь і навичок в професійній діяльності майбутнього правоохоронця. Програма тренінгового курсу складалась з таких навчальних модулів: «Основи побудови та адміністрування комп'ютерних систем та мереж», «Сучасні інформаційні технології та сервіси», «Основи побудови телекомунікаційних систем та мереж», «Основи забезпечення кібербезпеки, захисту інформації та протидії кіберзлочинності», «Інформаційні технології в діяльності органів та підрозділів поліції».

З метою знаходження додаткового навчального часу для проходження цими курсантами зазначеного тренінгу кафедрою інформаційних технологій та кібербезпеки академії (надалі – кафедра) була розроблена відповідна експериментальна Програма стажування, яка визначала, що ця категорія курсантів після двох місяців проходження стажування в практичних підрозділах Національної поліції, які направляли їх на навчання до академії, повертаються до м. Києва для продовження проходження стажування в Департаменті кіберполіції та одночасного навчання в академії на тренінгових курсах. Ця Програма стажування була рекомендована до впровадження рішенням Вченої ради академії та погоджена Головою Національної поліції України генералом поліції першого рангу Сергієм Князєвим. Реалізація такого варіанту стажування відповідає рекомендаціям розширеної наради Національної поліції України за участю ректорів вишів МВС (27.10.2017, м. Львів) і не суперечить засадам організації навчального процесу в вишах МВС України.

Результати випускного іспиту тренінгового курсу показали, що навчальний експеримент, коли курсанти поєднували навчання на зазначених курсах з проходженням стажування в практичних підрозділах Департаменту кіберполіції Національної поліції України, пройшов вдало. Всі курсанти, які навчались на тренінгових курсах, успішно засвоїли навчальний матеріал та отримали відповідні теоретичні знання і практичні вміння із застосування

сучасних інформаційних технологій та протидії кіберзлочинності. За результатами навчання на зазначених тренінгових курсах курсанти, під час випуску з академії, отримали відповідний сертифікат, підписаний Головою Національної поліції та ректором академії. Станом на сьогодні ці випускники вишу успішно працюють в практичних органах та підрозділах Національній поліції України.

У поточному навчальному році кафедра здійснює підготовку, у якості експерименту, 30 курсантів (1 навчальна група) 4 курсу за новою спеціалізацією «Інформаційно-аналітична підтримка (слідчої діяльності)» для органів досудового розслідування Національної поліції України. Навчальним планом їх підготовки, крім «звичайних» навчальних дисциплін з підготовки майбутніх слідчих, передбачено вивчення ними 4 навчальних дисциплін кафедри: у 7 семестрі – «Основи побудови та адміністрування інформаційно-комунікаційних систем та мереж» та «Сучасні інформаційні технології та сервіси»; у 8 семестрі – «Особливості розслідування злочинів у сфері інформаційних технологій» та «Інформаційно-аналітична підтримка службової діяльності слідчих підрозділів Національної поліції».

Підготовка в академії майбутніх «кіберслідчих» ґрунтується на досвіді науково-педагогічних працівників кафедри та на вдосконаленій матеріально-технічній базі кафедри та академії.

Використані джерела

1. Кудінов В. А. Підготовка фахівців з протидії кіберзлочинності / В. А. Кудінов, Ю. Ю. Орлов // Бюлетень з обміну досвідом роботи МВС України. – 2011. – № 188. – С. 23-34.
2. Кудінов В. А. Вирішення проблем відбору та підготовки кадрів правоохоронців щодо протидії кіберзлочинності / В. А. Кудінов // Кадровий вісник. – 2011. – № 1. – С. 51-68.
3. Кудінов В. А. Щодо можливості підготовки в Національній академії внутрішніх справ фахівців з протидії кіберзлочинності та торгівлі людьми / В. А. Кудінов // Актуальні питання протидії кіберзлочинності та торгівлі людьми : зб. матеріалів Всеукр. наук.-практ. конф. (Харків, 15 лист. 2017 р.). – Харків : ХНУВС. 2017. – С. 178-180.
4. Кудінов В. А. Особливості підготовки в Національній академії внутрішніх справ фахівців з кібербезпеки для Національної поліції України / В. А. Кудінов // Підготовка охоронців правопорядку в Харкові (1917–2017 рр.) : зб. наук. статей і тез доп. на наук.-практ. конф. до 100-річчя підготовки охоронців правопорядку в Харкові (Харків, 24 лист. 2017 р.). – Харків : ХНУВС, 2017. – С. 171-172.
5. Корнейко О. В. Про запровадження в Академії у якості експерименту тренінгового курсу «Сучасні інформаційні технології» / О. В. Корнейко, В. А. Кудінов // Кіберзлочинність в Україні : сучасні тенденції та напрями протидії : матеріали «круглого столу» (Київ, 23 лист. 2017 р.). – К. : НАВС, 2018. – С. 6-11.

Коротенко Г.М. – професор кафедри геоінформаційних систем, доктор технічних наук, професор;
Коротенко Л.М. – доцент кафедри програмного забезпечення комп'ютерних систем, кандидат технічних наук (Національний технічний університет «Дніпровська політехніка»);
Косиченко О.О. – доцент кафедри економічної та інформаційної безпеки, кандидат технічних наук, доцент (Дніпропетровський державний університет внутрішніх справ)

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДВИЩЕННЯ ШВИДКОСТІ РОЗКРИТТЯ ЗЛОЧИНІВ

Розвиток комп'ютерної галузі висвітлює все нові приклади застосування досягнень інформаційних технологій. Сьогодні, на перший план у боротьбі зі злочинністю у всьому світі виходять програмні засоби на базі штучного інтелекту і машинного навчання. Існує вагома причина, чому компанії та влада іноземних держав зацікавлені в тому, щоб таким чином намагатися використовувати штучний інтелект. З 2010 року США витрачають більш ніж 80 мільярдів доларів на рік на державних, місцевих та федеральних рівнях у боротьбі із злочинністю. Згідно оцінкам загальні витрати Сполучених Штатів на правоохоронні органи складають суму понад 100 мільярдів доларів на рік. Таким чином, видатки на функціонування правоохоронних органів та в'язниць складають значну частину бюджетів місцевого самоврядування [1].

Прямі державні витрати – це лише невелика частка того, як злочинність економічно впливає на життя міст та приватних осіб. Наприклад, жертви злочину можуть зіткнутися також і з медичними рахунками. Крім того, висока злочинність може зменшити вартість майна та змусити компанії витрачати більше на безпеку. А кримінальні справи можуть значно зменшити довгострокову перспективу працевлаштування особи. Професор університету Пенсільванії А.Чалфін здійснив огляд поточних досліджень, присвячених наслідкам економічного впливу злочинності, і більшість даних аналізу вказує на те, що останні складають приблизно 2% валового внутрішнього продукту в США [1].

Тому, напрями роботи у цій галузі можна умовно поділити на застосування засобів штучного інтелекту для виявлення злочинів і засобів для запобігання подальшим злочинам.

Ідеї багатьох з цих проектів полягають у тому, що злочини є відносно передбачуваними; це просто вимагає необхідність сортувати величезний обсяг даних, щоб знайти шаблони, які корисні для правоохоронних органів. Даний вид аналізу даних був технологічно неможливим кілька десятиліть

тому, але виявилось, що останнім часом розвиток машинного навчання досяг рівня вирішуваних задач.

Компанія ShotSpotter [2] використовує розумну міську інфраструктуру для тріангуляції місця розташування вогнепальної зброї. Згідно даних ShotSpotter, лише приблизно у 20 відсотках випадків пострілів люди сповіщають про це поліцію, і навіть коли люди повідомляють про подію, вони часто можуть лише надавати нечітку або потенційно неточну інформацію. А ось система компанії, що оснащена кількома звуковими датчиками, має змогу підбирати тип вогнепальної зброї згідно зареєстрованим звукам, а їх алгоритм машинного навчання, використовуючи тріангуляційні алгоритми, відтворюють координати місця події.

Для початку роботи системи ShotSpotter акустичні датчики та камери розміщуються по всьому місту. Коли головна програма запускається:

- офіцер, детектив або інші співробітники правоохоронних органів працюють з інтерактивною картою;
- під час виникнення звукового сигналу біля датчиків зйомки, останні запускають відповідні камери спостереження, які направляються в бік точок де були зафіксовані звуки пострілів;
- на основі звукових частот та зафіксованих об'ємів даних система обчислює місце де і між якими датчиками відбувається зйомка;
- на карті відповідне місце де було зафіксовано постріли відзначається червоним колом;
- на бічній панелі поруч з картою відображаються інші подробиці, такі як час фіксації події і кількість зроблених знімків;
- координати місця події та інша інформація можуть бути негайно направлені до співробітників поліції;
- користувач має можливість отримати доступ до кадрів камер, які перемістили напрям спостереження у бік місця стрільби.
- після інциденту вся інформація залишається в журналі, щоб користувач міг знайти відповідні дані та відео для цілей розслідування.

У дослідженні фірми зазначається, що офіцери поліції, користуючись такими даними змогли вийти на місце зйомки з достатнім часом, щоб знайти достовірні докази та запитати свідків, які ще перебували в цьому районі. Пізніше вони заарештували двох підозрюваних, повідомляє ShotSpotter.

SpotShotter стверджує, що система буде використовуватися в більш ніж 90 містах, включаючи Нью-Йорк, Чикаго та Сан-Дієго. Більшість їх клієнтів перебувають у США, але минулого року вони до свого списку клієнтів додали м. Кейптаун (Південна Африка).

Дуже цікавий підхід пропонує фірма Cortica [3], що заснована в Тель-Авіві в 2007 році, яка створює міські системи безпеки. Її програмне забезпечення з елементами штучного інтелекту може «прочісувати» в реальному часі кадри зйомки не тільки з камер спостереження, а також і безпілотників для пошуку злочинних об'єктів та оповіщення про виявлені правопорушення правоохоронних або міських чиновників. Фірма стверджує,

що її розробка пропонує такі можливості штучного інтелекту та комп'ютерного зору:

- користувач може шукати зображення або відео за допомогою текстового або зворотного пошуку;
- виконується збір груп зображень облич, пов'язаних з однією подією або проміжком часу;
- аналізуються фізична поведінка та рухи людей для визначення загрозливих та не загрозливих моделей руху.

Компанія також пропонує програмне забезпечення, що працює сумісно з дронами і дозволяє виконувати аналогічний аналіз зображень і фіксацію геоміток, а також можливість направляти дрони на автономні маршрути.

Компанія стверджує, що її програмне забезпечення може бути використане для управління дорожнім трафіком, міською безпекою, безпекою подорожей, спостереженням на різних об'єктах та моніторингу громадського транспорту.

На сайті корпорації Cortica розміщені відповідні матеріали та демонстраційні відео, а також програмне забезпечення, яке дозволяє користувачеві завантажувати або транслювати відео або зображення, коли вони записані. Програма дізнається, які шаблони цих зображень треба виділяти у якості аномальних об'єктів, що з'являються на цих зображеннях. Вона також може бути використана з рентгенівськими апаратами і призначена для виявлення певних форм, таких як зброя. Користувач також може обирати відповідні засоби керування програмою, щоб побачити конкретні зображення, виявлені на фотографії або на зображенні з відео.

Окрему нішу в боротьбі зі злочинами займає китайська компанія CloudWalk Technology [4]. Ця організація працює в галузі розпізнавання облич засобами ШІ і її технології широко застосовується у фінансовій сфері, державній безпеці та авіаційній галузі. Продукти CloudWalk Technology включають в себе термінали розпізнавання обличчя, відкривання дверей на основі сканування обличчя та сканування на базі інфрачервоних біноклів.

Поточним часом компанія з розпізнавання обличчя Cloud Walk Technology намагається реально передбачити, чи буде особа здійснювати злочин, перш ніж це станеться.

Система визначить, чи є які-небудь підозрілі зміни в їх поведінці чи незвичних рухах. Наприклад, якщо людина, здається, ходить туди і назад у певній місцевості знову і знову, це вказуючи на те, що вона може бути націлена на майбутній злочин. Також буде відслідковуватися людина з плином часу.

Всі ці системи дозволяють посилити боротьбу з криміналом і, зрештою, зниження рівня злочинності має широкі соціальні вигоди для громади.

Використані джерела

1. Faggella D. AI for Crime Prevention and Detection – Current Applications. WEB–сайт [Електрон. ресурс] / Режим доступу: URL: https://www.techemergence.com/ai-crime-prevention-5-current-applications/

2. [Електрон. ресурс] / Режим доступу: URL: Company ShotSpotter. chttps://www.shotspotter.com/
3. Cortica. WEB–сайт [Електрон. ресурс] / Режим доступу: URL: / Режим доступу: URL: https://www.cortica.com/
4. CloudWalk. WEB–сайт [Електрон. ресурс] / Режим доступу: URL: Technology https://www.crunchbase.com/organization/cloudwalk-technology

Коршенко В.А. - завідувач лабораторії, кандидат юридичних наук;
Пашнєв Д.В. - провідний науковий співробітник, кандидат юридичних наук, доцент (науково-дослідна лабораторія захисту інформації та кібербезпеки факультету №4 Харківського національного університету внутрішніх справ);
Загородній В.В. - начальник відділу організації відбору та проведення атестування поліцейських управління комплектування Департаменту кадрового забезпечення Національної поліції України

ВИКОРИСТАННЯ ПРОГРАМНОГО КОМПЛЕКСУ «СИСТЕМА ВІДБОРУ КАДРІВ ДО НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ» В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Реформа Національної поліції України, що триває, вимагає ефективного кадрового забезпечення правоохоронних органів, яке повинне розпочинатися від моменту прийняття на службу. Процедура відбору кандидатів та безпосередньо проходження встановлених етапів конкурсів на вакантні посади у підрозділах Національної поліції України повинна бути чіткою, прозорою, виключати корупційну складову, зручною для кандидатів і для працівників відповідних підрозділів кадрового забезпечення в територіальних органах та службах. Задля того щоб зазначені характеристики достатньою мірою були забезпечені в процесі відбору необхідно використовувати новітні інформаційні технології, адже інформатизація процесів є одним із пріоритетних напрямів реформування управління персоналом та організації діяльності Національної поліції України. З розвитком телекомунікаційних технологій для цих цілей все частіше використовуються електронні системи та програмні комплекси, які працюють на WEB технологіях. Впровадження новітніх електронних систем та програмних комплексів в процеси відбору, навчання, перепідготовки та підвищення кваліфікації кадрів, оцінки їх діяльності, планування кар’єри тощо, надають нові можливості особам, що вступають на службу та (або) навчаються у відомчих закладах вищої освіти, а також зручні управлінські та контролюючі інструменти працівникам підрозділів організації відбору та проведення атестації поліцейських

територіальних (міжрегіональних) органів поліції (далі – СОВПАП).

Однією з таких систем є система відбору кадрів до Національної поліції України, яка була розроблена науково-дослідною лабораторією захисту інформації та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ спільно з Департаментом кадрового забезпечення Національної поліції України та Департаментом інформаційно-аналітичної підтримки Національної поліції України.

Система складається з двох взаємодіючих частин: Інтернет-порталу для кандидатів на службу [1] та внутрішнього серверу для працівників СОВПАП.

Інтернет-портал виконує наступні функції:

- публікація інформації про конкурси, оголошені на вакансії в підрозділах Національної поліції України;
- прийняття анкет-заявок для участі в оголошених конкурсах;
- публікація результатів завершених конкурсів;
- розміщення довідкової інформації щодо етапів проведення конкурсу, контактів СОВПАП;
- особистий кабінет, в якому кандидат на службу може зареєструватися та ознайомлюватися із актуальною інформацією щодо проходження ним етапів своїх конкурсів.

Внутрішній сервер забезпечує працівникам СОВПАП доступ до наступних функцій:

- робота із конкурсами на вакансії в Національну поліцію України: оголошення, контроль проведення та підведення підсумків – визначення переможців;
- робота із анкетами кандидатів на вакансії в Національну поліцію України: редагування, призначення заходів в рамках етапів конкурсу, фіксація результатів;
- формування статистичних звітів.

Система була впроваджена в діяльність в листопаді 2017 року (тестова експлуатація відбувалася з грудня 2016 року) і зараз використовується в ході прийняття на службу до Національної поліції України. Система працює на віртуальних серверах. Технічну підтримку системи здійснюють співробітники Департаменту інформаційно-аналітичної підтримки Національної поліції України. Співробітники науково-дослідної лабораторії захисту інформації та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ здійснюють постійну програмну підтримку і модернізацію вказаної системи. На замовлення Департаменту кадрового забезпечення Національної поліції України постійно модернізується існуючий і розробляється та впроваджується новий функціонал. В 2018 році було впроваджено систему відбору кандидатів на навчання до вищих навчальних закладів МВС України [2]. Обидві системи планується включити у якості підсистем Системи управління персоналом Національної поліції України (знаходиться на стадії підготовки до тестового запуску) та інтегрувати в діючу загальну інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України».

Досвід експлуатації системи довів, що в сучасних умовах інтеграція інноваційних технологій в процес управління персоналом Національної поліції України є життєво необхідним підґрунтям, яке гарантує стабільність поповнення лав Національної поліції України, дотримання законності під час проходження служби в поліції та дозволяє сміливо дивитись у майбутнє.

Використані джерела

1. Інтернет портал системи відбору кадрів до Національної поліції України [Електронний ресурс]. – Режим доступу: https://nabir.np.gov.ua/
2. Інтернет портал системи відбору кандидатів на навчання до вищих навчальних закладів МВС України [Електронний ресурс]. – Режим доступу: https://osvita.np.gov.ua/

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

УДОСКОНАЛЕННЯ ФУНКЦІОНУВАННЯ СИСТЕМИ ОПЕРАТИВНОГО ІНФОРМУВАННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ ШЛЯХОМ СТВОРЕННЯ СИТУАЦІЙНИХ ЦЕНТРІВ

Наказом МВС України від 16 лютого 2018 року № 111 затверджена Інструкція з організації реагування на заяви та повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України (надалі – НПУ) [1, 2]. Відповідно до п. 2 розділу І зазначеної Інструкції під *оперативним інформуванням* розуміють єдину систему збирання, опрацювання та подання до чергової служби вищого рівня інформації про правопорушення або подію з метою організації контролю за встановленням і затриманням осіб, які вчинили кримінальні правопорушення, а також оперативного реагування на надзвичайні ситуації. Заяви та повідомлення про правопорушення або події працівниками чергової служби органів (підрозділів) поліції реєструються в інформаційних ресурсах інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» [3].

З метою забезпечення належного функціонування зазначеної єдиної системи збирання, опрацювання та подання до чергової служби вищого рівня інформації про правопорушення або подію використовується інтегрована інформаційна *система оперативного інформування* (далі – СОІ) НПУ, яка є подальшим розвитком автоматизованої СОІ Міністерства внутрішніх справ (надалі – МВС) України, створеної протягом 1992-2015 років [4, 5]. Необхідно відмітити, що для СОІ МВС України були розроблені достатньо потужні програмно-технічні засоби, які забезпечували її широкі можливості [6-10].

Станом на сьогодні СОІ НПУ представляє собою єдиний інформаційно-аналітичний комплекс нормативно-правових, організаційно-кадрових, програмно-технічних, інформаційно-телекомунікаційних та інших заходів і засобів, що здійснює цілодобову обробку оперативної інформації про кримінальні правопорушення та інші надзвичайні події, які сталися на території України [1-3]. НПУ вживає заходи для організації належного інформаційно-аналітичного забезпечення своєї діяльності, у тому числі функціонування СОІ. Одним з них є впровадження Ситуаційних центрів (надалі – СЦ).

Вважається, що Ситуаційний центр – це нова структура в органах НПУ, до завдань якого включено отримання, аналіз та обробку інформації про динаміку злочинності по всій території України [11]. СЦ – це підрозділ зі збору, обробки та аналізу інформації про рівень, структуру і динаміку злочинності по всій Україні. Існує Ситуаційний центр НПУ, де проводиться тільки збір і обробка інформації, а також СЦ в місті Києві та областях, в складі яких працює і служба «102» [12]. Так, зокрема, 23 серпня 2018 року новий СЦ Нацполіції презентували в м. Дніпрі [13]. СЦ – це сучасна форма організації аналітичної діяльності, яка базується на синтезі інформаційно-комунікаційних технологій, засобів накопичення і представлення інформації, комп'ютерних засобів підтримки прийняття рішень [14]. СЦ НПУ працюють цілодобово в двох режимах: стандартному або надзвичайному. При цьому його аналітики використовують три види аналізу: стратегічний, тактичний та практичний. Проведений аналіз роботи СЦ НПУ за останні два роки дозволяє зробити висновок щодо їх ефективності для удосконалення функціонування системи оперативного інформування Національної поліції України [12].

Використані джерела

1. Про затвердження Інструкції з організації реагування на заяви та повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України: Наказ МВС України від 16 лют. 2018 р. № 111. *Верховна Рада України*: [сайт]. URL: http://zakon.rada.gov.ua/laws/show/z0371-18.
2. Про Національну поліцію: Закон України від 02 лип. 2015 р. № 580-VIII. *Відомості Верховної Ради України*. 2015. № 40-41. Ст. 379.
3. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України»: Наказ МВС України від 03 серп. 2017 р. № 676. *Верховна Рада України*: [сайт]. URL: http://zakon.rada.gov.ua/laws/show/z1059-17.
4. Функціонування системи оперативного інформування МВС України / [В. А. Кудінов, П. П. Артеменко, О. В. Золотар та ін.]; за ред. В. А. Кудінова. *Спеціальна техніка. Загальна частина*: посіб. Київ: Київський нац. ун-т внутр. справ, 2007. С. 156–172.
5. Кудінов В. А. Становлення, сучасний стан і перспективи розвитку автоматизованої системи оперативного інформування МВС України про резонансні злочини та інші надзвичайні події. Бюлетень з обміну досвідом роботи МВС України. 2012. № 190. С. 9–27.
6. Кудинов В. А. Автоматизированный контроль качества и своевременности оперативного информирования МВД Украины. *Безпека дорожнього руху України*. 1999. № 3. С. 131–134.

7. Кудінов В. А. Програми контролю достовірності та попередньої обробки інформації бази даних АІС «Зведення» з обліку резонансних злочинів та інших надзвичайних подій МВС України. *Реєстрація, зберігання і обробка даних*. 2005. Т. 7. № 1. С. 80–88.
8. Кудінов В. А. Аналіз динаміки оперативної обстановки в країні з використанням можливостей системи оперативного інформування МВС України. *Захист інформації*. 2006. № 1. С. 67–71.
9. Кудінов В. А. Аналіз відповідності статистичних даних про резонансні злочини системи оперативного інформування МВС України офіційним показникам стану та структури злочинності. *Вісник Державного університету інформаційно-комунікаційних технологій*. 2008. Т. 6. № 3. С. 276–283.
10. Кудінов В. А. Аналіз оперативної обстановки можливостями автоматизованої системи оперативного інформування МВС України. *Бюлетень з обміну досвідом роботи МВС України*. 2012. № 190. С. 28–33.
11. Поліція відкриває ситуаційні центри. LexInform *Юридичні новини України*: [сайт]. URL: https://lexinform.com.ua/zakonodavstvo/politsiya-vidkryvaye-sytuatsijni-tsentry/
12. Ситуационный центр Нацполиции: анализ преступности, оперативной обстановки и координация подразделений. *112.ua*: [сайт]. URL: https://112.ua/statji/situacionnyy-centr-nacpolicii-analiz-prestupnostioperativnoy-obstanovki-i-koordinaciya-podrazdeleniy-431302.html.
13. Новий ситуаційний центр Нацполіції презентували в Дніпрі. Фоторепортаж. *Цензор. Нет.* URL: https://ua.censor.net.ua/photo_news/3082609/novyyi_sytuatsiyinyyi_tsentr_natspolitsiyi_prezentuvaly_v_dnipri_fotoreportaj.
14. Поняття Ситуаційного центру. URL: http://inmad.vntu.edu.ua/portal/static/952500A7-287E-4743-A7B1-0B8C1105B2CA.pdf.

Кулешник Я.Ф. - доцент кафедри інформатики, кандидат технічних наук, доцент;
Сеник В.В. - завідувач кафедри інформатики, кандидат технічних наук, доцент (Львівський державний університет внутрішніх справ)

АНАЛІЗ ПІДХОДІВ ДО ПРОЦЕСІВ АВТОМАТИЗАЦІЇ ОБРОБКИ ВІДБИТКІВ ПАЛЬЦІВ РУК

Звернення вчених до вивчення типів узорів на внутрішній поверхні кисті руки було пов'язане з вирішенням двох задач. Перша – створення натурно-наукової класифікації узорів, друга – розробка систем реєстрації злочинців за папілярними узорами нігтьових фаланг пальців рук. Першу класифікацію папілярних узорів здійснив чеський біолог Я.Е. Пуркін’є, який у 1828 р. розділив узори на дев'ять типів.

У подальшому класифікація узорів розвивалася та удосконалювалася вченими Аліксом, Гальтоном, Форжо, Тестю, Генрі та ін. Перші спроби удосконалення були скеровані на побудову якомога більш детальної класифікації. Так, наприклад, у першому варіанті класифікації,

запропонованому англійцем Ф. Гальтоном, пальцеві узори розподілялись на шістдесят класів. Така складна система виявилась для практики малопридатною. Потрібна була чітка і в той же час проста (коротка) система.

До такого варіанту врешті-решт і прийшов Ф. Гальтон, розділивши всі види пальцевих узорів на три основні типи: дуга, петля та завиток. Ця класифікація була доповнена англійським поліцейським чиновником Е. Генрі, який запропонував розрізняти ще один тип: складні узори. Таким чином створилася широко розповсюджена нині система класифікації Гальтона-Генрі. Ця система, доповнена елементами, запозиченими із системи класифікації німецького криміналіста Рошера, була покладена в основу реєстраційної системи пальцевих узорів.

За прийнятою в нашій країні системою всі папілярні узори розподіляються на три типи: дугові, петльові та завиткові з додатковою розбивкою кожного типу на різновидності у відповідності з особливостями будови узору. Серед всіх узорів дугові складають 5% по відношенню до інших типів, завиткові – 30% і петльові – 65%

Початок автоматизації дактилоскопічних обліків відноситься до 60^{x} рр. На створення першого покоління автоматизованих дактилоскопічних ідентифікаційних систем (АДІС) знадобилося десять років.

Аналогічно робота з впровадження АДІС ведеться у Франції, Чехії, Іспанії, Великій Британії. Нині у світі існує декілька автоматизованих дактилоскопічних систем: «Морфо» – Франція, «Принтрак» – США, «NEC» – Японія, «Папілон» – Росія, «Сонда» – Росія, Україна, «Дакто-2000» – Білорусь, «Моно-Ліза» – Угорщина, «ДЕХ» – Росія.

Локальні і глобальні характеристики відбитка пальців

Шкіра людини складається з двох шарів: епідермісу (epidermis), зовнішнього шару; дерми (derma), більш глибокого шару. На п'ятому місяці внутрішньоутробного розвитку людини дерма, до цього рівна, стає нерівною і починає набувати вигляду безлічі дермальних горбків (іноді їх називають сосочками), що чергуються між собою.

На вершинах складок – гребенях папілярних ліній знаходяться численні дрібні пори – зовнішні отвори вивідних проток потових залоз шкіри. Папілярні лінії на поверхні пальців рук утворюють різні візерунки, звані папілярним візерунками. Остаточно папілярний візерунок на поверхні пальців формується до 7 місяця внутрішньоутробного розвитку. З цього часу борозенки, що сформувалися на поверхні пальців, залишаються незмінними протягом усього життя людини [1].

У кожному відбитку пальця можна визначити два типи ознак: глобальні та локальні. Глобальні ознаки – ті, які можна побачити неозброєним оком (рис. 1). Інший тип ознак – локальні. Це локальні особливості папілярних ліній унікальні для кожного відбитка пальця. Їх виділення пов’язано з тим , що лінії відбитків пальців не є прямими. Вони часто зламані, розгалужені, змінюють напрямок і мають розриви.

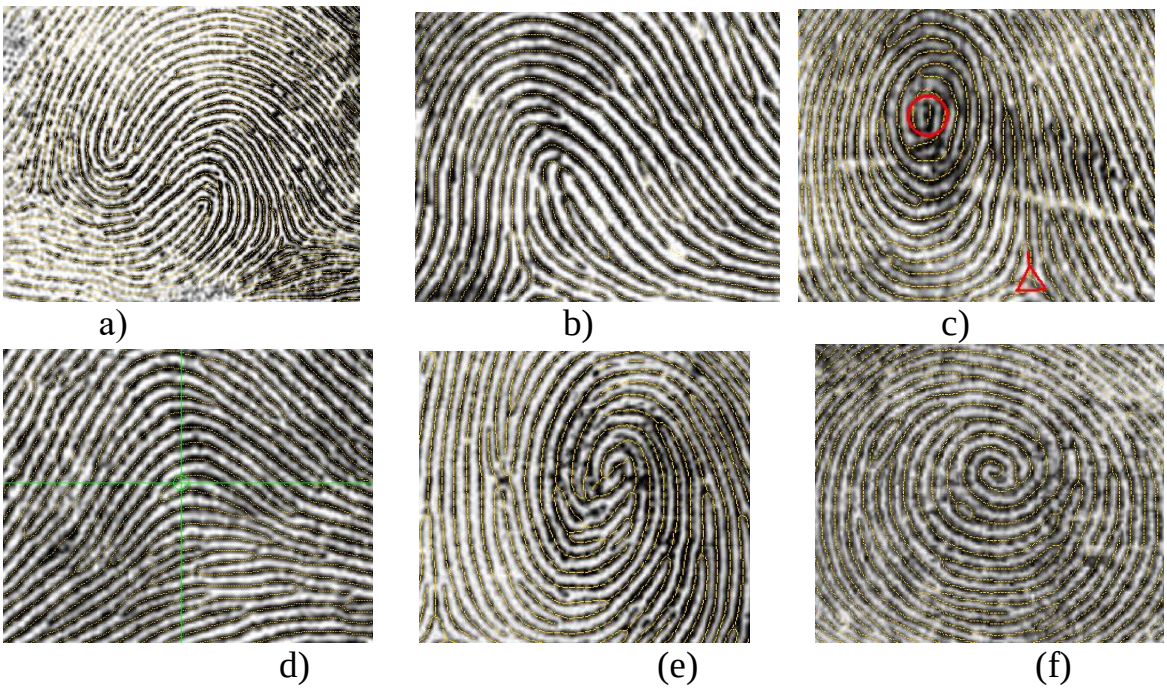


Рис. 1. Глобальні ознаки відбитка пальця: (a) – подвійна петля; (b) – звичайна петля; (c) – завиток (концентричні кола) і дельта; (d) – проста дуга; (e) – змішана ознака; (f) – завиток (спіраль)

Точки, в яких лінії закінчуються, розгалужуються або змінюють напрямок, називаються точками мінуціями. Ці точки забезпечують унікальну інформацію про відбиток пальця при ідентифікації особистості. Кожен відбиток містить до 70 мінуцій (рис. 2) [2].

Рис. 2. Локальні ознаки (кінцеві точки і точки розгалуження) на відбитку пальця

Поняття верифікації та ідентифікації особи

Якщо ви бачите людину і впізнаєте її, то ви її верифікуєте. Верифікація (аутентифікація) дає відповідь на запитання "Чи впізнаєте ви людину, яку бачите перед собою?". В голові людини проходить попарне порівняння отриманого набору даних з тим, що вже є в пам’яті і з його допомогою реалізується або ні підтвердження особистості людини. Результатом верифікації є або "впізнаний", або "не впізнаний", звичайно, з відповідною долею ймовірності. Ідентифікація дає відповідь на запитання "Хто ця

людина?". Технічно, це відбиток пальця порівнюється з відбитками, що вже є у відповідних базах даних. У зв'язку з тим, що бази даних можуть досягнути дуже великих розмірів та для зменшення обчислень, була проведена класифікація відбитків пальців. При ідентифікації проводиться порівняння тільки з тими відбитками які належать до того ж класу. Класифікація базується на наявності у відбитках сингулярних точок – глобальних ознаках відбитку пальця (рис. 1). Однакові глобальні ознаки, як показує практика, можуть мати зовсім різні люди, але не можливо мати однакові локальні ознаки. Тому глобальні ознаки використовують лише для розподілу бази даних на класи і на етапі аутентифікації. На другому етапі розпізнання, тобто для ідентифікації, використовують уже локальні ознаки.

Загальні принципи аналізу розпізнавання відбитків пальців

На сьогодні у світі використовують стандарти ANSI та ФБР США. У них визначені наступні вимоги до зображення якості відбитка:

– кожен відбиток повинен бути поданий до розгляду у форматі неархівованого TIF чи BMP файлу;

– зображення повинно мати роздільну здатність не нижче 500 dpi;

– зображення повинно бути напівтонованим з 256 рівнями яскравості;

– максимальний кут повороту зображення від вертикалі не більше 15 градусів;

– основні типи мінуцій – закінчення та розгалуження [2].

Відбитки пальців, отримані на спеціальних дактилокартах (рис. 3) за допомогою сканера вносяться в базу даних.

Алгоритм розпізнавання відбитку пальця у великій мірі залежить від якості отриманого зі сканера зображення папілярного узору [1]. Якщо якість хороша, то на відбитку пальця можна виокремити деякі характерні ознаки поверхні пальців, які в майбутньому можна використати з метою ідентифікації особи.

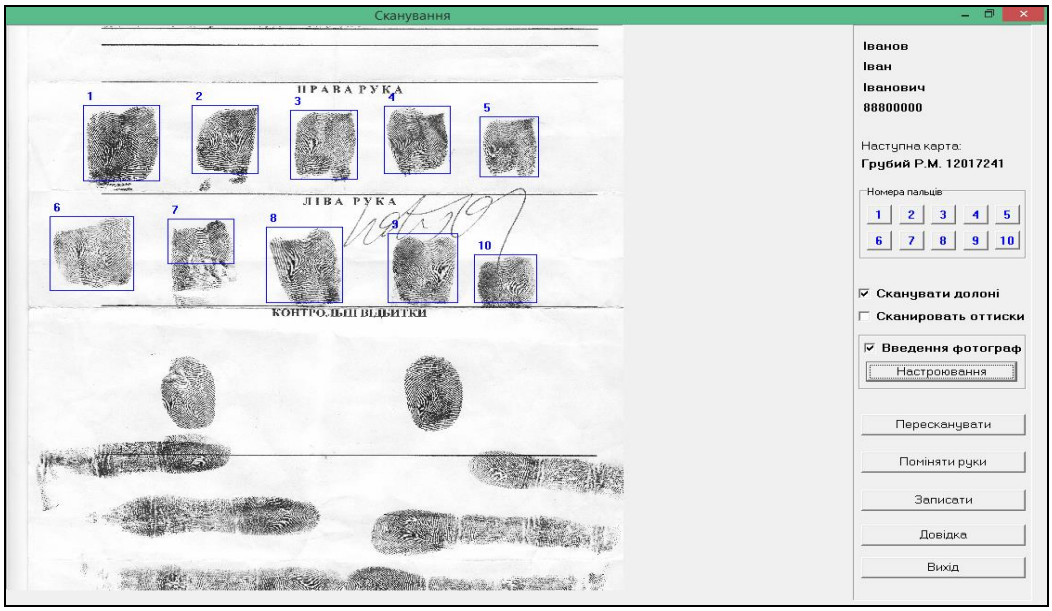


Рис. 3. Вікно після сканування дактилокарти АДІС «Сонда».

Якщо роздільна здатність сканера 300-500 dpi на зображенні поверхні пальця можна виділити достатньо велику кількість мінуцій, за якими можна їх класифікувати. В спеціалізованих автоматизованих системах використовують лише два типи особливих точок: кінцеві точки та точки розгалуження (див. рис. 2). В кінцевих точках чітко закінчуються (або перериваються) папілярні лінії, а в точках розгалуження відбувається роздвоєння лінії.

Весь алгоритм верифікації та ідентифікації особи полягає у наступному. Кожен палець нової, щойно введеної зі сканера дактилокарти, за глобальними ознаками порівнюється з відповідним пальцем уже існуючої в базі дактилокарти. В результаті ми отримаємо (або ні) рекомендаційний писок дактилокарт, котрі мають співпадіння за глобальними ознаками хоч одного (будь-якого) із пальців. Після цього, уже серед записів з рекомендаційного списку бази даних, вибирається та єдина дактилокарта, котра має співпадіння хоч за одним пальцем (слідом), тепер уже за локальними ознаками, з щойно введеною новою дактилокартою [3]. Таким чином здійснюються перший (верифікація) і другий (ідентифікація) етапи встановлення конкретної особи, чиї відбитки пальців були знайдені.

Якщо є можливість отримати зображення поверхні пальця з роздільною здатністю 1000 dpi на ньому можна віднайти деталі внутрішньої будови самих папілярних ліній, зокрема, пори потових залоз, і звичайно використовувати уже їх для ідентифікації особи. Однак цей метод мало поширений із за складності отримання в не лабораторних умовах зображення такої якості.

Використані джерела

1. Задорожный Виталий. Идентификация по отпечаткам пальцев / Виталий Задорожный // PC Magazine/Russian Edition №2. – 2004.
2. Дактилоскопия. [Электронный ресурс]. – Режим доступа к ресурсу: www.ru.wikipedia.org.
3. Гаспарян А.В. Система сравнения отпечатков пальцев по локальным признакам / А.В. Гаспарян, А.А. Киракосян // Вестник РАУ. Серия физико-математические и естественные науки. – 2006.

Куцак С.В. - старший викладач кафедри захисту інформації;
Хемішінець Є.В. - студент
(Запорізький національний технічний університет)

ЗАХИЩЕНІСТЬ ДАНИХ В МЕРЕЖАХ LTE

Невеликі компанії і стартапи (startup) часто переїжджають з місця на місце, а фрілансери (freelancer) і зовсім працюють звідки доведеться – дім, кафе, коворкінг (co-working). Один з ключових факторів налагодженої роботи – швидкий і надійний інтернет. Оперативно та якісно вирішити

проблему безпечного корпоративного інтернету можливо завдяки сучасним безпровідним мережам LTE.

LTE розглядається як еволюція технології UMTS, є стандартом високошвидкісного бездротового зв'язку передачі даних розроблений групою 3GPP визначеного специфікаціями Release 8, 9 та 10 [1]. Сама абревіатура LTE (Long Term Evolution) є зареєстрованою торговою маркою і знаходиться в розпорядженні Європейського інституту стандартів телекомунікації, як і логотипи «LTE», «LTE-Advanced», «LTE-Advanced Pro». В Україні з 2018 року ключові оператори мобільного зв'язку ввели в дію стандарт LTE-Advanced (LTE-A).

В даній роботі проводиться аналіз стану захищеності та вимог до механізмів безпеки LTE-мереж.

Існують чотири основні вимоги до механізмів безпеки технології LTE:

- забезпечити як мінімум такий же рівень безпеки, як і в мережах типу 3G, не завдаючи незручностей користувачам;
- забезпечити захист від Інтернет-атак;
- механізми безпеки для мереж LTE не повинні створювати перешкод для переходу зі стандарту 3G на стандарт LTE;
- забезпечити можливість подальшого використання програмно-апаратного модуля USIM (Universal Subscriber Identity Module, універсальна SIM-карта).

Останні два пункти забезпечуються використанням механізму 3GPP AKA (Authentication and Key Agreement) [2]. Вимоги ж безпеки до компоненту Evolved Packet Core, тобто до ядра мережі LTE, можуть бути виконані з використанням технології безпечної доменної зони (NDS - Network Domain Security) на мережевому рівні, як це описано в стандарті TS33.210.

Для закриття даних в мережах LTE використовується потокове шифрування методом накладення на відкриту інформацію псевдовипадкової послідовності (ПВП) за допомогою оператора XOR (виключне або) [3]. Ключовим моментом у схемі є той факт, що псевдовипадкова послідовність ніколи не повторюється. Алгоритми, що використовуються в мережах LTE, виробляють псевдовипадкову послідовність кінцевої довжини. Тому для захисту від колізій ключ, який використовується для генерації ПВП, регулярно змінюється, наприклад, при підключенні до мережі, в процесі передачі і т.д. У мережах 4G для генерації сеансового ключа необхідне використання механізму Автентифікації і Ключового обміну (AKA). Робота механізму AKA може зайняти частки секунди, необхідні для вироблення ключа в додатку USIM і для підтримання зв'язку з Центром реєстрації (HSS). Таким чином, для досягнення швидкості передачі даних мереж LTE необхідно додати функцію оновлення ключової інформації без ініціалізації механізму AKA.

Модель безпеки (Trust model) мережі LTE дуже схожа на модель, запропоновану в рамках мереж UMTS. Її можна грубо описати як мережу, що складається з надійної опорної мережі (Core network), а також сукупності

інтерфейсів між базовими станціями, користувацькими пристроями та опорною мережею, які вразливі для атак.

Щоб звести до мінімуму схильність атакам базову станцію, вона має забезпечити безпечне середовище, яке підтримує виконання таких чутливих операцій, як шифрування і розшифрування користувачів даних, зберігання ключів. Крім того, переміщення конфіденційних даних повинні обмежуватися цим безпечним середовищем. Заходи протидії: перевірка цілісності пристрою; взаємна аутентифікація базової станції оператора (видача сертифікатів); безпечні поновлення; механізм контролю доступу; синхронізація часу; фільтрація трафіку.

Навіть з розпочатими заходами безпеки, слід враховувати атаки на базові станції. Якщо атака успішна, то зловмисник може отримати повний контроль, включаючи доступ до всіх переданих даних, як від пристрою користувача, так і інформації, що передається до інших базових станцій.

Використані джерела

1. Long Term Evolution. Матеріал з Вікіпедії. [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/LTE.
2. Петр Хенкин, Ольга Трофимова. Защита данных в сетях LTE / Публикация ЗАО «Перспективный Мониторинг» [Електронний ресурс]. – Режим доступу: http://www.archive.li/e5buS.
3. LTE Security Architecture. [Електронний ресурс]. – Режим доступу: http://www.3glteinfo.com/lte-security-architecture/.

Лізунов С.І. - професор кафедри захисту інформації, кандидат технічних наук, доцент;
Муха О.С. – студент **(**Запорізький національний технічний університет)

АНАЛІЗ РІВНЯ ЗАХИСТУ ІНФОРМАЦІЇ В БПЛА

В даній роботі проводиться аналіз уразливості систем зв’язку, можливих реалізацій основних систем БПЛА у захищеному режимі, порівняння апаратних і програмних складових, що дозволяють реалізувати поставлені задачі.

В наш час основне завдання, що покладено на комплекси БПЛА, - проведення розвідки важкодоступних районів, в яких отримання інформації звичайними засобами, включаючи авіарозвідку, ускладнене або ж є небезпечним для здоров'я та навіть життя людей [1].

Безпілотні авіаційні комплекси, як правило, включають в себе оператора (пілот-оператор, пункт управління), безпілотний літальний апарат та канали зв'язку. Однак, їх захисту від зовнішніх програмно-апаратних впливів, не дивлячись на зростання кількості інцидентів, не приділяється

достатньої уваги [2].

Метою роботи є розробка апаратно програмної архітектури двостороннього зв’язку між БПЛА та мобільною наземною станцією. Вибір та реалізація алгоритмів шифрування та захисту відео потоку та потоків керування БПЛА [3]. Об'єкт дослідження – рівень захисту інформації в системах БПЛА. Предмет дослідження – моделі, методи та засоби захисту інформації з використанням програмно-апаратних та криптографічних систем. В ході проведення дослідження було розглянуто загальні відомості про сучасний стан сфери БПЛА, більш конкретно досліджено принципи систем зв'язку з БПЛА та способи їх злому. Проведений аналіз показав, що існують випадки злому зв'язку на поліцейських і воєнних БПЛА, а цивільні дрони є не захищеними взагалі. Задачі, які треба вирішити під час проведення дослідження: аналіз алгоритмів шифрування, стандартів передачі даних, опис головних характеристик камери БПЛА та алгоритмів синхронізації часу у розподілених системах.

Спираючись на проведені дослідження, виявлено, що задля вирішення поставлених задач було б доцільно розробити окремий модуль зв'язку, що може бути встановлений в будь-який корпус БПЛА. Модуль зв'язку повинен забезпечити захист від таких розповсюджених атак, як заглушення, підміна пакетів, GPS спуфінг та перехоплення даних. Для врахування специфіки завдань даного дослідження, проведено аналіз можливих рішень систем захисту інформації в БПЛА та отримано результати функціонування розроблених компонентів зв'язку.

Використані джерела

1. Бєлоносов Т. М. Розробка програмно-апаратної реалізації захищеного бездротового інтерфейсу до безпілотного літального апарату: Дипломна робота/ Т.М. Бєлоносов. – К., 2017. – 74 с.
2. Слюсар В. І. ЭЛЕКТРОНИКА: Наука, Технология, Бизнес / Слюсар В. І. – Москва : РИЦ Техносфера – 2010. – 56 с. – (Радиолинии связи с БПЛА: Примеры реализации).
3. Лізунов С.І., Панкова Т.Б. Криптографічний протокол захисту інформації в радіоканалах БПЛА. Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 18-22 квітня 2016 р.: збірник тез доповідей в 5 томах. – Запоріжжя, 2016. – Т.1. – С. 312-314.

Лізунов С.І. - професор кафедри захисту інформації Запорізького національного технічного університету, кандидат технічних наук, доцент

ПРАКТИЧНЕ ЗАСТОСУВАННЯ ЛОКАТОРІВ НЕЛІНІЙНОСТЕЙ

Здатність виявляти радіоелектронні об'єкти за допомогою локатора нелінійностей (ЛН) ґрунтована на фізичній властивості напівпровідникових приладів, яка полягає в тому, що при їх опроміненні електромагнітним

сигналом відбувається перетворення частоти сигналу в кратні гармоніки з їх подальшим випромінюванням в ефір. При цьому процес перетворення не залежить від стану опромінюваного радіоелектронного пристрою (активне або пасивне).

Багато хто оцінює ЛН по випромінюваній потужності, оскільки ця характеристика порівняно легка для сприйняття. Проте чутливість приймача так само важлива, як і потужність передавача. Необхідно зрозуміти, що ЛН з низькою потужністю випромінювання і якісним приймачем може мати більш високі характеристики по виявленню, чим потужний локатор з поганим приймачем. Також слід пам'ятати, що потужний локатор може вивести з ладу електронні прилади і навіть завдати шкоду здоров'ю людей.

Режим випромінювання безпосередньо пов'язаний з потужністю випромінювання. Існує два режими випромінювання: безперервний і імпульсний. Перевагою імпульсного режиму є менше споживання струму (за умови хорошої конструкції передавача). Частота випромінювання разом з його потужністю є основним параметром, що формує тактико-технічні характеристики (ТТХ) локатора. Ця обставина пов'язана з двома чинниками:

- частотною залежністю величини загасання радіохвиль в середовищі поширення як зондуючого сигналу, так і сигналів на вищих гармоніках;
- тим, що рівень потужності перетвореного сигналу тим вище, чим нижче частота локатора.

Про локатор нелінійності треба судити як по дальності виявлення нелінійностей, так і по його здібності розрізняти такі з'єднання. Велика дальність виявлення не обов'язково є перевагою конкретного ЛН: ви можете просто виявляти електронні пристрої, наприклад, в сусідньому приміщенні. Під час роботи ЛН повинен мати не лише достатню дальність виявлення, але і можливість відповідного регулювання потужності для забезпечення необхідної глибини виявлення в обстежуваному середовищі.

Історично моделі ЛН ґрунтувалися лише на порівнянні другої та третьої гармонік. Проте, також важливо використати методи аудіоаналізу напівпровідникових з'єднань, такі, як "ефект загасання" і фізичного впливу. Для максимальної надійності хороший локатор повинен використовувати декілька методів ідентифікації справжніх і неправдивих напівпровідників. Крім того, бажано, щоб ЛН мав декілька робочих частот для уникнення впливу зовнішніх завад у конкретних умовах роботи.

Підводячи підсумки, хотілося б сказати, що фізичні принципи, що використовуються локатором нелінійності, дозволяють виявляти переважну більшість сучасних потайно встановлених технічних засобів перехоплення інформації. Це дозволяє віднести його до класу універсальних пошукових приладів, що мають високу міру ефективності.

Разом з тим, необхідно пам’ятати, що випромінювання локаторів не проходять через екрануючі конструкції. У таких випадках на допомогу приходять звичайні металошукачі. Тому актуальним стає використання технічних засобів виявлення закладних пристроїв, що мають як ЛН, так і металошукач одночасно в одному корпусі.

Махницький О.В. – старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ.

ВИКОРИСТАННЯ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ДЛЯ КРАДІЖКИ ОСОБИСТИХ ДАНИХ

Сама слабка ланка в ланцюзі інформаційної безпеки - це людина. Використовуючи соціальну інженерію зловмисники отримують доступ до конфіденційних даних користувачів. Розглянемо, як саме це відбувається. Але для початку розберемося з самим поняттям соціальної інженерії.

Соціальна інженерія - метод отримання необхідного доступу до інформації, заснований на особливостях психології людей. Основною метою соціальної інженерії є отримання доступу до конфіденційної інформації, паролів, банківських даних і інших захищених систем. Термін соціальна інженерія з'явився не так давно, але сам метод отримання інформації таким чином використовується досить давно. Співробітники силових і відомчих структур, які хотіли б залучити деяку державну таємницю, використання політтехнологій, та й ми самі, при бажанні отримати щось, часто навіть не розуміючи цього, використовуємо методи соціальної інженерії.

Загальні типи соціальної інженерії та методи захисту від них.

Претекстінг - це набір дій, відпрацьованих за певним, заздалегідь складеним сценарієм, в результаті якого жертва може видати будь-яку інформацію або вчинити певну дію. Найчастіше даний вид атаки передбачає використання голосових засобів, таких як Skype, телефон і т.п.

Для використання цієї техніки зловмисникові необхідно спочатку мати деякі дані про жертви (ім'я співробітника; посаду; назва проектів, з якими він працює; дату народження). Зловмисник спочатку використовує реальні запити з ім'ям співробітників компанії і, після того як увійде в довіру, отримує необхідну йому інформацію.

Фішинг – техніка інтернет - шахрайства, спрямована на отримання конфіденційної інформації користувачів – авторизаційних даних різних систем. Основним видом фітингових атак є підроблений лист, відправлений жертві по електронній пошті, який виглядає як офіційний лист від платіжної системи або банку. У листі міститься форма для введення персональних даних (пін-код, логін і пароль і т.п.) або посилання на web-сторінки, де розташовується така форма. Причини довіри жертви до подібних сторінок можуть бути різні: блокування облікового запису, поломка в системі, втрата даних та інше.

Троянський кінь - це техніка ґрунтується на цікавості, страху або інших емоціях користувачів. Зловмисник відправляє лист жертві за допомогою електронної пошти, як додаток до якого знаходиться «оновлення» антивірусу, ключ до грошового виграшу або компромат на співробітника. Насправді ж у вкладенні знаходиться шкідлива програма, яка

після того, як користувач запустить її на своєму комп'ютері, буде використовуватися для збору або заміни інформації зловмисником.

Кви про кво (послуга за послугу) - дана техніка передбачає звернення зловмисника до користувача по електронній пошті або корпоративному телефону. Зловмисник може представитися, наприклад, співробітником технічної підтримки та інформувати про виникнення технічних проблем на робочому місці. Далі він повідомляє про необхідність їх усунення. У процесі «рішення» такої проблеми, зловмисник підштовхує жертву на вчинення дій, що дозволяють атакуючому виконати певні команди або встановити необхідне програмне забезпечення на комп'ютері жертви.

Дорожнє яблуко - цей метод є адаптацію троянського коня і полягає у використанні фізичних носіїв (CD, флеш-накопичувачів). Зловмисник зазвичай підкидає такий носій в загальнодоступних місцях на території компанії (парковки, столові, робочі місця співробітників, туалети). Для того, щоб у співробітника виник інтерес до даного носія, зловмисник може нанести на носій логотип компанії і якусь підпис. Наприклад, «дані про продажі», «зарплата співробітників», «звіт в податкову» і інше.

Зворотна соціальна інженерія - даний вид атаки спрямований на створення такої ситуації, при якій жертва змушена буде сама звернеться до зловмисника за «допомогою». Наприклад, зловмисник може вислати лист з телефонами і контактами «служби підтримки» і через деякий час створити оборотні неполадки в комп'ютері жертви. Користувач в такому випадку подзвонить або зв'яжеться по електронній пошті із зловмисником сам, і в процесі «виправлення» проблеми зловмисник зможе отримати необхідні йому дані.

Далі розглянемо, один з найпотужніших і універсальних інструментів, соціальної інженерії. Він має назву Social-Engineer Toolkit, його загальний вигляд на малюнку 1.

Мал.1. Загальний вид інструменту Social-Engineer Toolkit.

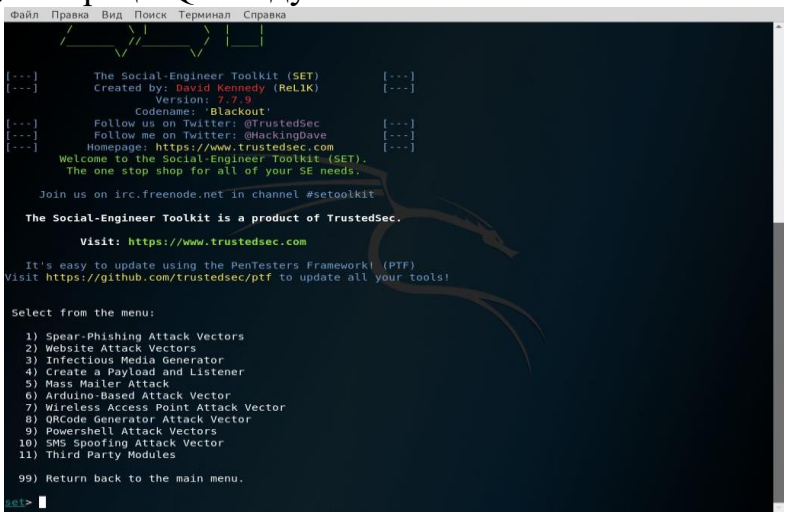
Основні напрямки використання інструменту.

Соціально-технічні атаки.

Розділ включає в себе список векторів для атак:

- Вектори атаки веб-сайтів.
- інфекційний медіа генератор.
- Створення корисного навантаження і слухача.
- масова атака.
- Вектор атаки на основі Arduino.
- Вектор атаки бездротової точки доступу.
- Вектор атаки генератора QRCode.
- Вектори атаки Powershell.

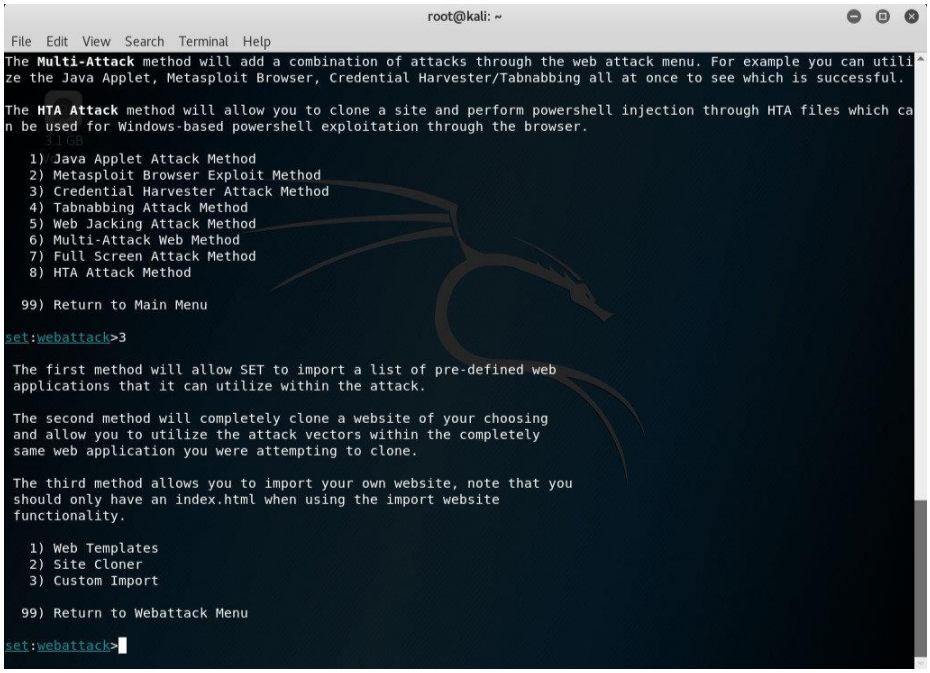
Сам розділ може працювати в декількох напрямках, починаючи від створення і впровадження шкідливих навантажень, масових атак, атак на різні точки Wi-Fi, генерації QR-коду та інше.



Мал. 2. Розділи соціально-технічної атаки в Social-Engineer Toolkit

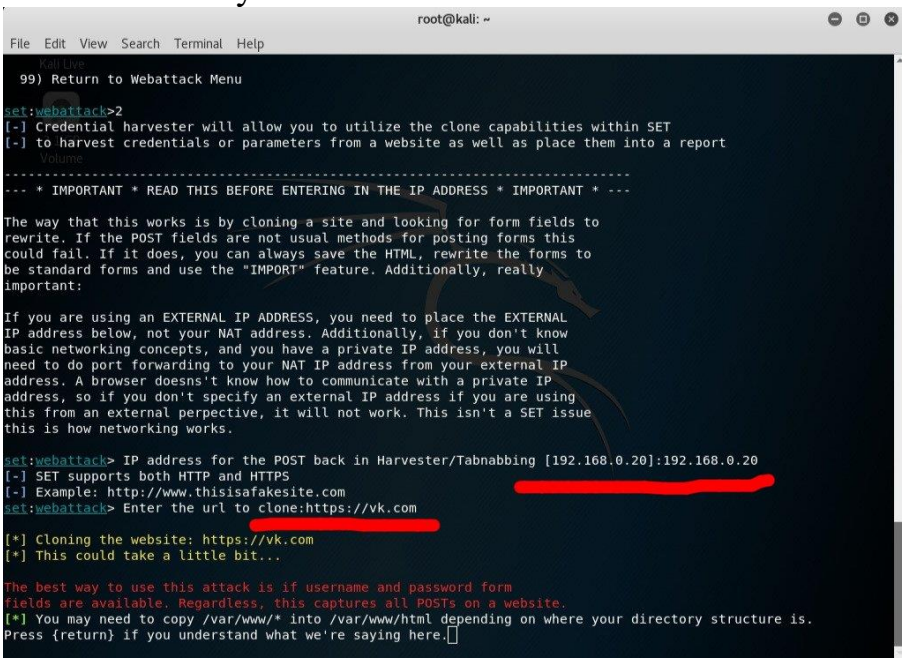
Далі розглянемо, як це працює на практиці.

Припустимо, зловмисникові необхідно зібрати дані про конкретну жертву, дізнатися логіни, паролі та мати доступ до всієї листуванні. Значить, для цього він використовує метод атаки на харвестер (тобто на збір інформації). Кіберзлочинець надходить наступним чином: вибирає пункт Social-Engineering Attacks (Соціально-технічні атаки), потім – Website Attack Vectors (Вектори веб-сайтів), після цього – Credential Harvester Attack Method (Спосіб атаки на харвестер). З'явиться три пункти меню: 1) Шаблони веб сайтів; 2) Клонування сайтів; 3) для користувача імпорт.



Мал. 3. Харвестерні тип вибір вектора атаки

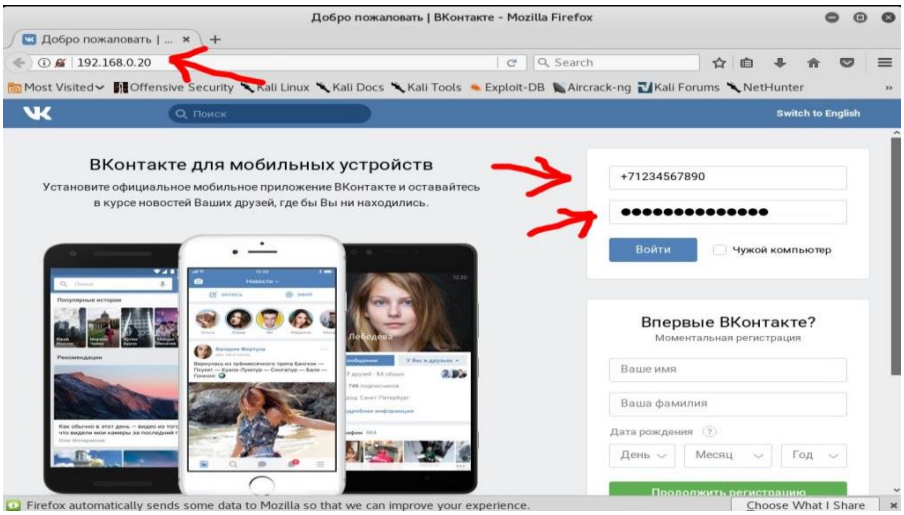
Далі зловмисник дізнається тип своєї мережевої адреси, так Social-Engineer Toolkit знатиме, куди перенаправляти всю зібрану інформацію. Для цього вводиться команда ifconfig. В даному випадку це адреса 192.168.0.20 (IP-адреса, що присвоюється вашому інтерфейсу) - його зловмисник буде клонувати і надалі атакувати. Приклад з соціальною мережею ВКонтакте показаний нижче на малюнку.



Мал. 4. Введення мережевого адреси і клонування сайту для атаки

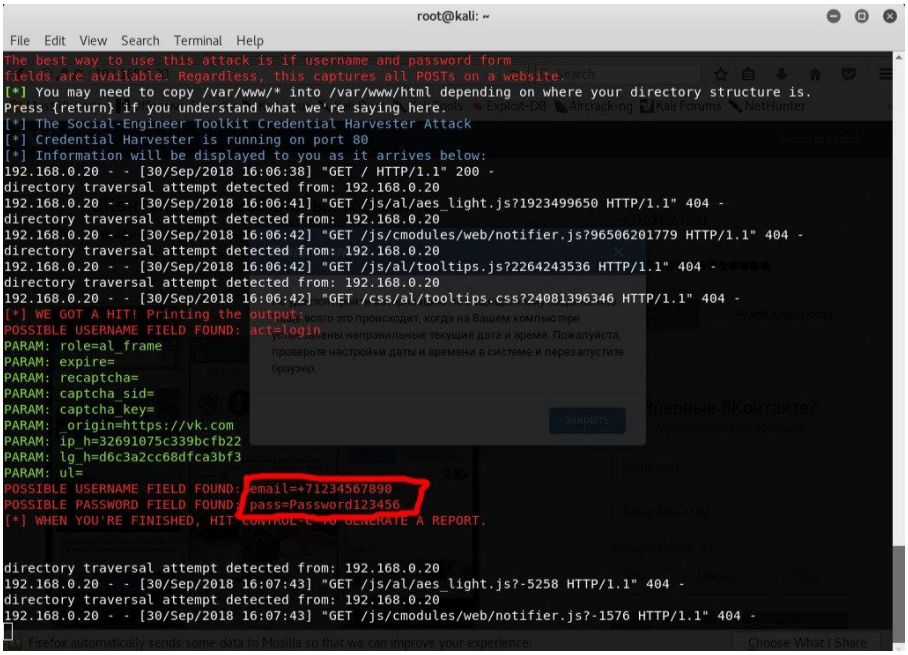
Після завершення конфігурації зловмисник використовує стандартний сервіс для конвертації посилання і відправляє її жертві. Зазвичай

надсилається посилання на фото або цікавий контент від імені друга або колеги. Після переходу за посиланням користувач бачить знайомий інтерфейс. Однак подивившись в адресний рядок, можна звернути увагу, що замість звичного адреси там зазначено той самий 192.168.0.20 Через неуважність багато хто просто не звертають на це увагу і вводять свої логін і пароль.



Мал. 5. Вид підробленої сторінки

Після введення своїх конфіденційних даних система пропонує жертві зайти пізніше, нібито стався якийсь збій або пара логін-пароль не розпізнає. Що ж тим часом бачить зловмисник? Логін і пароль, які ввела жертва. Тим самим він придбав повний доступ і тепер може вводити логін і пароль користувача сервісу, під його профілем входити в його акаунт і здійснювати в ньому все, що захоче.



Мал. 6. Кінцевий результат - зловмисник отримує логін і пароль.

Не виключено, що останні події, пов'язані з витоком персональних даних співробітників Ощадбанку , мали місце завдяки цьому інструменту. Він відмінно підходить для такого типу атаки, і з його допомогою можна також проводити масову розсилку клієнтам Ощадбанку від імені співробітників, чия база вже знаходиться в руках зловмисників. В цілому, Social-Engineer Toolkit - потужний інструмент, яким поки немає рівних. У більш ранніх версіях була функція відправки SMS від імені будь-якого абонента і будь-якої організації, але пізніше розробники відключили модуль. І якби він діяв в даний час, то проникнення в систему було б набагато легше, оскільки SMS-підтвердження як додатковий захист зараз поширене

Метод соціальної інженерії - це тонке мистецтво. Оволодівши їм, можна бути впевненим, що бажаний результат буде отримано в 90-95% - все залежить від кмітливості зловмисника і від підходу до певної жертві. Як правило, на цю вудку трапляються неуважні люди, які не так вимогливі до власної безпеки і рідко звертають увагу на незначні на перший погляд деталі (посилання в браузерному рядку, текст та інше). Слід зазначити, що досвідчені користувачі теж потрапляють на це, хоча і рідше.

Як же уникнути подібних неприємностей? Якщо ви використовуєте соціальні мережі для спілкування, то обов'язково крім введення логіну і паролю використовуйте двофакторну аутентифікацію, тим самим ви створите складність зловмисникові для проникнення в ваш профіль.

Уважно дивіться на посилання в браузерному рядку - як правило, він дуже схожий з оригіналом, різниця в парі букв або цифр. Так що неуважний користувач може і не помітити обману. Завжди краще перевірити ще раз, якщо є можливість: як правило, офіційні сайти справжніх організацій знаходяться на самому першому рядку пошукових систем. Якщо вам прийшла підозріла посилання або прохання від одного, подруги, колеги, то не полінуйтеся зв'язатися з адресатом іншим способом і уточнити, чи він її надіслав. Будьте пильні, бережіть свої дані.

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

ДЕЯКІ АСПЕКТИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ У ДЕРЖАВАХ ЄВРОПЕЙСЬКОГО СОЮЗУ

Без сумніву, можна стверджувати, що інформаційно-комунікаційні технології мають фундаментальний вплив на суспільство. У цьому сенсі можливості "інформаційного суспільства" є важливими для економічного зростання, освіти, конкуренції, комунікації та інформаційного обміну, можливостей мобільності та працевлаштування. Однак суспільство постійно

стикається з загрозою комп'ютерної злочинності і очевидним є те, що загроза повинна розглядатися в рамках глобальної проблеми, яка ставиться перед кримінальним правосуддям усіх країн шляхом розробки та широкого використання нових підходів для вирішення цієї проблеми. Усвідомлюючи цю ситуацію, Рада Європи представила для прийняття в листопаді 2001 року Конвенцію про кіберзлочинність, також відому як "Договір про кіберзлочинність" [1]. Цей договір відкритий для ратифікації світовим загалом, і ратифікований також Сполученими Штатами та ще декількома десятками країн. Договір містить положення, що стосуються як кримінального права, так і кримінально-процесуального законодавства та кримінального розслідування, а також взаємної допомоги при розслідуванні комп'ютерних злочинів. За баченням розробників Договору, вони поділяються на чотири основні категорії:

1) правопорушення проти конфіденційності та цілісності, незаконний доступ, незаконне перехоплення, перешкоджання передачі даних, системне втручання та неправильне використання пристроїв;

2) комп'ютерні правопорушення, такі як підробка та комп'ютерне шахрайство;

3) правопорушення, повязані із змістом контента, зокрема виробництво, розповсюдження та зберігання дитячої порнографії, поширення расистських та ксенофобських ідей;

4) правопорушення, повязані з порушенням авторських і суміжних прав.

Метою Договору є спонукання країн, що його ратифікують, до адаптації свого національного кримінально-процесуального законодавства до технологічних змін, у цьому сенсі Договір містить конкретні процедурні правила. Крім того, в положеннях Договору викладено ряд загальних принципів, що стосуються міжнародного співробітництва, екстрадиції, взаємодопомоги та обміну інформацією. З метою стимулювання міжнародного співробітництва передбачено низку правил щодо видачі підозрюваних за певних умов, а також встановлення інших форм співробітництва у сфері кримінального розслідування та кримінального переслідування за допомогою мережного контакту з доступністю 24/7.

Договір про кіберзлочинність став першим але вже не єдиним важливим міжнародним обов'язковим юридичним інструментом для вирішення питання про кіберзлочинність. 24 лютого 2005 року Рада Європейського Союзу прийняла Рамкове рішення 2005/222 / про кібератаки на інформаційні системи (далі - Рамкове рішення) з метою посилення співпраці між судовими та іншими компетентними органами, у тому числі поліції та інших спеціалізованих правоохоронних органів шляхом наближення національних норм кримінального законодавства у сфері кібератак на інформаційні системи [2]. Рамкове рішення складається з визначень "незаконного доступу", "втручання в дані" та "системного втручання" як кримінального правопорушення. Мета Рамкового рішення полягає у вирішенні значних прогалин та розбіжностей у національних

законодавчих актах, які можуть заважати боротьбі з організованою злочинністю та тероризмом, а також ускладнюють поліцейську та судову співпрацю у сфері боротьби з кібератаками на інформаційні системи.

Що стосується незаконного доступу до інформаційних систем, то Рамкове рішення встановлює, що держави-члени можуть вирішити, що це правопорушення буде здійснюватися лише тоді, коли доступ буде отримано "шляхом порушення заходів безпеки". Крім незаконного доступу, зазначені документи розглядають проблеми спаму, шпигунського програмного забезпечення, загального доступу та прав користувачів.

Напевно, нереально очікувати, що коли-небудь буде консенсус стосовно всіх заходів, необхідних для боротьби з кіберзлочинністю, і ще навіть не реалістичніше чекати, що кіберпростір буде вільним від кіберзлочинності. Хороша новина, однак, полягає в значному прогресі у пошуку загальних шляхів вирішення цього питання, і вони базуються на широкому і всебічному визначенні кіберзлочину. Безумовно, всі проблеми, пов'язані з кіберзлочинністю, ще не були розглянуті або навіть виявлені, але загальне визначення поняття кіберзлочинність та досягнення суттєвої адаптації законодавства є, як мінімум, двома важливими кроками у боротьбі проти цієї все більш важливої нової форми злочинів.

Використані джерела

1. CONVENTION ON CYBERCRIME, European Treaty Series - No. 185, Budapest, 23.XI.2001 . [Електрон. ресурс] / Режим доступу: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf
2. COUNCIL FRAMEWORK DECISION 2005/222/JHA of 24 February 2005. [Електрон. ресурс] /Режим доступу: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32005F0222 On attacks against information systems, Official Journal of the European Union, L 69/67

Міхальский Я.В. - аспірант кафедри кібербезпеки та інформаційного забезпечення;
Форос Г.В. - професор кафедри кібербезпеки та інформаційного забезпечення, кандидат юридичних наук, доцент (Одеський національний університет внутрішніх справ)

СУЧАСНИЙ СТАН ІНФОРМАЦІЙНОЇ ВІЙНИ В УКРАЇНІ

У сучасних умовах проблеми інформаційних воєн та їх протидії актуалізувалися у зв'язку з бурхливим розвитком інформаційних процесів та технологій, що дозволяють експлуатувати інформаційний простір країни, та маніпулювати засобами масової інформації та їх аудиторією.

Виникають все більше і більше інформаційних загроз інтересів людини і громадянина, суспільства та держави, національних інтересів України. Тому

необхідно усвідомити сучасний стан інформаційної війни в Україні її природу і технології інформаційної влади над людьми безконтрольність яких може призвести до знищення громадської думки в країні. А для протидії інформаційної війни необхідно, перш за все, розуміння суті подій, що відбуваються.

В даний час здійснюється інформаційна експансія не тільки в Україні, але і у всьому світі через мережу Інтернет та засоби масової інформації. Україна повинна здійснювати заходи для захисту своїх громадян, своєї культури, традиції і духовних цінностей від чужого інформаційного впливу. Виникає необхідність захисту національних інформаційних ресурсів та збереження конфіденційності інформаційного обміну по світових відкритих мереж, так як на цьому ґрунті можуть виникати політична та економічна конфронтація держав, нові кризи в міжнародних відносинах.

Все частіше громадськість звертає увагу на проблему інформаційної війни, тому що її об'єктом є свідомість людей, її метою – управління і маніпулювання громадською свідомістю та позицією.

Перш за все, інформаційна війна – це 1) дії, початі для досягнення інформаційної переваги шляхом завдання шкоди інформації, процесам, що базуються на інформації і інформаційних системах супротивника при одночасному захисті власної інформації, процесів, що базуються на інформації і інформаційних системах; 2) нефізична атака на інформацію, інформаційні процеси та інформаційну інфраструктуру; 3) найвищий ступінь інформаційного протиборства та спрямована на розв’язання суспільно-політичних, ідеологічних, національних, територіальних та інших конфліктів між державами, народами, націями, класами й соціальними групами шляхом широкомасштабної реалізації засобів і методів інформаційного насильства (інформаційної зброї) [2].

Мета інформаційної війни – послабити моральні і матеріальні сили супротивника або конкурента та зміцнити власні. Вона передбачає вжиття заходів пропагандистського впливу на свідомість людини в ідеологічній та емоційній сферах. Очевидно, що інформаційна війна – складова частина ідеологічної боротьби. Такі війни не призводять безпосередньо до кровопролиття, руйнувань, при їх веденні немає жертв, ніхто не позбавляється їжі, даху над головою.

Аналіз спеціальної літературі, дозволив дійти висновку, що основними завдання сучасних інформаційних війн є: створення атмосфери бездуховності, негативного ставлення до культури та історичної спадщини у суспільстві конкурента чи ворога; маніпулювання громадською думкою і політичною орієнтацією населення держави з метою створення політичного напруження та стану, близького до хаосу; дестабілізація політичних відносин між партіями, об’єднаннями та рухами з метою розпалення конфліктів, стимулювання недовіри, підозри, загострення ворожнечі, боротьба за владу; провокування соціальних, політичних, національно-етнічних і релігійних зіткнень; провокування, застосування репресивних дій з боку влади щодо опозиції; зниження рівня інформаційного забезпечення органів влади та

управління, інспірація помилкових управлінських рішень; уведення населення в оману щодо роботи державних органів влади, підрив їх авторитету, дискредитація їх дій; підрив міжнародного авторитету держави, її співпраці з іншими державами та ніші [4].

Проте слід розрізняти внутрішні та зовнішні інформаційні війни. Внутрішні, як сформулював В.Карпенко – це війни проти свого народу. Головний засіб такої війни – інформаційний ресурс, тобто, використання державних та залежних засобів масової інформації. При цьому стратегічне завдання – ідеологічна обробка населення в інтересах влади та олігархічних кланів. [3, с.291].

На сучасному етапі в інформаційній сфері України триває безперервна війна за збільшення впливу, контролю та управління ресурсами на даній території. Безперервні інформаційні атаки негативно впливають на формування внутрішньо та зовнішньополітичного іміджу країни, а отже на розвиток довірливих партнерських відносин з іншими гравцями на міжнародному полі. Сьогодні ми бачимо, що за умови подальшого збереження неурегульованості правом інформаційних відносин, фактично інформаційне суспільство формує всі передумови для розвитку нового виду тоталітаризму − інформаційного. Якщо, ще кілька років була актуальна теза проте, що перенесення віртуальності та театралізованості, нещирості, яка притаманна інформаційному суспільству, переноситься до реального життя.

Підсумовуючи вищевикладене, стає очевидним, що інформаційний розвиток відкриває широкі можливості для впливу на народи та владу, маніпулювання свідомістю та поведінкою людей навіть на віддалених просторах. Беручи до уваги процес глобалізації інформаційних мереж, що відбувається в світі, можливо припустити, що саме інформаційним видам війн буде відданий пріоритет у майбутньому. Потрібна серйозна увага фахівців різного профілю до цього питання, щоб уникнути найбільш негативних наслідків цієї війни не тільки для України, а і для всього людства.

Використані джерела

1. Інформаційна безпека України [Електронний ресурс] // https://uk.wikipedia.org/wiki/Інформаційна_безпека_України
2. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції [Електронний ресурс] / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. – Режим доступу: https://pidruchniki.com/15800119/politologiya/ponyattya_zmist_zagroz_informatsiyniy_bezpetsi
3. Карпенко В.О. Інформаційна політика та безпека. – К.: Нора-Друк, 2006. – С.291
4. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи / В. Петрик // Юридичний журнал. – 2009. – № 5. – С. 122-134

Мордвинцєв М.В. - провідний науковий співробітник, кандидат технічних наук, доцент;
Хлєстков О.В. - старший науковий співробітник;
Ницюк С.П. - старший науковий співробітник (Науково-дослідна лабораторія захисту інформації та кібербезпеки Харківського національного університету внутрішніх справ)

НАПРЯМОК РОЗВИТКУ СИСТЕМИ АВТОМАТИЗОВАНОГО ВІДЕОДОКУМЕНТУВАННЯ ПЕРЕМІЩЕННЯ ОБ'ЄКТА ДЛЯ ВИРІШЕННЯ ЗАВДАНЬ ПРАВООХОРОННИХ ОРГАНІВ

Запропонована система відеодокументування переміщень об'єкта для вирішення деяких завдань правоохоронних органів з використанням системи геолокації GSM оператора та GPS навігації

Для вирішення деяких завдань які вирішують правоохоронні органи необхідно мати данні о присутності об’єкта в тому чи іншому місці. Наявність мобільного пристрою не дозволяє однозначно ідентифікувати об’єкт. В той же час все частіше для забезпечення безпеки людей на вулицях та в містах великих скупчень людей встановлюються відео камери. Велика кількість камер встановлюється для контролю за дотриманням водіями правил дорожнього руху. Збільшується кількість веб-камер, які встановлюють комерційні організації. Системи відеодокументування переміщень об’єктів дозволяє значно підвищити ефективність роботи правоохоронних органів. Використання систем відеоспостереження в країнах Європейського Союзу та США значно сприяє оперативності реагування на правопорушення, швидкому встановленню осіб, які їх здійснюють, запобігання терористичним актам, пошук свідків правопорушень.

Наявність подібних систем є стримуючим чинником для правопорушника, навіть за відсутності співробітника правоохоронних органів.

На думку поліції, використання систем відеоспостереження в громадських місцях дозволить зменшити кількість правоохоронців на вулицях і при цьому зробить їх роботу більш ефективною. Використання запропонованої системи дозволить правоохоронним органам більш ефективно протидіяти правопорушникам.

Виникла думка пов’язати координати мобільного пристрою з координатами веб камери. Створити систему відеодокументування з використанням системи геолокації GSM оператора та GPS навігації.

В докладі пропонується спосіб відеодокументування за допомогою засобів відео фіксації, при цьому відбувається порівняння координат об'єкта, що має мобільний телефон або GPS навігатор із зоною спостереження

відеокамери, і автоматичне об'єднання фрагментів появи об'єкта в зоні видимості в один відеозвіт.

В даний час є всі технічні можливості для розробки і впровадження системи автоматичного створення відеозвітів (САСВ) за допомогою IP - камер.

Пропонується створення САСВ, в результаті якої правоохоронні органи зможуть отримати автоматично створений відеозапис про діяльність об’єкту спостереження.

САСВ має три складових: система панорамної зйомки, система ближньої зйомки, система індивідуальної зйомки [1].

Система панорамної і ближньої зйомки припускає встановлення IP-камер на вулицях, майданах, в великих будівлях, стадіонах [2]. При цьому встановлюється два види камер: ближньої і дальньої зйомки. Камери далекої зйомки документують панорамну картинку, в яку потрапить об’єкт спостереження, а камери ближньої зйомки виробляють зйомку в зоні своєї видимості на малій відстані. Останні доцільно встановлювати, як на вулицях , так і в приміщеннях.

Для того щоб отримати відео звіт про діяльність об’єкту спостереження правоохоронні органи замовляють цю послугу у мобільного оператора. Вказуючи номер мобільного телефону об’єкта спостереження. Мобільний оператор визначає точне положення об’єкта і сектор спостереження тієї чи іншої IP-камери за певною програмою записує відео фрагмент, коли об’єкт перебуває в зоні зйомки тієї чи іншої камери. Переходячи із зони зйомки від однієї камери до іншої, комп'ютерна програма монтує ці фрагменти в один фільм. Чергування фрагментів камер ближнього спостереження з фрагментами панорамних камер створить більш повне сприйняття переміщень об'єкта. Перемикання на панорамну IP-камеру відбувається при виході об'єкта із зони спостереження ближньої IP-камери.

Система індивідуальної зйомки передбачає доповнення створюваного фільму-звіту фрагментами індивідуальної IP-камери. Для цього особа яка веде спостереження повинна мати IP-камеру якщо існує покриття Wi-Fi, або камеру, сполучену з мобільним телефоном по якому передавати відео потік. При цьому фрагменти індивідуальної IP-камери через засоби мобільного оператора або через Wi-Fi канали зв’язку будуть автоматично вмонтовані у фільм-звіт.

Розглядаються напрямки використання видеофіксації переміщень об’єкта.

Перше це спостереження за об’єктом. Другий напрям це збір доказової бази присутності об’єкта в даному місті в даний час. Яка може бути використана як для звинувачення підозрюваного, так і для його захисту. Третій напрям це пошук свідків подій, які мають мобільні телефони і знаходились в полі зору веб-камери.

Висновки:

Удосконалення системи відеоспостереження дозволяє більш ефективно реалізовувати роботу правоохоронних органів. Система дозволить підвищити

ефективність діяльності поліції.

Система запатентована авторами: Мордвинцев М.В., Машкаров Ю.Г. Спосіб відео документування переміщень об'єкта за допомогою системи відео фіксації. Патент на корисну модель № 73635, 2012, -4 с.

Використані джерела

1. Мордвинцев М.В., Машкаров Ю.Г. Спосіб відео документування переміщень об'єкта за допомогою системи відео фіксації. Патент на корисну модель № 73635, 2012, - 4 с.
2. Мордвинцев Н.В., Усовершенствование систем видеонаблюдения при реализации задач правоохранительных органов. Издательский дом "Интернаука" Международный научный журнал 5 (1), с. 59-61

Нікуліщев Г.І. - старший викладач кафедри захисту інформації;
Гайтота Є. В., Чуницька В.В. - студентки (Запорізький національний технічний університет)

АНАЛІЗ ТА ПЕРСПЕКТИВИ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ У КІБЕРПРОСТОРІ

Згідно з Законом України "Про основні засади забезпечення кібербезпеки України" на Національну поліцію України покладені такі основні завдання: забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі, запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі.

До структури кримінальної поліції Національної поліції входить Кіберполіція – міжрегіональний територіальний орган, який забезпечує реалізацію державної політики в сфері протидії кіберзлочинності, завчасне інформування населення про появу нових кіберзлочинців, впровадження програмних засобів для систематизації кіберінцидентів тощо.

З розвитком технологій підвищується і рівень кіберзагроз, все частіше зловмисники діють у кіберпросторі. Для оперативного реагування на реалізацію загроз та їхнього упередження на базі Департаменту кіберполіції Національної поліції України поступово впроваджуються новітні технології та сервіси.

Так, у 2017 році створено цілодобовий «call-центр» для прийому заяв та звернень від громадян про злочини та правопорушення, що вчиняються в глобальній мережі. Протягом року до Кіберполіції по допомогу вже звернулось 9817 громадян. 90% з цих звернень вже розглянуто та опрацьовано Кіберполіцією в межах своєї компетенції та не пізніше ніж за три години після надходження. Важливо зауважити, що при надходженні інформації, що не належить до компетенції Кіберполіції, вона автоматично

перенаправляється до лінійного підрозділу поліції. На майбутнє, для охоплення ширшої аудиторії та виявлення кіберзлочинів, заплановано включення «call-центру» Кіберполіції в єдину мережу «call-центрів» Національної поліції України.

Також на сайті Кіберполіції громадяни, за допомогою інформаційного антишахрайського майданчика "stop fraud", мають змогу в режимі онлайн ознайомитися з поширеними випадками шахрайства, повідомити інформацію щодо шахраїв, вчасно не допустити списання або втрати грошей зі свого рахунку та оперативно заблокувати незаконно проведену транзакцію.

При виникненні загрози масових кібератак представники Кіберполіції інформують населення про заходи убезпечення та протидії, до яких громадяни можуть вдатися, через прес-релізи, виступи та публікації у ЗМІ.

Таким чином, Кіберполіція активно працює і впроваджує нові шляхи оперативного реагування на кіберзлочини. Спектр роботи Департаменту досить широкий, адже поліцейські займаються боротьбою з вірусами, DDoS-атаками, спамом, шахрайством з банківськими системами і крадіжкою особистих даних тощо. Крім того, відстежують поширення неправомірного матеріалу і нейтралізують піратський контент.

Аналізуючи діяльність Кіберполіції, можна дійти висновку, що для громадян посилився рівень безпеки у віртуальному просторі, а в перспективі користуючись інтернетом і його можливостями, українці зможуть отримувати допомогу поліцейських в режимі реального часу.

Тим не менш, експерти вважають, що розбудова Департаменту ще не дійшла до фінального етапу, він поки що не забезпечує свого представництва на достатньому рівні, а його обмежений складне має можливості реалізовувати всі визначені законом функції. Зокрема і тому повноваження Національної поліції у сфері захисту інформації в перспективі навряд чи зміняться [1, с. 1].

Втім, на тлі гібридної війни, яку змушена вести Україна, подекуди виникають спроби наділити силові органи непритаманними їм функціями. Так, 21 червня 2018 року Верховна Рада України включила в порядок денний законопроект №6688 "Про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері" авторства окремих депутатів. Цей законопроект, зокрема, впроваджує механізми тимчасового блокування сайтів, зобов'язує провайдерів встановлювати технічні засоби обмеження доступу та передбачає високі штрафні санкції, включно з кримінальною відповідальністю, за невиконання вимог блокування.

Спираючись на думку Головного науково-експертного управління Верховної Ради України, до явних недоліків законопроекту можна віднести занадто широке визначення підстав для обмеження доступу до веб-сайтів, відсутність належних механізмів контролю за діями уповноважених органів та їх представників, гарантій захисту прав людини, граничних термінів тимчасового блокування веб-сайтів, не повна узгодженість з Конституцією України та іншими законодавчими актами, а також з міжнародно-правовими

зобов'язаннями України [2, с. 2-3].

На думку авторів, прийняття цього проекту як Закону видається малоймовірним, враховуючи його недоліки та попередню кількість невдалих спроб внесення його до порядку денного сесії Верховної Ради України.

Натомість, варто зосередитись на втіленні положень Стратегії розвитку системи Міністерства внутрішніх справ України до 2020 року, зокрема в частині підвищення ефективності роботи і взаємодії через максимальне використання інформаційно-комунікаційних технологій у реалізації завдань органами системи МВС та розвиток кадрового потенціалу та соціального захисту працівників.

Використані джерела

1. Закон і бізнес: Кіберзахист для обраних [Електронний ресурс]: Закон і бізнес 15.06.2018. – Режим доступу: http://zib.com.ua/ua/print/133258-rozdollyu_informaciynih_zlochiniv_zakon_pro_kiberbezpeku_ne_.html

2. Висновок на проект Закону України «Про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері» [Електронний ресурс]: Верховна Рада України 05.09.2018. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id= &pf3511=62236&pf35401=462812

Охрименко С.А. – доктор экономических наук, профессор;
Борта Г.Р. – кандидат экономических наук (Лаборатория информационной безопасности Молдавской Экономической Академии)

КРИМИНАЛЬНЫЕ ГРУППЫ В ТЕНЕВОЙ ЦИФРОВОЙ ЭКОНОМИКЕ

В докладе предпринята попытка рассмотрения, в первую очередь, связи традиционной «классической» организованной преступности с продуктами и услугами теневой цифровой экономики (ТЦЭ). На вопрос – «Использует ли преступность информационные и коммуникационные технологии в своей деятельности?» - ответ будет положительным. Защищенные средства коммуникаций, цифровая подпись, стеганография, технологий отмывания преступных доходов – все это далеко не полный перечень используемых информационных и коммуникационных технологий. Кроме того, именно представители данных групп являются первыми покупателями и распространителями продуктов и услуг ТЦЭ.

Противостояние в рамках криминальной экономики и правоохранительными органами в области информационных и коммуникационных технологий началось со смены парадигмы – когда

действия одиночек были направлены на извлечение прибыли в результате разработки специальных программ, компьютерных манипуляций и т.д.[1,2,3]. Появление на ранних этапах зловредных и разрушающих программных злоупотреблений привело к формированию рынка компьютерных вирусов, червей, троянских коней, репликаторов и т.д. С расширением научной базы исследований стали появляться комплексные механизмы воздействия на ресурсы информационных систем криминальной направленности (например, концепция GRID-систем переросла в концепцию создания бот-систем). Постепенно происходило переливание новых знаний в области организации информационно-вычислительного обслуживания в среду криминальной направленности. Определенное влияние на данный процесс оказали специальные органы государственной власти, которые разрабатывали соответствующие механизмы воздействия в условиях противостояния между государствами.

Действенным примером использования информационных и коммуникационных технологий, системы SWIFT, судов различных уровней, является операция, получившая название «Ландромат» [5]. Следует отметить, что подобная схема была реализована в Болгарии, Сербии, Прибалтийских странах, Украине, России и затронула Национальные и коммерческие банки, Правительства и судебную систему. Все это должно стать предметом дальнейших углубленных исследований общественности и правоохранительных органов.

Считаем возможным предложить для анализа новую схему организации ТЦЭ с точки зрения криминальной направленности. Следует выделить несколько групп горизонтальной направленности: наука и научная деятельность, собственно разработчики, распространители криминальных продуктов и услуг, реализаторы криминальных действий (программ и услуг) в соответствии с требованиями заказчиков, дополнительные действия, обеспечивающие отмывание денежных средств и т.д.

Выделяются следующие виды финансово-ориентированных киберпреступлений: фишинг, кибервымогательство, финансовое мошенничество, киберпреступления, связанные с вторжением в личную жизнь, кража персональных данных, шпионаж, нарушение авторского права, спам, социальные и политические мотивированные киберпреступления, преступления на почве ненависти и домогательства, кибербуллинг, киберпреступления, связанные с недозволенными действиями, противозаконная порнография, груминг, распространение наркотиков и оружия и др.

Следует обратить внимание на последний отчет «Рынок преступных киберуслуг» [6], подготовленный Positive Technologies и «Актуальные киберугрозы. I квартал 2018 года» [7]. Была дана оценка минимальной и средней стоимости различных инструментов и услуг, которые продаются на площадках DarkWeb. Так, например, взлом сайта с получением полного контроля над веб-приложением обойдется злоумышленнику всего в 150 $, а стоимость целевой атаки на организацию в зависимости от сложности может

превысить 4500 $. Наиболее дорогим оказалось вредоносное программное обеспечение (ВПО) для проведения логических атак на банкоматы. Цены на подобное готовое вредоносное программное обеспечение этого класса начинаются от1500$.

На рынке преступных киберуслуг широко распространены криптомайнеры (20%), хакерские утилиты (19%), ВПО для создания ботнетов (14%), RAT (Remote Access Trojans, троянские программы для удаленного доступа) и трояны-вымогатели (доля каждого — 12%), а основным спросом закономерно пользуются услуги, связанные с разработкой и распространением ВПО (55%).

Проведенное исследование показало, что спрос на услуги по созданию ВПО на сегодняшний день превышает предложение в три раза, а по его распространению — в два раза. Такое положение дел позволяет говорить о востребованности среди киберпреступников новых инструментов, которые становятся все доступнее благодаря партнерским программам, сервисам по аренде ВПО и моделям распространения «как услуга». Как сообщают эксперты, большая часть запросов на взлом в DarkWeb имеет отношение к поиску уязвимостей на сайтах (36%) и получению паролей от электронной почты (32%). Среди предлагаемых услуг лидируют взлом учетных записей социальных сетей (33%) и электронной почты (33%). Аналитики Positive Technologies связывают эти данные с желанием одних людей получить доступ к переписке других. С другой стороны, эти взломы меньше других требуют от атакующего каких-либо технических навыков [8].

В соответствии с Глобальным прогнозом [9], ожидается, что размер рынка кибербезопасности вырастет с 138 млрд. в 2017 году, до 232 млрд. дол. США к 2022 году, а нехватка рабочих мест в области кибербезопасности - одна из самых серьезных проблем, с которыми будут сталкиваться предприятия.

Использованные источники

1. Машевский Ю. CrimeWare: новый виток противостояния. сайт [Електрон. ресурс] / Режим доступу: URL: http://www.infosecurity.ru/_gazeta/content/100430/exp1.shtml
2. 4 наиболее распространенные формы киберкриминала. сайт [Електрон. ресурс] / Режим доступу: URL: https://www.securitylab.ru/analytics/490171.php
3. IDC впервые посчитала, сколько в России платят за исследования киберкриминала сайт [Електрон. ресурс] / Режим доступу: URL: http://www.cnews.ru/news/top/2017-03-07_idc_vpervye_poschitala_skolko_v_rossii_platyat
4. Кибербандиты в России и мире. сайт [Електрон. ресурс] / Режим доступу: URL: http://www.banki.ru/news/daytheme/?id=7243229.
5. The Russian Laundromat. сайт [Електрон. ресурс] / Режим доступу: URL: https://www.rise.md/english/the-russian-laundromat/
6. Рынок преступных киберуслуг 2018. сайт [Електрон. ресурс] / Режим доступу: URL:https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Darkweb-2018-rus.pdf
7. Актуальные киберугрозы I квартал 2018 года. [Електрон. ресурс] / Режим доступу: URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2018-Q1-rus.pdf
8. Рынок преступных киберуслуг: спрос втрое превышает предложение сайт [Електрон. ресурс] / Режим доступу: URL: https://www.anti-malware.ru/news/2018-07-25-1447/26944

9. How to Make More Money as a Cybersecurity Expert. https:// сайт [Електрон. ресурс] / Режим доступу: URL: i. medium.com/polyswarm/how-to-make-more-money-as-a-cybersecurityexpert.html

Прокопов С.О. - старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ПРОБЛЕМИ ПІДГОТОВКИ ФАХІВЦІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ ЗА ІНФОРМАЦІЙНИМ НАПРЯМОМ У НАВЧАЛЬНИХ ЗАКЛАДАХ СИСТЕМИ МВС

Уміння знаходити необхідну інформацію, робити аналітичні висновки на підставі зібраної інформації та використовувати їх для вирішення службових завдань є вкрай необхідним навиком працівників будь-яких підрозділів Національної поліції. Отримання знань та особливо практичних навичок роботи з інформаційними потоками є одним з важливих завдань у підготовці фахівців Національної поліції. Проблемам, пов'язаним з підготовкою поліцейських за інформаційним напрямом, приділяли багато науковців, а саме О.М. Бандурка, В.Г. Хахановський, В.М. Струков та інші.

Найголовнішою проблемою інформаційної підготовки курсантів та слухачів навчальних закладів системи МВС є повна відсутність доступу до реальних інформаційних баз даних Інформаційного порталу Національної поліції (за виключенням НАВСУ). Вона не має позитивного вирішення на протязі багатьох років незважаючи на розуміння керівництва МВС про необхідність усунення цієї проблеми. Все це є основною вадою у набутті практичного досвіду використання відомчих інформаційних ресурсів курсантами, слухачами-заочниками, практичними працівниками, які направляються у ВНЗ на курси підвищення кваліфікації на строк до одного місяця.

Викладачі кожного з навчальних закладів пробують самотужки розробити хоч-якісь емулятори інформаційно-телекомунікаційних систем Національної поліції. Так викладачі кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ розробили та впровадили у навчальний процес емулятор інформаційної системи «ЦУНАМІ», який став інформаційно-технічною платформою [1] навчально-ділової гри «Лінія 102». Цей новітній метод практичної підготовки майбутніх правоохоронців у теперішній час керівництвом Національної поліції впроваджений у всіх відомчих поліцейських навчальних закладах.

Відсутність можливості роботи з реальними інформаційно-пошуковими системами Національної поліції вимушує викладачів впроваджувати у навчальний процес інші способи отримання інформації,

наприклад в Дніпропетровському державному університеті внутрішніх справ в дисципліні «Інформаційне забезпечення професійної діяльності» впроваджена тема «Пошук інформації з відкритих джерел мережі Інтернет» [2]. У 2018 році впроваджена нова тема «Основи аналітичної діяльності», у якій розглядаються основні методики аналітики, курсанти та слухачі вчаться працювати з однією з найкращих аналітичних програмних комплексів IBM i2 Analyst's Notebook [3].

Отримання курсантами та слухачами Дніпропетровського державного університету внутрішніх справ навичок щодо пошуку інформації з відкритих джерел Інтернету та роботі з аналітичними оболонками є необхідними, але вони можуть тільки доповнювати уміння з використання основних баз даних Інформаційного порталу Національної поліції.

Підводячи підсумок доповіді. Хочеться в котрий раз зазначити, що тільки після під'єднання поліцейських навчальних закладів до інформаційних систем Національного порталу, значно покращиться рівень підготовки правоохоронців за інформаційним напрямом.

Використані джерела

1. Гавриш О.С., Махницький О.В., Прокопов С.О. Інформаційно-технічна платформа інтерактивного комплексу з підготовки здобувачів вищої освіти та практичних працівників Національної поліції в ДДУВС/ Наукова стаття. Науковий журнал Право і суспільство. – 2017. – № 1-1. – с. 128–141.
2. Прокопов С.О. Використання пошуку інформації з відкритих джерел мережі Інтернет у навчальному процесі Дніпропетровського державного університету внутрішніх справ. 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.
3. Краснобрижий І.В.. Прокопов С.О., Рижков Е.В. Інформаційне забезпечення професійної діяльності / Навчальний посібник – Дніпро: Дніпропетровський державний університет внутрішніх справ, 2018. – 218 с.

Проценко О.О. - викладач кафедри кримінального процесу Одеського державного університету внутрішніх справ, кандидат юридичних наук

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ СЛІДЧИХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

За останні роки розвитку українського суспільства рівень злочинності значно зростає, а також удосконалюється засоби та способи скоєння правопорушень. Значного поширення набула злочинність з міжрегіональними та міжнародними зв'язками, що потребує систематизації значних масивів інформації, здобутої з різноманітних джерел. Більша

кількість злочинців мають суттєву підготовку, використовують для вчинення злочинів сучасні інформаційні технології та телекомунікаційні засоби. При цьому злочинність швидко пристосовується до методів боротьби з нею, зокрема, шляхом активної протидії оперативно-розшуковим заходам, гласним та негласним слідчим (розшуковим) діям. Водночас інформаційно-аналітичне забезпечення слідчих підрозділів Національної поліції України, підрозділів кримінальної поліції потребує правового врегулювання на законодавчому та відомчому рівні.

У сучасних умовах передове місце у боротьбі зі злочинністю, займають інформаційні технології. Інформаційно-аналітичні системи, як у США, так і в більшості інших розвинутих країн є джерелом необхідної інформації для детективів та значним ресурсом економії часу. В Україні навіть за умови отримання оперативно значимої інформації, оперативні та слідчі підрозділи практично позбавлені можливості ефективного застосування оперативно-розшукового потенціалу через невиправдано ускладнену процедуру отримання дозволу як на НС(Р)Д так і на оперативно-розшукові заходи. Порядок отримання дозволу на проведення ОРЗ та НС(Р)Д, займає такий проміжок часу, що часто відпадає сама доцільність такого заходу. Нажаль, після останніх змін до КПК України тільки проблемних питань у слідчих побільшало.

Проаналізувавши, наукові надбання вчених необхідно зазначити, що актуальність використання інформаційних технологій зростає й у зв'язку з інтенсивним впровадженням у діяльність слідчих підрозділів Національної поліції України (далі – НП України) засобів комп'ютерної техніки. Цей процес впливає на організацію розслідування кримінальних правопорушень, методичне забезпечення працівників НП України, а здійснення автоматизованого пошуку відомостей щодо будь-яких об'єктів (осіб, предметів, подій) сприяє науково-організаційної праці, оптимізує збирання, зберігання, систематизацію та аналіз доказової інформації. Для вирішення питання щодо негласних слідчих (розшукових) дій нині накопичений чималий досвід застосування новітніх технологій у процесі попередження, виявлення та розслідування злочинів, розшуку підозрюваного та обвинуваченого, провадження окремих слідчих (розшукових) дій, здійснення судових експертиз [1]. Інформаційно-аналітичне забезпечення в діяльності підрозділів досудового розслідування Національної поліції України посідає дуже важливе місце та є комплексом організаційних, правових, технологічних засобів, які забезпечують процес збирання, отримання, обробки, поширення, аналізу та використання інформаційних ресурсів, необхідних для виконання визначених чинним законодавством завдань та функцій цих органів. В рамках інформаційно-аналітичної діяльності поліції органи досудового розслідування відповідно до чинного КПК України, Положення про ведення Єдиного реєстру досудових розслідувань, затвердженого наказом Генеральної прокуратури України від 06.04.2016 р. № 139, Інструкції про порядок ведення єдиного обліку в органах поліції заяв і повідомлень про вчинені кримінальні правопорушення та інші події,

затвердженої Наказом МВС України від 06.11.2015 № 1377, повинні вносити відповідну інформацію, що пов’язана із формуванням та веденням Єдиного реєстру досудових розслідувань (ЄРДР). ЄРДР це створена за допомогою автоматизованої системи електронна база даних, відповідно до якої здійснюється збирання, зберігання, захист, облік, пошук, узагальнення даних, які використовуються для формування звітності, а також надання інформації про відомості, внесені до Реєстру. ЄРДР утворено та ведеться відповідно до вимог КПК України з метою забезпечення: єдиного обліку кримінальних правопорушень та прийнятих під час досудового розслідування рішень, осіб, які їх учинили, та результатів судового провадження; оперативного контролю за додержанням законів під час проведення досудового розслідування; аналізу стану та структури кримінальних правопорушень, вчинених у державі [2].

Відповідно до положень ст. 2 Закону України «Про захист персональних даних» від 01.06.2010 № 2297-VI, персональні дані це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Так, у ст. 32 Конституції України зазначено, що ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки.

Керуючись положеннями Конституції України, КПК, у необхідних випадках, пов'язаних із таємницею приватного життя осіб, слідчий, прокурор попереджає учасників кримінального провадження, яким стали відомі відомості досудового розслідування у зв'язку з участю в ньому про їх обов'язок не розголошувати такі відомості, а також роз'яснює наслідки незаконного їх розголошення. Таким чином, таємниця досудового розслідування це важлива умова встановлення істини, а в багатьох випадках є передумовою захисту сфери особистого життя людей, які стали учасниками процесу. Тому забезпечення нерозголошення даних кримінального провадження є як однією з гарантій установлення істини, так і захисту прав і свобод людини.

Кримінальна відповідальність слідчих Національної поліції України за вчинені ними діяння, що призвели до порушень прав і свобод людини, пов’язаних з обробкою інформації передбачена Розділом XVI Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку КК України (наприклад, частиною 1 статті 361- 2, передбачена кримінальна відповідальність за несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації; частиною 1 статті 362 Кримінального кодексу України – несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електроннообчислювальних машинах (комп'ютерах),

автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї) [2].

Технічне забезпечення слідчих підрозділів НП України є актуальним з огляду на новації, що містяться в положеннях КПК України, які закріплюють сучасні інструменти для боротьби зі злочинністю та застосування яких повинно чітко відповідати вимогам чинного законодавства. В України вже накопичено чималий досвід використання різноманітних інформаційних та інформаційно-телекомунікаційних систем оперативно-розшукового та інформаційно-довідкового призначення. Наказом НП України від 30 грудня 2015 р. № 228 створено Департамент інформаційної підтримки та координації поліції (далі – ДІПКП) «102» НП України, який організовує та здійснює передбачені законодавством України заходи, спрямовані на інформаційно-аналітичне та інформаційно-пошукове забезпечення правоохоронної діяльності й захист персональних даних під час їх обробки у структурних підрозділах апарату НП України. ДІПКП визначає основні напрями діяльності поліції у сфері інформатизації, здійснює інформаційно-пошукову та інформаційно-аналітичну роботу, бере участь у розроблені проектів нормативно-правових актів МВС із питань, що належать до компетенції поліції та стосуються інформаційно-аналітичного забезпечення, а також оброблення персональних даних в органах і підрозділах поліції. За допомогою комп’ютерної техніки не тільки раціоналізуються інформаційні процеси, але й упроваджуються комп’ютеризовані системи підтримки прийняття слідчими, експертами, оперативними співробітниками, суддями відповідних рішень.

Отже, впровадження та використання нових інформаційно-комунікаційних технологій є головною умовою покращення роботи щодо встановлення підозрюваного або його розшуку, а також діяльності підрозділів НП України та функціонування правоохоронної системи загалом. При цьому є проблеми фінансового забезпечення, низький рівень володіння співробітниками відповідними інформаційними ресурсами та навичками роботи з новою технікою або новими системами. У нинішніх умовах швидкого технічного процесу кожен працівник НП України повинен бути прогресивним користувачем інформаційно-комунікаційних технологій. Крім того, слідчим НП необхідно проходити курси підвищення кваліфікації з метою отримання нових знань, умінь і навичок під час застосування в повсякденній роботи інформаційних технологій.

Використані джерела

1. Інформаційно-аналітичне забезпечення діяльності підрозділів кримінальної поліції : збірник наукових статей за матеріалами доповідей Всеукраїнської науково-практичного семінару 23 березня 2018 року / упорядники А.В. Баб'як, В.В. Сеник, Т. В. Магеровська /. – Львів: ЛьвДУВС, 2018. – 209 с.
2. Рогатюк І.В. Використання інформаційних технологій у досудовому розслідуванні: сучасний стан і перспективи розвитку / І.В. Рогатюк // Науковий вісник Національної академії внутрішніх справ. – 2013. – № 3. – С. 312–320.
3. Інформаційні технології / Вікіпедія [Електронний ресурс]. – Режим доступу :

https://uk.wikipedia.org/wiki.
4. Інформатика : [навч. посібник] / [А.Ю. Гаєвський]. – 2-ге вид., доповн. – К. : «Видавництво А.С.К.», 2007. – 512 с. 4.
5. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України : [монографія] / Б.А. Кормич. – О. : Юридична література. – 2003. – 271 с. 5.
6. Іщенко П.П. Інформаційне забезпечення слідчої діяльності : [науково-практичний посібник] / П.П. Іщенко ; під ред. Є.П. Іщенко. – М.: Юрлитинформ, 2011. – 168 с.
7. Тертышник В.М. Уголовный процесс. Издание 3-е дополненное и переработаное. – Харьков, 2000.
8. Перспективні інформаційні технології у правовій сфері. М., 1993. С. 76-134.Глава II. Наука кримінального процесу.

Рибальченко Л.В. - доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат економічних наук, доцент

ВПЛИВ ІНФЛЯЦІЙНИХ ПРОЦЕСІВ НА ФІНАНСОВУ БЕЗПЕКУ ДЕРЖАВИ

Однією з актуальних проблем, яка впливає на економічний розвиток України є інфляція, яка не залишає осторонь жодного українця, підприємця, галузь, промисловість, державу. Особливістю інфляції виступають проблеми, пов'язані з зайнятістю населення, матеріальним та духовним станом. Немає жодної країни в світі, яка б не зазнала втрат від інфляції.

Безпека країни залежить від таких чинників, як стан грошово-кредитної системи країни, дефіциту бюджету, державного боргу країни, бюджетної, податкової та інфляційної політики тощо. Тому зменшення рівня інфляції, зростання рівня життя населення та зміцнення фінансової безпеки держави є актуальним і важливим питанням сьогодення.

Зниження рівня інфляції та її керованість виступають основними напрямами державного регулювання антиінфляційної політики. Існує широкий набір заходів, які використовується для зменшення інфляції в грошово-кредитних, бюджетних, податкових установах в політиці доходів тощо.

Однією з основних причин високої інфляції є суттєве перевищення внутрішнього попиту над пропозицією, зростання грошової маси і об'ємів кредитування, підвищення ціни на продукти харчування, енергоресурси та інші товари, що викликає знецінення коштів суб'єктів господарювання та населення.

Розглядаючи соціальний аспект фінансової безпеки, варто враховувати і додаткові фактори, що періодично можуть виникати у країні (заборгованість із заробітної плати, пенсій, стипендій, інших соціальних виплат) і обумовлюють соціальну напруженість у суспільстві [1].

Для стабілізації економіки необхідно застосовувати методи

антиінфляційної політики. Одним з факторів, який впливає на стан грошово-кредитної політики є рівень доларизації грошового обігу, високе значення якого вказує на залежність економіки країни від коливань курсу іноземної валюти. Рівень інфляції впливає на стан внутрішньої стабільності країни.

Аналіз рівня безпеки грошово-кредитного сектору в Україні засвідчив, що на даний час існує безліч недоліків у проведенні монетарної політики, а саме: надмірна питома вага готівки в грошовому обігу, зменшення обсягів довгострокового кредитування, високий рівень доларизації тощо.

Для підвищення міжнародної конкурентоспроможності України необхідно створити заходи щодо регулювання інфляції, які забезпечать економічну та соціальну стабільність в країні. Рівень інфляції додатне залежить від вартості банківських кредитів та рівня тіньової економіки. Так як в державі протягом багатьох років спостерігалась тенденція щодо зростання рівня тінізації економіки, висока вартість банківських кредитів, то ці фактори виступають одними з основних показників загрози фінансової безпеки України.

Проведене дослідження показало, що індекс інфляції з кожним роком зростає через незбалансованість державних доходів та витрат, наявність дефіциту бюджету, широке використанням внутрішніх запозичень з метою покриття бюджетного дефіциту, що призводить до збільшення грошової маси в обігу, а отже й стимулює підвищення цін. Тому фінансова безпека держави є важливою складовою національної безпеки, яка на протязі багатьох років знаходиться на дуже низькому рівні завдяки впливу низки дестабілізуючих факторів, що призводять її до такого стану, а саме: високий рівень тіньової економіки, недовіра населення до банківської системи, низький рівень інвестиційної, макроекономічної, інноваційної, демографічної, зовнішньоекономічної, соціальної та енергетичної безпеки [2]. Для зміцнення фінансової безпеки України необхідно вживати стратегічні заходи на державному рівні, які мають бути спрямовані на стабілізацію економіки країни, у тому числі і шляхом вдосконалення законодавчої бази.

Використані джерела

1. Офіційний сайт Державної служби статистики України [Електронний ресурс]. – Режим доступу:: www.ukrstat.gov.ua

2. Рядно О.А., Рибальченко Л.В. Антиінфляційна політика фінансової безпеки держави // Вісник економічної науки України. – 2016. - №2(31). – С. 161-166.

Рудий Т.В. – професор кафедри інформатики, кандидат технічних наук, доцент;
Магеровська Т.В. – доцент кафедри, кандидат фізико математичних наук, доцент;
Сеник С.В. – науковий співробітник відділу організації наукової роботи, здобувач кафедри адміністративно-правових дисциплін (Львівський державний університет внутрішніх справ)

ОКРЕМІ АСПЕКТИ ПРОВЕДЕННЯ АНАЛІЗУ РИЗИКІВ ПІД ЧАС ПОБУДОВИ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Проведення аналізу ризиків є важливою частиною етапу розробки політики безпеки, яка є невід'ємною частиною підготовчого етапу побудови комплексних систем захисту інформації [1-3].

Проведення аналізу ризиків має на меті: 1) дослідити моделі загроз ресурсам інформаційної системи; 2) дослідити моделі порушників та наслідки, які можуть настати в результаті реалізації потенційних загроз (тобто, визначити рівень заподіяної шкоди); 3) визначити моделі, які можна буде застосувати для побудови системи захисту інформації.

У процесі проведення аналізу ризиків необхідно виконати наступні дії:

1. *Визначити складові інформаційно-телекомунікаційної системи та інформаційні ресурси, які будуть захищатися.* Тут мають бути визначені критичні точки з погляду безпеки інформації, складові і ресурси інформаційно-телекомунікаційної системи, на які може здійснюватися атака або які самі по собі становлять загрозу порушення безпеки (об'єкти захисту). З цією метою можуть бути використані відомості п. 3 додатку [3], отримані за результатами дослідження середовища функціонування інформаційно-телекомунікаційної системи.

2. *Провести ідентифікацію загроз безпеці інформації з об'єктами захисту*. Під час цього встановлюється відповідність моделі загроз безпеці інформації та об'єктів захисту, тобто складається таблиця «складова (ресурс) інформаційно-телекомунікаційної системи – можливі загрози». У даній таблиці кожній складовій (ресурсу) має бути зіставлений опис потенційного впливу загрози. Внаслідок створення таблиці можливе уточнення списку загроз і об'єктів захисту, що може спричинити коригування моделі загроз.

3. *Оцінити ризики.* Під час цього етапу слід оцінити гранично допустимий та реальний (існуючий) ризики виникнення кожної із загроз упродовж певної тривалості часу, тобто ймовірності її здійснення упродовж цього інтервалу. З метою оцінки ймовірності здійснення загрози слід розглянути кілька градацій (ступенів). При цьому слід вважати, що кожна подія є найгіршим варіантом з огляду захисту інформації. Практично для

основної кількості загроз немає змоги одержати достовірні дані про ймовірність їх настання, тому доводиться обмежуватися окремими показниками. У таких випадках величина ймовірності виникнення загрози розраховується у кожному окремому випадку емпіричним чи експертним шляхом, з врахуванням практичного досвіду експлуатації таких чи подібних інформаційно-телекомунікаційних систем. Оцінка ризиків може приймати смислове (наприклад, низька, середня висока, дуже висока ймовірність реалізація загрози) або числове значення. Так чи інакше, у кожному з випадків ризик не має перевищувати гранично допустиму величину. Якщо ж він перевищує її, то у такому випадку слід запроваджувати додаткові методи, заходи чи засоби захисту. Також рекомендується розробити заходи щодо зниження ймовірності виникнення загроз та величини ризиків.

4. *Оцінити величину можливих збитків, які можуть настати внаслідок реалізації загроз*. У даному випадку аналогічно виконується якісна або числова оцінка нанесеної шкоди, яка може настати внаслідок реалізації загроз в інформаційно-телекомунікаційній системі. Бажано, щоб дана оцінка у сукупності враховувала розмір очікуваної шкоди від втрати інформацією кожної із властивостей (цілісності, доступності, конфіденційності тощо) або від втрати внаслідок загрози управління інформаційно-телекомунікаційною системою. Під час даного оцінювання можна використовувати ті ж методи, що і під час аналізу ризиків. Величина завданої шкоди може визначатися як розміром фінансових втрат, так і за якісними показниками (наприклад, завдана шкода низька, середня, висока тощо).

5. *Провести вибір способу побудови комплексної системи захисту інформації.* Враховуючи ступінь секретності чи рівень конфіденційності інформації, яка опрацьовується в інформаційно-телекомунікаційній системі, рівня її критичності, величини шкоди, яка може бути завдана внаслідок реалізації загроз, фінансових та інших матеріально-технічних ресурсів, які є у власника інформаційно-телекомунікаційної системи тощо, проводиться обґрунтування щодо доцільності вибору варіанту побудови комплексної системи захисту інформації. При цьому можливий один із трьох варіантів:

- забезпечення необхідного рівня захисту інформаційних ресурсів за мінімальних фінансових та матеріальних затратах і допустимого рівня обмежень на способи їх опрацювання в інформаційно-телекомунікаційній системі;
- забезпечення необхідного рівня захисту інформаційних ресурсів при допустимих фінансових та матеріальних затратах і заданого рівня обмежень на способи їх опрацювання в інформаційно-телекомунікаційній системі;
- забезпечення максимального рівня захисту інформаційних ресурсів за необхідних фінансових та матеріальних затратах і мінімального рівня обмежень на способи їх опрацювання в інформаційно-телекомунікаційній системі.

Якщо в інформаційно-телекомунікаційній системі опрацьовується інформації, яка складає державну таємницю, то у такому випадку слід

використовувати останній варіант побудови комплексної системи захисту інформації.

6. *Оцінити затрати на створення комплексної системи захисту інформації*. Попередній розрахунок затрат на ліквідацію загроз безпеці інформації виконують з врахуванням обраного варіанту побудови комплексної системи захисту інформації і наявних на це коштів. На етапі розробки проекту комплексної системи захисту інформації формуються пропозиції стосовно вибору засобів та заходів захисту інформації, а також проводиться оцінка їх залишкового ризику, наприклад, за критерієм «ціна – якість». При цьому обирається найоптимальніша пропозиція. У випадку, якщо залишковий ризик перевищує допустиму величину, то слід внести зміни до засобів та заходів захисту. Після цього усі процедури виконуються заново до отримання потрібного результату.

Таким чином, дотримання розглянутої послідовності проведення аналізу ризиків на підготовчому етапі створення комплексної системи захисту інформації дозволить дослідити моделі загроз інформаційним ресурсам і моделі порушників, наслідків, які можуть настати унаслідок реалізації потенційних загроз, а також спроектувати, на його основі, моделі захисту інформації в інформаційно-телекомунікаційній системі.

Використані джерела

1. НД ТЗІ 1.1-005-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення / Затверджено наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 12.12.2007 р. № 232. – Київ, 2007.

2. НД ТЗІ 1.6-003-04. Створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації / Затверджено наказом ДСТСЗІ СБ України від 10.03.2004 № 04. – Київ, 2004.

3. НД ТЗІ 3.1-001-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексів технічного захисту інформації. Передпроектні роботи / Затверджено наказом Адміністрації Держспецзв’язку від 12.12.2007 № 232. – Київ, 2007.

4. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі / Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 № 22 із змінами згідно наказу Адміністрації Держспецзв’язку від 28.12.2012 № 806. – Київ, 2012.

Сидоренко К.Г. - начальник відділу Управління захисту економіки в Дніпропетровській області ДЗЕ НП України**;**
Кокарєв І.В. - доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат економічних наук, доцент

ВДОСКОНАЛЕННЯ СИСТЕМИ СПЛАТИ МИТНИХ ПЛАТЕЖІВ

На виконання доручення Міністерства внутрішніх справ України та вимог постанови Кабінету Міністрів України «Про реалізацію експериментального проекту щодо створення умов для унеможливлення ухилення від сплати митних платежів» від 20.06.2018 № 479 [1] (далі – Постанова) управлінням захисту економіки (далі – УЗЕ) було проведено заходи щодо унеможливлення ухилення від сплати митних платежів на території Дніпропетровської області.

У рамках виконання вищезазначеного доручення ДЗЕ та Постанови КМУ [1], з метою плідної співпраці відомств з подолання таких негативних явищ, як ухилення від сплати податків, боротьба з якими входить до їх компетенції, та інших функцій та задач УЗЕ в області підготовлено та направлено ряд листів для отримання доступу до автоматизованої системи митного оформлення «Інспектор-2006» та надання безперешкодного цілодобового доступу в зони митного контролю працівникам УЗЕ. В той же час було розроблено алгоритм дій по відпрацюванню підприємств імпортерів, направлено орієнтування територіальним підрозділам з метою викриття протиправних схем під час здійснення імпортних операцій.

Окрім цього, до Дніпропетровської митниці ДФС направлені листи щодо проведення спільних оглядів/переоглядів товарів, які завозяться на митну територію підприємствами-імпортерами та мають ознаки ризиковості. При цьому були проведені огляди товарів, транспортних засобів по підприємствам імпортерам, які були вказані в листах. За результатами митних оглядів, порушень законодавства з питань митної справи не виявлено, окрім випадку зміни митної ставки з 0 до 5%.

У результаті здійснених заходів за матеріалами УЗЕ в області у період 10 місяців 2018 року відкрито шість кримінальних провадження, з яких чотири - за фактом зловживання службовим становищем посадовцями митних постів області. Так, виявлено протиправну діяльність посадових осіб Дніпропетровської митниці ДФС, які зловживаючи службовим становищем, сприяли заниженню митних платежів при імпорті товару.

Крім того, було виявлено протиправну діяльність службових осіб двох організацій, які у період 2017-2018 років перевозили з держав Європейського союзу без сплати митних платежів через митний кордон, як

гуманітарну допомогу, медичне обладнання для комунальних закладів Дніпропетровської області. При цьому фактично, зловживаючи службовим становищем, умисно, з корисливих мотивів, більшу частину зазначеного обладнання збували СПД, чим спричинили тяжкі наслідки.

На одному із підприємств виявлено протиправну діяльність посадових осіб, які протягом 2017 – 2018 років вносили завідомо недостовірні відомості до податкової та митної звітності, з метою отримання бюджетного відшкодування з податку на додану вартість.

Виявлено протиправну діяльність посадових осіб двох підприємств, які зловживаючи службовим становищем, під час проведення розмитнення імпортних товарів та сировини на митних постах м. Дніпро, внесли в офіційні документи недостовірні відомості щодо вартості товарів, чим занизили вартість митних платежів, що спричинило тяжкі наслідки. Виявлено протиправну діяльність посадових осіб митного посту Дніпропетровської митниці ДФС, які вступивши в злочинну змову з суб'єктами господарювання внаслідок порушення чинного законодавства спричинили тяжкі наслідки. В свою чергу внесені відомості до ЄРДР щодо можливого факту незаконного збагачення співробітників Дніпропетровської митниці ДФС.Оголошено 7 повідомлення про підозру за ч. 3 ст. 369 КК України, ч. 1,2 ст. 361-2 КК України, ч. 2 ст. 364 КК України, ч. 1 ст. 366-1 КК України [2]. У рамках кримінального провадження викрито та задокументовано злочинну схему з системного вимагання та отримання співробітником Дніпропетровської митниці ДФС неправомірної вигоди від фізичних осіб за проведення безперешкодного розмитнення автотранспортних засобів за посередництвом брокера. У результаті здійснених заходів за адміністративною практикою УЗЕ в області за 10 місяців 2018 року складено вісім адміністративних протоколів у відношенні співробітників Дніпропетровської ДФС за ч. 1 ст. 172-6 та за ч. 2 ст. 172-6 [3].

Таким чином, УЗЕ в Дніпропетровській області ведеться системна робота по виявленню економічних злочинів, яка дозволяє значно понизити їх рівень.

Використані джерела

1. Про реалізацію експериментального проекту щодо створення умов для унеможливлення ухилення від сплати митних платежів: Постанова Кабінету Міністрів України від 20.06.2018 № 479 [Електронний ресурс]. – Режим доступу: http://www.zakon.rada.gov.ua

2. Кримінальний кодекс України від 05.04.2001 № 2341-III [Електронний ресурс]. – Режим доступу: http://www.zakon.rada.gov.ua

3. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X [Електронний ресурс]. – Режим доступу: http://www.zakon.rada.gov.ua

Страхова О. П. - викладач кафедри медичної та та фармацевтичної інформатики і новітніх технологій;
Каблуков А.О. - доцент кафедри медичної та та фармацевтичної інформатики і новітніх технологій, кандидат технічних наук, доцент
(Запорізький державний медичний університет)

ЗАСТОСУВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ У СТВОРЕННІ ЕКСПЕРТНИХ СИСТЕМ ПРОФЕСІЙНОГО СПРЯМУВАННЯ ДЛЯ ОПТИМІЗАЦІЇ ДІЯЛЬНОСТІ СПІВПРАЦІВНИКІВ МІНІСТЕРСТВА ВНУТРІШНІХ СПРАВ УКРАЇНИ

Завдяки виникненню хмарних технологій, що стали наступним кроком розвитку інформаційних систем і мереж, з'явилася можливість організації різноманітних професійних співдружностей, з'єднаних спільною метою діяльності. Територіальні розбіжності нині не є перешкодою спілкуванню професіоналів. Завдяки розвиненню методів кодування, шифрування та перешкоджання несанкціонованому доступу, виникають можливості обміну професійними міркуваннями у режимі онлайн одночасно певною кількістю фахівців.

В той же час, такий обмін думками може бути більш продуктивним, коли він може бути підтриманий необхідними професійними інформаційними інструментами.

Одним з таких засобів є експертні системи професійного спрямування.

Використання хмарних технологій у застосуванні експертних систем в поточній професійній діяльності співпрацівників різних підрозділів органів внутрішніх справ України дозволить фахівцям створювати робочі висновки на більш високому професійному рівні, навчати молодих фахівців передовим методам професійної роботи, і водночас удосконалювати інформаційне наповнення професійного середовища, весь час оновлюючи і розширюючи його контент.

Створення експертних систем, структура яких була б придатна для роботи за хмарними технологіями, повинне відбуватися на певній програмній платформі. Придатними для таких програмних продуктів є, наприклад, платформи що застосовуються для розробки дистанційних навчальних курсів університетів. Вони мають у своєму складі засоби і використання існуючих розробок експертних систем, вже наповнених відповідною інформацією, і створення нових структур експертних систем, що доповнюють і розвивають вже існуючі.

У Запорізькому державному медичному університеті ведеться розробка інформаційного базису, придатного для різноманітних професійних експертних систем, що здатні постійно розвиватися, на базі навчальної

платформи дистанційного навчання edX, розробленої Масачусетським технологічним інститутом. В них можлива одночасна робота декількох користувачів з одним і тим самим фрагментом створюваної експертної системи, що надає змогу враховувати внесок кожного професіонала у розробку спільного інформаційного продукту.

Впровадження інформаційних можливостей новітніх технологій, зокрема, хмарних технологій, експертних систем, у навчальну та повсякденну професійну роботу співпрацівників МВС України здатне підвищить професійну оснащеність фахівців, створити професійне інформаційне середовище, що удосконалювало б працю, навчання, професійне спілкування співробітників МВС.

Використані джерела

1. Субботін С. О. Подання й обробка знань у системах штучного інтелекту та підтримки прийняття рішень: Навчальний посібник. — Запоріжжя: ЗНТУ, 2008. — 341 с.
2. Биков В.Ю. Хмарна комп'ютерно-технологічна платформа відкритої освіти та відповідний розвиток організаційно-технологічної будови іт-підрозділів навчальних закладів / В.Ю. Биков // Теорія і практика управління соціальними системами. – 2013. – № 1. – с. 81-98.
3. Вакалюк Т.А. Можливості використання хмарних технологій в освіті / Т.А. Вакалюк // Актуальні питання сучасної педагогіки. Матеріали міжнародної науково-практичної конференції (м. Острог, 1-2 листопада 2013 року). – Херсон: Видавничий дім "Гельветика", 2013. – С. 97–99.
4. Chelikani A, Kumar G. Analysis of Security Issues in Cloud Based E-Learning. – University of Boras, 2011. – p.74 17.
5. Shor R.M. Cloud computing for learning and performance professionals . –American Society for Training & Development, 2011. – 20 p

Струков В.М. - завідувач кафедри інформаційних технологій Харківського національного університету внутрішніх справ, кандидат технічних наук, доцент

ПЕРСПЕКТИВИ РОЗВИТКУ ТА ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНІСТЬ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Відповідно з результатами роботи семінару-наради керівників управлінь організаційно-аналітичного забезпечення та оперативного реагування, інформаційно-аналітичної підтримки головних управлінь Національної поліції в Автономній Республіці Крим та м. Севастополі, областях та м. Києві за участю керівництва Національної поліції та структурних підрозділів центрального органу управління поліції, а також Консультативної місії Європейського Союзу в Україні, яка проходила в ГУ

НП в Закарпатській області в м. Ужгороді з 14.06.18 по 16.06.18., основна увага подальшої інформатизації діяльності Національної поліції буде спрямована на підвищення ефективності напрямків по лінії ДІАП, ДОАЗОР, Кримінального аналізу, Департаменту стратегічних розслідувань.

Основними напрямами реформування по лінії діяльності ДОАЗОР на сьогоднішній день є продовження створення регіональних ситуаційних центрів та їх інтеграція з міськими центрами 101, 103 та створення єдиних міських ситуаційних центрів 112 за моделлю «Безпечне місто». Одним із основних елементів САЦ передбачається система електронної відео фіксації автомобілів та інших об'єктів (скупчень людей) та їх розпізнавання в автоматичному режимі. Такі системи вже працюють в Маріуполі (система UASC на основі програмно-технічного забезпечення фірми Hulett Pakkard. Юридичним власником системи є ГУНП), в Чернігові (на основі програмно-технічного забезпечення міської комерційної фірми. Фінансують і є власниками системи муніципальні власті. ГУНП є користувачем системи.) та ін. Основною проблемо в даному напрямку є відсутність єдиного джерела фінансування, що спотворює різні форми реалізації у різних регіонах і різні форми взаємовідносин з органами місцевої влади. Так, наприклад, в більшості областей місцеві ситуаційні центри передбачають єдиний екстрений телефон – 112 (європейська модель), а в Харкові – 911 (американська модель).

По лінії діяльності ДІАП основними напрямами реформування є: а) подальший розвиток основної інформаційно-пошукової системи Національної поліції - ІП НПУ на платформі Технічного завдання на розробку ІПНПУ, затвердженого Головою Національної поліції України в жовтні 2017 р., б) подальша інтеграція і централізація інформаційних обліків НПУ, створення механізму більш ефективного функціонування ЄРДР і інших міжвідомчих баз даних, в) перехід з трьохрівневої системи реєстрації і обліку подій на дворівневу, створення потужних ЦОД (центрів обробки даних) і застосування хмарних технологій.

В питаннях оцінки діяльності підрозділів НПУ всі учасники дійшли до згоди, що одним з основних елементів в оцінці є думка населення. Перенесення акценту на оцінку діяльності поліції з боку населення повинно передбачати можливість для населення отримання об'єктивної інформації про діяльність підрозділів НПУ, що до сих пір є певною проблемою. Одним із найкращих і перспективних інструментів в цьому напрямі є портал police.kh.ua.

Тютченко С.М. – старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

МЕТОДИ ОЦІНКИ РІВНЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

На основі аналізу результатів фінансово-господарської діяльності підприємств здійснюється оцінка функціональних і сумарних критеріїв його економічної безпеки, розраховуються їх відхилення від планових значень, аналізуються причини виникнення цих відхилень. Після цього виробляються рекомендації щодо корегування набору корпоративних ресурсів, систем стратегічного і поточного планування фінансово-господарської діяльності підприємства, а також системи оперативного управління його діяльністю.

Рівень економічної безпеки підприємства можна оцінювати на основі визначення сумарного критерію, що розраховується на основі оцінок кваліфікованих експертів за частковими функціональними критеріями економічної безпеки підприємства.

Розрахунок сумарного критерію економічної безпеки підприємства здійснюється за формулою[1, с. 63]:

$$I = \sum_{i=1}^{n} K_i * D_i \qquad (1)$$

де:

K_i - значення часткових функціональних критеріїв економічної безпеки;

D_i - питома вага значущості функціональних складових економічної безпеки (при цьому сума усіх питомих ваг D_i для усіх функціональних складових, по яких ведеться розрахунок, дорівнює 1).

Для визначення вагового значення кожного показника використовується формула Фішберна, в основі якої лежить принцип ранжування показників [1, с. 53]:

$$K_i = \frac{2 * (m - i - 1)}{m * (m + 1)} \qquad (2)$$

Найбільший вплив на економічну безпеку мають показники фінансової стабільності підприємства, оскільки відображають залежність підприємства від зовнішніх чинників. Вони характеризують захищеність підприємства від зовнішніх загроз, пов’язаних із нестабільністю банківського сектора та можливістю неплатоспроможності підприємств-партнерів.

Кожному із показників за допомогою експертного методу, надається свій ранг залежно від впливу показників на фінансову безпеку промислового підприємства, при цьому найменше значення рангу означає найбільший вплив, а найбільше – найменший. Ранг повинен переглядатися залежно від стану ринкової кон'юнктури, ситуації як на фінансовому ринку, так і в реальному секторі, а також ураховувати специфіку діяльності галузі або самого підприємства, його стратегію та цілі.

Крім цього, часткові функціональні критерії економічної безпеки підприємства по кожній з її складових можна розраховувати на основі оцінки збитків економічної безпеки підприємства і ефективності заходів щодо їх запобігання.

До функціональних складових сумарного критерію економічної безпеки підприємства відносяться: фінансова, інтелектуальна, кадрова, техніко-технологічна, політико-правова, інформаційна, екологічна, силова.

Даний метод розрахунку сумарного критерію економічної безпеки підприємства містить значну частку суб'єктивного фактора оцінки експертів. Це відбивається як в оцінці, так і в процесі розподілу питомої ваги функціональних складових при розрахунку цього критерію. Але, саме відсутність чітко заданих параметрів оцінки дозволяє найбільш ефективно адаптувати даний метод оцінки діяльності підприємства на специфіку конкретного підприємства.

Аналіз рівня економічної безпеки підприємства проводиться на основі порівняння значення сумарного критерію економічної безпеки підприємства з отриманими раніше значеннями, або з розрахованими для порівняння значеннями цього критерію для аналогічних підприємств даної галузі. Крім того, порівнюються поточні і минулі оцінки часткових функціональних критеріїв і виявляються ступені впливу зміни стану функціональних складових на зміну значення сумарного критерію економічної безпеки підприємства.

Для оцінки впливу кожної зі складових необхідно визначити сукупний функціональний критерій. Він розраховується як відношення сукупного запобігання шкоди по даній складовій економічної безпеки підприємства до суми витрат на реалізацію заходів щодо запобігання збитків від негативних впливів і загального понесеного збитку за складовою. Сукупний функціональний критерій розраховується за формулою:

$$P = \frac{Z}{S + Y} \tag{3}$$

де:

P-сукупний функціональний критерій рівня забезпечення функціональної складової економічної безпеки підприємства;

Z- сукупний збиток по складовій;

S - сумарні витрати в аналізованому періоді на реалізацію заходів щодо запобігання збитків по даній функціональній складовій економічної безпеки підприємства;

Y - загальний понесений збиток по даній функціональній складовій економічної безпеки підприємства.

Розрахований сукупний критерій економічної безпеки порівнюється з аналогічними критеріями економічної безпеки споріднених підприємств галузі. Якщо критерій досліджуваного підприємства вище, ніж у його конкурентів, можна вважати, що підприємство знаходиться в стані відносної економічної безпеки. Цей критерій в подальшому може бути використаний для отримання прогнозів фінансово-економічного стану фірми, які служать для практичного маркетингу, управління фінансами, фінансового менеджменту, а також при поточному управлінні фірмою.

Розрахунок показників економічної безпеки підприємства є важливим елементом для швидкого реагування на можливі недоліки в управлінні підприємством, що можуть бути перешкодою ефективному протистоянню зовнішніх та внутрішніх загроз підприємства та оперативному внесенню відповідних коректив щодо усунення слабких місць. Лише за цих умов можливий стабільний економічний розвиток промислового підприємства, що функціонує в умовах мінливого та нестабільного зовнішнього середовища.

Використані джерела

1. Рета М.В. Методичні підходи до оцінки рівня фінансової безпеки підприємства // Вісник Національного технічного університету «ХПІ». Серія «Технічний прогрес та ефективність виробництва». – 2013. – № 21. – с. 29–37.
2. Портнова Г.О. Фінансова безпека підприємств: сучасні погляди щодо сутності та оцінки // Збірник наукових праць Національного університету державної податкової служби України. – 2012. – № 1. – с. 345–355.
3. Макарова И.Л. Анализ методов определения весовых коэффициентов в интегральном показателе общественного здоровья / И.Л. Макарова // Символ науки. – 2015. – № 7–1. – с. 87–95.

Цільмак О.М. - професор кафедри криміналістики, судового медицини та психіатрії Одеського державного університету внутрішніх справ, доктор юридичних наук, професор

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ КРИМІНАЛІСТИЧНОГО ПРОФАЙЛІНГУ

На сучасному етапі реформування органів правопорядку існує нагальна потреба в модифікації та модернізації усіх їх видів діяльності. У системі Національної поліції існує багато різновидів професійної діяльності (кадрова, психологічна, оперативно-розшукова, слідча, превентивна та ін.), однак, є нагальна потреба у запровадженні такого виду діяльності як криміналістичний профайлінг (від англ. «profile» – профіль). Саме завдяки результативної складової зазначеного виду діяльності (психолого-віктимологічного портрету жертви злочину та психолого-криміналістичного

портрету злочинця), – відбувається розкриття особливо тяжких злочинів проти життя та здоров'я особи, а також злочинів проти статевої свободи та статевої недоторканості особи; серійних злочинів та тощо.

Необхідність розробки психологічного портрету злочинця, на думку зарубіжних фахівців (Douglas J., Munn C., [1], Ressler R., Burgess A., Douglas J. [2], Пастушені О., [3, с. 15], Анфіногенова А., [4, с. 16] та ін.), виникає при досудовому розслідуванні особливо тяжких злочинів, коли констатується істотна або повна відсутність відомостей про злочинця, а саме під час: вбивств, що містять ознаки маніпуляцій злочинця з трупом жертви; вбивств з посмертними колотими і різаними пораненнями; вбивств на сексуальному ґрунті з ознаками садистського катування жертви; зґвалтувань; «Безмотивних» підпалів і вибухів та ін.

Криміналістичний профайлінг – це діяльність по складанню психолого-віктимологічного портрету жертви злочину та психолого-криміналістичного портрету злочинця.

Процесуальною складовою криміналістичного профайлінгу є дослідження й оцінка джерел інформації стосовно елементів і компонентів криміналістичної характеристики злочину.

Результативною складовою криміналістичного профайлінгу є складання достовірного психолого-віктимологічного портрета жертви злочину та психолого-криміналістичного портрета злочинця.

Психолого-віктимологічний портрет жертви злочину – це комплексна інтегральна характеристика індивідуально-психологічних особливостей, властивостей, рис, ознак, прикмет особи та криміногенно-провокуючих факторів, умов та обставин, які стали підґрунтям для вибору її в якості жертви.

Психолого-криміналістичний портрет злочинця – це комплексна інтегральна характеристика індивідуально-психологічних особливостей, властивостей, рис, ознак, прикмет злочинця; його злочинної мети та мотивів, основних способів та форм поведінки (дій, вчинків), настановлень, уподобань тощо.

Необхідно підкреслити, що криміналістичний профайлінг для органів досудового розслідування є доволі необхідним та перспективним різновидом діяльності.

Аналізуючи діяльність зарубіжних профайлерів, нами встановлено, що мета, завдання та предмет та об'єкт криміналістичного профайлінгу залежить від часових меж, тобто може стосуватися минулого, теперішнього та майбутнього. Так, наприклад, *основною метою ретроспективного криміналістичного профайлінгу* є надання рекомендацій стосовно напрямів розшуку злочинця, який скоїв особливо тяжкий злочин проти життя та здоров'я особи, злочин проти статевої свободи та статевої недоторканості особи; серію злочинів та тощо. *Основною метою поточного криміналістичного профайлінгу* є надання рекомендацій щодо найбільш ефективних методів та прийомів психологічного впливу на особу злочинця для унеможливлення реалізації його злочинних планів. *Основною метою*

перспективного криміналістичного профайлінгу є надання рекомендацій щодо вжиття найбільш дієвих заходів для запобігання особливо тяжкому злочинові.

На сучасному етапі зазначена діяльність потребує удосконалення її інформаціно-аналітичного забезпечення. Одним із перспективних напрямів комп'ютеризації процесу досудового розслідування є розробка систем, завдання яких полягає в автоматизації процесів пошуку та встановлення особи злочинця та визначення ймовірних місць скоєння серійних злочинів.

Додаткову актуальність і обґрунтованість даної проблеми надають вагомі результати в зазначеному виді діяльності, щодо інформатизації процесу розслідування злочинів в США, Канаді, і деяких країнах ЄС, хоча у вітчизняній науці і практиці ці досягнення залишаються маловідомими. Так, в західних країнах ще з 1980-1990 рр. використовуються такі інформаційно-аналітичні комплекси як INPOL, VICAP, КАЧЕМ, а також інші системи централізованого обліку та аналізу обставин і способу скоєння злочину. В Росії була розроблена (ВНДІ МВС РФ) АІПС «Монстр», покликана складати психологічні портрети злочинців, проте вона давала інформацію вельми низької якості, яка не могла в достатній мірі сприяти створенню пошукового портрета особи зловмисника за тими чи іншими психологічними і соціально-демографічними ознаками [1].

Тому, розробка програмного інформаційно-аналітичного забезпечення криміналістичного профайлінгу має дуже важливе значення для досудового розслідування особливо тяжких кримінальних правопорушень.

Використані джерела

1. Каримов В. Х. Автоматизированные информационно-поисковые системы криминалистического назначения: современное состояние, тенденции и перспективы развития. – М.: Юрлитинформ, 2014.

СТУДЕНТИ ТА КУРСАНТИ ПІД НАУКОВИМ КЕРІВНИЦТВОМ

Волошина В.В. – студентка юридичного факультету; науковий керівник **Тютченко С.М. –** старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

Останнім часом економіка України перебуває в умовах складного реформаційного періоду. Підприємства функціонують у динамічному зовнішньому середовищі, в умовах постійних змін та часткової невизначеності. Через це виникають загрози його розвитку та ефективній діяльності. Задля підтримки стабільного розвитку і функціонування фінансової системи в умовах нестійкого зовнішнього середовища потрібно безперервна розробка, впровадження та вдосконалення адаптивних механізмів забезпечення фінансової безпеки підприємства. Отже, внаслідок цього оцінка фінансової безпеки вітчизняних підприємств нині є дуже актуальною.

Механізм фінансової безпеки надає підприємству наступні можливості:

- самостійно розробляти та впроваджувати власну фінансову стратегію;
- забезпечувати залучення і використання фінансових ресурсів підприємства;
- забезпечити фінансову незалежність підприємства;
- вчасно ідентифікувати внутрішні і зовнішні загрози та небезпеки фінансовому стану підприємства;
- забезпечити фінансові інтереси власника підприємства.

Зовсім нещодавно в сучасній економіці з’явилась категорія «фінансова безпека підприємств» як самостійний об’єкт управління. Вона є головною складовою економічної безпеки, бо у будь-якій економічній системі фінанси виконують провідну функцію. Фінансова безпека - це кількісно та якісно детермінований рівень фінансового положення підприємства, який забезпечує захищеність його фінансових інтересів від реальних і потенційних внутрішніх та зовнішніх загроз. Для стійкого зростання підприємства визначають параметри на основі фінансової філософії й конструюють необхідні умови фінансової підтримки [1].

Вдосконалення механізму забезпечення фінансової безпеки підприємства необхідне для того, аби пом’якшити або уникнути дії загроз, які можуть негативно вплинути на розвиток підприємства та реалізацію фінансової стратегії.

Забезпечення фінансової безпеки – це системний процес, який поєднує в собі три основних компоненти: оцінку та діагностику фінансово-

господарської діяльності підприємства; доцільне та своєчасне застосування антикризових (стабілізаційних) заходів для уникнення внутрішніх і зовнішніх загроз діяльності підприємства; формування заходів та рекомендацій щодо забезпечення фінансового розвитку і конкурентоспроможності підприємства за всіма етапами його життєвого та операційного циклів [2].

Досягнення безперебійного та безперервного процесу перетворення капіталу в капітальні блага забезпечує зростання фінансової незалежності, рівня майнового положення, рентабельності, ринкової та ділової активності.

Важливим елементом економічної безпеки підприємства є його ресурсне забезпечення. Можна визначити критерії оцінки ресурсів, що в умовах конкуренції забезпечують його переваги . До основних критеріїв відносяться [3]:

- цінність;
- раритетність;
- неповторність;
- замінність.

Найважливішою складовою ефективного розвитку підприємства є забезпечення його фінансової безпеки. В сучасних ринкових економічних умовах підприємству потрібно створювати власну систему безпеки, яка допоможе своєчасно виявляти зовнішні та внутрішні загрози і ліквідовувати їх; вдосконалювати контролюючу систему діагностики фінансового стану підприємства для забезпечення стабільності та стійкості.

Використані джерела

1. Бланк И.А. Управление финансовой безопасностью предприятия // навчальний посібник – К. : Эльга, Ника-Центр, 2009. – 784.

2. Шкарлет, С.М. Формування економічної безпеки підприємств засобами активізації їх інноваційного розвитку // Автореф. дис. докт. екон. наук: 08.00.04. / С.М. Шкарлет. – Київ, 2007. – 24 с.

3. Роль ресурсної концепції в стратегічному управлінні підприємством // [Електронний ресурс] – Режим доступу: https://helpiks.org/9-3061.html

Воробець Х.О. - курсант факультету економіко-правової безпеки; науковий керівник - **Кокарєв І.В.** – доцент кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

МІЖНАРОДНА СПІВПРАЦЯ В ПРОТИДІЇ ТІНЬОВІЙ ЕКОНОМІЦІ

Тіньова економіка в сучасних соціально-політичних умовах розвитку країни, відмивання коштів як механізм забезпечення функціонування тіньових економічних відносин, «відтік» капіталів за наявності дефіциту інвестиційних ресурсів та низької капіталізації фондового ринку є найбільш

загрозливими для нашої держави соціально-економічними чинниками, що «зсередини» підривають фінансову систему, детермінують інші суто криміногенні явища та вияви корупції, а також впливають на імідж України як надійного зовнішньоекономічного партнера.

У сучасному глобалізованому світі одним з дієвих засобів детінізації економічних процесів та повернення до легального обігу виведених з нього активів є фінансові розслідування, які охоплюють комплекси заходів протидії розкраданням державних коштів, кіберзлочинності, виявам корупції, ухиленню від сплати податків, легалізації злочинних доходів, фінансуванню тероризму, торгівлі зброєю, наркотиками, людьми тощо [1].

Масив даних на цей час уже настільки значний, що слідчому чи детективу (і навіть цілим підрозділам) не вдається обробити їх традиційним «паперовим» способом. Вихід убачаємо в автоматизації аналітичних процесів, застосуванні спеціальних програмних продуктів пошуку та фіксації доказової інформації, зокрема електронних відображень. Такі програми – головна зброя аналітика XXI століття. Їх уміле використання неможливе без обміну досвідом та напрацювань зарубіжних фахівців.

За підтримки європейських партнерів вітчизняні правоохоронні та інші державні інституції з досвідом фінансових розслідувань підлягають активному реформуванню. Уже функціонують Національна поліція, реорганізуються органи прокуратури, створюється Державне бюро розслідувань (ДБР) [2]. Передбачається суттєве оновлення особового складу за рахунок молодих фахівців, які вкрай потребують оволодіння сучасним інструментарієм виявлення та розкриття економічних злочинів з використанням правильно побудованих систем збирання та аналізу інформації про рух коштів, майна, людей.

Відбулися позитивні зрушення, завдяки яким стало можливим фахове відстеження фінансових потоків та вжиття допустимих заходів щодо арешту й конфіскації доходів тіньовиків. Ідеться, зокрема, про оновлене антикорупційне законодавство, уніфікацію процедур реєстрації та доступу до державних реєстрів і баз даних, запровадження електронного декларування, системи ProZorro, відкритих реєстрів юридичних осіб та фізичних осіб-підприємців (із зазначенням кінцевого бенефіціара), бази власників майна, земельних ділянок тощо [3].

Проблему тіньової економіки вважається одним із основних глобальних ризиків світової економіки, з приводу чого офіційно було заявлено на Всесвітньому економічному форумі в 2011 році. Серед основних причин збільшення тіньової економіки було названо постійне розширення світових комунікацій, економічну нерівність та неспроможність глобального управління і контролю. Парламентська асамблея Ради Європи (ПАРЄ) головними чинниками тінізації економіки визначила тіньову зайнятість і тінізацію фінансових потоків.

За оцінками Міжнародної організації праці (МОП) нелегальний ринок праці має значне поширення в країнах, що розвиваються, де досягає понад 30 % ВВП. Фахівці тінізації фінансових відносин вважають, що глобалізації

фінансових систем сприяє розвиток Міжнародних банківських мереж і поширення електронних торговельних операцій. Як наслідок створюються сприятливі умови для маніпулювання фінансовими інструментами з метою ухилення від оподаткування та відмивання коштів, зокрема шляхом трансфертного ціноутворення [4].

У різних джерелах обсяги тіньової економіки в Україні фіксують на рівні від 30 до 50 % ВВП. За рахунками Мінекономрозвитку в 2016 році рівень тіньової економіки становив 35 % від офіційного ВВП. Розрахунок рівня тіньової економіки було проведено відповідно до Методичних рекомендацій розрахунку рівня тіньової економіки, затверджених наказом Мінекономіки від 18 грудня 2009 р. № 123 [5].

Важливою інституціональною загрозою економічній безпеці України є корупція. За цим показником Україна станом на 2017 р. посіла найнижчі позиції серед усіх країн – учасниць дослідження EY. Корупція як соціальне явище існує в певних інституціональних межах, в яких економічні, політичні, правові, соціальні процеси впливають на неї, а корупція чинить зворотній вплив на ці сфери. Вкрай небезпечною, специфічною та багаторівневою формою в системі інституціональних загроз економіки України є тіньова парадержава.

Тіньова прадержава – це утворення макроекономічного рівня державного типу, в якому через високий рівень корупції та тінізації державні послуги та суспільні блага розподіляють за ринковими принципами. У такому утворенні остаточно формуються та ефективно діють корупційні ринки державних послуг і суспільних благ[6].

Тіньова прадержава охоплює ринки: адміністративно-господарських рішень, державних посад, кадрової політики, державних привілеїв, державної освіти та науки, державного захисту прав і свобод громадян, виборчу систему тощо. Інституціональним базисом існування та розвитку тіньової парадержави є високий рівень тіньової економіки та корупції [7].

У результаті дослідження світових тенденцій тінізації економікипов’язаних з транс націоналізацією фінансових систем, розвитком міжнародних міжбанківських транзакцій та поширенням електронної комерції доведено що сьогодні відбувається процес подальшої глобалізації тіньових відносин у загальносвітовому масштабі, який супроводжується недостатньою координацією дій міжнародної спільноти щодо детінізації світових фінансових та торгівельних потоків з’ясовано , що тіньова економіка є об’єктивним явищем, яке притаманне економічним системам всіх країн світу, а її рівень визначається рівнем розвитку економічної системи, складністю виявлення всіх можливих варіантів прояву процесів тінізації та морально-культурними характеристиками країни особливості прояву тіньової економіки в різних країнах засвідчують її нижчий рівень в економічно розвинених країнах порівняно з країнами, які розвиваються встановлено, що у структурі тіньової економіки в країні переважає кримінальна складова, тоді як у розвинених країнах більшу частку займає неформальна економіка визначено системні фактори тінізації національної

економіки.

Використані джерела

1. Про державну реєстрацію юридичних осіб, фізичних осіб – підприємців та громадських формувань: Закон України від 15 трав. 2003 р. № 755-IV // Урядовий кур'єр. – 2003. – № 188.
2. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України від 14 жовт. 2014 р. № 1702-VII // Голос України. – 2014. – № 216.
3. Звіт про проведення національної оцінки ризиків у сфері у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, та фінансуванню тероризму: [Електронний ресурс]. – Режим доступу: http://www.sdfm.gov.ua/content/file/Site_docs/2016/20161125/zvit_ ukr.pdf.
4. Директива Європейського Парламенту та Ради про запобігання використанню фінансової системи для відмивання грошей та фінансування тероризму, що вносить зміни до Регламенту (ЄС) № 648/2012 Європейського Парламенту та Ради і припиняє дію Директиви 2005/60/ЄС Європейського Парламенту та Ради і Директиви Комісії 2006/70/ЄС [Електронний ресурс] : Директива, 20 трав. 2015 р. № 2015/849. – Режим доступу: http://www.sdfm.gov.ua/content/file/Site_docs/2016/20160516/DIRECTIVE%20(EU)%202015_UA.htm.
5. Стратегія національної безпеки України : Указ Президента України від 26 трав. 2015 р. № 287 // Офіц. вісн. України. – 2015. – № 43. – Ст. 14.
6. The Global Risks Report 2017. The World Economic Forum 2017. [Electronic recourse] / The World Economic Forum. – 2017. – Mode of access: https://www.wefo. – Title from the screen.
7. Про затвердження Методичних рекомендацій розрахунку рівня тіньової економіки [Електронний ресурс] : наказ Міністерства економіки України від 18 лют. 2009 р. № 123 // Міністерство економіки України : [веб-сайт]. – 2017. – Режим доступу: http://www.me.gov.ua.

Дегтяр В.А. - курсант факультету економіко-правової безпеки; науковий керівник **Кокарєв І.В. –** доцент кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

ЕКОНОМІЧНІ ЗЛОЧИНИ У ЖИТЛОВО-КОМУНАЛЬНОМУ ГОСПОДАРСТВІ

Побудова стабільно економічно-розвинутої країни – перш за все, успішне функціонування соціальної сфери суспільства, що стає першоступенем добробуту та процвітання громадян. Економічний розвиток соціальної сфери постає перед нами як комплекс житлово-комунального господарство. Щодо визначення поняття «житлово-комунального господарства» - одна з найважливіших галузей економіки та міського господарства, яке забезпечує життєдіяльність міста, також забезпечення населення, підприємств, організацій необхідними житлово-комунальними послугами [1, с. 54-56]. З цього огляду, дана галузь зосереджує в собі інтереси як населення, так і державних та органів місцевого самоуправління,

тому економічні злочини в цій сфері є одними з найрозповсюдженішими.

На сьогодні розглядом та дослідженням даного питання займається коло вітчизняних та зарубіжних вчених, слід зазначити наступні прізвища: Стащак М.В., Бабяк А.В., Губська А.В., Шендрик В.В. та ін. Головним завданням даного дослідження є характеристика основних економічних злочинів у житлово-комунальному господарстві [2].

Перейдемо до безпосередньої характеристики та класифікації таких злочинів. На сьогодні відповідно до чинного законодавство сфера ЖКГ структурована за 14 галузями, вони приставлені: житловим господарством, водопровідно-каналізаційним господарством, теплопостачанням, електропостачанням, газопостачання, дорожнім господарством, зеленим господарством, благоустроєм і санітарним очищенням, зовнішнім освітленням, ритуальним обслуговуванням.

Перш за все у сфері житлово-комунального господарства можуть вчинятися такі злочини:

- порушення порядку реєстрації господарської та підприємницької діяльності, що включає надання послуг, виконання робіт з забезпечення належного стану житлового фонду(житлові та допоміжні приміщення);
- створення фіктивних підприємств для надання послуг з проведення реконструкцій, ремонту та технічної експлуатації житлового фонду;
- легалізація доходів установами будівництва та житлово-комунального господарства України, комунального господарства та благоустрою отриманих з консолідованого державного бюджету України;
- отримання прибутку (орендна плата) за незаконне використання нежилих приміщень, що знаходяться у комунальній власності;
- незаконна зміна(підвищення/зниження) тарифів на комунальні послуги;
- наголошення на фінансовій неспроможності підприємств, що обслуговують сферу ЖКГ;
- шахрайство з фінансовими ресурсами (ст. 222 ККУ);
- фальсифікація засобів вимірювання (ст. 226 ККУ) на підприємствах, що надають житлово-комунальні послуги;
- незаконна приватизація державного, комунального майна (ст. 233) і т.д. [5].

Перелік цих злочинів є невичерпним, причиною є латентність економічних злочинів, що ускладнює їх розслідування та розкриття, а для науковців дослідження. Таким підтвердженням може виступити такий приклад: модернізація котельні комунального підприємства підрядною організацією. Січень 2018 року, Львівщина. Основна мета незаконне освоєння коштів керівником цього підприємства коштів, виділених на забезпечення загально-будівельних, монтажних та оздоблювальних робіт.

Правоохоронці встановили даний факт, що призвів до збитків понад 2 мільйонів гривень, через що було відкрито кримінальне провадження за ч. 2 ст. 364 Кримінального кодексу України [4].

Таким чином, шляхами вирішення та запобіганню злочинів, вчинених у сфері житлово-комунального господарства, працівникам підрозділів захисту економіки повинні бути відомі особливості житлового фонду регіону, механізм його функціонування, характеристика та зміст діяльності основних сфер ЖКГ, повинно бути забезпечення здійснення моніторингу економічного стану та фінансових ресурсів, щодо забезпечення виконання відповідних робіт, стану діяльності та розвитку об'єктів житлово-комунальної галузі, для повного та всебічного розгляду таких злочинів, а також їх безпосереднє розкриття.

Використані джерела

1. Оперативно-розшукова протидія злочинам у сфері житлово-комунального господарства : монографія / [А. В. Баб'як, А. В. Губська, М. В. Стащак та ін.]; за заг. наук. ред. В. В. Шендрика. Львів : Галицька видавнича спілка, 2013. 170 с.
2. Про житлово-комунальні послуги : Закон України від 09.11.2017 № 2189–VIII. URL: http://zakon3.rada.gov.ua/laws/show/2189-19.
3. Протидія підрозділами ДСБЕЗ МВС України злочинності у сфері житлово-комунального господарства : монографія / [А. В. Баб`як, М. В. Стащак, В. В. Шендрик та ін.]; за заг. наук. ред. В. П. Захарова та В. В. Шендрика. Львів : ЛьвДУВС, 2013. 220 с.
4. Електронний ресурс, режим доступ: [http://old.npu.gov.ua/mvs/control/main/uk/publish/article/2226057]
5. Кримінальний кодекс України. Електронний ресурс, режим доступ: [http://zakon.rada.gov.ua/laws/show/2341-14]

Дембицька Т.П. - курсант факультету економіко-правової безпеки; науковий керівник **Кокарєв І.В**. – доцент кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

ЕКОНОМІЧНІ ЗЛОЧИНИ В СФЕРІ ДЕРЖАВНИХ ЗАКУПІВЕЛЬ

Державне майно є одним із найбільш привабливих об'єктів злочинних зазіхань, а сфера державних закупівель є однією з найбільш криміногенних з цієї точки зору. «Перекачування» державних коштів у кишені недобросовісних державних посадовців і підприємців стало поширеним явищем. Злочинців приваблюють величезні кошти, які виділяються державою для закупівель товарів, робіт і послуг щороку. Так, у 2011–2013 рр. державним організаціям, установам і підприємствам виділялося на державні закупівлі 325–400 млрд. грн. За різними даними, у 2013 р. корумповані чиновники розкрали від 15 до 40 % виділених на закупівлю товарів і послуг

коштів (2013 р. – понад 110 млрд. грн.). У 2014 р. ситуація в галузі почала змінюватися: брак коштів у бюджеті, пильна увага громадськості та широкий резонанс за виявленими корупційними схемами зробили свою справу, але все одно, поки вона далека від ідеалу. Отже, сфера державних закупівель має постійно бути в зоні особливої уваги з боку державних контролюючих і правоохоронних органів.

Закупівлі товарів, робіт та послуг є невід'ємною складовою функціонування будь-якої держави. Без налагодженої системи державних закупівель держава не може повноцінно виконувати свої функції. За даними Міністерства економічного розвитку і торгівлі (МЕРТ) України, обсяг державних закупівель товарів, робіт і послуг У 2014 р. склав 260,2 млрд. грн., в І кварталі 2015 р. – близько 103,5 млрд. грн. [3]. Але значна частина коштів, що виділяється державою на закупівлі, витрачається неефективно, а в деяких випадках просто розкрадається.

Однією з основних причин неефективного використання державних коштів у цій сфері є високий рівень корупції. За оцінками спеціалістів, річні втрати від корупційних зловживань в сфері державних закупівель складають 10 – 15 % видаткової частини державного бюджету, або 35 – 50 млрд грн [4]. Причиною таких значних втрат є поширення хабарництва та інших корупційних злочинів як з боку розпорядників державних коштів, так і з боку учасників торгів.

Корупція представляє собою надзвичайно небезпечне явище. Вона зневажає законні права і інтереси громадян, гальмує хід впровадження економічних реформ, підриває авторитет демократичних інститутів держави, зумовлює розкрадання національного багатства.

Поняття "корупція" вже довгий час є предметом численних дискусій серед економістів, політологів, соціологів та ін. У загальному сенсі корупція означає корисливе використання свого положення в суспільстві в особистих цілях. Словник іншомовних слів визначає корупцію як "підкупність і продажність державних, політичних і громадських діячів, посадових осіб" [5].

Вважається, що корупція розпочинається з обміну взаємними послугами, який з часом породжує систему надання незаконних відносин. За надану послугу корупціонер одержує хабар у грошовій чи іншій формі. Особа, що приймає хабар, повинна мати певну владу. Тому особо небезпечною є державна, а саме бюрократична і політична корупція.

В документах ООН вказується, що корупція – це зловживання державною владою для одержання вигоди в особистих інтересах, інтересах третіх осіб або груп [6]. Наприклад, державні службовці часто хабарничають при видачі різних дозволів, ліцензій, тобто встановлюють плату за надання послуг, офіційним власником яких є держава.

У прийнятому Законі України "Про засади запобігання і протидії корупції" корупція трактується як "використання особою … наданих їй службових повноважень та пов'язаних із цим можливостей для одержання неправомірної вигоди" [1]. Під неправомірною вигодою в Законі розуміються

“грошові кошти або інше майно, переваги, пільги, послуги, нематеріальні активи, що їх без законних на те підстав обіцяють, пропонують, надають або одержують безоплатно чи за ціною, нижчою за мінімальну ринкову” [1].

Внаслідок величезних обсягів коштів, пов’язаних із закупівлями державою товарів, робіт і послуг, ця важлива сфера діяльності створює родючий ґрунт для корупційних правопорушень і зловживань. Слід зазначити, що ці терміни не є тотожними. У законодавстві корупційне правопорушення трактується як “умисне діяння, що містить ознаки корупції … за яке законом встановлено кримінальну, адміністративну, цивільно-правову та дисциплінарну відповідальність” [1]. Проте у багатьох випадках важко довести, що мало місце умисне порушення законодавства, хоча результати закупівель вказують на ознаки корупційної змови. Навпаки, іноді законодавчі норми порушуються без злого наміру, внаслідок недостатньої кваліфікації членів комітетів з конкурсних торгів, поганого знання швидкоплинного законодавства, браку часу на проведення закупівель тощо.

Корупційні правопорушення у сфері державних закупівель мають місце як з боку розпорядників державних коштів, так і з боку учасників торгів. За даними МЕРТ, в Україні найбільш поширеними зловживаннями є наміри замовників здійснити закупівлю товару у певного заздалегідь визначеного виробника. У свою чергу, цей результат може бути досягнутим як шляхом уникнення від конкурентних процедур проведення закупівель, так і шляхом надання неправомірної переваги одному із учасників торгів. Уникнення від конкурсних торгів залишається, напевне, найпоширенішою проблемою при здійсненні державних закупівель.

Незважаючи на значне скорочення підстав для використання спрощених процедур закупівлі протягом двох останніх років, в січні-березні 2015 р. біля 62 % від загальної вартості укладених договорів про закупівлю товарів, робіт і послуг припадало на переговорну процедуру закупівлі та закупівлі в одного учасника [3]. Значна частка таких договорів пов’язана із закупівлями у природних монополій, наприклад, у постачальників комунальних послуг, але поширеними є також різноманітні правопорушення.

Так, Державною фінансовою інспекцією в 2014 р. були виявлені такі правопорушення: – здійснення закупівель без застосування процедур, визначених Законом про державні закупівлі;

– необґрунтоване застосування процедури закупівлі в одного учасника;

– надання неправдивих відомостей для застосування неконкурентної процедури закупівлі;

– поділ предмета закупівлі на частини з метою ухилення від застосування передбачених законом закупівельних процедур, тощо [3].

Значні правопорушення при здійсненні державних закупівель мають місце і серед учасників торгів. Найбільш поширенішим з них є змова між учасниками закупівельних процедур з метою отримання переваги одним із них. Сутність таких змов полягає в тому, що конкуренти ще до проведення торгів домовляються про те, хто саме представить “найкращу” пропозицію для отримання контракту. Іноді потенційні учасники взагалі утримуються від

надання тендерних пропозицій, але частіше вони надають пропозиції із свідомо завищеними цінами або заниженими якісними показниками. Заздалегідь визначений таким чином переможець торгів потім розраховується з учасниками змови часткою одержаного прибутку у прямій (грошові кошти) чи непрямій (субпідряди, взаєморозрахунки) формі.

Наведені вище правопорушення при здійсненні державних закупівель суттєво знижують ефективність використання державних коштів. Слід сподіватися, що впровадження електронних закупівель в Україні, яке очікується після вступу в дію нового закону про публічні закупівлі у 2016 р., сприятиме скороченню корупційних зловживань у цій сфері. Також слід рекомендувати запровадження передового західного досвіду в сфері державних закупівель, зокрема, щодо підвищення відповідальності за змови серед всіх учасників торгів.

Використані джерела

1. Закон України "Про засади запобігання і протидії корупції" від 07.04.2011 р. № 3206-VI [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/3206-17.
2. Закон України "Про публічні закупівлі" від 25 грудня 2015 р. № 922-VIII [Електронний ре- сурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/922-19.
3. Міністерство економічного розвитку і торгівлі України. Звіти щодо аналізу функціонування системи державних закупівель [Електронний ресурс]. – Режим доступу : http://www.me.gov.ua/ Documents/List?lang=uk-UA&tag=Zviti.
4. Іванов О. В. Щодо подолання корупції у сфері державних закупівель в Україні. Аналітична записка [Електронний ресурс] / О. В. Іванов ; Національний інститут стратегічних досліджень при Президентові України. Режим доступу: http://www.niss.gov.ua/articles/1486.
5. Словник іншомовних слів / за ред. О. С. Мельничука. − К. : Головна редакція "Українська радянська енциклопедія" (УРЕ), 1974. – 776 с.
6. Декларація Організації об'єднаних націй про боротьбу з корупцією і хабарництвом у міжнародних комерційних операціях від 16 грудня 1996 р. // Міжнародні правові акти та законодав- ство окремих країн про корупцію / упоряд. : М. І. Камлик та ін. – К. : Школяр, 1999. – 480 с.

Джараєва А.А. – студентка юридичного факультету;
науковий керівник **Рибальченко Л.В.** – кандидат юридичних наук, доцент кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

ТРУДОВА МІГРАЦІЯ УКРАЇНЦІВ ЯК ЗАГРОЗА ЕКОНОМІЧНІЙ БЕЗПЕЦІ КРАЇНИ

Протягом останнього десятиліття в Україні відбулися кардинальні зміни в соціальній, політичній та економічній сферах життя. Під тиском принципово нових тенденцій і явищ у соціально-економічному та політичному середовищі збільшується чисельність трудових мігрантів.

Зростаючі обсяги трудової міграції, призводять до дисбалансу між попитом і пропозицією на робочу силу на локальних, регіональних та національному ринках праці, а також суттєво впливають на подальший розвиток суспільства.

Останнім часом в Україні все більше загострюються політичні та соціально-економічні проблеми. Участь країни у неоголошеній війні у східних регіонах активізує чинники впливу на збільшення масштабів трудової міграції. У зонах військових дій склалися вкрай несприятливі умови для життя і майбутнього розвитку як регіону так і суспільства в цілому. Такий стан, безробіття, зруйновані помешкання, відсутність необхідних засобів для існування, призвели до неймовірного збільшення обсягів трудової міграції.

Здійснення економічних реформ та євроінтеграційний курс країни вимагає ефективного використання всього потенціалу країни. Темпи економічного та соціального розвитку залежать від раціонального розміщення продуктивних сил та ефективного використання робочої сили у територіальному розрізі.

Економічна безпека країни є важливою складовою системи національної безпеки, що формує захист національних інтересів, забезпечує стійкий соціально-економічний розвиток в країні, формує механізм протидії внутрішнім та зовнішнім загрозам, сприяє підвищенню рівня життя населення та розвитку системи міжнародної економічної взаємозалежності.

Міграція зумовлена відсутністю перспектив і можливостей швидкого зростання та покращення стандарту життя. Додаткові труднощі з вирішенням щоденних проблем стають поштовхом покинути рідну країну. На міграційні процеси основний вплив має рівень економічного розвитку країни, а особливо явище конвергенції, тобто вирівнювання як рівня життя, так і рівня цін в різних країнах. Подібним чином представляється співвідношення зарплат між Україною та європейськими країнами.

Хвиля міграції українців до Польщі з 1990 до 2000 рр. зросла на 2,5%, з 2000 до 2010 рр. майже на 4%, а з 2010 до 2020 (прогноз) рр. майже на 50%. За прогнозами Державного комітету статистики України у 2020 році міграція українців до Польщі буде становити 57,2%, що є дуже високим показником і має негативний вплив на вітчизняну економіку.

Якщо українці не вирішать повернутися, наша економіка зазнає збитків, тому що не лише не поверне собі витрат на їх освіту, але й не буде мати відповідних працівників. Виїжджають у більшості кваліфіковані працівники, дуже часто з вищою освітою. Це негативно впливає на український ринок зайнятості.

Високий рівень безробіття, а також можливість заробити більше грошей за однакові зусилля спричинюють еміграцію перш за все мобільних осіб, підприємницьких та освічених, які в Україні також мали шанс знайти роботу. Одним із наслідків масового виїзду на легальну роботу в країнах ЄС є те, що в Україні недостатньо працівників в основних професіях. Дуже бажано для нашої економіки, щоб емігранти повернулися на батьківщину.

Таким чином, для розвитку вітчизняної економіки, актуальним є

питання врегулювання міграційних процесів шляхом стимулювання повернення своїх співвітчизників, формування належної законодавчої бази для розвитку інтелектуального потенціалу в Україні.

За результатами дослідження виявлення чинників та особливостей міграційного руху населення, є пропозиція про необхідність запропонувати Уряду України розробити заходи щодо повернення мігрантів на батьківщину шляхом підвищення рівня зарплати, створення високоякісних робочих місць, створення умов для повернення науковців та обдарованої молоді, які хочуть повернутися в країну і вкладати кошти в економіку, з відповідними умовами та фінансовими гарантіями, підвищення рівня якості життя населення, що позитивно вплине на економічний розвиток України.

Використані джерела

1. Michał Siudak, "Ukraińska geopolityka" Wybór tekstów źródłowych, Polskie Towarzystwo Polityki Zagranicznej, Częstochowa 2017, ss. 190.
2. Міністерство соціальної політики України. [Електронний ресурс]. – Режим доступу: http://msp.gov.ua
3. Державна служба статистики України. [Електронний ресурс]. – Режим доступу: http://www.ukrstat.gov.ua/

Захарчук М. М. – студент;
науковий керівник **Махницький О.В. –**
старший викладач кафедри економічної та інформаційної безпеки безпеки

РОЗПОВСЮДЖЕННЯ НАРКОТИЧНИХ РЕЧОВИН ЧЕРЕЗ СОЦІАЛЬНІ МЕРЕЖІ

Соціальні мережі у просторах сучасного суспільства також обумовлені тим, що мережі перетворилися на своєрідний глобальний координаційний центр соціальних зв'язків, оскільки вони здатні компенсувати не тільки нормативний вакуум, а й регулювати комунікативні процеси у віртуальному просторі, що є особливою властивістю сучасного рівня розвитку системи соціальних комунікацій. Проблема розгляду соціальних мереж, як конструктора соціального середовища сучасного суспільства актуалізує дослідження змісту функціональних можливостей комунікації з використанням соціальних мереж, характеру та вимог до спілкування в умовах нового соціального середовища. Сьогодні широкої популярності набуває мережева комунікація, зокрема, соціальні мережі. Останні виступають інструментом, за допомогою якого велика кількість користувачів глобальної мережі отримує додаткові можливості у спілкуванні та поширенні інформації різного соціально-культурного значення. Проблемна ситуація пояснюється виникненням протиріч між швидким поширенням спілкування у мережевому просторі та рівнем науково-теоретичного узагальнення соціологічних проявів їх впливу на суспільні зв’язки, формуванням мережевої культури, процесами самоорганізації мережевих спільнот і

намаганням використання старих схем регулювання віртуальних соціальних зв’язків.

Вже ні для кого не є таємницею, що за допомогою соцмереж можна заробляти. Потрібно тільки визначитися зі спеціалізацію та поєднати це зі своїми уміннями. Чим, власне, і займаються деякі українці та отримують гроші, іноді, навіть не виходячи з власної оселі. А іноді це потребує деяких заходів що до розповсюдження посилань на он-лайн доступ до інформації. Найчастіше таким займаються в більшості люди які торгують наркотиками, на різних будівлях,парках, стінах, і т.д. Вони роблять рекламу свого продукту для вжитку і залишають в посиланні для зв'язку з ними.

Сам по собі продаж товарів з використанням соцмереж не є неправомірним (якщо це не зброя, наркотики та інші товари, обіг яких заборонено). В українському законодавстві немає нормативного акту, який би забороняв продаж товарів через соціальні мережі.

З точки зору нашого законодавства, це буде продаж товарів на замовлення поза офісного чи торгового приміщення. Такий продаж має бути оформлений відповідним чином. Другий момент, полягає в тому, що самостійний, регулярний продаж через соціальні мережі з метою отримання прибутку підпадає під визначення підприємницької діяльності і має здійснюватися суб'єктом підприємницької діяльності фізичною або юридичною особою, зареєстрованою у встановленому ЗУ "Про реєстрацію юридичних осіб та фізичних осіб – підприємців". Це теж порушується такими продавцями, адже у переважній більшості, свою діяльність вони ніяк не оформляють. Третій момент: вони повинні платити податки, але не роблять цього. Цікаво, що працівники податкової достатньо часто відвідують соціальні мережі і знають про такий вид торгівлі. Вони знають, що ці продавці мають зареєструватися як суб'єкти підприємницької діяльності, повинні сплачувати єдиний соціальний внесок, зареєструватися як платник податків, обрати для себе найбільш придатну систему оподаткування і платити єдиний соціальний внесок і єдиний податок, однак не дуже переймаються цим.

Продавці заборонених препаратів та сервіси для такої торгівлі складають суттєву частку даркнету, або «темного» Інтернету — сайтів, які доступні тільки через спеціально зашифровані технології, на кшталт браузеру Tor. Для комунікації між собою учасники ринку використовують спеціально захищену «темну» пошту Sigaint та шифрувальне ПЗ Pretty Good Privacy (PGP). Оплата відбувається в криптовалюті Bitcoin, тому придбання забороненого «зілля» через Інтернет забезпечує майже стовідсоткову анонімність.

«Темні» сайти функціонують, як вітрина, а угода купівлі-продажу має ознаки депонованого правочину. На першій стадії сервіс резервує готівкові кошти, допоки сторони не узгодять всі деталі. Система зворотного зв’язку дозволяє оцінювати покупку та залишати коментарі, щоб допомогти іншим користувачам обрати надійного контрагента — точнісінько так, як на легальних майданчиках Amazon та eBay. Адміністрація ресурсу отримує 5-

10% комісійних із кожної угоди, а також має право обмежувати продаж окремих категорій товарів (наприклад, зброї). Форуми, скарги та будь-які інші клієнтські звернення опрацьовують, як і в звичайному «світлому» Інтернеті, з тією лише різницею, що модератори отримають платню у криптовалюті Bitcoin.

Як тільки угода укладена і гроші заброньовано, наркотики надійно фасують в вакуумні пакети, не залишаючи відбитків пальців, та занурюють у відбілювач чи порошковий хлор, щоб унеможливити відстеження методами сучасних технологій ЦРУ. Адреса на пакунку завжди надрукована. Для відправлення використовують, зазвичай, декілька різних поштових відділень, розташованих на вулицях без камер зовнішнього спостереження. Новачкам часто дістається спочатку порожній пакунок (щоб перевірити маршрут доставки на відсутність спостереження) і лише потім — замовлений товар. Найкмітливіші покупці, щоби посилити власну безпеку, замовляють доставку на адресу сусідів, які наразі у від'їзді, але чиї поштові скриньки легкодоступні. Судячи з коментарів та спілкування на форумах, наркотики успішно потрапляють за адресою приблизно у 90% випадків.

Попри продумані запобіжні заходи, до останнього часу жодному онлайн-магазину заборонених товарів не вдалось довго протриматись. Перший і найбільш популярний — SilkRoad— протримався 3 роки. Потім ФБР вийшло на Росса Ульбріхта, засновника Silk Road та ідейного натхненника всіх подальших інтернет-магазинів наркотиків та зброї. Наразі «Суворий пірат Робертс» відбуває довічне ув'язнення за відмивання грошей, кіберзлочини та змову з метою продажу наркотиків.

Нащадок, Silk Road 2, проіснував в мережі всього рік, перш ніж правоохоронці припинили його діяльність. Продавці та покупці мігрували до наступних найбільших сервісів — Evolution та Agora. Перший зник у 2015 році з віртуальними коштами на рахунках клієнтів (в еквіваленті $12 млн.). Потім припинив роботу і сайт Agora, перервавшись на «технічні роботи», які тривають вже понад рік. На сьогодні найбільшим залишається магазин Alphabay, хоча нещодавно запрацювала четверта версія «Шовкового шляху», яка може відтягнути на себе частину аудиторії.

На мою думку, інтернет-продаж, хоча і є досить зручним для використання людиною, але водночас є досить небезпечним. Тому що можливо потрапити в пастку і шляхом маніпуляцій шахраїв, і в результаті крайнім виявися саме ти. Інтернет залишає по собі кучу доказів за допомогою яких доказів про те, що ти причетний може достатньо виявитися для того щоб звинувачений був повністю оправданий.

Використані джерела

1. Колесниченко М. Популярні соціальні мережі Facebook, Twitter та ВКонтакте вже давно перестали бути просто каналом комунікації і стали рушійними інструментами для ведення бізнесу. [Електронний ресурс] // tsn.ua – 2018. - Режим доступу: https://tsn.ua/groshi/ukrayinci-bez-problem-zaroblyayut-u-socmerezhah-do-10-tisyach-griven.html

2. Прогнімак К. «Темний бік» інтернет-економіки — як працює онлайн-ринок наркотиків. [Електронний ресурс] // imena.ua – 2018. - Режим доступу: https://www.imena.ua/blog/light-on-the-dark-web/

Казакова Л.А. – студентка**;**
науковий керівник **Гавриш О.С. –**
викладач кафедри економічної та
інформаційної безпеки;
(Дніпропетровський державний
університет внутрішніх справ)

ВИКОРИСТАННЯ ТЕЛЕГРАМ БОТІВ ЯК ПЛАТФОРМИ ДЛЯ ПРОДАЖУ НАРКОТИЧНИХ РЕЧОВИН

Telegram - це хмарний месенджер з клієнтськими додатками, доступними для всіх популярних мобільних операційних систем, а також для комп'ютерних операційних систем.

Він був заснований російським підприємцем Павлом Дуровим в 2013 році. У 2016 році Telegram заявила, що налічувала сто мільйонів користувачів, відправляючи мільярди повідомлень в день.

Однак відсутність контролю, комфорту і анонімності, пропоновані Telegram, є ідеальними умовами для початку незаконного обігу наркотиків. На цій арені додаток вперше використовувалося переважно для консультування клієнтів, і тільки невеликі магазини darknet продавали наркотики у Telegram. Влітку 2016 з'явилися перші боти телеграм.

Боти - це просто облікові записи Telegram, якими управляє програмне забезпечення, а не люди, - і вони часто будуть мати функції AI. Вони можуть робити все: навчити, грати, шукати, транслювати, нагадувати, підключатися, інтегруватися з іншими службами або навіть передавати команди в Інтернет речей.

Сьогоднішнє оновлення 3.0 для додатків Telegram робить взаємодію з ботами супер-легкою. У більшості випадків вам навіть не доведеться вводити нічого, тому що боти наддадуть вам набір призначених для користувача кнопок.

Розпізнати ім'я бота просто: воно розпочинається зі значка @ і закінчується на «bot». Наприклад, @ytranslatebot перекладе ваші повідомлення будь-якою мовою світу і дозволить спілкуватися в іноземному чаті. @ImageBot знайде в Інтернеті зображення по ключовому слову. @AlertBot розбудить вас замість годинника.

У січні 2017 року постачальники почали користуватися послугою на регулярній основі - практично в кожному магазині darknet був бот Telegram.

Telegram давно вважається місцем для безпечного анонімного спілкування, тому терористи цінують додаток. Крім того, функції можуть бути розширені через скрипти - ідеально підходить для перетворення додатку чата на торгову платформу. Початок роботи легкий: встановити додаток,

включити посилання Telegram - з веб-сайту, сторінки Facebook або друга.

Після цього додаток Telegram розвивався з дня на день. Продажі, вироблені за допомогою ботів телеграм, досягли 60%. Використовуючи безпечний зв'язок, користувачам не доводилося використовувати Tor взагалі - клієнти могли просто клацнути по екрану мобільного телефону.

Збільшення трафіку Telegram пояснюється також тим, що восени 2017 року на всіх великих російських ринках darknet на своїх серверах спостерігалися важкі DDoS-атаки.

Ситуація ще більше підігрівалася підробленими новинами в захоплених поліцією серверах Hydra's (провідних російських DNM). Дилери, а також їх клієнти знайшли хорошу і зручну альтернативу, відмова Telegram 10 листопада 2017, Дуров почав масивну «зачистку». Більшість ботів були заборонені протягом 24 годин.

Величезна аудиторія була втрачена, продажі зменшилися, і люди повернулися до DNM. «Жертви» були ідентифіковані з використанням ключових слів в їх повідомленнях, таких як «солі» і «спеції».

В даний час боти телеграм забороняються тільки за скаргами. Якщо в магазині немає серйозних конкурентів, він може існувати близько місяця, ті хто не рекламують своїх ботів, швидше за все, будуть існувати ще довше - до двох місяців.

Але, продавці знайшли рішення - вони переписують ботів на API користувачів, що ускладнює відправку скарг і затримує логічне завершення кожного автопродажу ботом. Перспектива торгівлі Telegram також заснована на використанні інтегрованої криптовалюти TON, яка буде запущена навесні 2018 року.

Майбутні розробки: TON. Telegram Open Network (TON) наддасть можливість здійснювати платежі всередині Telegram. Він включає в себе чотири етапи розробки: платежі TON, блокування TON, послуги TON DNS і TON.

Перевага цієї блокової платформи - автоматична настройка активності непослідовних користувачів, яка дозволяє перерозподіляти ресурси для інших проектів. Він вирішує проблему масштабованості, що сприяє скороченню комісії і прискоренню транзакцій в порівнянні з існуючими криптовалютами.

Компанія здійснює свою початкову пропозицію монет (ICO), щоб залучити $ 1,2 млрд. Незважаючи на те, що продавці DNM втрачають зв'язок з Telegram, реалізація TON може знову змінити ситуацію.

Як видалити бота? Боротися з новими схемами поширення надзвичайно складно. Частенько, розповсюджувачі закладок наркотичних речовин не знають свого дилера навіть в обличчя – отримують пакетики в умовному місці, а оплата робиться дистанційно на карту або «веб-мани». Продавець знаходиться в місті, отримує і фасує товар, служить посередником між ботом і розповсюджувачем, але того, хто управляє ботом, він теж не знає: організатор каналу поширення може керувати бізнесом з будь-якого місця планети, зв'язок через мессенджер коштує копійки. Коли наркобізнес був

зав'язаний на телефонних номерах, ці номери запросто відключалися – співробітникам органів досить було зв'язатися з оператором зв'язку.

Калініченко О.І. - студентка;
науковий керівник **Мирошниченко В.О.** - доцент кафедри економічної та інформаційної безпеки, кандидат технічних наук, доцент
(Дніпропетровський державний університет внутрішніх справ)

ПОРІВНЯЛЬНІЙ ОГЛЯД ДОВІДКОВО-ПОШУКОВИХ СИСТЕМ

У сучасному світі, спеціалісти різних професій доволі часто шукають необхідну їм інформацію на сторінках Інтернету. Щодня в мережі з'являються мільйони нових документів і саме тому виникла необхідність створення таких засобів, які б дозволили легко орієнтуватися в інформаційних ресурсах глобальних мереж, швидко та надійно знаходити потрібну інформацію. Адже без систем пошуку більшість із документів залишилися б непотрібними або взагалі не були б ні ким знайдені.

Пошукова система **–** це програмне забезпечення, що надає доступ до колекції слабоструктурованої інформації. Орієнтація на слабоструктуровані дані, тобто дані, які не можна представити у вигляді реляційної таблиці. В даному визначенні пошукової системи мається на увазі інформація різного роду, тобто текст, аудіо, відео, зображення [1].

Найпоширенішою ПС в світі є ***Google*** *(https://www.google.com),* яка має додаткові інструменти та сервіси. В Google застосовуються 2 важливих принципи: аналіз тексту документа і підрахунок вхідних посилань. Пошук ведеться на раніше проіндексованій базі зворотних індексів [2]. Найзручнішою функцією є *"cache"*. Завдяки їй, користувачі можуть переглядати раніше знайдену сторінку або сервер, навіть якщо вони вже були видалені. За допомогою Google можна знайти сторінки, що не містяться в його базі даних. Це можливо, тому що пошуковий павук індексує текст посилань зі сторінок [3].

Другої за популярністю ПС є ***Bing*** *(http://www.bing.com)*, яка має чудові можливості пошуку відео, які, на думку деяких людей, навіть краще, ніж у Google. У цій системі більше параметрів автозаповнення, при введенні запитів користувача. Bing відстежує більше взаємозв'язків між окремими веб-сайтами, завдяки чому пошук схожих варіантів спрощується. Також Bing надає пошукову систему Yahoo з її обчислювальними серверами [4].

Yahoo! *(https://www.yahoo.com)* також доволі популярна система, що обслуговує мільйони запитів щодня. Yahoo – єдина чисто каталогова система, у якої немає власної пошукової машини. Незважаючи на це, список категорій є найбільш повним і простим – дуже легко визначити, в якому

розділі знаходиться потрібна інформація. При заданні критеріїв пошуку, потрібно пам'ятати, що вона шукає ці слова тільки в назві і описі сторінки, оскільки повнотекстового індексу на Yahoo немає. Тому не слід вказувати при пошуку занадто багато термінів або синонімів [5].

Особливість ***AltaVista*** *(https://www.altavista.com)* полягає в можливості вести пошук за ускладненими критеріями відбору та забезпеченні підтримки безлічі мов. Також вона містить послуги з індексуванням інформації і можливість миттєвого пошуку в величезних базах даних. AltaVista здійснює розробку корпоративних пошукових систем внутрішнього користування. Ліцензує технології пошуку підприємствам, у тому числі для використання у внутрішніх мережах. Вона користується каталогами Yahoo, і ярлики над пошуковим рядком дозволяють знаходити в мережі зображення, музику, відео, а також тематичні розділи, наповнені вручну [6].

Yandex *(https://yandex.ru/company)* має найбільшу базу даних, яка має кластерну структуру і розміщена на кількох серверах. Ця ПС відрізняється від інших тим, що в ній послівний індекс для незнайомих слів організований так само, як і для словникових. Релевантність документів обчислювалася в залежності від частотних характеристик шуканих слів, ваги слова або виразу, близькості шуканих слів в тексті документа один до одного. В даний час Yandex є найповнішою базою документів серед російських ПС, а також найбільш пізнаваною маркою [7].

Baidu *(http://www.baidu.com)* – лідер серед китайських пошукових систем. Вона містить близько 800 млн. веб-сторінок, приблизно 100 млн. зображень і понад 15 млн. медіафайлів. За даними агентства ComCore, ця ПС щомісяця обробляє понад 10 млрд. пошукових запитів. Згідно з даними шанхайського агентства Iresearch, вона контролює 63% китайського ринку інтернет-пошуку. Також, окрім найголовнішого призначення – пошуку, Baidu надає користувачам багато додаткових сервісів [8].

META *(https://meta.ua)* – найвідоміша потужна та повнотекстова українська ПС, яка має оригінальну базу даних. Вона підтримує розвинені мови запитів, пошук за окремими полями документів. Виконує пошук з урахуванням морфології української, російської та англійської мов. Посилання супроводжуються анотаціями. Швидкий та зручний перегляд результатів [9].

У сучасному світі *ІПС* є найбільш потужним механізмом пошуку мережевих інформаційних ресурсів Інтернету. Головне завдання кожної ПС – здатність надати користувачам саме ту інформацію, яка їм потрібна.

Сучасні моделі ПС, зазвичай, базуються, на ймовірно-статистичних алгоритмах, які орієнтовані на відбір текстової інформації за відносно простими формальними правилами і ознаками. Для більш якісного відбору текстових ресурсів, відповідаючих запиту користувача використовуються деякі зі штучні прийомів апріорного призначення релевантності ресурсу. Наприклад, у вигляді індексів цитування та частоти знаходження ключових слів на даному ресурсі.

Саме тому, щоб задовольнити безперервно зростаючі потреби інтернет-користувачів, розробники пошукових машин постійно вдосконалюють алгоритми та принципи пошуку, додають нові функції та можливості, всіляко намагаються пришвидшити роботу системи.

Використані джерела

1. Поняття пошукової системи [Електронний ресурс] : Режим доступу https://ukrbukva.net/page,2,65382-Poiskovye-sistemy-Interneta.html
2. Принципи роботи Google [Електронний ресурс] : Режим доступу https://semantica.in/blog/chto-takoe-google-2.html
3. Функції Google [Електронний ресурс] : Режим доступу https://www.bibliofond.ru/view.aspx?id=576639#text
4. Пошукова система Bing [Електронний ресурс] : Режим доступу https://sitechecker.pro/ru/search-engines/
5. Пошукова система Yahoo [Електронний ресурс] : Режим доступу https://www.bibliofond.ru/view.aspx?id=576639#text
6. Пошукова система AltaVista [Електронний ресурс] : Режим доступу https://works.doklad.ru/view/4yqZXQ0Pous.html
7. Пошукова система Yandex [Електронний ресурс] : Режим доступу https://www.bibliofond.ru/view.aspx?id=576639#text
8. Пошукова система Baidu [Електронний ресурс] : Режим доступу https://www.bibliofond.ru/view.aspx?id=576639#text
9. Пошукова система META [Електронний ресурс] : Режим доступу http://freepapers.ru/22/poshukov-sistemi/223837.1490219.list2.html
10. Інформаційно-пошукові системи світу. – Львів, 1999

Козлова Д. С. – студентка;
науковий керівник - **Тютченко С.М**. - старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

ФІНАНСОВІ РИЗИКИ ЯК ДЕСТРУКТИВНІ ЧИННИКИ ВПЛИВУ НА ФІНАНСОВУ БЕЗПЕКУ ПІДПРИЄМСТВА

Прибуток – це матеріальний показник ефективності економічної діяльності підприємства, який залежить від багатьох факторів та має на нього безпосередній вплив. Фінансова діяльність підприємства пов’язана з багатьма транзакціями, операціями, угодами, що несуть за собою не лише можливість збагачення, а й значні фінансові ризики. Саме тому для забезпечення фінансової стабільності на підприємстві необхідно розробляти концепцію безпеки та стратегію управління з урахуванням ризиків, що супроводжують діяльність підприємства. Ризики, що пов’язані із можливістю виникнення неочікуваних матеріальних витрат, зниженням або відсутністю прибутку, втратою частини капіталовкладень для підприємства класифікуються як фінансові ризики. Ці ризики виникають на будь-якому етапі господарської діяльності в результаті відносин з фінансовими

структурами та підприємствами.

Причини виникнення фінансових ризиків різноманітні й можуть з'явитися непередбачено в процесі діяльності підприємства. Вони поділяються на зовнішні та внутрішні. До основних зовнішніх причин формування фінансових ризиків можна віднести наступні: слабку і нестабільну економіку країни; економічну кризу; інфляцію; підвищення рівня конкурентної боротьби; зниження цін на світовому ринку; політичні чинники та ін. Усі ці причини мають зовнішнє, щодо підприємства, походження і тому підприємство їх контролювати не може. До внутрішніх причин формування фінансових ризиків можна віднести: підвищення витрат на підприємстві, низький рівень управління, відсутність планування, незадовільну фінансову політику підприємства та ін [1].

Для подальшої регуляції та уникнення всіх фінансових ризиків має бути налагоджена внутрішня фінансова політика, яка залежить лише від внутрішніх факторів організації підприємства. Цілеспрямоване використання ресурсів підприємства, узгодження процесу виробництва та реалізації, виконання актуальних завдань в сукупності і являє собою фінансову політику компанії. Варто відзначити, що установлювати та регулювати її мають право лише засновники, уповноважені ними особи та володар контрольного пакету акцій.

Учасники фінансового ринку, в ході реалізації фінансових ризиків, можуть зазнати масштабних збитків або ж втратити абсолютно весь капітал. Ось чому, так важливо вміти ідентифікувати ризики та уникнути їх. Виявити їх можна методом безпосереднього аналізу кожної операції, та співставленні її з кожним можливим ризиком. При цьому, важливим інструментом регуляції ризиків є правильно встановлена належність їх до конкретного середовища.

На рис. 1 відображено основні види фінансових ризиків[2].

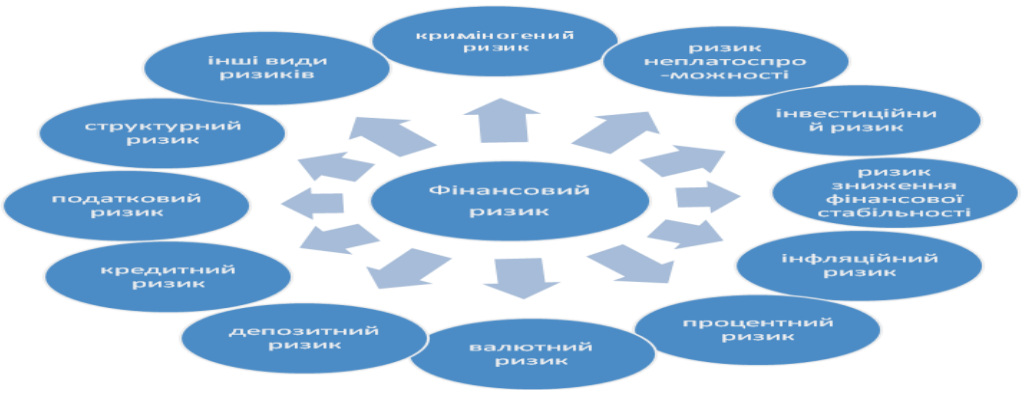


Рис. 1. Основні види фінансових ризиків [2]

Фінансові ризики зосереджені в багатьох сферах фінансового впливу на підприємство. І в незалежності від того, які за станом ризики-пасивні чи активні, вони несуть собою загрозу цим сферам. Адже їх реалізація – це лише питання часу, і в будь-якому випадку вони наноситимуть шкоду системам

підприємства, якщо їм ефективно не протидіяти методом ідентифікації, профілактики, оцінювання та страхування.

Все вищеперераховане і є основним аспектом фінансової безпеки підприємства, яка класифікується як фінансовий стан, який характеризується:

- по-перше, збалансованістю і якістю сукупності фінансових інструментів, технологій і послуг, що використовуються підприємством;
- по-друге, стійкістю до внутрішніх і зовнішніх загроз;
- по-третє, здатністю фінансової системи підприємства забезпечувати реалізацію його фінансових інтересів, місії і завдань достатніми обсягами фінансових ресурсів;
- по-четверте, забезпечувати ефективний і сталий розвиток цієї фінансової системи [3] .

Якщо визначити фінансові ризики, як деструктивні чинники фінансової безпеки, тобто ті, які виводять з ладу всю систему функціонування даної структурної одиниці (в перекладі з латинського destructivus «руйнівний», від дієслова destruere «ламати; руйнувати»), можна зробити висновки, що управління та регуляція ризиків, з точки зору підприємства, є необхідними для продуктивної роботи та отримання максимального прибутку.

Деструктивність ризиків полягає у тому, що вони є впливовим фактором, який може як і мотивувати організацію, так і пригнічувати. Звернемо увагу, на те, що ризики можуть сприйматися підприємством у три етапи: виклик, загроза, небезпека. І на останньому етапі дуже важливо прийняти відповідні заходи забезпечення фінансової безпеки. В першу чергу для цього необхідно визначити стратегію та тактику підприємства і вже відштовхуючись від них, забезпечувати розвиток розробки концепції фінансової безпеки, які базуються на:

- забезпеченні високого ступеню узгодження та гармонізації фінансових інтересів підприємства з інтересами оточуючого середовища та інтересами його персоналу;
- наявності на підприємстві стійкої до загроз фінансової системи, яка спроможна забезпечувати реалізацію фінансових інтересів, місії і завдань;
- збалансованості і комплексності фінансових інструментів і технологій, які використовуються на підприємстві;
- зростанні постійності і динамічності розвитку фінансової системи (підсистеми) підприємства [3] .

Отже, ризики дійсно впливають на фінансову безпеку підприємства, наражаючи на небезпеку її функціонування, шляхом впливу на всі сфери фінансової діяльності. Для боротьби з ризиками, перш за все, необхідна відповідна стратегія і тактика та налагоджена система менеджменту підприємства.

Використані джерела

1. Бланк И.А. Управление финансовой безопасностью предприятия // навчальний посібник – К. : Эльга, Ника-Центр, 2009. – 784.

2. Шкарлет, С.М. Формування економічної безпеки підприємств засобами активізації їх інноваційного розвитку // Автореф. дис. докт. екон. наук: 08.00.04. / С.М. Шкарлет. – Київ,

2007. – 24 с.
3. Роль ресурсної концепції в стратегічному управлінні підприємством // [Електронний ресурс] – Режим доступу: https://helpiks.org/9-3061.html

Кордіна Р.О. - факультету підготовки фахівців для органів досудового розслідування;
науковий керівник **Прокопов С.О.** - старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровського державного університету внутрішніх справ)

СИСТЕМА ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Інформація впливає на держави, суспільства та людей сьогодні більш ефективніше, ніж політичні, економічні та військові засоби. Впровадження сучасних інформаційних технологій (ІТ), телекомунікаційних систем, кількісних змін у сфері інформаційних взаємодій призвело до якісної зміни підходів до вирішення існуючих проблем та виникнення нових, які не існували на більш ранніх етапах розвитку інформаційного суспільства. Важливою сферою підвищення ефективності функціонування спеціалізованих інформаційних систем Національної поліції є інтеграція з глобальним Інтернетом. У багатьох випадках, завдяки ступеню інтеграції, вирішено два основні завдання. По-перше, географічно розподілені підсистеми інформаційних систем стали об'єднані. По-друге, користувачі Інтернету мають доступ до відкритої інформації ІС. Нерідко при вирішенні обох завдань використовують Веб-сайт (веб-портал), який, крім того, відіграє репрезентативну роль в Інтернеті.

Інформаційно-аналітична робота може виявити та визнати закономірності в контексті досліджень злочинності, порушення громадського порядку, дорожньо-транспортних пригод та ін.). З іншої сторони, інформаційно-аналітична робота узагальнює результати щоденної діяльності поліції для протидії негативним соціальним явищам. Він охоплює аналіз стану злочинності та заходи, спрямовані на охорону громадського порядку протягом певного періоду часу, вивчення ефективності та практичної доцільності певної форми роботи, її законодавче регулювання, використання інформації для протидії порушенням правопорядку, боротьби з злочинністю, інші напрямки діяльності поліції, визначені законодавством України [1].

Закон України "Про національну поліцію" [2] визначив як одну з напрямків своєї діяльності - інформаційно-аналітичну. Різноманітність завдань та функцій, які здійснюються в процесі функціонування системи МВС України, використовує різні форми діяльності. Найважливіші види

інформаційної діяльності для цілей програми представлені в Законі України "Про інформацію" [3]. Такою є діяльність із отримання, використання, розповсюдження й зберігання, а також захисту інформації легітимним чином.

Структура інформаційно-аналітичної діяльності має включати в себе інформаційну підтримку, інформаційну та аналітичну обробку, створення баз даних, в тому числі пошук інформації та методи їх реалізації.

Для ефективної реалізації цих функцій в рамках окремого територіального поліцейського органу необхідні об'єктивно встановлені та встановлені критерії для збору інформації, встановлено процедуру її обробки. Варто зазначити, що технологія збору та обробки даних повинна охоплювати всі сфери діяльності складових елементів Національної поліцейської системи, визначених Законом України "Про Національну поліцію" та компонентами Міністерства внутрішніх справ України (Державна служба України з питань надзвичайних ситуацій, Державна міграційна служба України, Державна прикордонна служба України, Національна гвардія України [4]), показники оцінки надійності, релевантності, інших зовнішніх та внутрішніх властивостей зібраної та обробленої інформації.

Оптимізація завдання пошуку, відбору та систематизації інформації, необхідної для роботи поліції, базується на розробці єдиного інформаційного простору системи МВС України, який логічно визначається як сукупність спеціалізованих баз даних з технологіями їх управління та використання, інформаційними та телекомунікаційними системами та мережами, а також інформаційно-аналітичні заходи, що діють на основі загальних принципів та загальних правил, що забезпечують інформаційну взаємодію між Міністерством внутрішніх справ України та громадянами [5].

Департамент інформаційної підтримки та координації діяльності поліції «102» Національної поліції України є основним підрозділом в системі інформаційно-аналітичного забезпечення діяльності органів та підрозділів Національної міліції України, яка надає організаційно-методичне керівництво. У своєму правовому положенні цей департамент є структурним підрозділом апарату центрального органу Департаменту національної поліції України, який організовує та здійснює діяльність, передбачену законодавством України, спрямовану на інформаційно-аналітичне та інформаційне виявлення правоохоронна діяльність, захист персональних даних під час обробки в структурних підрозділах Національної поліції України [6].

Крім того, служба інформаційних технологій Міністерства внутрішніх справ України повинна бути класифікована як спеціальна категорія. Крім того, кожна діяльність поліції щодо отримання інформації з інформаційних ресурсів, передбачених статтями 26, 27 Закону України "Про національну поліцію", зафіксована в спеціальному електронному архіві, який доручено цій службі [7].

Підрозділи організаційно-аналітичного забезпечення та оперативної реагування (далі - ОАЗОР) займають центральне місце в інформаційно-аналітичному супроводі поліції, в тому числі забезпечення інформаційного

обігу. У той же час слід зазначити, що порядок обміну інформацією в тій чи іншій мірі забезпечується всіма підрозділами та органами Національної поліції. Однак для ряду підрозділів центральними є завдання та функції у сфері забезпечення інформаційного обігу; до таких, разом з підрозділами ОАЗОР, до складу службових підрозділів та інших підрозділів Національної поліції, які займаються забезпеченням обігу інформації. Зокрема, відповідно до Положення про Департамент організаційно-аналітичного забезпечення та оперативного реагування Національної міліції України, затвердженого наказом Національної міліції від 27 листопада 2015 р. № 126, цей відділ здійснює збирання, оцінювання, аналіз інформації про кримінальну ситуацію в Україні, резонансні кримінальні правопорушення, порушення громадської безпеки та порядку, інші надзвичайні ситуації та реагують на них. Аналогічна функція на регіональному рівні також призначена адміністраціям ОАЗОР, які зобов'язані збирати, оцінювати та аналізувати інформацію про злочинність на території служби, кримінальні правопорушення, порушення громадської безпеки та порядку, інші надзвичайні події та заходи щодо реагування, вжиті підрозділи основних підрозділів з метою усунення недоліків (п.2 ст.1 розділу III Типового положення про управління організаційно-аналітичного забезпечення та оперативного реагування головних управлінь Національної поліції України в Автономній Республіці Крим та м. Севастополі, областях, м. Києві, затвердженого Наказом МВС України від 22 січня 2016 р. № 39) [8]

Департамент ОАЗОР готує оперативні зведення та інформаційні документи про злочини та події, обмінюється такою інформацією з іншими правоохоронними органами у встановленому порядку; готує комплексні аналітичні матеріали про стан операційної ситуації в державі, проекти управлінських рішень з підвищення ефективності діяльності поліції у боротьбі з злочинністю та зміцненні правопорядку.

Управління ОАЗОР готується з урахуванням пропозицій та матеріалів підрозділів ГУ такої інформації: комплексна оцінка кримінальної ситуації в зоні обслуговування за півроку та рік; узагальнені матеріали на основі роботи засідань ради та зустрічей керівництва ГУ; аналітичні звіти про операційну ситуацію на території служби та заходи, вжиті підрозділами ГУ з метою зміцнення правопорядку; доповідних записок керівництву ГУ з проблемних питань діяльності підрозділів ГУ [9].

Чергові підрозділи також відіграють важливу роль у реалізації цього адміністративно-правового інструменту. Таким чином, обов'язок чергового формувати повсякденне оперативне резюме (п. 3.6.1, п. 3.6 Інструкції з організації діяльності чергових частин органів і підрозділів внутрішніх справ України, направленої на захист інтересів суспільства і держави від протиправних посягань, затвердженої Наказом МВС України № 181).

Отже, підрозділи організаційно-аналітичного забезпечення та оперативного реагування займають центральне місце в інформаційно-аналітичному супроводі поліції, в тому числі забезпечення інформаційного обігу. Не викликає сумнівів, що головною особливістю професійної придатності працівників на всіх рівнях є вимога досконалого знання

інформаційних технологій, вміння накопичувати, обробляти та аналізувати зростаючі потоки інформації, використовуючи для цього найсучасніші технологічні засоби ІТ, прогресивне розвиток якого, у свою чергу, призведе до постійного вдосконалення навичок роботи з ними

Використані джерела

1. Наказ МВС України від 12.10.2009 № 436 «Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України». [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/z1256-09
2. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII // Відомості Верховної Ради. – 2015. – № 40-41. – Ст.379.
3. Про інформацію: Закон України від 02.10.1992 № 2657-XII // Відомості Верховної Ради. – 1992. – № 48. – Ст.650.
4. Постанова Кабінету Міністрів України від 28.10.2015 № 878 «Про затвердження Положення про Міністерство внутрішніх справ України». [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/878-2015-%D0%BF
5. Наказ МВС України від 26.09.2013 № 920 «Про затвердження Порядку організації доступу до інформаційних ресурсів під час інформаційної взаємодії між Міністерством внутрішніх справ України, Державною міграційною службою України та Державною прикордонною службою України». [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/z1771-13
6. Департамент інформаційної підтримки та координації поліції «102» Національної поліції України [Електронний ресурс]. – Режим доступу: http://www.npu.gov.ua/uk/publish/article/1820541
7. Шорохова Г.М. Визначення суб'єктів інформаційного забезпечення діяльності органів і підрозділів Національної поліції України / Г.М. Шорохова // Сучасні проблеми адміністративного права та процесу : тези доп. учасників Всеукраїнської науково-практичної конференції (м. Харків, 30 червня 2017 р.) / МВС України, Харків. нац. ун-т внутр. справ, каф. адмін. права і процесу ф-ту № 3. – Харків, 2017. – 295 с. – С.265-268
8. Про затвердження Інструкції з організації діяльності чергової служби органів (підрозділів) Національної поліції України http://zakon2.rada.gov.ua/laws/show/z0750-17
9. Про затвердження Типового положення про управління організаційно-аналітичного забезпечення та оперативного реагування головних управлінь Національної поліції України в Автономній Республіці Крим та м. Севастополі, областях, м. Києві : Наказ Міністерства внутрішніх справ України від 22 січня 2016 р. № 39 // Офіційний вісник України. – 2016. – № 16. – Ст. 400.

Кравцан В.В. – студентка;
науковий керівник **Тютченко С.М.** –
старший викладач кафедри економічної та
інформаційної безпеки
(Дніпропетровський державний
університет внутрішніх справ)

ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Здатність підприємства до стабільного стійкого розвитку окреслюється ступенем захисту від внутрішніх і зовнішніх загроз, який дозволяє швидко

реагувати на зміну в середовищі функціонування і характеризує рівень його фінансової захищеності. Розвиток підприємства неможливий без надійної системи фінансової безпеки. В умовах сучасної нестабільності економічної системи кожне підприємство повинно створювати сприятливі умови для забезпечення високого рівня своєї фінансової безпеки, що дає можливість розробляти та запроваджувати самостійну фінансову стратегію, підтримувати достатній рівень досконалої конкуренції на ринку.

Реалізація фінансового механізму фінансової безпеки підприємства вимагає певного керування та організації. В основі організації має бути цільовий підхід щодо забезпечення основного призначення фінансової безпеки. З огляду на визначення механізму фінансової безпеки як системи важелів, інструментів та методів функціонування суб'єкта підприємницької діяльності, що постійно забезпечує його фінансові інтереси, останні можуть бути покладені в основу такої організації у якості мети, що має бути досягнута. Економічне середовище існування підприємства, зокрема наявність зовнішніх та внутрішніх загроз при цьому не обумовлюються, однак така сталість функціонування має бути досягнута, в тому числі, в умовах кризових процесів та явищ. Крім того, слід виходити з аксіом фінансової безпеки, а саме, загальності, унікальності та відкритості.

Фінансово-економічний механізм управління фінансовою безпекою підприємства у науковій літературі розглядається як сукупність управлінських, економічних, фінансових способів гармонізації інтересів підприємства з інтересами суб'єктів зовнішнього середовища. Кінцевим результатом роботи зазначеного механізму є вплив на процес розробки та реалізації управлінських рішень з урахуванням особливостей діяльності підприємства, що забезпечує зростання ринкової вартості підприємства та максимізацію отриманого ним прибутку [1, с. 105]. Механізмом забезпечення фінансової безпеки підприємства називають сукупність чітко визначених дій зі створення умов гарантування його захисту від негативного впливу внутрішніх і зовнішніх загроз. Ці дії можуть містити в собі сукупність організаційних, фінансових і правових методів впливу з боку суб'єктів управління фінансами підприємства, спрямованих на своєчасне виявлення, попередження, нейтралізацію та ліквідацію загроз фінансовій безпеці даного суб'єкта підприємництва [2,с. 141]. Тобто, механізм управління забезпеченням фінансової безпеки підприємства передбачає вплив суб'єктів фінансової безпеки на об'єкт – фінансову діяльність підприємства, що впливає перш за все на стан його фінансових ресурсів з урахуванням дії фінансових ризиків та загроз.

Отже, фінансово-економічний механізм управління забезпеченням фінансової безпеки є складовою частиною комплексної системи управління підприємством, дія якої спрямована на:

– сприяння стабільному розвитку, підвищенню ефективності й конкурентоспроможності підприємства;

– формування та збільшення його фінансово-економічних ресурсів зі створенням системи захисту від зовнішніх та внутрішніх чинників.

До основних елементів фінансово-економічного механізму управління забезпеченням фінансової безпеки підприємства слід віднести три блоки [3,с. 19]:

– інформаційно-організаційний блок – це система, що складається з організаційного, інформаційно-аналітичного, нормативно-правового та програмно-технічного забезпечення;

– функціонально-аналітичний блок – згруповує елементи, призначені для діагностування фінансової безпеки підприємства, здійснення оцінки управління безпекою та проведення на підставі отриманих даних, виявлення ризиків та загроз;

– контрольно-моніторинговий блок – контроль процесу реалізації стратегії управління фінансовою безпекою підприємства, її коригування на основі оцінки ефективності стратегії управління фінансовою безпекою.

Використання запропонованого фінансово-економічного механізму управління забезпеченням фінансової безпеки підприємства допоможе обрати оптимальну стратегію управління фінансовою безпекою, засвідчувати критерії оцінки її ефективності на підставі належного інформаційно-аналітичного забезпечення.

Використані джерела

1. Шевчук І.Л., Ставерська Т.О. Фінансова безпека у системі економічної безпеки держави // Економічна безпека в умовах глобалізації світової економіки : [колективна Е45 монографія у 2 т.]. – Дніпропетровськ: «ФОП Дробязко С.І.», 2014. – Т. 1. – С. 286-298.

2. Пігуль Н. Г., Дехтяр Н. А., Боярко І. М. Особливості забезпечення фінансової безпеки акціонерних товариств / Н. Г. Пігуль, Н. А. Дехтяр, І. М. Боярко. // Проблеми і перспективи розвитку банківської системи України : збірник наукових праць. – 2013. – Вип. 37. – С. 140-146.

3. Крутова А. С., Ставерська Т. О., Шевчук І. Л. The problems of the enterprises financial security / А. С. Крутова, Т. О. Ставерська, І. Л. Шевчук // Економічна стратегія і перспективи розвитку сфери торгівлі та послуг : зб. наук. пр. / [редкол. : О. І. Черевко (відпов. ред.) та ін.]. – Харків : ХДУХТ, 2015. – Вип. 1 (21). – С. 92-105.

Михайленко С.В. – курсант факультету підготовки фахівців для органів досудового розслідування;
науковий керівник **Прокопов С.О.** - старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровського державного університету внутрішніх справ)

ПРОБЛЕМИ ТА МОЖЛИВОСТІ ВИКОРИСТАННЯ ХМАРНОГО СХОВИЩА В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Можливість зберегти дані в мережі, а потім отримати до них доступ з будь-якого куточка світу - це одна з кращих речей, подарованих нам хмарними обчисленнями. Якщо у вас є Інтернет і немає бажання витрачатися

на окремий зовнішній жорсткий диск під резервні копії важливих документів, фотографій і навіть образів системних дисків, вам на допомогу прийдуть «хмари» [2].

«Хмара» - це не просто віддалений сервер, адже сервер може раптово згоріти. «Хмара» - це ціла мережа серверів, що утворює віртуальне сховище. Ваш файл поділяється на рівні частини, кожна з яких зберігається на окремому сервері. Таким чином, якщо той чи інший сервер вийде з ладу, його обов'язки тут же візьме на себе інший сервер [2].

Переконавшись, що дані сервери є дуже функціональними можна прийти до висновку, що вони можуть служити непоганими помічниками у великих компаніях для зберігання величезного об’єму інформації та зручного доступу до неї усіх кому до неї буде відкрито доступ.

Отже цим сервісом можна скористуватися і для більш масштабних організаціях. Наприклад можна застосувати для створення хмарного сховища Національної поліції. Прогрес не стоїть на місці, а кабінети слідчих і досі завалені купами справ. Це дуже не надійно і не зручно у користуванні. Адже, щоб знайти якусь інформацію потрібно витратити багато часу. А в електронному вигляді зберігати на комп’ютері небезпечніше ніж у паперовому вигляді.

Все тому, що комп’ютери дуже не захищені від вірусів, адже ніякий антивірус не може дати 100% захист. А все тому , що разом з розвитком технологій розвиваються і комп’ютерні «паразити», тому електронна інформація перебуває у небезпеці.

Також проблемою є доступ до інформації на персональному комп’ютері. Будь-який професіональний хакер може з легкістю дістати всю йому потрібну інформацію навіть з віддаленого ПК. І навпаки, інші поліцейські, які потребують доступу до інформації на іншому ПК повинні витрачати дорогоцінній час і користуватися файлообмінниками та флеш-накопичувачами.

А створивши спеціальне хмарне сховище для Національної поліції , яке буду обслуговувати спеціальний орган, що буде забезпечувати безпеку його використання і конфіденційність інформації , що там зберігатиметься. А доступ до неї буде відкритий лише для уповноважених на те осіб.

Але у безпеці хмарних сховищ ми також не можемо бути впевнені на всі сто відсотків. З точки зору вірусів все нормально, адже компанії, що надають ці сервіси, надійно захищають свої сервери, а от щодо конфіденційності є питання. І питання ці стосуються дотримання конфіденційності самими компаніями, що надають хмарний сервіс. Тому створення окремого органу, що обслуговуватиме хмарне сховище Національної поліції є досить доцільним і виправданим.

Наразі Верховна Рада підтримала у першому читанні законопроект, який дозволяє зберігати інформацію державних органів у хмарних сховищах. За відповідний проект закону проголосували 229 народних депутатів.

Законопроект спрямований на створення умов впровадження новітніх технологій, зокрема при обробці інформації (крім інформації, яка в

установленому порядку віднесена до державної таємниці), якою володіють органи державної влади, інші державні органи, органи місцевого самоврядування. Проектом передбачається сформувати передумови для подальшого розвитку платформ інформаційно-комунікаційних технологій у різних сферах суспільного життя, насамперед у сферах державного управління, освіти та науки [1].

Документом пропонується ввести до законодавства поняття "система хмарних обчислень" та "надавач хмарних послуг" та розширити можливості щодо використання різних засобів захисту при обробці у системі хмарних обчислень інформації, яка не становить державної таємниці.

Також пропонується впровадити можливості використання систем хмарних обчислень, які мають сертифікати відповідності національним або міжнародним стандартам у сфері захисту інформації та впровадити концепцію зобов'язань надавача хмарних послуг [1].

Отже, можемо прийти до висновку, що наша країна стежить за технічним прогресом, і хоч не достатньо швидко, але намагається за ним встигати. Про, що свідчать ряд законопроектів спрямованих на впровадження більш сучасних технік у всі сфери життя країни.

Використані джерела

1. Рада підтримала створення українського хмарного сховища. [Електронний ресурс]. – Режим доступу: https://www.epravda.com.ua/news/2016/09/20/606110

2. Коли ти у хмарах. [Електронний ресурс]. – Режим доступу: https://pingvin.pro/novyny-kompanij/koly-ty-v-hmarah-perevagy-ta-ryzyky-servisiv-hmarnyh-shovyshh.html

Михайлова О.Ю. - слухач магістратури факультету підготовки фахівців для підрозділів кримінальної поліції; науковий керівник **Рижков Е.В.** - завідувач кафедри економічної та інформаційної безпеки, кандидат юридичних наук (Дніпропетровський державний університет внутрішніх справ)

АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ СЛІДЧОГО НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

На теперішній час інформаційна складова нашого життя досягла неймовірної концентрації. У зв'язку з стримким розвитком комп'ютерної техніки (як апаратної так і програмної її частин), а також удосконаленням комунікаційних інформаційних мереж передачі даних між різноманітними комп'ютерними комплексами, людина поринула у віртуальну середу, де проводить іноді більше часу ніж у реальному світі. І в цьому віртуальному світі на людину обрушується неймовірна кількість інформаційних пакетів, орієнтуватись у яких дедалі стає все складніше. В даному випадку від

людини чи об'єднаної групи осіб потребуються не тільки навички по пошуку потрібної інформації, але ще і навички по перевірці отриманої інформації на достовірність, актуальність. Але головні навички полягають у систематизації та аналізу отриманої інформації.

Вже майже рік при Національній поліції України активно функціонує Ситуаційний центр. До цього моменту в Україні аналогів відповідного підрозділу не існувало. Даний Ситуаційний центр здійснює аналіз вчинених злочинів на території обслуговування впродовж доби, обставин події кожного з правопорушень, дій поліцейських. Дана інформація відіграє важливу роль у повсякденній діяльності співробітника Національної поліції України, адже, наприклад, на її основі, керівники відділів (відділень) поліції можуть прийняти рішення стосовно проведення певних оперативно-розшукових та профілактичних заходів, з метою недопущення подальшого вчинення злочинів, посилення охорону громадського порядку та забезпечення публічної безпеки для виявлення правопорушників та їх затримання.

На нашу думку, на сьогодні в Національній поліції використовують такі види аналізу, такі як кримінологічний включає в себе аналіз динаміки і рівня злочинності, тактичний аналіз здійснюється протягом доби. Саме такий аналіз роблять аналітики Ситуаційного центру Національної поліції України, кримінальний аналіз опрацьовує кожен окремий злочин. Також, існують й інші види кримінального аналізу. Наприклад, стосовно рівня, на якому відбувається аналіз на рівні України, на рівні конкретної області, на рівні району у населеному пункті. Ми вважаємо, що існує об'єктивність та суб'єктивність проведення кримінального аналізу. Об'єктивність проведення кримінального аналізу залежить від програмного забезпечення, наявності конкретний обліків, які містять необхідну інформацію, а також наявність самої інформації. Суб'єктивність аналітичної роботи залежить від конкретного суб'єкта, який проводить аналіз, професійних навичок суб'єкта та особистого досвіду суб'єкта.

Зараз, у повсякденній діяльності слідчого Національної поліції України, існує проблема програмного забезпечення. Лише один Єдиний реєстр досудових розслідувань, який у момент його запровадження та на даний момент відіграє одну з найважливіших ролей для слідчого та став дійсно вагомим внеском в полегшення та систематизацію досудового розслідування, не полегшить слідчу діяльності. Враховуючи навантаження слідчого відділу (відділення) поліції в Україні процес досудового розслідування потребує запровадження нових програмних продуктів, та й взагалі введення в дію електронного кримінального провадження. Практика розслідування кримінальних правопорушень закордоном, дає нам підстави вважати, що слідчий не повинен годинами виписувати від руки протоколи та проводити певні маніпуляції, пов'язані з копіюванням документів, а повинен витрачати цей час для спілкування з учасниками кримінального провадження та для інтелектуально-логічного аналізу вчиненого злочину.

Враховуючи великі об'єми інформації, на все це необхідно витратити велику кількість часу, тому, у цьому, на нашу думку, середньостатистичному слідчому відділів (відділень) поліції в Україні прийде на допомогу візуально-аналітичний комплекс IBM I2. Дане програмне забезпечення не є досить популярним, проте, особи, котрі вже користувалися ним, відчули його значущість та допомогу. IBM i2 застосовується у різних сферах та призначений для:

- упорядкування та систематизування розрізнених даних в єдине узгоджене подання;
- визначення ключових осіб, подій, зв'язків і закономірностей, які не завжди можна виявити іншими способами;
- отримання розуміння структури, ієрархії і способів дій злочинних організацій;
- побудови версій та розроблення схем за певним кримінальним провадженням.

Отже, можемо зробити висновок, що на даний момент, в Національній поліції України йде запровадження підрозділів, які спеціалізуються на здійсненні аналітичної роботи. Аналітичне забезпечення в діяльності слідчого відіграє велику роль для розуміння динаміки та рівня злочинності, а також для вивчення розповсюдженості конкретного виду злочину на території обслуговування.

Також, на сьогоднішній день програмне забезпечення слідчого майже повністю відсутнє. Деякі програмні продукти дали б змогу слідчому відділу (відділення) поліції більш швидко та якісно вести досудове розслідування, при цьому витрачаючи менше часу. За допомогою візуально-аналітичного комплексу IBM I2 співробітник органу досудового розслідування зможе упорядковувати та систематизувати розрізнені дані в єдине узгоджене подання, визначати ключових осіб, подій, зв'язки і закономірності, отримувати розуміння структури, ієрархії і способів дій злочинних організацій, а також будувати версії та розробляти схеми за певним кримінальним провадженням.

Одоєвцев А.В., Битюцьких О.О. - курсанти факультету підготовки фахівців для органів досудового розслідування;
науковий керівник **Прокопов С.О.** - старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

АКТУАЛЬНІ ПИТАННЯ ІНФОРМАЦІЙНОЇ ВІДКРИТОСТІ ОРГАНІВ ПОЛІЦІЇ

У сучасних умовах відбувається переосмислення принципів, підходів і цінностей у побудові всієї правоохоронної діяльності, в тому числі

визначення ролі, місця і статусу органів поліції, на які держава покладає місію захисту прав та інтересів кожної людини. Все це свідчить про актуальність дослідження усіх питань, пов’язаних з органами поліції.

Одним із факторів побудови правової держави та громадянського суспільства є інформаційна відкритість діяльності органів державної влади як гарантів становлення державного ладу України. У цих умовах виникає необхідність постійного, надійного взаємозв'язку між органами публічної влади та широкими колами громадськості, зростає роль інформаційних відносин, адже сьогодні є загальновизнаним, що рівень цивілізованості і демократизму відносин між владою і громадськістю в значній мірі визначається ступенем «відкритості» влади [1, с. 22].

На думку вчених, прямий відкритий діалог влади та населення – це одна з найважливіших вимог владного управління в демократичному суспільстві [2, с. 22]. Крім цього, інформаційне забезпечення діяльності органів державної влади можна розглядати як інструмент демократії. Так, демократія неможлива без прозорості діяльності органів влади, де інформаційна забезпеченість відіграє значну роль, так само як і відкритість влади не може бути забезпечена за відсутності демократично організованої влади.

Принцип відкритості державної влади є її обов'язком із забезпечення можливості вільного доступу громадян до здійснення управління державними справами. Відкритість і прозорість поліції - це основні вимоги до ефективності діяльності поліції, сформованої демократичним шляхом [3, с. 18].

Зважаючи на актуальні проблеми та завдання щодо реформування Міністерства внутрішніх справ та у зв’язку з прийняттям Закону України “Про національну поліцію” [4] особливого значення набувають питання вдосконалення організації взаємодії поліції з громадськими інститутами та громадянами з метою забезпечення суспільної довіри до поліції, відповідно – більш успішного здійснення законодавчо закріплених основних напрямів її діяльності. Правовою основою цього процесу є ст. 9 закону, яка визначає, що поліція здійснює свою діяльність на засадах відкритості та прозорості в межах, визначених Конституцією та законами України [5, с. 4].

Органи Національної поліції забезпечують постійне інформування органів державної влади та органів місцевого самоврядування, а також громадськості про свою діяльність у сфері охорони та захисту прав і свобод людини, протидії злочинності, забезпечення публічної безпеки й порядку [6, с. 165].

Інформаційна відкритість у діяльності органів поліції є індикатором рівня демократії у суспільстві, необхідною умовою забезпечення передбачених Конституцією України прав громадян на інформацію та участь в управлінні державними справами. Інформаційна відкритість влади дозволяє громадянам отримувати адекватне уявлення та формувати критичні судження про стан українського суспільства, про позицію і дії органів публічної влади, підвищувати дієвість та ефективність громадського контролю за діяльністю органів публічної влади.

Таким чином, забезпечення стабільності та ефективності функціонування органів державної влади та системи державного управління, в тому числі органів поліції, за умов трансформаційних процесів безпосередньо залежить від наявності взаємодії громадянського суспільства та держави, у якій відкритість і прозорість відіграють провідну роль. Отже, інформаційна відкритість виступає надійним інструментом в налаштуванні двостороннього зв'язку між державою і громадянським суспільством з метою досягнення консенсусу, ефективної та належної реалізації прав і свобод людини та громадянина.

Впровадження та поширення використання сучасних інформаційних технологій в діяльності органів поліції на всіх напрямках, при прийнятті управлінських рішень, в забезпеченні праці поліцейських сьогодні потребує розробки методичних та практичних рекомендацій. Тому особливої актуальності набувають теоретичні та прикладні розробки щодо запровадження в Україні поліції європейського зразка.

Україна поступово приводить національне законодавство у відповідність з європейськими стандартами функціонування органів поліції, які позитивно вплинуть на процес реформування правоохоронної діяльності.

Використані джерела

1. Демократичні засади організації і функціонування вищих органів державної влади України : монографія / Ю.Г. Барабаш, І. І. Дахова, О. П. Євсєєв, та ін. ; за заг. ред. Ю.Г. Барабаша. — Х. : Право, 2013. — 272 с.
2. Буренко В.И. Политическая власть как объект социального регулирования : автореф. дис. на соискание учен. степени д-ра. полит. наук : спец. 09.00.10 "философия образования" / В.И. Буренко — М., 2000. — 49 с.
3. Романенко Є. Відкритість та прозорість як структурні рівні транспарентності державного управління та їх комунікативні функції / Є. Романенко // Теоретичні та прикладні питання державотворення. – 2014. – Вип. 14. – С. 17-31.
4. Про Національну поліцію: Закон України від 2 липня 2015 року // Відомості Верховної Ради України. – 1991. – № 40-41. – Ст. 379.
5. Калаянов Д.П. Правова основа реалізації принципу відкритості та прозорості в діяльності Національної поліції України / Д.П. Калаянов // Південноукраїнський правничий часопис. – 2017. – № 2. – С. 3 - 5.
6. Квітка Я. М. Принцип відкритості та прозорість у діяльності поліції / Я. М. Квітка, К. А. Гусєва // Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. – 2016. – Вип. 1. – С. 164-173.

Паслюченко А.А., студентка;
науковий керівник **Мирошниченко В.О.** - доцент кафедри економічної та інформаційної безпеки, кандидат технічних наук, доцент
(Дніпропетровський державний університет внутрішніх справ)

БЕЗПЕКА ОСОБИСТИХ ДАНИХ ТА ПРИВАТНІСТЬ - ГОЛОВНИЙ МІФ СУЧАСНОСТІ

Якщо ви думаєте що ваші особисті данні у безпеці - ви помиляєтесь. За вашим життям стежать скрізь. Пошта відстежує всі ваші замовлення та листування. Компанії, що надають комунальні послуги реєструють скільки води та електроенергії ви споживаєте. У багатьох комерційних та приватних установах (будинки, офіси, школи, дитячі садки, банки, університети …) люди живуть, навчаються та працюють під наглядом відеокамер. До речі, камери з магазинів можуть продивлятися всі кому не лінь. Телефонні дзвінки прослуховуються. Уміст СМС – повідомлень може зберігатися у операторів зв`язку до року. Через дзвінки та повідомлення дуже легко дізнатися ваше місцезнаходження. Онлайн - магазини збирають інформацію не тільки про те, що ви купуєте, а ще й про те що ви думали купити. Тобто про всі ваші дії на сайті. І я не один раз помічала, що після того чи іншого мого відвідування якогось сайту, у мене весь час з`являлась на екрані реклама з подібними товарами. Податкова служба збирає інформацію про ваші доходи все життя. Кредитні картки записують кожну покупку та мають інформацію від вашого імені до політичних переконань. Всі викладені в інтернет фото завдяки геолокації дають інформацію про ваше переміщення, не кажучи про те, що саме фото дає змогу знати вас в обличчя.

Окрему увагу я хочу приділити Google. Будь – який користувач комп`ютера чи смартфона так чи інакше використовує цю систему пошуку.

Google відкрито заявив, що збирає інформацію про своїх користувачів. Він має данні про ваші переміщення, навіть якщо геолокація на вашому смартфоні вимкнена. Ви можете навіть вийняти СІМ-картку з вашого смартфона, але результату це не дасть. Данні продовжать збиратися. Магія. Також незалежно від того видалили ви історію пошуку чи ні, Google знатиме і пам`ятатиме все що ви колись шукали та всі програми якими користувалися. Ця пошукова система складає ваш так званий «рекламний профіль» виходячи з вашої історії пошуку. Тобто вік ,стать, захоплення, рівень доходів, сімейний стан та, навіть, вашу ймовірну вагу.

У свою чергу Google дає нам змогу побачити скільки інформації зібрано на нас. Це окрема база даних під назвою Google STILL. Є окремі посилання переходячи за якими ми можемо отримати всю цю інформацію. Та будьте готові, що вона важитиме 3 - 10, а інколи й більше гігабайт. Там будуть всі покупки здійснені через Google, музика яку ви слухаєте,

електронна пошта та всі контакти, збереженні колись зображення, інформація з календарів і так далі…

Ваші смартфони та ПК несуть за собою ще одну небезпеку. Влада може у будь-який час прослуховувати ваші дзвінки та переглядати файли на вашому смартфоні. Більше того, будь-який навіть не надто навчений хакер може підключитися до камери чи мікрофону на вашому пристрої. Він має змогу робити фотографії без вашого відома, переймати звук з мікрофона та використовувати у своїх цілях. Загалом це відбувається для того, щоб дізнатися якісь паролі чи цікаву інформацію з вашого приватного життя.

Отже, все здіяне вами у мережі приховати не вийде. Кожен крок та кожне навіть випадково відкрите зображення залишить свої сліди глибоко у системі. Можна лише спробувати бути обачнішим. Ніколи не пізно заклеїти веб - камеру та мікрофон, перевіряти на що саме просять дозвіл скачані вами програми. Але від постійного шпигування сховатися все ж не можна. Технології вже надто тісно переплелися з нашим життям.

Тому хотілося б закінчити словами веб - розробника Ділана Каррана:

«Це одна із найбільш божевільних речей сучасної епохи. Ми ніколи не дозволили б уряду або корпорації встановити камери/мікрофони в нашому будинку або відстежувати наше місце розташування. Але ми зробили це за власним бажанням, бо, хай йому грець! – «Я хочу дивитися милі відео з песиками»

Плескачова В.С. – курсант факультету підготовки фахівців для органів досудового розслідування, науковий керівник **Прокопов С.О. -** старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

КІБЕРБЕЗПЕКА «РОЗУМНОГО» МІСТА

Актуальність даної теми зумовлена тим, що в останні десять років у багатьох країнах почали реалізацію проекти з розвитку сучасної міської інфраструктури на базі широкого використання сучасних технологій, особливо засобів інформаційно-комунікаційних технологій (ІКТ). Цей задум, який отримав назву «розумне» місто (Smart City), згуртовує навколо себе міську владу, громадських діячів та бізнесменів. Концепцію Smart City можна визначити як використання цифрових і комунікаційних технологій з метою покращення якості та ефективності міських послуг, зменшення витрат і споживання ресурсів, розширення співробітництва з громадянами. Багато організацій в світі працюють над цими технологіями.

«Розумні» міста визначаються також як «місто знань», «цифрове місто», «кібермісто», «екомісто» – в залежності від цілей міського планування. Вони проводять постійний моніторинг важливих об'єктів інфраструктури – автомобільних доріг, мостів, тунелів, залізниць, метро, аеропортів, морських портів, систем зв'язку, водопостачання, енергопостачання, найважливіших будівель з метою оптимального розподілу ресурсів і забезпечення безпеки. Вони постійно нарощують число надаваних населенню послуг, забезпечуючи стійке середовище, яке сприяє благоустрою і збереженню здоров'я громадян. «Розумними» можуть бути як нові міста, які відразу будуються як «розумні», або, що частіше, звичайні міста, які крок за кроком стають «розумними». Подібні проекти відносяться до інфраструктурних і їхній бюджет становить десятки мільярдів доларів, як при будівництві нових «розумних» міст з нуля, так і при модернізації існуючих міських систем. Реалізуються вони завжди з ініціативи урядів або місцевої влади із залученням бізнес-партнерів.

Зчитування знаків авто в ДТП, розпізнавання обличчя, наближення та наведення різкості – все це вміють камери, які є важливою складовою «розумного» міста. Прикладом є система «Гарпун», яка нещодавно почала використовуватись Національною поліцією України. Для працівників правоохоронних органів це відіграє важливу роль у розкритті злочинів, бо практично вже по всьому місту встановлені відеокамери, до яких має доступ ще й правоохоронець. Ці записи з камер працівник правоохоронних органів може в подальшому використати як доказ при розкритті адміністративного правопорушення чи злочину.

З огляду на сучасні темпи інновацій вже найближчим часом моделі «розумних» міст стануть поширеними реальними і популярними стратегіями міського розвитку. Для того щоб формування «розумних» міст стало наступним етапом процесу урбанізації потрібні і нові стандарти. З огляду на велике значення стандартизації для створення «розумних» міст, різноманітні заходи здійснюються Міжнародною організацією по стандартизації та Міжнародним союзом електрозв'язку.

Проблеми безпеки смарт-міст мають за своєю природою міжнародний рівень і притаманні містам по всьому світу. Громадська інфраструктура, як і раніше, являє собою особливо привабливу мішень для злочинців і терористів. У міру того, як світ стає все більш урбанізованим, міські високотехнологічні центри із цифровими технологіями збільшують вразливість суспільства. Міста є критично важливими інфраструктурами у всіх можливих сенсах, і якщо їх комп'ютеризація проводиться без урахування кібербезпеки з самого початку, проблеми, що можуть виникнути, сягнуть куди більш драматичного розмаху ніж знайомі і часто обговорювані питання кібербезпеки сьогоднішньої критичної інфраструктури. Це завдання треба вирішувати на ранній стадії, інакше вартість і складність створення «розумного» міста може надзвичайно ускладнити вирішення проблем безпеки на наступних етапах реалізації. З Інтернетом речей (IoT), який продовжує стимулювати розвиток розумних міст, міські інфраструктури стають все більш комплексними, але

залишаються легкими для проникнення.

Значна кількість пристроїв Інтернету речей надає можливості атаки на дані мережі. У масштабах міста, в якому тисячі пристроїв спілкуються одночасно як з користувачами, так і між собою, наслідки для безпеки стають значними. Мережа може бути порушена певними хакерами, зловмисниками або й одиночними гравцями. Вразлива кібератака може бути здійснена з одного смартфона або робочого місця. Кожна з функціональних систем розумного міста може викликати інтерес з боку внутрішніх і зовнішніх зловмисників. Вони можуть поставити під загрозу надання послуг, спровокувати серйозні інциденти в наданні критично важливих послуг, створити мережі типу ботнет, які складаються із скомпрометованих пристроїв, і використовувати їх для виконання завдань, відмінних від тих, для яких вони були спочатку призначені [4].

Основними проблемами інформаційних систем «розумних» міст з точки зору кібербезпеки є велика кількість технологій і практичних рішень, які повинні взаємодіяти і зв'язуватися один з одним, нерівна якість різних вбудованих технологій, дистанційна і безпосередня експлуатація інформаційних систем Smart City, величезні обсяги даних для аналізу і зберігання. І всі ці проблеми поряд з багатьма іншими слід розглядати завчасно, до «порозумнішання» кожного міста. Модернізація і «доповнена кібербезпека» не варіант для концепції «розумних» міст. Ризики занадто великі і українські міста повинні використовувати шанс розглядати кібербезпеку з самої ранньої стадії на всіх можливих рівнях.

З метою забезпечення кіберстійкості «розумних» міст з'явилася міжнародна ініціатива Securing Smart Cities, активно підтримувана рядом організацій в усьому світі. Заявленою місією ініціативи є визначення викликів кібербезпеки, що стоять перед «розумними» містами, і вироблення ефективних рішень протидії. Це включає просування кращих практик в галузі кібербезпеки і кіберрішень для всіх технологій, що використовуються в «розумних» містах. Ініціатива націлена на вирішення кіберпроблем на кожному етапі розвитку Smart City – від планування до фактичної реалізації інтелектуальних міст. У кінці листопада 2015 року ініціатори Securing Smart Cities випустили розроблені спільно з Cloud Security Alliance керівні принципи для прийняття за основу технологій «розумного» міста [2].

Використані джерела

1. Концепція Київ Смарт Сіті 2020. – Режим доступу : http://kscf.in.ua/ Smart_City_UKR_Print_final.pdf

2. Cyber Security Guidelines for Smart City Technology Adoption. − Access mode : http://securingsmartcities.org/wp-content/uploads/2015/11/

3. Les données numériques : le cœur des villes intelligentes et leur plus grande menace. − Mode d'accès :http://www.lebigdata.fr/les-donnees-numeriques-lecoeur-des-villes-intelligentes-et-leur-plus-grande-menace1911

4.Sécuriser les smart cities. − Mode d'accès : http://www.lesechos.fr/ideesdebats/cercle/cercle-145555-la-securite-des-smart-cities-nouvel-enjeu-pour-lesgouvernements-1183369.php

Сокол Р.В. – студентка**;**
науковий керівник **- Гавриш О.С. –**
викладач кафедри економічної та
інформаційної безпеки;
(Дніпропетровський державний
університет внутрішніх справ)

ІНФОРМАЦІЙНА ВІЙНА В УКРАЇНІ З РФ: ПІДМІНА ПОНЯТЬ

Поняття інформаційної війни є на сьогодні одним із найпопулярніших, зокрема тому, що людство живе у так звану інформаційну епоху. Поняття "інформаційна війна" ввів у науковий обіг американський дослідник М. Маклюен, який проголосив тезу "Істинно тотальна війна – це війна за допомогою інформації" [1]. Ще 30 років тому він проголосив, що на сучасному етапі економічні зв'язки і відносини усе більше приймають форму обміну знаннями, а не обміну товарами. А засоби масової комунікації саме є новими "природними ресурсами", що збільшують багатства суспільства. Тобто боротьба за капітал, простори для збуту відходять на другий план, а головним зараз стає доступ до інформаційних ресурсів, знань, що приводить до того, що війни ведуться більше в інформаційному просторі та за допомогою інформаційних видів озброєнь.

Інформаційно-комп'ютерна революція відкриває широкі можливості для впливу на народи та владу, маніпулювання свідомістю та поведінкою людей навіть на віддалених просторах. Беручи до уваги процес глобалізації комунікаційних мереж, що відбувається у світі, можливо припустити, що саме інформаційним видам агресії буде наданий пріоритет у майбутньому.

У наш час демонструються збільшені можливості інформаційного впливу на масову свідомість. У числі яскравих прикладів інформаційної війни можна назвати холодну війну СРСР – США, що привела до розпаду СРСР. З новіших інформаційних війн, як приклад, можна взяти інформаційну війну Росії з Україною .

Кожна інформаційна війна має свої наслідки, і Україна в цьому плані не виняток. За той час, що проводиться інформаційна війна на Україну, ми, як країна, зазнали наступні втрати: 1) збільшення еміграції населення (за даними державної служби статистики України на момент початку революції в країні у 2013 р. еміграція населення склала 22,187 осіб, в той час як на момент кінця 2015 р. еміграція населення складає 372,156 осіб [2]; 2) втрата частини території (анексія Криму, окупація частини Донецької і Луганської областей); 3) спад промислового виробництва. І якщо при звичайній війні приходять до бажаного результату через залякування і знищення, то в інформаційній війні все робиться багато в чому через маніпуляцію свідомістю і громадською думкою. І щоб розібратися наскільки серйозною і непростою є ця проблема для держави, варто звернути увагу на механізми впливу інформаційного потоку на населення. Пересічний український громадянин володіє більшою інформацією щодо подій в сусідній державі,

аніж у себе вдома, завдяки повсякденній цілеспрямованій роботі російських мас-медіа. І ця тенденційна інформація щоденно впливає на свідомість наших громадян.

Відсутність дієвого аналітично-пропагандистського центру в Україні дається взнаки. Хіба не є загрозою існуванню української незалежної демократичної держави той факт, що українські громадяни, які перебувають за кордоном, отримують оперативну інформацію з російських супутникових телеканалів. Проблема інформаційної диспропорції стосується й миротворчих військових контингентів. Нам відома нейтральна позиція України, але в Косово етнічні албанці ототожнюють українців з росіянами, з усіма наслідками. Розігрування російською стороною "кримської карти" вже стало хрестоматійним прикладом. У Севастополі відкрито філію Московського державного університету, а єдина українська гімназія в Сімферополі котрий рік тулиться без приміщення. Вважати це лише питанням освіти було б наївним.

З метою розколу українського суспільства і демонстрації Заходу неспроможності українського державотворення, російське керівництво почало втілювати дезінтеграційні проекти «Крим» та «Новоросія». Їх ідеологічним обґрунтуванням стала концепція «розділеного народу», відновлення «історичної справедливості». Фактично офіційною стала ідеологія пострадянського реваншу, що включає в себе образ Росії – збирачки розділеного штучними кордонами «русского мира». Кремль вдається до історичних маніпуляцій, які нібито мають обґрунтувати право Росії на ті чи інші території. У риториці весни 2014 р. найбільш активно задіяним виявилася категорія «русского мира», співзвучна з символічними поняттями «споконвічно російська земля», «місто російської військової слави». Історично неправдиві й хибні в логічному та правовому сенсах аргументи мають на меті переконати українців та світове співтовариство, що Крим – споконвіку російський, а входження Криму до складу України у 1954 р. – результат волюнтаризму Хрущова [3].

Інформаційна війна путінської Росії проти України призвела до того, що більше половини опитаних росіян готові воювати з українцями. Вірусом ненависті насамперед заражені молоді люди, які ніколи не були в Україні і не мають контактів із її громадянами. Старших людей лякають "бандерівцями-головорізами, які прийшли до влади". Це результат планомірної тотальної брехні, яка розробляється ідеологами Кремля, транслюється телебаченням" [4]. Щороку Росія витрачає проти України на інформаційну війну до 4 млрд дол. [5]. В. Філіпчук на "круглому столі" на тему "Як виграти інформаційну війну" зазначив, що Росія веде структуровану інформаційну війну, яка є складовою частиною гібридної війни. Росія використовує будь-який привід в інформаційній війні проти України. Якщо немає нового, його вигадують, висновують з будь-якої інформації.

Слід відзначити, що російські історичні наративи, які використовуються в інформаційній війні проти України, нерідко суперечать один одному. Однак не слід розцінювати це як ознаку непрофесіоналізму чи

безвідповідальності фахівців пропагандистського цеху Російської Федерації. Навпаки, це один із керівних принципів, якого дотримується російська пропаганда. Відтак, поки українська сторона переймається спростуванням дезінформації та виправдовується, в інформаційне поле вже вкидаються нові фейки та інформаційні бомби. Україна займає позицію захисту, оборони від потоку російської дезінформації. Така позиція в інформаційній війні є програшною для України.

У результаті відповідного висвітлення подій засобами масової інформації, через різні джерела у населення складається певне уявлення про ту чи іншу країну (яскравий приклад – зміна відношення росіян до українців після інформаційної війни на телебаченні). Таким чином, імідж країни продуктивно створюється мовними ЗМІ. Засоби масової інформації мають значну кількість прийомів впливу на суспільну свідомість. Інформаційна війна виступає засобом для досягнення будь-якої мети сторони, яка веде цю війну. Як і будь-який засіб, інформаційна війна призначена для виконання певних функцій, а саме – для контролю громадською думкою та масовою свідомістю і їх певною корекцією.

Використані джерела

1. Що таке інформаційна війна [Електронний ресурс]. — Режим доступу : my.elvisti.com/sergandr/iv.html.
2. Державна служба статистики [Електронний ресурс]. – Режим доступу: http://ukrstat.gov.ua
3. Информационные войны [Электронный ресурс] // Библиотека «пси-фактора». – Режим доступу: http:// psyfactor.org/lybr62-1.htm – Название с экрана.
4. Манойло А.В. Государственная информационная политика в особых условиях: Монография [Текст] / А.В. Манойло. – 2003. – 388 с.
5. Інформаційна безпека держави у контексті протидії інформаційним війнам. Навч. посібник / В.Б. Толубко та інш. – К.: НАОУ, 2003. – 340 с

Соловей І.Ю. - курсант факультету економіко-правової безпеки;
науковий керівник **Кокарєв І.В. -** доцент кафедри економічної та інформаційної безпеки, кандидат економічних наук, доцент (Дніпропетровський державний університет внутрішніх справ)

ДЕЯКІ АСПЕКТИ ПОШИРЕННЯ ЕКОНОМІЧНОЇ ЗЛОЧИННОСТІ

Перехід України до ринкової економіки, розвиток підприємництва, заохочення конкуренції, розширення зовнішньої торгівлі сприяли створенню нових підходів для злочинної діяльності у сфері економіки. У даному виді злочинів з’являються більш складні та віртуозні способи вчинення, підвищується їх суспільна небезпечність. І, як результат, за ступенем безпечності та поширеності, зокрема, однією з основних є економічна

злочинність, яка поширилась на всі галузі господарювання, сформувавши сферу тіньової економіки.

Падіння обсягів виробництва призвело до зростання безробіття з притаманним їй катастрофічним зниженням рівня життя населення. Нездатність держави створити необхідну кількість робочих місць для праці стала очевидним фактом. Відсутня також дійова й реальна соціальна програма допомоги безробітним. Тому закономірними й природними стали спроби різних верств населення, що залишилися без засобів для існування, знайти тіньову нішу в нових економічних реаліях. Саме тому, на нашу думку, обрана тема дослідження є надзвичайно актуальною на сьогоднішній день і потребує детального дослідження.

Економічна злочинність – це сукупність умисних корисливих злочинів і осіб, які їх вчинили, у сфері легальної і нелегальної економічної діяльності, головним безпосереднім об'єктом яких є відносини власності і відносини у сфері виробництва, обміну, розподілу і споживання товарів та послуг [1].

Причини вчинення корисливих злочинів у сфері економіки носять як об'єктивний, так і суб'єктивний характер. Економічні відносини, їх суперечливість і негативний характер породжують злочинність у цілому. Кримінологічні дослідження показують, що входження в ринкову економіку породило серйозне протиріччя між засобом виробництва, що укладається, і організаційно-господарськими рішеннями, які реалізують основні напрямки економічної політики [2 ,с. 36] .

Умовно обставини, що сприяють відносній поширеності і живучості антисоціального економічного поводження можна розподілити на 2 групи:

• організаційно-господарські;

• соціально-психологічні.

Перша група охоплює такі найбільш істотні обставини, як витрати економічної політики, недоліки чинної системи контролю; відставання правотворчої діяльності від потреб господарської практики й ін. У безпосередньому зв'язку із конкретними діяннями частіше інших знаходяться такі обставини як: недоліки системи обліку і звітності, поточного контролю з боку керівника, зневага до вимог по підбору осіб на ревізорські і матеріально відповідальні посади.

Друга група обставин пов'язана з недоліками правовиховної роботи, із загальною непідготовленістю населення й, особливо, середньої управлінської ланки до рішення складних економічних завдань на основі нової економічної ідеології, обумовлюється нерозривністю демократичних традицій саморегуляції суспільних процесів в економіці та ін.

Чинниками, що стримують розвиток організованої тіньової підприємницької діяльності, є проблеми, пов'язані з невиконанням умов договорів, які укладаються на тіньових ринках. Через те, що у тіньовому бізнесі багато угод укладаються на основі усних домовленостей, органам державної влади важко визначити обсяг тіньового бізнесу та правильно обрати засоби впливу на його учасників. Згідно з підходом Г. Беккера, від дій злочинців залежить пропозиція злочинів, від дій споживачів незаконно

виготовлених і реалізованих товарів – попит на злочини, а заходи правового виявлення і покарання вважають своєрідним регулюванням цього «ринку» [3,с.141].

Рівень злочинності у сфері економіки став загрожувати національній безпеці України, існуванню українського суспільства, і ця проблема перетворилася із загально-соціальної на політичну. Динаміка розвитку цієї злочинності виявляє з року в рік неухильну загальну тенденцію до зростання. Характер динаміки (тенденції) свідчить про зростання соціальної небезпеки й заподіяної шкоди окремими злочинцями чи злочинними угрупуваннями. У структурі економічної злочинності за розміром заподіяної шкоди домінують злочини в банківській сфері, у сфері міжнародних економічних відносин.

Офіційна статистична картина економічної злочинності не відтворює загальних процесів, які в ній відбуваються, внаслідок її значної неповноти. Відшкодування збитків державі за результатами діяльності правоохоронних органів по викриттю цих злочинів ні в якій мірі не компенсує витрати на їх утримання. Причини неухильного зростання злочинів у сфері економіки обумовлені перш за все глобальною соціально-економічною й політичною кризою в державі, тому організація ефективної системи протидії економічній злочинності можлива тільки на основі єдності загально соціальних, соціально-кримінологічних і кримінально-правових заходів.

Використані джерела

1. Конституція України// Відомості Верховної Ради України , 1996, № 30, ст. 141- [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua /laws

2. Кримінальний кодекс України // Відомості Верховної Ради України, 2001, № 25-26, ст.131 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws

3. Глущенко В. В. Економічна злочинність , прийоми приховування і методи ії виявлення. / В.В. Глущенко //Вісті Кримінологічної асоціації України. Вип 1.-Х.: В-цтво Харк. нац. ун-ту внутр. справ, 2004.- С. 173- 175.

Хитрук Р.О. – курсант факультету економіко-правової безпеки;
науковий керівник **Кокарєв І.В. -** доцент кафедри економічної та інформаційної безпеки, кандидат економічних наук, доцент (Дніпропетровський державний університет внутрішніх справ)

ЕКОНОМІЧНІ ЗЛОЧИНИ У СФЕРІ ЗОВНІШНЬОЕКОНОМІЧНОЇ ДІЯЛЬНОСТІ

Сьогодні Україна - активний учасник міжнародних зовнішньоекономічних відносин. Вихід на міжнародний ринок відкрив широкий спектр можливостей для ефективного та прибуткового ведення підприємницької діяльності для суб’єктів господарювання. Після лібералізації зовнішньоекономічної діяльності права учасників цієї сфери

отримали всі без винятку суб'єкти підприємницької діяльності, у тому числі і фізичні особи, міжнародні об'єднання, неприбуткові організації, об'єднання фізичних і юридичних осіб, державні органи та органи місцевого самоврядування.

Визнання України суверенною державою, здобуття ознак повноправного суб'єкта міжнародного співтовариства стали своєрідним каталізатором, що зумовив стрімке підвищення активності учасників зовнішньоекономічних відносин у різних сегментах економіки. На міжнародному рівні з боку держави відзначалося прагнення до встановлення цивілізованого рівноправного діалогу, який би ґрунтувався на послідовній державній стратегії щодо захисту вітчизняної економіки від деструктивного впливу зовнішніх економічних та кримінальних чинників.

Аналізуючи тіньову складову зовнішньоекономічної сфери господарювання, а також визначаючи масштаби загроз кримінального характеру зовнішньоекономічній безпеці України від учинення учасниками ЗЕД деліктних проступків, дослідникові неминуче доведеться акцентувати увагу на особливостях провадження господарської діяльності у цій сфері. Необхідно зазначити, що така діяльність, набуваючи транснаціонального характеру, підпадає під вплив окремих чинників. При цьому відбувається взаємодія законодавства України та правових норм тих іноземних держав, представники яких є учасниками фінансово-господарських операцій. Серед таких чинників ми пропонуємо виділити найбільш загальні, а саме:

1. Укладання та виконання угод (контрактів), які за формою реалізації значно різняться від господарських договорів між суб'єктами підприємництва всередині країни, а також повинні відповідати вимогам міжнародних договорів України;

2. Вільний вибір сторонами контракту грошової одиниці для проведення розрахунків, необхідність одержання передбачених законодавством дозволів (ліцензій) на здійснення окремих фінансово-господарських операцій, у тому числі щодо переміщення окремих груп товарів чи послуг через державний кордон, їх кількості (квотування, ліцензійне обмеження);

3. Дотримання спеціальних законодавчих норм у сфері ЗЕД, пов'язаних з обмеженням строку та встановленням форм розрахунків;

4. Особливий порядок іноземного представництва з боку фірми-контрагента (наприклад вимога подання довіреності на здійснення представницьких функцій, оформлену згідно із законом країни, де офіційно зареєстровано контору іноземного суб'єкта господарської діяльності) та ін.

Статистичні дані та висновки незалежних експертів свідчать про те, що сферу зовнішньоекономічної діяльності пронизують численні схеми тіньового капіталообороту, які супроводжують експортно-імпортні операції. Насамперед це - виведення валюти в офшорні зони та на банківські рахунки підставних фірм українських резидентів за кордоном, деперсоніфікація реальних власників інвестиційних коштів, які вкладаються в найбільш прибуткові галузі української економіки, а також учинення інших

протиправних дій, що створюють реальну загрозу зовнішньоекономічній безпеці. Все це значно підриває національну економічну безпеку України, оскільки збільшення питомої ваги іноземного капіталу в ключових галузях економіки веде до втрати можливості державного впливу на формування політики в таких сферах економічної діяльності.

Практика засвідчує, що на будь-якому етапі зовнішньоекономічної операції суб'єктами ЗЕД можуть бути вчинені дії, які межують з порушеннями кримінального законодавства, та містять реальні загрози національній безпеці України. Це відбувається внаслідок негативного впливу штучно створеного дисбалансу під час взаємодії фінансово-господарського та правового механізмів, при цьому функції координатора перебирають на себе корумповані представники правоохоронних та контрольно-дозвільних органів. Вони в ручному режимі, на власний розсуд вирішують питання щодо розміру податків, митних платежів, обов'язкових зборів, кількості та сортності товарів тощо. Злочинна діяльність вказаної категорії осіб зумовлює настання значних матеріальних збитків, що відображаються на мінімізації бюджетних надходжень, неправомірному зменшенні фінансових результатів від підприємницької діяльності суб'єктів цієї сфери при нарахуванні розмірів платежів до централізованих та децентралізованих фондів коштів, неправомірному виведенні валюти за межі України.

Згідно зі спільною вказівкою Генеральної прокуратури, МВС, СБУ, ДПА України № 12-157окв від 02.06.2004 р. щодо єдиного порядку обліку злочинів у сфері економіки до злочинів у зовнішньоекономічній діяльності необхідно відносити злочини, пов'язані з порушенням резидентами та органами валютного контролю (Державна податкова служба, Державна митна служба, НБУ інші уповноважені банки) вимог законів про зовнішньоекономічну діяльність, передусім при укладанні контрактів, здійсненні розрахунків, відшкодування ПДВ; злочини, скоєні на підприємствах усіх форм власності при проведенні таких дій: експорту або імпорту товарів; наданні вітчизняним та іноземним суб'єктам господарської діяльності послуг, у тому числі виробничих, транспортно-експедиційних, страхових, консультаційних, маркетингових, експортних, інвестиційних, посередницьких, брокерських, агентських, консигнаційних, управлінських, облікових, аудиторських, юридичних, туристичних, щодо працевлаштування за кордоном та інших послуг, що не заборонені законами України; наукової, науково-технічної, науково-виробничої, навчальної та іншої кооперації з іноземними суб'єктами господарської діяльності; міжнародних фінансових операцій та операцій з цінними паперами; кредитних і розрахункових операцій (у т. ч. повернення валютної виручки) між вітчизняними та іноземними суб'єктами господарської діяльності; товарообмінних (бартерних) операцій та іншої діяльності, побудованої на формах зустрічної торгівлі між вітчизняними та іноземними суб'єктами господарювання; лізингових операціях між вітчизняними та іноземними суб'єктами господарської діяльності; незаконному ввезенні в Україну і вивезені за її межі товарів; при проведенні службової діяльності працівників митних

органів [3].

Отже, можемо констатувати, що спільними зусиллями влади і компетентних органів можна суттєво обмежити тіньову складову сфери зовнішньоекономічної діяльності, мінімізувати втрати бюджету від контрабанди товарів до України та спрямувати додаткові фінансові надходження до централізованих та децентралізованих фондів коштів. Аналіз показує, що навіть фрагментарні та непослідовні спроби наведення ладу в цій сфері практично одразу дають відчутний позитивний ефект у формі збільшення надходжень до Держбюджету.

Використані джерела

1. Перепелица А. И. Уголовно-правовая борьба с организованной преступностью в сфере хозяйственной деятельности / А. И. Перепелица // Правові проблеми боротьби зі злочинністю. – 2002. Книга 2. – С. 154.
2. Зелинский А. Ф. Понятие «преступная деятельность» / А. Ф. Зелинский // Сов. государство и право. – 1978. – № 10. – С. 98–100.
3. Щодо єдиного порядку обліку злочинів у сфері економіки: (Спільна вказівка Ген. прокуратури, МВС, ДПА та Служби безпеки України від 02.06.2004 р. № 12-157) [Електронний ресурс]. – Режим доступу : stat@uvddon.donec.ua
4. Документування злочинних дій хабарників: [методич. рекомендації] / за ред. В. І. Литвиненка ; [упоряд.: В. С. Гарлицький, О. О. Дульський, В. М. Конорєв, В. Б. Моцар]. – К. : РВВ МВС України, 2001. – 80 с. – С. 6.
5. Загрози без кордонів [Електронний ресурс] / Український Інтерпол: шляхом розвитку. – Режим доступу : http://www.niss.gov.ua/Tasko/017.htm
6. Про рішення РНБОУ від 11 верес. 2009 р. «Про стан злочинності у державі та координацію діяльності органів державної влади у протидії злочинним проявам і корупції» : Указ Президента України від 27 жовт. 2009 р. № 870/2009 [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua
7. Науково-практичний коментар Кримінального кодексу України / за ред. М. І. Мельника, М. І. Хавронюка. – [6-те вид., переробл. та доповн.]. – К. : Юридична думка, 2009. – 1236 с.

Хоменко В.М. , Савченко В.О. - студентки юридичного факультету; науковий керівник: **Косиченко О.О.** – доцент кафедри економічної та інформаційної безпеки, кандидат технічних наук, доцент (Дніпропетровський державний університет внутрішніх справ)

ПРОБЛЕМИ ЛАТЕНТНОСТІ КІБЕРЗЛОЧИННОСТІ

У зв’язку із розвитком всесвітньої мережі Інтернет з’явився новий вид злочинності, а саме – кіберзлочинність. З кожним днем вона набирає оберти та несе за собою незворотні наслідки. Дана проблематика загострює необхідність боротьби зі злочинами такого роду: створення комп’ютерних систем, технологій з підвищеним рівнем безпеки в мережі, законодавчої бази,

незаконного обігу інформації, поширення не ліцензованого програмного забезпечення для комп'ютерів.

Теоретико-методичні та науково-практичні основи попередження дій кіберзлочинців були закладені у дослідженнях таких науковців: В. Голубєва, А. Долгової, К. Касперськи, М. Кастельса, Т. Кесаревої, Л. Куракова, Р.Лемоса, А. Лукацького, І. Рассолова, С. Смірнова.

Термін «кіберзлочинність» у нормативних документах невизначений. Концепція даного визначення була сформована завдяки діяльності правоохоронних органів розвинутих країн Європи та світу.

Латентна злочинність – це частина злочинності, яка складається зі злочинів, що фактично були вчинені, але не отримали відображення у офіційній загальнонаціональній кримінально-правовій статистиці.

Якщо розглядати види латентності злочинності, то до них слід віднести наступні:

1. *Природна (прихована) латентність* – це сукупність злочинів, про вчинення яких не стало відомо компетентним органам та інформація про які не відображена відповідним чином у офіційній кримінальній статистиці. Причинами цього виду латентності може бути, зокрема, відсутність потерпілого та свідків злочину (т. 3. "злочини без жертви"), незначна шкода, заподіяна злочином, небажання потерпілого заявляти про вчинений щодо нього злочин (наприклад, внаслідок родинних відносин із правопорушником або через почуття сорому чи страху), вдале приховання злочинцем слідів злочину тощо.
2. *Штучна (приховувана) латентність* – це сукупність злочинів, відомості щодо яких надійшли до правоохоронних органів, але при цьому реєстрації останніми події злочину не відбулося. Причинами виникнення штучної латентності можуть бути відмова у реєстрації заяви про злочин, помилкова або умисно невірна кваліфікація вчиненого як некримінального (цивільно-правового, адміністративного, дисциплінарного) правопорушення.
3. *Суміжна (межова, прикордонна) латентність* – це сукупність злочинів, які не оцінюються потерпілими як вчинені щодо них протиправні діяння. Причинами цієї латентності може бути необізнаність громадян із положеннями кримінального закону, вплив на оцінку вчиненого специфічних традицій певної місцевості тощо.

До подій, пов'язаних зі злочином можна віднести ситуації, при яких комп'ютер – знаряддя для вчинення злочинів, з метою порушення авторських прав, громадської безпеки, прав власності, моральності.

<u>*Класифікація кіберзлочинів:*</u>

1) правопорушення проти конфіденційності, цілісності і доступності комп'ютерних даних і систем, зокрема: - незаконний доступ, наприклад, шляхом злому, обману та іншими засобами; - нелегальне перехоплення комп'ютерних даних; - втручання у дані, включаючи навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це; - втручання у систему, включаючи умисне створення серйозних

перешкод функціонуванню комп'ютерної системи, наприклад, шляхом розподілених атак на ключову інформаційну інфраструктуру; - зловживання пристроями, тобто виготовлення, продаж, придбання для використання, розповсюдження пристроїв, комп'ютерних програм, комп'ютерних паролів або кодів доступу метою здійснення кіберзлочинів;

2) правопорушення, пов'язані з комп'ютерами, включаючи підробку і шахрайство, вчинені з використанням комп'ютерів;

3) правопорушення, пов'язані зі змістом інформації, зокрема, дитяча порнографія, расизм і ксенофобія;

4) правопорушення, пов'язані з порушенням авторських та суміжних прав, наприклад незаконне відтворення і використання комп'ютерних програм, аудіо/відео та інших видів цифрової продукції, а також баз даних і книг.

У той же час, з урахуванням мотивації злочинців, кіберзлочини представляється можливим умовно розділити на наступні категорії: кібершахрайство з метою заволодіння коштами; кібершахрайство з метою заволодіння інформацією (для власного користування або для подальшого продажу); втручання в роботу інформаційних систем з метою отримання доступу до автоматизованих систем управління (для навмисного пошкодження за винагороду або для нанесення шкоди конкурентам); інші злочини.

Ознайомившись з інформацією наданою вище можна зрозуміти, що кіберзлочини відрізняються від інших тим, що вони здійснюються за допомогою сучасної техніки (інтернет, комп’ютери, операційні системи, модернізована електронна техніка, тощо).

У 2008 році в десятці найбільш небезпечних загроз, що відзначаються фахівцями, були мережі ботів - «цілеспрямовані» атаки на урядові сайти, приватні підприємства та кінцевих користувачів. А в 2013 році, згідно прогнозом фахівців McAfee, на перший план вийшли загрози, пов`язані звикористанням мобільного доступу в Мережу.

Злочинність в кіберпросторі - одна з найгостріших проблем, з якою зіткнулося міжнародне співтовариство протягом останніх десятиліть у зв`язку з розвитком інформаційних технологій.

Щоб уявити собі масштаби і обороти цього кримінального бізнесу, досить навести деякі приклади. Віртуальні шахраї, заволодівши через Мережу номерами більш ніж мільйона банківських карт - громадян США, одночасно зробили розкрадання в 130 банкоматах в 49 містах Америки. При цьому вся операція зайняла не більше 30 хвилин, а розмір прибутку злочинців склав близько 9 млн. доларів, які потім були переведені на рахунки в різні держави, в основному в пострадянському просторі. У 2010 р. ФБР висунуло звинувачення проти 37 жителів Росії, України та інших східноєвропейських країн, підозрюваних у використання комп`ютерного вірусу для злому американських банківських рахунків.

Найбільш поширені злочини, які відносяться до другої і третьої категорії – це злом баз даних і виведення з ладу комп'ютерних систем

компаній і державних організацій, а також крадіжка інновацій або технологій.

На нашу думку, кіберзлочинність можливо охарактеризувати наступним чином – це злочинність, так званому «віртуальному просторі», яка змодельована за допомогою сучасної техніки. На сьогодні на електронних носіях та електронних базах знаходиться відомості про осіб, предмети, факти, події, явища та процеси.

Законодавство України, в особах голови держави та інших посадових осіб згідно діючого законодавства прагне захистити своїх громадян та мінімізувати кількість постраждалих від даного злочину.

Тому у 2016 р. Указом президента була затверджена Стратегія кібербезпеки України, а пізніше відбулося підписання Указу про створення Національного координаційного центру кібербезпеки. У вересні 2016 року Верховна Рада України у прийняла Закон "Про основні засади забезпечення кібербезпеки України".

Дуже важливим фактом є те, що національний законодавець закріпив у Кримінальному Кодексі України у розділі XVI злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. В Кримінально-процесуальному Кодексі також закріплені положення щодо злочинів в сфері ІТ-технологій. Та все ж таки тих норм, що закріплені в чинному законодавстві недостатньо, і вони не завжди є ефективними.

Останнім часом в Україні постало нове, дуже серйозне випробування; яке поширюється досить стрімко. Це створення таких інтернет-банд як "Синій кит", "Тихий дім", "Кити пливуть Вгору", "Море китів", "Біжи або помри", "Розбуди мене в 4.20", F57, F58, FF33, D28 тощо. Метою таких сайтів є пропаганда самогубства серед дітей та підлітків. Слід зазначити, що жертвами стають діти, в яких є проблеми з батьками, з друзями в школі, тобто особливо вразливі діти, які не отримують необхідної уваги та любові.

Однією з головних проблем, чому злочини в сфері інформаційних технологій мають низький рівень розкриття, є те, що людям не вистачає спеціальних знань. У зв'язку з тим, що бурхливий розвиток інформаційних технологій методики судово-експертного дослідження даних об'єктів вимагають постійного оновлення та доопрацювання. Кожного року змінюються операційні системи, формати даних, протоколи і середовище перенесення даних, технічні засоби, що забезпечують процеси передання та обрабки інформації.

Сліди кіберзлочинів досліджуються за допомогою комп'ютерно-технічної експертизи та експертизи відео- та звукозапису. А щодо наукової експертизи, то він повністю залежить від рівня професійної підготовки експертних кадрів. У світі досить ретельно підходять до проблеми боротьби з кіберзлочиннами, і до її вирішення безпосередньо залучається державна влада. Адже ту кількість інформації, яка протікає по мережі Інтернет щоденно, просто нереально контролювати самостійно. Тому, починаючи з 2009 року, влада США розпочала створення власних кібервійськ — Агенство

національної безпеки, яке також опікується питаннями інформаційної війни. У ЕС функціонує Агенство з мережевої та інформаційної безпеки, у НАТО створений комітет з кібернетичної оборони, а також Спільний центр з кібернетичної оборони.

Так, відомий російський виробник антивірусного програмного забезпечення "Лаборатория Касперского" за останні роки виявив декілька бойових вірусів, які є настільки складними, що їх розробкою, без сумніву, фундаментально і багато часу займалися великі за чисельністю групи фахівців найвищої кваліфікації, а вартість розробки цих шкідливих програм оцінена в 100 мільйонів доларів США. Один з таких вірусів уже був застосований в Іраку під час бойових дій.

Під час інформаційних війн зброєю виступають засоби масової інформації, соціальні мережі, "тролінг" та блогсфери. Що стосується України, то в даній країні відсутні власні майданчики для обміну інформації (Facebook, Twitter, YouTube, Вконтакте, Однокласники тощо) на відміну від зарубіжних країн, також країна не підтримує національні елетронні програми, ми не випускаємо власних електронних приладів тощо. А це означає, що ми дуже вразливі під час будь-якої інформаційної війни. Кіберзлочинність в Україні розвинена чи не найвище серед усіх європейських країн. Ми вважаємо, що наша держава повинна приділити набагато більше уваги даному питанню, дана прогалина робить нас дуже вразливими.

Для забезпечення кібербезпеки існують різноманітні міжнародні договори, так у 2002 році Організація Об'єднаних Націй видала резолюцію Генеральної Асамблеї, де були прийняті "Елементи для створення глобальної культури кібербезпеки". В документі зазначається 9 основних взаємодоповнюючих елементів, які держави-учасники повинні дотримуватися, серед них: обізнаність, відповідальність, реагування, етика, демократія, оцінка ризику, проектування та впровадження засобів забезпечення безпеки, управління забезпеченням безпеки та переоцінка.

Підсумовуючи усе вище зазначене, вважаємо за доцільне підкреслити наступні моменти: ми маємо неймовірний світ сучасних технологій, які повинні працювати на благо людей. Все, що іде всупереч засадам демократичного суспільства, повинно бути засуджено за законом, тільки через відповідну законодавчу базу справедливий неупереджений суд в суспільстві встановлюється справедливість і порядок. необхідно внести деякі доповнення до Кримінального Кодексу України, які будуть гарантувати кібербезпеку людей. До таких злочинів можна віднести : дефейс, шантажування, вбивство, екстремізм в мережі, наклеп, образи, фішинг, комп'ютерне шпигунство тощо.

Використані джерела

1. Бондаренко О. С. та Рєпін Д. А. – Кіберзлочинність в Україні: причини, ознаки та заходи протидії - [Електрон. ресурс] / Режим доступу: http://www.pap.in.ua/1_2018/73.pdf

2. В. Б. Дзюндзюк та Б. В. Дзюндзюк – поява та розвиток кіберзлочинності – [Електрон. ресурс] / Режим доступу: http://www.kbuapa.kharkov.ua/e-book/db/2013-1/doc/1/01.pdf
3. Панфілов О. Ю. – До проблеми оцінки сучасного рівня інформаційної безпеки України – Зовнішня торгівля: право, економіка,фінанси, № 3 – 2012 [Електрон. ресурс] / Режим доступу: http://zt.knteu.kiev.ua/files/2012/03(62)2012/3_12_34.pdf

Цісар Б.О. - курсант факультету економіко-правової безпеки;
науковий керівник – **Кокарєв І.В.** - доцент кафедри економічної та інформаційної безпеки, кандидат економічних наук, доцент
(Дніпропетровський державний університет внутрішніх справ)

ЕКОНОМІЧНА БЕЗПЕКА В УКРАЇНІ

Проблемність економічної безпеки в умовах подальшої глобалізації набуває статусу найвищого пріоритету в державній політиці. Виняткове значення вона має при аргументації прийняття політичних рішень. Науково-концептуальні засади про економічну безпеку забезпечують формування відповідної політики на рівні держави чи суб'єктів нижчих організаційних рівнів. Система забезпечення економічної безпеки передбачає здійснення постійного моніторингу соціально-економічних процесів з точки зору їхнього впливу на стан економічної безпеки, оцінку з цих позицій стратегічних програм, нормативно-правових актів, а також аналіз ефективності поточних рішень у сфері економічної політики.

Термін «національна безпека» започатковано США, який вперше офіційно було використано Президентом Сполучених Штатів Теодором Рузвельтом. У своєму посланні Конгресу в 1934 р. він виправдовував захоплення зони майбутнього Панамського каналу інтересами «національної безпеки США». У 1947 р. Конгресом США було прийнято закон «Про національну безпеку». Відтак проблема національної безпеки стала однією із стрижневих у наукових дослідженнях американських і західноєвропейських учених у соціологічній, політологічній та економічній галузях. Після Другої світової війни США вирішили максимально використати тогочасні можливості свого впливу. Саме тоді американці й розробили концепцію національної безпеки, а на її основі — доктрину державної безпеки. Закон США «Про національну безпеку» зобов'язав усі державні структури провадити цілеспрямовану політику щодо воєнно-політичного протистояння з Радянським Союзом та державами Варшавського договору [1].

У науковій літературі наводиться багато поглядів на визначення поняття «економічна безпека держави». Визначення вітчизняних та зарубіжних фахівців відрізняються різноманітністю підходів і суттєво розбігаються за змістом [2]. Зокрема, на думку Л.І. Дмитриченка, економічна безпека — це стан держави, за якого вона має можливість створювати і розвивати

ефективні умови для перспективного розвитку та зростання добробуту громадян. Основним критерієм економічної безпеки країни вважається здатність її економіки зберігати або, принаймні, швидко поновлювати рівень суспільного відтворення в умовах критичного зменшення (припинення) поставок ресурсів (товарів, послуг, технологій тощо) або кризових ситуацій внутрішнього чи зовнішнього характеру [3]. На думку В. А. Ліпкана, національна безпека — це свідомий цілеспрямований організований вплив суб'єкта управління на реальні загрози й небезпеки, завдяки якому державні та недержавні інституції створюють сприятливі умови для прогресуючого розвитку українських національних інтересів, джерел добробуту конкретної особи, суспільства й держави, а також забезпечують ефективне функціонування системи національної безпеки України [4, с. 26].

Попри велику кількість публікацій, водночас, залишається багато невирішених проблем у теорії та практиці економічної безпеки, яка є основною складовою національної безпеки держави. Окрім того, ситуацію ускладнює відсутність системності стосовно понятійного апарату у цій сфері, а також обґрунтованих пропозицій щодо впровадження сучасних методів та моделей управління економічною безпекою на всіх рівнях управління економікою. Наведене, а також динамічні зміни у сучасному політико-соціальному і економічному світовому середовищі зумовлюють подальших досліджень поняття економічної безпеки.

Більшість дослідників економічної безпеки доходять висновку, що основними структурними елементами економічної безпеки, які необхідно застосувати при її аналізі на рівні держави, є такі:

- енергетична безпека;
- фінансова безпека;
- соціальна безпека;
- інноваційно-технологічна безпека;
- продовольча безпека; зовнішньоекономічна безпека.

В системі національної безпеки економічна безпека забезпечує чітко визначені функції, несе у собі суттєве функціональне навантаження. Її сутність полягає у тому, яка вона є матеріальною основою національної суверенності, що визначає реальні можливості у забезпеченні інших видів безпеки. Тобто економічна безпека — це підґрунтя для функціонування всіх інших її елементів, що входять у цю систему (військової, технічної, продовольчої, екологічної).

В узагальненому, синтезованому змісті національну безпеку найбільш об'єктивно трактувати як спроможність держави своєчасно реагувати на внутрішні та зовнішні дестабілізуючі чинники, які проявляються у формі економічної, соціальної, політичної, військової та інших загроз, наявність яких може спричинити глибокі соціально-економічні потрясіння та порушення цілісності країни.

Оскільки безпека держави у всіх її формах реалізується через відповідне державне фінансування, основою якого є створений внутрішній валовий продукт, то чи не найважливішою її складовою є саме економічна безпека.

Вона характеризується таким станом національної економіки, який дає змогу зберігати стійкість до внутрішніх і зовнішніх загроз, забезпечує конкурентоспроможність держави, її незалежність від зовнішнього середовища та економічний добробут населення.

Загалом можна дотримуватись позиції, що забезпечення економічної безпеки держави має здійснюватися як складова національної безпеки держави, що потребує орієнтації на стратегічні напрями її розвитку. Тому науковцями й акцентується на важливості коригувати будь-які наміри у сфері економічної безпеки відповідно до Стратегії національної безпеки України на 2010–2015 роки [5]**.** Сьогодні як ніколи загострюється надзвичайно важливе питання забезпечення економічної безпеки України, що є одним з найважливіших національних пріоритетів і вимагає посиленої уваги представників владних структур, громадських і політичних рухів, науковців, широких кіл громадськості. Забезпечення економічної безпеки є гарантом державної незалежності України, умовою її сталого розвитку та зростання добробуту громадян. Тому досить важливим є ретельне дослідження економічного становища нашої держави і прийняття кардинальних рішень щодо його покращення.

Використані джерела

1. Кириченко О. А. Проблеми управління економічною безпекою суб'єктів господарювання : монографія / О. А. Кириченко, В. С. Сідак, С. М. Лаптєв та ін. — К. : УЕП «Крок», 2008. — 401 с.
2. Бесчастний А. В. Економічна безпека України у контексті світової економічної кризи // Економіка і держава. — 2009. — № 15. — С. 67–69.
3. Дмитриченко Л. И. Государственное регулирование экономики: методология и теория : монография. — Донецк: УкрИТЭК, 2008. — 330 с.
4. Ліпкан В. А. Теоретико-методологічні засади управління у сфері національної безпеки України / В. А. Ліпкан. — К. : Текст, 2005. — 350 с.
5. Стратегія національної безпеки України на 2010–2015 рр. Електронний ресурс. — Режим доступу: http://www.cirs.kiev.ua/cs/en/home/98-2010-2015-.html.

Черкас К.Ш. - курсант факультету економіко-правової безпеки;
науковий керівник **Кокарєв І.В.** - доцент кафедри економічної та інформаційної безпеки
(Дніпроптеровський державний університет внутрішніх справ)

ШЛЯХИ ОТРИМАННЯ ЗЛОЧИННИХ ПРИБУТКІВ В УКРАЇНІ

У ст. 209 Кримінального кодексу України надано поняття «відмивання» доходів, одержаних злочинним шляхом як «вчинення фінансової операції чи укладання угоди з коштами або іншим майном, одержаним унаслідок вчинення суспільно небезпечного протиправного діяння, що передувало легалізації (відмиванню) доходів, а також вчинення дій, спрямованих на

приховання чи маскування незаконного походження таких коштів або іншого майна чи володіння ними, прав на такі кошти або майно, джерела їх походження, місцезнаходження, переміщення, а так само набуття, володіння або використання коштів чи іншого майна, одержаних унаслідок вчинення суспільно небезпечного протиправного діяння, що передувало легалізації (відмиванню) доходів» [1].

Актуальність теми полягає в тому, що більше половини організацій світової торгівлі входить у великі корпорації. І половина світової торгівлі проходить через офшорні центри, оскільки корпорації змінюють прибуток, де вони можуть уникнути податків. Також, шахрайство здійснюється через офшорні оболонки та банківські рахунки, і це відбувається у глобальному масштабі.

Як свідчить світова практика, у підприємства є три основні легальні джерела отримання прибутку:

- перший - прибуток утворюється за рахунок монопольного становища підприємства з випуску тієї чи іншої продукції або (та) унікальності продукту. Підтримка цього джерела на відносно високому рівні передбачає постійне оновлення продукту. Тут слід враховувати такі протидіючі сили, як антимонопольна політика держави і зростаюча конкуренція з боку інших підприємств;
- другий - пов'язаний безпосередньо з виробничою і підприємницькою діяльністю. Практично це стосується всіх підприємств. Ефективність його використання залежить від знання кон'юнктури ринку і вміння адаптувати розвиток виробництва під цю постійно мінливу кон'юнктуру. Тут усе зводиться до проведення відповідного маркетингу. Величина прибутку в даному випадку залежить, по-перше, від правильності вибору виробничої спрямованості підприємства з випуску продукції (вибір продуктів, що користуються стабільним і високим опитуванням), по-друге, від створення конкурентоспроможних умов продажу своїх товарів і надання послуг (ціна, строки поставок , обслуговування покупців; післяпродажне обслуговування); по-третє, від обсягів виробництва (чим більший обсяг виробництва, тим більше маса прибутку), по-четверте, від структури зниження витрат виробництва;
- третій – прибуток виникає в результаті інноваційної діяльності підприємства. Його використання передбачає постійного оновлення продукції, забезпечення її конкурентоспроможності, зростання обсягів реалізації та збільшення маси прибутку [2].

При виборі шляхів збільшення прибутку орієнтуються в основному на внутрішні фактори, що впливають на величину прибутку. Збільшення прибутку підприємства може бути досягнуто за рахунок збільшення випуску продукції; поліпшення якості продукції; продажу зайвого устаткування та іншого майна або здачі його в оренду; зниження собівартості продукції за рахунок більш раціонального використання матеріальних ресурсів, виробничих потужностей і площ, робочої сили і робочого часу; диверсифікації виробництва; розширення ринку продажу і т.д.

Але, крім цього існують ще й нелегальні, або кримінальні шляхи одержання прибутку та схеми «відмивання» грошей. Відмивання грошей – це процес, за допомогою якого створюються, існують і використовуються доходи, які отримані за межами законодавчої та нормативно-правової бази держави.

Відмивання грошей – досить складний процес. Доходи, отриманні злочинним шляхом, проводяться через складові фінансової системи з метою приховання їхнього незаконного походження і надання їм виду легально отриманих. Сам процес відмивання грошей являє собою складну послідовність операцій в системі фінансових розрахунків. Між тим аналіз міжнародних нормативних актів дозволяє виділити кілька основних складових:

– розміщення - це впровадження наявних коштів у фінансові інструменти, а також розміщення їх у містах віддалених від місць їхнього походження;

– шарування - відокремлення незаконних доходів від їхніх джерел шляхом створення складного ланцюга фінансових операцій, спрямованих на маскування послідовності сліду цих доходів;

– інтеграція - створення схем легальності злочинно отриманим фінансовим коштам. Гроші знаходять фіктивне легальне джерело походження та інвестуються в реальну економіку.

Відмивання грошей загрожує економічній та соціальній стабільності як окремої держави, так і світової спільноти загалом. Тому важливо здійснювати ефективні заходи боротьби з легалізацією незаконних доходів. Успішна система протидії відмиванню коштів допоможе також зменшити кількість шахрайств та інших злочинів, адже зі зростанням ймовірності покарання та зменшенням можливостей до легалізації доходів у злочинців знижуватимуться стимули до протиправних дій.

Використані джерела

1. Андрушко П. П. Проблеми кваліфікації легалізації (відмивання) грошових коштів та іншого майна, здобутих злочинним шляхом. Правова держава /П. П. Андрушко // Щорічник наукових праць Інституту держави і право ім. В. М. Корецького НАН України. – Вип. 13. – К., 2012. – С. 334–346.
2. Ситник Г., Баранов Р. Світовий досвід щодо здійснення боротьби з легалізацією (відмиванням) доходів, одержаних злочинним шляхом, для України / Г. Ситник, Р. Баранов // Інвестиції: практика та досвід. – 2014. – № 17. – С. 213-216.
3. Грищенко О. Проблеми боротьби із «відмиванням брудних коштів» [Електронний ресурс] / О. Грищенко. – Режим доступу до статті: http://www.justinian.com.ua/article.php?id=1816
4. Клочко А.М. Окремі питання легалізації коштів, отриманих злочинним шляхом у банківській сфері / А.М. Клочко // Форум права. – 2014. – № 1. – С. 228–232 [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/j-pdf/FP_index.htm_2014_1_40.pdf

Шостак А.О. - студентка юридичного факультету; науковий керівник - **Рибальченко Л.В.** - доцент кафедри економічної та інформаційної безпеки, кандидат економічних наук, доцент (Дніпропетровський державний університет внутрішніх справ)

НАПРЯМИ ПОСИЛЕННЯ ІННОВАЦІЙНОЇ СКЛАДОВОЇ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ

Підвищення ефективності національної економіки безпосередньо пов'язане з прискореним та безпечним розвитком інноваційної сфери. Саме інноваційна безпека сприяє підйому і подальшому розвитку економіки, її технологічній модернізації. При цьому інноваційна безпека дає можливість реалізації конкурентних переваг національній економіці на світових ринках. При переході до нових соціально-економічних відносин, відбувається посилення існуючих та утворення нових факторів, що негативно впливають на інноваційну безпеку економічної системи.

Інноваційний розвиток і безпека – це дві невід'ємні складові економічної системи. Сучасна інноваційна модель розвитку, має значну кількість різноманітних підсистем, яким характерні як позитивні так і негативні фактори впливу. Це характеризується тим, що внаслідок впровадження інновацій, виникає неузгодженість у стійкому функціонуванні всієї системи. Внаслідок цього порушується механізм системи розвитку та управління, відбувається збій окремих підсистем і утворюються небезпечні фактори впливу.

Інноваційна безпека направлена на досягнення стану високотехнологічного, стабільного, економічно-ефективного забезпечення інноваціями економіки і соціальної сфери країни, а також створення умов для модернізації галузей виробництва, формування і реалізації політики стабільного соціально-економічного розвитку країни.

Важливість інновацій для забезпечення економічної безпеки держави пояснюється й тим, що саме за рахунок їх упровадження можна швидко вирішувати проблеми подолання наслідків економічної чи фінансової кризи. Перебудова виробничих зв'язків та переорієнтація промислового сектору, а також перетворення України в експортера інноваційних технологій дозволить значно підвищити рівень конкурентоспроможності економіки, що приведе до стабілізації національних ринків за рахунок припливу закордонного капіталу. Для того, щоб інноваційні відносини стали стабілізуючим фактором економічного розвитку, слід розробити дієві механізми господарсько-правового забезпечення державного регулювання в цій сфері. А для розуміння природи їх ефективної реалізації доцільно провести ґрунтовний теоретико-методологічний аналіз.

Інновації втілюються у вигляді нових технологій, видів продукції, організаційно-технічних і соціально-економічних рішень виробничого, фінансового, комерційного та іншого характеру. На мікроекономічному рівні інновація розглядається як результат інноваційної дальності підприємства, втілений у формі конкретного продукту, в на макроекономічному рівні, на рівні держави, інновації розглядаються як додатковий елемент економічного потенціалу, за рахунок якого можна підвищити рівень конкурентоспроможності економіки.

Розвиток інноваційної діяльності повинен стати невід'ємною складовою реформування економіки країни для посилення інноваційної безпеки. Важливо зазначити, що криза інноваційної сфери становить загрозу економічній безпеці країни, тому необхідно вдосконалювати механізми державного регулювання інноваційної сфери, здійснювати заходи, спрямовані на підвищення інноваційної мотивації господарюючих суб'єктів. Першочерговим завданням підвищення рівня інноваційної безпеки є подолання існуючих загроз та використання інноваційного потенціалу. Тому, на нашу думку, головні напрями посилення інноваційної безпеки є такими:

- розвиток державних наукових і науково-технологічних організацій, що - здійснюватимуть ефективну координацію наукових досліджень;
- створення нових передових технологічних укладів, інтенсивне технологічне оновлення базових секторів економіки;
- підвищення якості і доступності освіти та підготовки наукових кадрів
- політична стабілізація та визначення пріоритетів у зовнішній політиці – чітка орієнтація на створення зони вільної торгівлі з ЄС;
- створення умов для вільної конкуренції – зменшення адміністративних бар'єрів та преференцій на шляху руху капіталів;
- прийняття пакету законів щодо ліквідації корупції, зменшення адміністративного тиску на бізнес та сприяння відділенню бізнесу від влади;
- визначення пріоритетних для надання державної фінансової підтримки інвестиційних проектів, спрямованих на розвиток експорту та імпорту виробництва, високотехнологічної конкурентоспроможної продукції, розвиток інфраструктурних і базових секторів економіки.

Таким чином, головними загрозами інноваційній безпеці України є низька результативність інноваційної діяльності, недостатнє фінансування, зниження кількості спеціалістів, які виконують науково-технічні роботи, використання застарілих технологій. Активізація інноваційної діяльності, стимулювання технологічних змін у виробництві, вдосконалення інституційно-правового та інформаційно-аналітичного забезпечення зумовлять посилення інноваційної безпеки України. Подальшого дослідження потребують питання вдосконалення методики оцінки інноваційної безпеки України для визначення і формування шляхів усунення загроз.

Використані джерела

1. Гордуновський О.І. Сучасний стан та напрями посилення інноваційної безпеки України / О.М. Гордуновський // Фінановий простір. – 2014. – № 2 (14). – С. 23-29.

2. Барановський О.І. Фінансова безпека в Україні (методологія оцінки та механізми забезпечення) : монографія / О. І. Барановський. – К. : Київ. нац. торг.-екон. ун-т, 2014. – 759 с.

Наукове видання

ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Матеріали Всеукраїнського науково-практичного семінару

(м. Дніпро, 23 листопада 2018 р.)

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