КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ННІППЕ ЛьвДУВС

КАФЕДРА ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ ТА СПЕЦІАЛЬНОЇ ТЕХНІКИ

ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ПРОБЛЕМИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ, СПЕЦІАЛЬНИХ ТЕХНІЧНИХ ЗАСОБІВ У ДІЯЛЬНОСТІ ОВС, НАВЧАЛЬНОМУ ПРОЦЕСІ, ВЗАЄМОДІЇ З ІНШИМИ СЛУЖБАМИ

Збірник наукових статей за матеріалами доповідей
науково-практичної конференції
14 грудня 2012 р.

ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ПРОБЛЕМИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ, СПЕЦІАЛЬНИХ ТЕХНІЧНИХ ЗАСОБІВ У ДІЯЛЬНОСТІ ОВС, НАВЧАЛЬНОМУ ПРОЦЕСІ, ВЗАЄМОДІЇ З ІНШИМИ СЛУЖБАМИ

Збірник наукових статей за матеріалами доповідей науково-практичної конференції

14 грудня 2012 р.

Львів
2012

ББК 32.973
П 78

Рекомендовано до друку Вченою радою
Навчально-наукового інституту права, психології та економіки
Львівського державного університету внутрішніх справ
(протокол № 2 від 29.10.2012р.)

РЕДАКЦІЙНА КОЛЕГІЯ

П 78 Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами. Збірник наукових статей за матеріалами доповідей науково-практичної конференції 14 грудня 2012 року. – Львів: ЛьвДУВС, 2012. – 233 с.

У збірнику вміщено наукові статті за матеріалами доповідей, підготовлених учасниками науково-практичної конференції «Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами», що проводилася 14 грудня 2012 р. у Львівському державному університеті внутрішніх справ.

ББК 32.973

КАФЕДРА ОПЕРАТИВНО-РОЗШУКОВОЇ
ДІЯЛЬНОСТІ ТА СПЕЦІАЛЬНОЇ ТЕХНІКИ

ВІТАЛЬНЕ СЛОВО

до учасників 12-ої науково-практичної конференції
«Проблеми застосування інформаційних технологій,
спеціальних технічних засобів у діяльності ОВС,
навчальному процесі, взаємодії з іншими службами»

Кафедра інформаційних технологій (ІТ) з 2011 р. є загальноінститутським структурним підрозділом Навчально-наукового інституту права, психології та економіки ЛьвДУВС. У 2012-13 н.р. у складі кафедри ІТ працює 10 співробітників (9 викладачів і 1 ст. лаборант), серед яких один доктор наук, два професори та п'ять кандидатів наук. Про значний науковий і творчий потенціал викладачів кафедри ІТ свідчить захист за останні чотири роки двох дисертаційних робіт на здобуття наукового ступеня кандидата фізико-математичних наук, а також підготовка до захисту ще трьома працівниками кафедри дисертацій за фізико-математичним і технічним спрямуванням. Доцільно особливо відзначити рооту двох доцентів, які активно працюють над докторськими дисертаціями.

За 11 місяців 2012 р. науковцями кафедри ІТ опубліковані 1 монографія, 5 навчальних посібників, 12 наукових статей (5 статей у співавторстві з аспірантами). Результати досліджень апробувались та опубліковані в матеріалах 2 міжнародних конференцій та симпозіумів, 2 міжвузівських, а також зроблено і надруковано 12 доповідей на університетських науково-практичних заходах.

4 конференційні публікації виконані сумісно зі студентами і курсантами.

Вагомі досягнення кафедри у винахідницькій галузі (38 патентів). У січні-листопаді 2012 р. кафедра ІТ подала 14 заявок на винаходи і отримала 5 патентів та 5 позитивних рішень. 12 винаходів опубліковані у співавторстві з пошукувачами вчених звань. Більшість патентів отримана на винаходи у сфері спеціальної техніки МВС та МНС. Авторський колектив винахідників технічних засобів спеціального призначення очолюють генерал-лейтенант міліції, д.ю.н., професор, Заслужений юрист України Цимбалюк М.М. і д.т.н., професор, Заслужений винахідник України Керницький І.С.

Маючи такий істотний творчий доробок, можна сподіватися на достойну участь кафедри ІТ в конкурсі винахідницької діяльності серед технічних кафедр системи відомчої вищої освіти МВС України і на обґрунтоване змагання ЛьвДУВС за провідне місце серед ВНЗ МВС у галузі винахідництва.

Кафедра оперативно-розшукової діяльності та спеціальної техніки (ОРДСТ) створена у 1993 році. До професорсько-викладацького складу кафедри входить 17 осіб – три доктори юридичних наук, дев'ять кандидатів юридичних наук та два кандидати технічних наук. У 2011-12 рр. науково-викладацьким складом кафедри ОРД підготовлено з проблем боротьби з організованою та економічною злочинністю 4 монографії, 5 навчальних посібників, опубліковано 28 наукових статей; на кафедрі проведено 11 успішних апробацій дисертаційних робіт на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 За звітний рік 2 працівникам кафедри присуджено наукові ступені кандидатів юридичних наук.

Хочемо висловити думку колективів кафедр ІТ та ОРДСТ про те, що традиційна 12-та конференція сприятиме висвітленню найновіших досягнень науковців у галузі інформаційних технологій та спецтехніки, мобілізуватиме їх на подальші дослідження і спричинить інтеграцію зусиль провідних вчених у науково-технічному розвитку практичних підрозділів ОВС.

Щиро зичимо учасникам конференції творчих злетів, вагомих досягнень, особистих успіхів і плідної роботи.

З ПОВАГОЮ ТА НАЙКРАЩИМИ ПОБАЖАННЯМИ

Завідувач кафедри ІТ *Іван Керницький*
Начальник кафедри ОРДСТ *Андрій Баб'як*
14 грудня 2012 р.

І. НАУКОВО-МЕТОДИЧНІ, НОРМАТИВНО-ПРАВОВІ ТА ПРОГРАМНО-ТЕХНІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОПЕРАТИВНІЙ ДІЯЛЬНОСТІ ОРГАНІВ ВНУТРІШНІХ СПРАВ

ЩОДО ЗДІЙСНЕННЯ ОПЕРАТИВНО-РОЗШУКОВОГО ПОПЕРЕДЖЕННЯ ЗЛОЧИНІВ ПІДРОЗДІЛАМИ ОРГАНІВ ВНУТРІШНІХ СПРАВ

Долженков О.Ф.,
директор ННІФЕБП Одеського державного університету внутрішніх справ д.ю.н., професор
Криволапчук В.О.,
здобувач кафедри оперативно-розшукової діяльності Одеського державного університету внутрішніх справ

Безкомпромісна боротьба зі злочинністю у всіх сферах суспільного життя, ефективна протидія криміналітету є однією із важливих складових забезпечення як національної, так і економічної безпеки держави. Провідне місце у цьому займають оперативні підрозділи органів внутрішніх справ, які здійснюють боротьбу зі злочинністю за допомогою специфічних оперативно-розшукових методів, заходів та засобів. Оперативним підрозділам МВС України, як суб'єкту ОРД, статтею 5 Закону України «Про оперативно-розшукову діяльність» надано право здійснювати оперативно-розшукову діяльність, головним завданням якої є пошук і фіксація фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України. Статтею 7 цього Закону передбачено також здійснення оперативно-розшукового попередження злочинів, тобто «вживати необхідних оперативно-розшукових заходів щодо попередження, своєчасного виявлення, припинення і розкриття злочинів та викриття причин і умов, які сприяють вчиненню злочинів, здійснювати профілактику правопорушень». Першочергове місце у даному випадку

повинні займати дії щодо попередження та недопущення настання суспільно небезпечних наслідків, заподіяння шкоди людині, що залишається одним із пріоритетних напрямків діяльності органів внутрішніх справ у боротьбі зі злочинністю, оскільки забезпечує виявлення й усунення її підґрунтя. Ця значущість попередження злочинів визначається тим, що криміногенні чинники найбільш піддаються впливу тоді, коли вони ще не набрали сили, знаходяться у стані зародження і тому легше піддаються усуненню.

У оперативно-розшуковому попередженні злочинів можна виділити такі складові елементи:

- профілактика злочинів – діяльність щодо виявлення й усунення причин цих злочинів і умов, що сприяють їх вчиненню (загальна профілактика), а також встановлення осіб, схильних до вчинення злочинів через антигромадський спосіб життя, поведінку, систематичне вживання алкогольних напоїв, наркотиків, вплив на них з метою недопущення з їх боку злочинів (індивідуальна профілактика);
- запобігання (недопущення) злочинів – діяльність щодо встановлення осіб, які замислюють чи готують конкретний злочин, і вжиття необхідних заходів, що виключають реалізацію їхніх намірів;
- припинення злочинів – діяльність щодо виявлення осіб, які готуються до вчинення злочинів або вчиняють замах на них, і вжиття необхідних заходів для припинення їхніх злочинних дій.

По своїй природі оперативно-профілактичний вплив є превентивною дією на основі реалізації норм оперативно-розшукового права. Якщо немає підстав притягати особу до кримінальної відповідальності, але її наміри твердо спрямовані на вчинення протиправних дій або ж конкретизувалися підготовчі до злочину дії, то оперативним працівником повинні прийматися попереджувально-профілактичні заходи. Необхідно зазначити, що в цілому попереджувально-профілактичний потенціал оперативно-розшукової діяльності виражається в реальних повноваженнях оперативних підрозділів проникати безпосередньо в кримінальне середовище, приховано спосте-

рігати за допомогою оперативних можливостей за зародженням і розвитком злочинної діяльності, виявляти й фіксувати при цьому фактичні дані протиправної діяльності тощо.

При попередженні злочинів використовуються, як правило, всі сили, засоби і методи в комплексі, залежно від конкретних умов і обставин. Перш за все, це стосується питань індивідуальної профілактики. Оперативні підрозділи повинні виявляти осіб, поведінка чи дії яких дають підстави вважати про виникнення протиправного умислу та приймати заходи, націлені на схиляння особи до відмови від вчинення злочину або створення обстановки, яка перешкоджає реалізації протиправних намірів. До вказаних заходів відноситься встановлення оперативного спостереження за поведінкою та діями особи, проведення з нею бесід за місцем роботи чи проживання, а також з його рідними чи дружніми зв'язками. Такі бесіди спрямовані на затвердження думки про невідворотність покарання, матеріальну та моральну шкоду, що можуть понести рідні та близькі об'єкту профілактики. Добровільне волевиявлення особи не скоювати злочин під психологічним впливом інших осіб не залежить від того, за чиєю ініціативою виникла і зміцнилася ідея про відмову. Головне, щоб вона оволоділа особою, щодо якої здійснюється профілактика, і привела її до того, щоб утриматися від подальшого здійснення дій для досягнення злочинного результату.

До індивідуального впливу на осіб, які замислюють чи готують вчинення злочину, варто також віднести заходи щодо притягнення їх до кримінальної відповідальності. У цьому випадку встановлюються в діях таких осіб ознак готування до вчинення злочину, тобто вчинення в процесі підготовки дій, караних в кримінальному порядку, а також наявності в цих діях самостійного складу злочину (незаконне придбання зброї, придбання предметів, які планується використати для вчинення злочину тощо).

В сучасних умовах працівники оперативних підрозділів ОВС України вкрай недостатньо уділяють уваги запобіганню злочинам. Зазначені недоліки у профілактиці злочинів обумовлює також система оцінки роботи оперативних підрозділів, які більшою мірою орієнтовані не на попередження, а лише на

розкриття злочинів, що неминуче призводить до збільшення останніх. Така ситуація є неприпустимою та потребує корегування шляхом відомчого нормативного врегулювання. Цим цілям може служити доповнення звітності показниками, що реально відбивають роботу оперативних підрозділів щодо попередження злочинів на стадіях задуму, готування та замаху.

МЕТОДОЛОГІЯ ОЦІНКИ РІВНІВ ЗАХИЩЕНОСТІ ІНТЕГРОВАНОЇ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ОПЕРАТИВНОГО ІНФОРМУВАННЯ МВС УКРАЇНИ

Кудінов В.А.,
начальник кафедри інформаційних технологій Національної академії внутрішніх справ, к.ф.-м.н., доцент
Корченко О.Г.,
завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету, д.т.н., професор

Для забезпечення оперативного інформування в органах і підрозділах внутрішніх справ (далі – ОВС) України була створена інтегрована інформаційно-телекомунікаційна система оперативного інформування (далі – СОІ) МВС України [1]. Вона представляє собою комплекс нормативно-правових, організаційно-кадрових, програмно-апаратних та інших заходів та засобів, що здійснює цілодобову обробку оперативної інформації про резонансні злочини та інші надзвичайні події, які сталися на території України [2, 3].

Головними цілями функціонування СОІ МВС України є своєчасне, достовірне, повне та якісне інформування керівництва Міністерства внутрішніх справ України, зацікавлених інстанцій, держави про реальний стан й динаміку оперативної обстановки в цілому в Україні та окремих її регіонах для прийняття впливових управлінських рішень на її покращання, а також постійне стеження за своєчасністю вирішення та розкриттям резонансних злочинів, ліквідації наслідків інших надзвичайних подій [1].

Дана система функціонує в корпоративній мережі ОВС України, а завдання щодо забезпечення її функціонування

покладені на чергові частини ОВС України. Тому питання забезпечення захисту СОІ МВС України безпосередньо пов'язані з розв'язанням проблем захисту функціонування корпоративної мережі та програмно-технічного комплексу чергових частин ОВС України, що знайшло відображення в низці наукових робіт.

Так, зокрема, в роботі [4] серед основних напрямів розвитку СОІ МВС України запропоновано розробити та впровадити відповідні комплексні заходи та засоби захисту оперативної інформації. Зазначена комплексна система захисту інформації (далі – КСЗІ) дозволить запобігти або ускладнити можливість реалізації загроз для оперативної інформації, а також знизити потенційні збитки у разі їх здійснення, локалізацію та ліквідацію наслідків їх впливу [5-6].

Питанням аналізу загальної структури корпоративної мережі ОВС України, а також моделей об'єкта захисту інформації і можливого порушника безпеки мережі, присвячена стаття [7]. Загальна математична модель об'єктів захисту інформаційно-телекомунікаційної системи оперативного інформування МВС України розглянута у роботі [8]. У роботі [9] розглянуто проблеми створення комплексної системи захисту корпоративної мережі ОВС України. Методичний підхід до формалізації задачі оцінювання ефективності системи захисту інформаційної системи ОВС України, а також аналіз множини векторів-показників прояву погроз об'єктам захисту цієї інформаційної системи, наведений у статті [10]. В роботі [11] здійснена оцінка коефіцієнта оперативної готовності програмно-апаратних засобів захищеної СОІ МВС України щодо обробки інформації. Аналізу та оцінці ефективності КСЗІ в системі оперативного інформування МВС України присвячені роботи [12, 13].

Таким чином, розроблена методологія оцінки рівнів захищеності інтегрованої інформаційної системи оперативного інформування МВС України. Відмітимо, що створення комплексної системи захисту оперативної інформації про резонансні злочини та інші надзвичайні події в СОІ МВС України дозволить забезпечити ефективний захист інформації та ресурсів з її обробки від можливих загроз, а тим самим забезпечить якісне та своєчасне інформування керівництва

міністерства, зацікавлених інстанцій, держави про резонансні злочини та інші надзвичайні події, що сталися в країні, прискорить розкриття резонансних злочинів по «гарячих слідах» та ліквідацію наслідків інших надзвичайних подій.

1. Про вдосконалення реагування на повідомлення про злочини, інші правопорушення і події та забезпечення оперативного інформування в органах і підрозділах внутрішніх справ України: Наказ МВС України від 4 жовтня 2003 року № 1155.
2. Кудінов В.А. 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: посібник. – К.: Київський нац. ун-т внутр. справ, 2007. – С. 156-172.
3. Про порядок приймання, реєстрації та розгляду в органах і підрозділах внутрішніх справ України заяв і повідомлень про злочини, що вчинені або готуються: Наказ МВС України від 14 квітня 2004 року № 400.
4. Кудінов В. А. Проблеми застосування інформаційних технологій в інтегрованій інформаційній системі оперативного інформування МВС України / В. А. Кудінов // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами: матеріали наук.-практ. конференції, Львів, 14 груд. 2011 р. – Львів: Львівський держ. ун-т внутр. справ, 2011. – С. 64–68.
5. Кудінов В.А. Комплексний захист інформації в системі оперативного інформування МВС України / В.А. Кудінов // Управління розвитком: зб. наук. праць за матеріалами І міжнар. наук.-практ. конф. «Безпека та захист інформації в інформаційних і телекомунікаційних системах», Харків, 28-29 трав. 2008 р. – 2008. – № 7. – С. 39-40.
6. Кудінов В.А. Організація комплексного захисту програмно-апаратних засобів інформаційної системи «Зведення» МВС України від несанкціонованих дій / В.А. Кудінов, О.А. Лупало // Спеціальна техніка у правоохоронній діяльності: IV міжнар. наук.-практ. конф., Київ, 26-27 лист. 2009 р.: тези доп. – К.: Київський нац. ун-т внутр. справ, 2009. – С. 175-176.
7. Кудінов В.А. Корпоративна мережа ОВС України та моделі її захисту від порушників безпеки / В.А. Кудінов, В.О. Хорошко // Захист інформації. – 2004. – № 1. – С. 26-35.
8. Кудінов В. А. Загальна математична модель об’єктів захисту інформаційно-телекомунікаційної системи оперативного інформування МВС України / В. А. Кудінов // Сучасний захист інформації. – 2011. – № 1. – С. 21–25.

9. Кудинов В.А. Проблемы создания комплексной системы защиты корпоративной сети органов внутренних дел Украины / В.А. Кудинов, В.А. Хорошко // Тр. XIII Межд. научной конф. «Информатизация и информационная безопасность правоохранительных органов» (25-26 мая 2004 г.). – М.: Академия управления МВД России, 2001. – С. 137-140.
10. Кудінов В.А. Методичний підхід до формалізації задачі оцінювання ефективності системи захисту інформаційної системи ОВС України / В.А. Кудінов, В.О. Хорошко // Захист інформації. – 2004. – № 4. – С. 11-18.
11. Кудінов В.А. Оцінка коефіцієнта оперативної готовності програмно-апаратних засобів захищеної автоматизованої системи оперативного інформування МВС України щодо своєчасної та якісної обробки відкритої інформації / В.А. Кудінов, В.О. Хорошко // Вісник Східноукраїнського нац. ун-ту ім. В. Даля. – 2009. – № 6, Ч. 1. – С. 82-85.
12. Кудінов В. А. Оцінка ефективності комплексної системи захисту інформації в системі оперативного інформування МВС України / В. А. Кудінов // Сучасна спеціальна техніка. – 2011. – № 1. – С. 91–96.
13. Кудінов В.А. Аналіз ефективності функціонування комплексної системи захисту відкритої інформації в інформаційно-телекомунікаційній системі оперативного інформування МВС України / В.А. Кудінов // Сучасні інформаційно-комунікаційні технології: V міжнар. наук.-технічна конф., Ялта, 5-9 жовт. 2009 р.: тези доп. – К.: ДУІКТ, 2009. – С. 167-168.

ІНФОРМАЦІЙНА БЕЗПЕКА БАЗ ДАНИХ

Кулешник Я.Ф.,
доцент кафедри інформаційних технологій ЛьвДУВС, к.т.н., доцент
Рудий Т.В.,
доцент кафедри інформаційних технологій ЛьвДУВС, к.т.н., доцент
Бичинюк І.В.,
викладач кафедри інформаційних технологій ЛьвДУВС

Системи керування базами даних стали основним інструментом, що забезпечує збереження великих масивів інформації. Сучасні інформаційні додатки спираються в першу чергу на СКБД із багатьма користувачами. Саме тому пильна увага сьогодні приділяється проблемам гарантування інформаційної безпеки, що визначає ступінь безпеки організації, компанії в цілому [1].

Під *інформаційною безпе-*

кою розуміють захищеність інформації від випадкових і навмисних впливів природного або штучного характеру, які призводять до збитку власників або користувачів інформації.

З метою захисту інформації в базах даних найважливішими є такі аспекти інформаційної безпеки:

- *умови доступу* (можливість одержати деяку необхідну інформаційну послугу);
- *цілісність* (несуперечність інформації, її захищеність від руйнування і несанкціонованої зміни);
- *конфіденційність* (захист від несанкціонованого прочитування).

Проблема гарантування інформаційної безпеки є комплексною, тому її вирішення має розглядатися на різних рівнях: законодавчому, адміністративному, процедурному і програмно-технічному [2]. Сьогодні особливо гостро в Україні постає проблема розробки законодавчої бази, яка гарантувала б безпечне використання інформаційних систем.

Практично всі СКБД призначені для роботи в середовищах із багатьма користувачами, але мають для цього різні можливості.

Обробка даних у середовищах з багатьма користувачами передбачає виконання програмним продуктом таких функцій:

- блокування бази даних, файла, запису, поля;
- ідентифікацію станції, що встановила блокування;
- відновлення інформації після модифікації;
- контроль за часом і повторення звертання;
- обробку транзакцій;
- роботу з мережними системами.

До основних програмно-технічних заходів, застосування яких дозволить вирішити деякі з названих вище проблем, належать:

- аутентифікация користувача і встановлення його ідентичності;
- керування доступом до баз даних;
- підтримка цілісності даних;
- протоколювання й аудит;
- захист комунікацій між клієнтом і сервером;

- подолання загроз, специфічних для СКБД.

1. Перевірка прав користувача додатків бази даних найчастіше здійснюється або через відповідні механізми операційної системи, або через певний SQL-оператор: користувач ідентифікується своїм ім'ям, а засобом аутентифікації служить пароль. Подібна система створює значні складності для повторних перевірок і робить неможливими подібні перевірки перед кожною транзакцією.

2. *Керування доступом* до баз даних спирається на реалізацію такого мінімального набору дій:

- довільне керування доступом;
- гарантування безпеки повторного використання об'єктів;
- використання міток безпеки;
- примусове керування доступом.

Довільне керування доступом – метод обмеження доступу до об'єктів, що ґрунтується на врахуванні особистості суб'єкта або груп, до яких входить суб'єкт. Ця технологія забезпечує власнику об'єкта (подання, сервера бази даних, процедури, таблиці) передання за власним бажанням привілеїв іншій особі. Цією особою в даній ситуації може бути суб'єкт-користувач, група користувачів. Головна перевага довільного керування доступом – гнучкість. Однак такі супутні характеристики, як розосередженість керування і складність централізованого контролю створюють чимало проблем для гарантування безпеки даних.

Варто звернути увагу і на гарантування *безпеки повторного використання* баз даних суб'єктами. Це означає позбавлення прав для входу в інформаційну систему всіх користувачів, що залишили компанію.

Мітка безпеки складається з двох частин – рівня таємності і списку категорій. Перша складова залежить від додатка і у стандартному варіанті може виглядати як спектр значень від ««бсо- лютно секретно» до «несекретно». Друга складова дозволяє описати предметну область, розділяючи інформацію «по відсіках», що сприяє кращій захищеності. Механізм міток безпеки не скасовує, а доповнює довільне керування доступом: користувачі, як і раніше, можуть оперувати з таблицями тільки в рамках своїх привілеїв, одер-

жувати тільки частину даних. Основна проблема при використанні міток безпеки – підтримка їх цілісності. Це означає, що всі об'єкти і суб'єкти мають бути позначені, і при будь-яких операціях з даними мітки повинні залишатися правильними.

Примусове керування доступом ґрунтується на зіставленні міток безпеки суб'єкта й об'єкта. Для читання інформації об'єкта необхідне домінування мітки суб'єкта над міткою об'єкта. При виконанні операції запису інформації в об'єкт необхідне домінування мітки безпеки об'єкта над міткою суб'єкта. Цей спосіб керування доступом називається примусовим, тому що не залежить від волі суб'єктів. Він знайшов застосування в СКБД, що характеризуються підвищеними заходами безпеки.

3. *Забезпечення цілісності даних* – не менш важливе завдання, ніж керування доступом. З погляду користувачів СКБД основними засобами підтримки цілісності даних є обмеження і правила. Обмеження можуть міститися безносередньо в реля- ційній моделі даних, а можуть задаватися в процесі створення таблиці. Табличні обмеження можуть стосуватися групи стовпців, окремих атрибутів. Посилальні обмеження відповідають за підтримку цілісності зв'язків між таблицями. Обмеження накладаються власником таблиці і впливають на результат наступних операцій з даними. Правила дозволяють виконувати задані процедури при певних змінах бази даних. На відміну від обмежень, що забезпечують контроль простих умов, правила дозволяють перевіряти і підтримувати співвідношення будь-якої складності між елементами даних у базі. Однак при використанні правил як інструмента інформаційної безпеки помилка в складній системі правил може призвести до непередбачених наслідків для всієї бази даних.

4. *Протоколювання і аудит* передбачають:

- виявлення незвичайних і підозрілих дій користувачів та ідентифікацію осіб, що здійснили ці дії;
- оцінку можливих наслідків порушення, що відбулося;
- надання допомоги;
- організацію пасивного захисту інформації від нелегальних дій користувача.

5. Проблема *захисту комунікацій між клієнтом і сервером* в інформаційних системах не є специфічною для

СКБД. Для забезпечення захисту інформації виділяється сервіс безпеки, до функцій якого входять аутентифікація, шифрування й авторизація.

6. *Внутрішні проблеми БД.* Однак головне джерело загроз для СКБД міститься у самій природі баз даних. Нерідко потрібну, але недоступну за статусом інформацію можна одержати шляхом логічного висновку. Наприклад, використовуючи операцію додавання, а не вибору (на яку немає прав), можна аналізувати коди завершення вС^Ь-операторів. Для боротьби з подібними загрозами використовується механізм розмноження рядків для СКБД, що підтримує мітки безпеки. Агрегування – метод одержання нової інформації шляхом комбінування даних, добутих легальним шляхом з різних таблиць бази даних. Боротися з агрегуванням можна шляхом ретельного проектування моделі даних і максимального обмеження доступу користувача до інформації.

Деякі СКБД передбачають засоби гарантування безпеки даних. Такі засоби забезпечують виконання таких операцій:

- шифрування прикладних програм;
- шифрування даних;
- захист паролем;
- обмеження рівня доступу (до бази даних, до таблиці, для користувача).

Високий рівень безпеки даних може бути реалізований, якщо призначати користувачам різні права доступу на рівні файлу, поля, а також організувати автоматичне шифрування даних. Гарними характеристиками гарантування безпеки є призначення паролів для індивідуальних користувачів або груп користувачів і присвоєння різних прав доступу окремо таблицям, запитам, звітам, макрокомандам або новим об'єктам на рівні користувача або групи.

1. Гордієнко І.В. Інформаційні системи і технології в менеджменті. – К. : КНЕУ, 2003.
2. Гужва В.М. Інформаційні системи і технології на підприємствах. – К. : КНЕУ, 2001.

ПОНЯТТЯ ТА СУТНІСТЬ ІНФОРМАТИЗАЦІЇ

Ковалів М.В.,
завідувач кафедри конституційного, адміністративного та міжнародного права ЛьвДУВС, к.ю.н., професор

Інформатизація – це сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, спрямованих на створення умов для задоволення інформаційних потреб, реалізації прав громадян і суспільства на основі створення, розвитку, використання інформаційних систем, мереж, ресурсів та інформаційних технологій, що ґрунтуються на застосуванні сучасної обчислювальної та комунікаційної техніки.

Як показує досвід інших країн, інформатизація сприяє забезпеченню національних інтересів, поліпшенню керованості економікою, розвитку наукомістких виробництв та високих технологій, зростанню продуктивності праці, вдосконаленню соціально-економічних відносин, збагаченню духовного життя та подальшій демократизації суспільства.

Інформатизацію умовно можна поділити на такі види.

Інформатизація стратегічних напрямів розвитку державності, безпеки та оборони – комплекс заходів, спрямованих на створення і розвиток інформаційно-аналітичних, обчислювальних та автоматизованих систем, центрів і мереж, які забезпечують роботу органів державної влади та органів місцевого самоврядування. Особливістю завдань цього напряму є складність їх, пов'язана з необхідністю оброблення великого обсягу різноманітної інформації, що надходить зі значної кількості джерел, а також з високими вимогами до швидкості та форми її надання, достовірності, актуальності, безпеки.

Інформатизація процесів соціально-економічного розвитку – комплексне та збалансоване вирішення завдань соціально-економічного розвитку на сучасній інформаційно-аналітичній, системно-технічній базі за допомогою ситуаційних центрів забезпечення інформаційної підтримки функціонування державного сектору економіки, проведення виваженої бюджетно-кредитної та податкової політики, виникнення конкуренто-

спроможних виробництв галузей промисловості у стратегічно важливих сферах. Систему моніторингу та застосування сучасних інформаційних технологій забезпечать наукові підходи у розв'язанні соціальних проблем суспільства.

В основу цього напряму інформатизації покладається створення баз даних і знань, а також засобів обробки їх, орієнтованих на ефективну інформатизацію органів державної статистики і точне прогнозування процесів соціально-економічного розвитку, зокрема інформаційно-довідкових систем ринку праці, товарів і послуг, контролю якості споживчих товарів тощо з подальшим використанням їх для формування систем електронної комерції.

Інформатизація пріоритетних галузей економіки – це комплекс автоматизованих систем оброблення даних та управління різного рівня і призначення, які взаємопов'язані на основі принципів технологічної, організаційної, документаційної, програмної та інформаційної сумісності та утворюють цілісну інформаційну інфраструктуру.

В умовах формування ринкових відносин важливими завданнями є такі: підвищення ефективності функціонування галузей за рахунок оптимізації структури виробництва і транспортних засобів та необхідної координації робіт усіх управлінських підрозділів, вирішення проблеми комплексної автоматизації виробництва на основі сучасних стандартів і технологій, яка охоплює процеси від проектування та підготовки виробництва до безпосереднього автоматизованого виробництва.

Інформатизація банківської діяльності – створення системи розрахунків у реальному часі для виконання великих та термінових платежів, системи безготівкових розрахунків за товари та послуги, електронного реєстру застав майна, електронної системи Центрального депозитарію державних цінних паперів. Важливе значення також буде мати створення системи інформаційно-аналітичної взаємодії Національного банку України, Міністерства фінансів України, Державної податкової адміністрації України та Державного казначейства України.

Інформатизація в галузі екології та використання природних ресурсів – на основі картографічних баз даних передбачається створення багатоцільової інформаційно-

технологічної бази з використанням геоінформаційних технологій збирання, зберігання, аналізу всієї сукупності відомостей для моделювання і подальшого прогнозування екологічного стану територій.

Передбачається створення комплексу програмно-апаратних засобів для вирішення питань прогнозування забруднення навколишнього середовища, аналізу та оцінки ризику еколого-економічних конфліктів, прогнозування наслідків техногенного впливу і природних катастроф для надійного захисту екологічного простору України, раціонального використання природних ресурсів на основі підвищення узгодженості управління різними видами виробничої діяльності.

Інформатизація освіти спрямовується на формування та розвиток інтелектуального потенціалу нації, удосконалення форм і змісту навчального процесу, впровадження комп'ютерних методів навчання та тестування, що дасть можливість вирішувати проблеми освіти на вищому рівні з урахуванням світових вимог. Серед них: індивідуалізація навчання, організація систематичного контролю знань, можливість враховувати психофізіологічні особливості кожної дитини тощо. Результатами інформатизації освіти мають бути:

- розвиток інформаційної культури людини (комп'ютерної освіченості);
- розвиток змісту, методів і засобів навчання до рівня світових стандартів;
- скорочення терміну навчання і тренування на всіх рівнях підготовки кадрів та підвищення якості такого навчання і тренування;
- інтеграція навчальної, дослідницької та виробничої діяльності;
- удосконалення управління освітою;
- кадрове забезпечення усіх напрямів інформатизації України шляхом спеціалізації та інтенсифікації підготовки відповідних фахівців.

Інформатизація наукової діяльності – це заходи, спрямовані на підвищення ефективності наукових досліджень, створення потужної системи науково-технічної інформації та її використання на різних етапах наукової діяльності за умови активізації

всіх її форм; створення умов для широкої комп'ютеризації та математизації природничих і гуманітарних наук, входження до світової інформаційної мережі баз даних та знань, формування в майбутньому «об'єднаного», чи «колективного», інтелекту. Інформатизація вітчизняної науки дасть змогу підвищити практичну віддачу, прискорити інтеграцію у світову науку.

У сфері культури головними завданнями є збереження інформації про пам'ятки матеріальної і духовної культури, архівні документи, забезпечення швидкого доступу до вітчизняних і світових досягнень культури. З цією ж метою передбачається створити комп'ютерні інформаційні системи для поширення культурних еталонів, стандартів і досягнень вітчизняної культури, насамперед створити електронні копії творів та архівів видатних діячів національної культури, представити їх у системах глобальних комп'ютерних комунікацій для ефективного використання у сфері освіти та виховання, що дасть змогу в будь-якій точці України отримувати не тільки необхідну інформацію з економічних, агробіологічних, зоотехнічних, медичних, маркетингових, технологічних, юридичних питань, а й відповідні знання з історії та культури України, культури інших народів через автоматизовані бібліотеки тощо.

Наведений перелік сфер не є вичерпним. Сфера інформатизації буде розширюватися.

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У СФЕРІ ІНФОРМАЦІЙНИХ ВІДНОСИН

Цимбрівський Т.С.,
доцент кафедри конституційного, адміністративного та міжнародного права ЛьвДУВС, к.ю.н.

Міжнародна інформаційна діяльність полягає у забезпеченні громадян, державних органів, підприємств, установ і організацій офіційною документованою або публічно оголошуваною інформацією про зовнішньополітичну діяльність України, про події та явища в інших країнах, а також у цілеспрямованому поширенні за межами України державними органами й об'єднаннями громадян, засобами масової інформації та громадянами всебічної інформації про Україну.

Відповідно до законодавства України її громадяни мають право на вільний і безперешкодний доступ до інформації через зарубіжні джерела, включаючи пряме телевізійне мовлення, радіомовлення і пресу тощо.

Правове становище і професійна діяльність акредитованих в Україні іноземних кореспондентів та інших представників іноземних засобів масової інформації, а також інформаційна діяльність дипломатичних, консульських та інших офіційних представників зарубіжних держав в Україні регулюються законодавством України, відповідними міжнародними договорами, укладеними Україною.

В Україні створення і діяльність спільних організацій у галузі інформації за участю вітчизняних та іноземних юридичних осіб і громадян регулюються законодавством України. Якщо міжнародним договором встановлено інші правила, ніж ті, які містяться в законодавстві України, що регулює відносини в галузі інформації, то застосовуються норми міжнародного договору, укладеного Україною (ст. 50 Закону України «Про інформацію»).

Міжнародне співробітництво в галузі інформації з питань, що становлять взаємний інтерес, здійснюється на основі міжнародних договорів, укладених Україною та юридичними особами, які займаються інформаційною діяльністю.

Державні органи та інші юридичні особи, які займаються інформаційною діяльністю, можуть безпосередньо здійснювати зовнішньоекономічну діяльність у власних інтересах, а також в інтересах індивідуальних і колективних споживачів, яких вони обслуговують і яким гарантують одержання зарубіжної інформації (ст. 51 Закону України «Про інформацію»).

Міжнародне співробітництво у сфері науково-технічної інформації та міжнародна інформаційна діяльність регулюються згідно з чинним законодавством (ст. 20 Закону України «Про науково-технічну інформацію»).

Відповідно до чинного законодавства Україні між державний обмін науково-технічною інформацією здійснюється відповідно до угод, підписаних Україною.

Держава забезпечує відкритий і рівноправний доступ своїх громадян і громадян держав – партнерів за угодами до інформаційних ресурсів спільного користування.

Відповідно до законодавства уряд України визначає національний інформаційний центр, який координує міждержавний обмін науково-технічною інформацією (ст. 21 Закону України «Про науково-технічну інформацію»).

Діяльність іноземних фізичних та юридичних осіб в Україні у сфері науково-технічної інформації. Іноземні юридичні та фізичні особи, а також особи без громадянства можуть інвестувати розвиток сфери науково-технічної інформації України відповідно до чинного законодавства (ст. 22 Закону «Про науково-технічну інформацію»).

Міжнародне співробітництво у сфері інформатизації спрямовується на підвищення економічної ефективності та науково-технічного рівня виконання Національної програми інформатизації. З цією метою до виконання окремих завдань (проектів) Національної програми інформатизації можуть залучатися іноземні юридичні та фізичні особи, іноземні інвестиції.

Держава розвиває і підтримує всі форми міжнародного співробітництва у сфері інформатизації, які не суперечать законодавству та державним інтересам України (ст. 27 Закону України «Про національну програму інформатизації»).

Міжнародне співробітництво у галузі зв'язку. Встановлення правових, організаційних, технологічних і фінансових відносин з міжнародними організаціями зв'язку, а також представництво України в цих організаціях за дорученням Кабінету Міністрів України, здійснення співробітництва з організаціями зв'язку іноземних держав, міжнародний правовий захист інтересів України у питаннях зв'язку покладається на Адміністрацію зв'язку України, а питання використання радіочастот та радіоелектронних засобів на міжнародному рівні – на Головне управління з питань радіочастот при Кабінеті Міністрів України.

Адміністрація зв'язку України представляє Україну в Міжнародному союзі електрозв'язку (МСЕ), Всесвітньому поштовому союзі та залучає до цієї роботи інші організації, міністерства і відомства. Координує участь інших міністерств та відомств у роботі МСЕ Державна комісія з питань зв'язку та радіочастот.

Міжнародне співробітництво в галузі зв'язку здійснюється на основі чинного законодавства та відповідних міжнародних договорів України (ст. 31 Закону України «Про зв'язок»).

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ МВС

Рудий Т.В.,
доцент кафедри інформаційних технологій ЛьвДУВС, к.т.н., доцент
Кулешник Я.Ф.,
доцент кафедри інформаційних технологій ЛьвДУВС, к.т.н., доцент
Бичинюк І.В.,
викладач кафедри інформаційних технологій ЛьвДУВС
Горпинченко Є.Г.,
методист із впровадження новітніх та інформаційних технологій економічного факультету ЛьвДУВС

Політика інформаційної безпеки (ПІБ) документально описує і регламентує систему управління інформаційною безпекою інформаційних систем (ІС) оперативних підрозділів МВС, відповідає вимогам чинного законодавства України та міжнародних угод, базується на рекомендаціях міжнародних стандартів ISO/IEC 27001:2005, ISO/IEC 17799/2005 [1, 2].

Метою політики інформаційної безпеки є впровадження та ефективне управління системою забезпечення інформаційної безпеки (ІБ), спрямованої на захист інформаційних активів, забезпечення безперервного функціонування сервісів ІС, мінімізування ризиків ІБ.

Основним завданням впровадження ПІБ є захист інформаційних активів від зовнішніх та внутрішніх, навмисних і ненавмисних загроз. ПІБ розповсюджується на всі аспекти діяльності ІС та застосовується до всіх інформаційних активів, які можуть справляти матеріальний інтерес для кримінальних структур у разі несанкціонованого витоку.

Аналіз наявних у вільному доступі матеріалів стосовно проблеми безпеки інформаційних активів ІС дає змогу виявити недоліки у методології розроблення ПІБ систем захисту, які суттєво впливають на ефективність їх функціонування. Серед них відзначимо:

- ПІБ системи захисту інформаційних активів ІС не враховує динаміки зміни загроз;
- недостатній рівень стійкості системи захисту ІС до відмов та відновлення після збоїв;

- необхідність зосередження ресурсів підтримки систем безпеки інформаційних активів ІС на найбільш критичних напрямах;
- відсутність ефективних методик попереднього оцінювання ефективності системи безпеки інформаційних активів ІС;
- ігнорування законодавчими аспектами та вимогами міжнародних стандартів у галузі ІБ при проектуванні надійної системи захисту.

Як основні об'єкти в області запровадження ІБ, розглядаються наступні види активів:

- інформаційні активи: інформація та дані у довільному вигляді, що отримуються, зберігаються, обробляються, передаються, оголошуються, (до цього виду необхідно віднести знання працівників, бази даних та системи бігметричного ідентифікування, документація, навчальні матеріали, описи процедур, інформація на фізичних носіях);
- програмне забезпечення: прикладне програмне забезпечення (ПЗ), системне ПЗ, сервісне ПЗ та довільне інше ПЗ, незалежно від форми отримання (придбання, власного розроблення, таке, що вільно розповсюджується), яке використовується працівниками для роботи та у процесі взаємодії з іншими службами;
- фізичні активи: працівники, програмно-апаратні засоби інформаційних технологій (ІТ) (комп'ютерні мережі (КМ) і мережеві технології, сервери, робочі станції, між мережеві екрани, телекомунікаційне обладнання, обладнання зв'язку, маршрутизатори, АТС), приміщення, технологічне обладнання, технічні засоби;
- сервісні активи: інформаційні та комунікаційні сервіси (корпоративні КМ спеціального призначення, Internet, E-mail, спеціальні канали зв'язку), інші технічні сервіси (опалення, освітлення, системи сигналізацій та моніторингу), усі сервіси, пов'язані з отриманням, наданням, використанням, передавання та знищенням активів, усі юридичні та фізичні особи, організації, установи та підприємства (а також їх працівники), яким передані певні послуги на ІТ-аутсорсинг [3].

Для кожного активу визначаються можливі ризики та шляхи їх мінімізування, тобто рекомендуємо використати ризик-орієнтований підхід. Оцінювання можливих ризиків активів провадиться за чотирма основними критеріями безпеки:

- доступність – забезпечення безперервного доступу до інформаційних та супутніх активів ІС, спеціальних КМ та сервісів згідно з наданими працівникам повноваженнями та правами у мінімально необхідному обсязі;
- цілісність – захист точності/коректності та повноти активів і методів оброблення інформації;
- конфіденційність – забезпечення доступності до активів ІС, корпоративних КМ спеціального призначення, інформації для офіційно авторизованих користувачів у мінімально необхідному обсязі;
- спостережливість – забезпечення можливості визначення – хто, що і коли робив з тим або іншим інформаційним активом (забезпечення принципу невідмови від вчинених дій).

ПІБ регламентує управління доступами та паролями, чіткий розподіл ролей та обов'язків, визначення вимог ІБ для кожного активу. Впровадження ПІБ в інформаційні системи забезпечує підтримку рівня безпеки на належному рівні, що у свою чергу передбачає:

- постійне навчання працівників у сфері ІБ;
- проведення контролю безпеки та доступу до ІС;
- управління інцидентами, категоріювання та забезпечення конфіденційності інформації;
- антивірусний захист, резервне копіювання, ліцензійну чистоту програмного забезпечення, вхідний/вихідний контроль за обміном інформацією у ІС;
- забезпечення фізичної безпеки та інших аспектів ІБ.

Документи ПІБ розробляє підрозділ безпеки ІТ. Постійний контроль за впровадженням, виконанням, вдосконаленням та підтриманням ПІБ в актуальному стані також покладений на працівників підрозділу безпеки ІТ.

Для зменшення ризиків виникнення інцидентів ІБ, пов'язаних з зовнішніми і внутрішніми, навмисними та ненавмисними впливами, елементарною необізнаністю працівників у

галузі ІТ необхідно розробити та запровадити систему управління інцидентами інформаційної безпеки (СУІБ), яка є базовою частиною загальної системи управління інформаційною безпекою (СУІБ). СУІБ дозволяє виявляти, враховувати, реагувати й аналізувати події та інциденти ІБ. Без реалізування цих процесів неможливо забезпечити рівень захищеності, який є адекватним до вимог міжнародних стандартів і галузевих норм.

Управління інцидентами, це важливий процес, який забезпечує можливість спочатку виявити інцидент, а потім за допомогою коректно обраних засобів підтримки якомога швидше його усунути.

Основна задача управління інцидентами – якомога швидше відновити роботу сервісів і звести до мінімуму негативний вплив інциденту на роботу ІС для підтримки якості і доступності сервісів на максимально можливому рівні. Штатною вважається робота сервісів, що не виходить за рамки угоди про рівень обслуговування.

Цілі, які ставлять перед СУІБ є такими:

- відновлення штатної роботи сервісів у найкоротші терміни;
- зведення до мінімуму вплив інцидентів на функціонування ІС;
- забезпечення злагодженого оброблення всіх інцидентів і запитів обслуговування;
- зосередження ресурсів підтримки ІБ на найбільш важливих напрямах;
- надання відомостей, які дозволять оптимізувати процеси підтримки, зменшити кількість інцидентів і запланувати управління.

Використовуючи найкращі, перевірені часом напрацювання для оброблення збоїв довільних видів, рішення з управління інцидентами дозволяють використовувати ресурси залежно від пріоритетів оперативної діяльності, управляти рівнями обслуговування, а також краще контролювати роботу ІТ-сервісів.

Для реалізування системи управління інцидентами інформаційної безпеки необхідно виконати такі роботи:

- надати ресурси для розроблення та впровадження системи СУІБ;
- здійснити фахову підготованість працівників;

- визначити область функціонування СУІБ;
- розробити комплекс процесів СУІБ;
- впровадити процеси СУІБ та інтегрувати їх з уже функціонуючими процесами, такими як інвентаризування активів, аналіз ризиків та оцінювання ефективності;
- розробити архітектуру і комплекс програмно-технічних засобів з автоматизації процесів СУІБ і моніторингу подій.

У результаті проведених робіт буде запроваджена СУІБ, яка розв'язуватиме наступні задачі:

- оперативний моніторинг стану ІБ в рамках функціонування ІС;
- виявлення, облік, реагування, розслідування та аналіз інцидентів ІБ;
- інформування вищого керівництва про поточний стан ІБ.
- Таким чином, необхідно реалізувати комплексний підхід щодо розв'язання наступних задач:
- виявлення, інформування та облік інцидентів ІБ
- реакція на інциденти ІБ, включаючи застосування необхідних засобів для запобігання, зменшення і відновлення завданого збитку;
- аналіз реалізованих інцидентів, з метою планування превентивних заходів захисту і поліпшення процесу забезпечення ІБ в цілому.

Для оброблення подій та інцидентів ІБ необхідно організувати процес реагування на інциденти. Основними задачами процесу реагування на інциденти інформаційної безпеки є:

- забезпечення координування реагування на інцидент;
- підтвердження/спростування факту виникнення інциденту;
- мінімізування порушень порядку роботи і пошкодження даних, відновлення в найкоротші терміни працездатності ІС при її порушенні у результаті інциденту;
- мінімізування наслідків порушення конфіденційності, цілісності і доступності інформації у ІС;
- створення умов для порушення цивільної або кримінальної справи проти зловмисників;
- захист активів ІС;

- забезпечення збереження і цілісності доказів виникнення інциденту, створення умов для накопичення і зберігання точної інформації про інциденти, що мали місце, про корисні настанови;
- швидке виявлення та/або попередження подібних інцидентів у майбутньому;

Як висновок відзначимо, що при експлуатуванні систем менеджменту інформаційної безпеки процес управління інцидентами є одним з найважливіших у постачанні даних для аналізу функціонування таких систем, оцінювання ефективності використовуваних заходів, зниження ризиків і планування удосконалення роботи ІС.

1. Когут В.В. Порядок атестування систем технічного захисту інформації / В.В. Когут, Т.В. Рудий, Я.Ф. Кулешник. Проблеми діяльності кримінальної міліції в умовах розбудови правової держави // Матеріали науково-звітної конференції факультету кримінальної міліції Львівського державного університету внутрішніх справ 12 березня 2010 р. –Львів: ЛьвДУВС. 2010, – с. 90-97.
2. Рудий Т.В. Специфіка протидії злочинам у сфері інформаційних технологій / Т.В. Рудий, В.М. Слижук, І.М. Ганич, А.В. Нечепуренко. Проблеми діяльності кримінальної міліції в умовах розбудови правової держави // Матеріали V звітної науково-практичної конференції факультету кримінальної міліції Львівського державного університету внутрішніх справ 14 квітня 2011 р. – Львів: ЛьвДУВС. 2011, – с. 176-180.
3. Руда О.І. Аутсорсинг у сфері інформаційних технологій / О.І. Руда, І.І. Руда / Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами // Матеріали науково-практичної конференції 24 грудня 2010 р. – Львів: ЛьвДУВС. 2010, – с. 196-200.

МЕТОДОЛОГІЯ ІНФОРМАЦІЙНОГО ПРАВА

Єсімов С.С.,
доцент кафедри конституційного, адміністративного та міжнародного права ЛьвДУВС, к.ю.н.

Методологія інформаційного права, як і інші галузі права перебуває у стадії розвитку. Об'єктивно вона поєднує методологічні засади

права, інформатики, соціальної кібернетики та інших гуманітарних і технічних наук.

Методологічна основа інформаційного права щодо з'ясування нових соціальних явищ базується на теорії цивілізаційного підходу. Відповідно до цього підходу визначаються адаптовані положення системного підходу, зокрема такі постулати: стадійність (визначення меж стадій чи то за хронологічним, чи то за територіальним або іншим множинними чинником), полілінійність та унікальність (чинники, що характеризують особливість, відмінність) розвитку людства.

Виходячи з цих методологічних чинників, можна зазначити, що на межі третього тисячоліття чітко визначились основні проблеми людства і сценарії подальшого розвитку планетарної (глобальної) цивілізації. Прискорюються процеси самоорганізації нового етапу розвитку культури суспільства (як образу цивілізації) – інформаційного суспільства, ноосферні чинники якого можуть стати своєрідними гарантами сценарію м'якого виходу з планетарної кризи, якою завершено розвиток глобальної індустріальної цивілізації.

Сьогодні методологія наукових досліджень поряд з використанням перевірених часом традиційних методів і підходів потребує нових для усвідомлення складних соціальних процесів, які мають і культурологічно-правову спрямованість. У цих умовах пошук та аналіз нових парадигм пізнання цілком природні. Визначимо кілька з них, які вплинули на розкриття поняття, сутності та змісту предмета (об'єкта) дослідження.

Останнім часом вчені все більше приділяють увагу одному з найбільш інтегральних спрямувань методології вивчення соціального буття – соціальній синергетиці.

Соціальна синергетика (від гр. synergeia – співпраця, співдружність) – новий напрям міждисциплінарних досліджень, який використовує нелінійне мислення для виявлення загальних закономірностей і тенденцій на основі самоорганізації соціальних систем; пояснення становлення нових структур у відкритих соціальних системах на засадах пошуку співвідношення потреб та інтересів різних суб'єктів соціальних відносин: людини, соціальних груп, суспільства, держави, світового співтовариства.

Під соціальною самоорганізацією розуміються процеси виникнення і функціонування систем, сформованих різними

чинниками (а не одним – керівним) у просторово-часових вимірах та певному колу осіб. Одним із постулатів синергетики є те, що всі системи перебувають у мінливих станах, поблизу від особливих критичних точок (точок біфуркації), навколо яких динаміка систем стає вкрай несталою. У цих умовах система під дією найнезначніших (маргінальних) та випадкових впливів може кардинально і зовсім непередбачено змінити свій стан. Такий перехід у соціальних системах характеризується як виникнення нового порядку зі старого, який віджив свій час.

Синергетика передбачає якісно іншу картину світу порівняно з тими уявленнями, які лежали в основі як класичного, так і некласичного природознавства та суспільствознавства (сформованого у першій половині XX ст.). Образ світу постає як множина нелінійних процесів.

Важливе пізнавальне значення мають такі методологічні постулати синергетики щодо соціальних систем:

- неможливо традиційними детерміністськими методами описувати еволюцію складно організованих систем;
- розвиток цих систем виявляє можливість альтернативних шляхів, що передбачає свободу вибору та відповідальність людини, громади, суспільства, людства;
- неможливий абсолютний контроль (особливо з одного центру) будь-якої сфери реальності, в тому числі й розвитку суспільства, який був проголошений традиційною наукою, особливо теорією соціального управління та соціальною кібернетикою;
- у критичних точках (точках біфуркації) несталості соціальних систем діяльність кожної людини або групи людей може мати вирішальне значення в макросоціальних змінах (роль особистості в історичному процесі, змін суспільства);
- збільшується відповідальність певної громади і людства в цілому за долі універсуму, оскільки вони в змозі цілеспрямовано уникати біфуркаційних станів, особливо в соціальній сферах, суттєво впливати на екологію (еволюцію природи та суспільства).

Велику роль у формуванні методології науки інформаційного права відіграють як гуманітарні (філософія, філософія права, соціологія, когнітологія, праксеологія тощо), так і фізико-

математичні науки, особливо технічна та біологічна кібернетика, інформатика тощо, на межі яких формуються нові наукові дисципліни, через які адаптуються їхні методології до конкретної сфери суспільних відносин щодо інформації.

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ УЧАСНИКІВ КРИМІНАЛЬНОГО СУДОЧИНСТВА В УМОВАХ РЕФОРМУВАННЯ ПРАВООХОРОННОЇ СИСТЕМИ

Тарасенко Р.В.,
доцент кафедри економічної безпеки Одеського державного університету внутрішніх справ к.ю.н.

Забезпечення безпеки учасників кримінального судочинства є правозастосовчим видом державної діяльності, тому кожна з її складових підлягає нормативному врегулюванню, здійснюваному на різних рівнях. Правову основу здійснення цієї роботи можна визначити як сукупність правових норм, що закріплюють можливість і створюють умови для реалізації заходів безпеки, визначають етичні, організаційно-тактичні та інші положення цього зрізу діяльності. Центральне місце в системі правового регулювання забезпечення безпеки учасників кримінального судочинства займає Закон України «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві», прийнятий 23 грудня 1993 року. Цей Закон встановлює граничний перелік осіб, які мають право на забезпечення безпеки, визначає та характеризує основні заходи забезпечення безпеки, права та обов'язки осіб, щодо яких здійснюються заходи безпеки, та органів, які забезпечують безпеку, визначає підстави і приводи для вжиття заходів безпеки, їх скасування, порядок прийняття рішення про їх застосування тощо. Проте окремі передбачені Законом гарантії правового і соціального захисту особам, які сприяють правоохоронній діяльності та беруть участь у кримінальному судочинстві, все ж мають не тільки декларативний характер. Мова йде про можливість окремих учасників процесу ініціювати застосування заходів безпеки, про можливість проведення закритого судового розгляду в справах

про осіб, взятих під захист, забезпечення конфіденційності даних про таку особу шляхом обмеження відомостей про неї в матеріалах кримінального провадження, проведення впізнання поза візуальним спостереженням того, кого впізнають.

На реалізацію даних гарантій спрямовані, перш за все, норми кримінально-процесуального законодавства. Так реалізуються положення Законів України «Про оперативно-розшукову діяльність» та «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві». До речі чинний Кримінальний процесуальний кодекс України закріплює майже аналогічні механізми реалізації гарантій безпеки осіб, взятих під захист, що були прописані у КПК України 1960-го року.

Так, у ч. 2 ст. 27 діючого КПК передбачено, що слідчий суддя, суд може прийняти рішення про здійснення кримінального провадження у закритому судовому засіданні впродовж усього судового провадження або його окремої частини у випадку необхідності забезпечення безпеки осіб, які беруть участь у кримінальному провадженні, а також якщо здійснення провадження у відкритому судовому засіданні може призвести до розголошення таємниці, що охороняється законом. Якщо судовий розгляд відбувався у закритому судовому засіданні, судове рішення проголошується прилюдно з пропуском інформації, для дослідження якої проводилося закрите судове засідання та яка на момент проголошення судового рішення підлягає подальшому захисту від розголошення.

Ч. 4 ст. 228 діючого КПК закріплює можливість з метою забезпечення безпеки особи, яка впізнає, проводити впізнання в умовах, коли особа, яку пред'являють для впізнання, не бачить і не чує особи, яка впізнає, тобто поза її візуальним та аудіоспостереженням. При пред'явленні особи для впізнання особі, щодо якої вжито заходів безпеки, відомості про особу, взяту під захист, до протоколу не вносяться і зберігаються окремо. Відповідно до ст. 232 діючого КПК України допит осіб, впізнання осіб чи речей під час досудового розслідування можуть бути проведені у режимі відеоконференції при трансляції з іншого приміщення (дистанційне досудове розслідування) у випадку необхідності забезпечення безпеки осіб. З цією ж метою у режимі відеоконференції може

здійснюватися судове провадження під час трансляції з іншого приміщення, у тому числі яке знаходиться поза межами приміщення суду (дистанційне судове провадження.

Ряд статей чинного КПК надає право окремим учасникам кримінального судочинства заявляти клопотання про забезпечення безпеки. Так, свідок має право заявляти клопотання про забезпечення безпеки у випадках, передбачених законом (п. 8 ч. 1 ст. 66). Потерпілий має право на забезпечення безпеки щодо себе, близьких родичів чи членів своєї сім'ї, майна та житла (п. 5 ч. 1 ст. 57). Підозрюваний, обвинувачений має право заявляти клопотання про проведення процесуальних дій, про забезпечення безпеки щодо себе, членів своєї сім'ї, близьких родичів, майна, житла тощо (п. 12 ч. 3 ст. 42). Перекладач, експерт, спеціаліст також мають право заявляти клопотання про забезпечення безпеки у випадках, передбачених законом (п. 4 ч. 2 ст. 68, п. 7 ч. 3 ст. 69, п. 6 ч. 4 ст. 71).

Ст. 65 діючого КПК передбачає: «свідки, що є особами, до яких застосовані заходи безпеки, не можуть бути допитані щодо дійсних даних про їх особи» (п. 9 ч. 2 ст. 65). Особи, які мають відомості про дійсні дані про осіб, до яких застосовані заходи безпеки, не можуть бути допитані щодо цих даних (п. 10 ч. 2 ст. 65).

Таким чином, можна стверджувати, що чинний КПК України не передбачає жодних принципово нових механізмів реалізації гарантій безпеки учасників кримінального судочинства. Фактично розглянуті вище норми КПК повністю дублюють положення КПК 1960-го року, тільки іншими формулюваннями. Більш того, у діючому КПК зовсім відсутні значні позитивні зрушення, що були передбачені статтями 52-1, 52-2, 52-3. 52-4 та 52-5 КПК 1960-го року. Ст. 52-1 «Забезпечення безпеки осіб, що беруть участь у кримінальному судочинстві» передбачала право на забезпечення безпеки з боку держави для будь-якої особи, яка бере участь у кримінальному судочинстві, в т.ч. для «особи, яка заявила до правоохоронного органу про злочин або в іншій формі брала участь у виявленні, запобіганні, припиненні і розкритті злочину чи сприяла цьому». У цілому, положення зазначеної статті, а також статей 52-2 «Права і обов'язки осіб, щодо яких здійснюються заходи безпеки», 52-3 «Нерозго-

лошення відомостей про особу, щодо якої здійснюються заходи безпеки», 52-4 «Порядок скасування заходів безпеки», 52-5 «Оскарження рішень про відмову в застосуванні заходів безпеки або про їх скасування» не тільки частково дублювали, а й суттєво доповнювали з процесуальної сторони положення Закону України «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві». Дуже шкода, що у новому кримінально-процесуальному законодавстві дуже мало уваги приділено саме цим гуманним положенням, а один з найважливіших принципів кримінального процесу всіх демократичних спільнот фактично не отримав свого розвитку.

На підставі розглянутого висловлюємо свої побажання щодо необхідності внесення в діючий КПК України доповнень, які передбачатимуть вищевказані можливості. Слід зазначити, що ці прогалини неодмінно відіб'ються в ненайкращій бік на практичній роботі органів внутрішніх справ, що протидіють злочинності засобами та методами оперативно-розшукової діяльності. Адже в усьому світі громадяни, які сприяють правоохоронним органам у негласній формі, становлять основну частку осіб, взятих під захист.

ОПЕРАТИВНЕ ПРОГНОЗУВАННЯ ЗЛОЧИННОСТІ В ІНФОРМАЦІЙНОМУ ЗАБЕЗПЕЧЕННІ ОВС

Маркарян Г.О.,
доцент кафедри спеціальної техніки, інформатики та інформаційних технологій ДЮІ МВС України, к.т.н.
Хашев Я.В.,
курсант факультету кримінальної міліції ДЮІ МВС України

З метою успішного виконання завдань у сфері боротьби із злочинністю правоохоронні органи повинні мати уявлення не лише про загальні методи розкриття злочинів, а й знати механізм впливу конкретних місцевих умов на стан злочинності в регіоні. Тому боротьба зі злочинністю має розпочинатися ще з розробки моделей прогнозування злочинності і планування її попередження, оскільки прогноз злочинності є основою для організації боротьби зі злочинністю взагалі.

Прогнозування – це процес розробки обґрунтованого судження про можливий стан об'єкту в майбутньому, або альтернативних шляхах і термінах досягнення цих станів [1]. Прогнозування відіграє значну роль при плануванні діяльності ОВС. Але в роботі оперативних підрозділів ОВС часто виникає необхідність прийняття рішень в оперативному режимі. Наявність науково обґрунтованих оперативних прогнозів дозволяє мінімізувати час на прийняття таких рішень та зумовлює їх об'єктивність.

Враховуючи той факт, що в сучасних умовах керування роботою правоохоронних органів реалізується суб'єктивним чином, актуальність оперативного прогнозування в діяльності підрозділів ОВС не викликає жодних сумнівів.

Основна мета оперативного прогнозування злочинності полягає у здатності правильно та швидко визначити найзагальніші показники, що характеризують розвиток (зміну) злочинності в майбутньому, виявленні її позитивних і негативних тенденцій, а також у пошуку на цій основі способів зміни або стабілізації цих тенденцій у необхідному для суспільства і держави напрямі [2]. Оперативному прогнозуванню властиві такі функції:

- прогнозування ймовірної поведінки членів організованих злочинних формувань після скоєння злочинів, що необхідно для вибору тактичних прийомів їх виявлення і затримання;
- прогнозування ймовірної ситуації, яка може скластися в період оперативної перевірки, чим визначається вибір і розстановка нових сил, підбір засобів і обрання тактики оперативної перевірки;
- прогнозування ймовірної поведінки негласних спів робітників в певних умовах при виконанні завдань оперативних працівників, що необхідно для їх спеціальної підготовки, спілкування та інформаційно-тактичного забезпечення їх діяльності;
- прогнозування поведінки неформальних груп з антигромадською спрямованістю – для визначення необхідності, форм і методів профілактичного втручання (з метою запобігання їх переростання в організовані злочинні формування);

- прогнозування індивідуальної злочинної поведінки, яке здійснюється з тією ж метою, що і прогнозування поведінки неформальних груп [3].

Існуюча методологія кримінологічного прогнозування базується на статистичному підході. Статистичні закономірності, що характеризують розвиток соціально-правових явищ, можуть використовуватися в прогнозі для звуження «зони пошуку», тобто служити досить надійними орієнтирами у виборі загального напряму прогнозу розвитку злочинності і пов'язаних з нею явищ. Статистичний підхід до прогнозування виходить з правил того, що прогноз, зроблений на підставі виявлених закономірностей, стає тим надійніше, чим більше число об'єктів, які утворюють відповідну статистичну сукупність.

В оперативно-розшуковому прогнозуванні зазначений підхід знайшов відображення в передбаченні конкретних подій, або декількох варіантів розвитку тактично значимих подій. Серед типів передбачення слід відмітити наступні:

1. Передбачення настання яких-небудь подій на основі повторюваності тих або інших явищ. Воно базується на встановленні зв'язків між спостережуваними явищами. Наприклад, з наступом робочого дня щодня на певному об'єкті з'являються ті або інші особи, та є можливість візуально спостерігати і фіксувати їх контакти. Прогноз припускає повторення тієї ж ситуації і в день проведення необхідних оперативно-розшукових дій.
2. Передбачення за аналогією: якщо при певних обставинах людина діє якимось чином, то в подібній ситуації слід очікувати аналогічних дій з її боку. Передбачення за аналогією дозволяє визначати місце і час ймовірної появи злочинців; воно використовується для оперативного прикриття об'єктів з метою виявлення кишенькових злодіїв, шахраїв, спекулянтів, грабіжників.

Слід зазначити, що вказані методи ефективно діють тільки при чітко визначених обставинах. Але реалії свідчать про те, що на практиці працівникам ОВС частіше за все приходиться приймати рішення в умовах невизначеності та ризику. Для прогнозування саме в таких умовах найбільш ефективним постає метод математичного моделювання, реалізація якого

здійснюється в декілька етапів. Перш за все проводиться аналіз взаємозв'язків між соціально-правовими процесами, дослідження їх впливу на розвиток злочинності, в результаті чого визначаються як фактори, що сприяють зростанню злочинності, так і фактори, які нівелюють це явище. На підставі виявлених залежностей розробляється модель динаміки соціально-правових процесів, тобто їх опис у вигляді математичних функцій від часу, що дає можливість здійснити прогноз злочинності на будь-який період майбутнього [4].

Таким чином, оперативне прогнозування забезпечує визначення оптимального варіанта науково обґрунтованих заходів підвищення ефективності діяльності ОВС у сфері боротьби зі злочинністю.

Розробка динамічних моделей для оперативного управління діяльністю підрозділів ОВС являє наукову новизну дослідження. Перспективами розвитку цього напрямку можна вважати інтегрування підсистеми оперативного прогнозування до інформаційного забезпечення, що використовується в діяльності ОВС.

1. Прогноз : Матеріал з Вікіпедії – вільної енциклопедії [Електронний ресурс] – 2012. – Режим доступу : http://uk.wikipedia.org/
2. Александров Ю.В. Кримінологія: Курс лекцій / Александров Ю.В., Гель А.П., Семаков Г.С. – К.: МАУП, 2002. – 295 с.
3. Овчинский С.С. Оперативно-розыскная информация / Овчинский С.С. ; под ред. А.С. Овчинского и В.С. Овчинского. – М. : ИНФРА-М, 2000. – 367 с.
4. Маркарян А.О. Динамическая модель прогноза выдачи кредитов / Маркарян А.О. // Искусственный интеллект. – 2003. – № 3. – С.368-373.
5. Франке Э. Оперативно-розыскная деятельность в борьбе с организованной преступностью [Электронный ресурс] / Э.Франке. – Международная Академия Наук Сан-Марино, Европейский Университет Права, Москва, 1997р. – Режим доступу : http://gm3d.ru/referaty_po_kriminalistike/diplomnaya_rabota_operativno-rozysknaya.html
6. Прогнозування злочинності, його практичне значення? [Електронний ресурс] – 2012. – Режим доступу : http://advokatonline.org.ua/prohnozuvannya-zlochynnosti-joho-praktychne-znachennya/
7. Прогнозування злочинності і його методи [Електронний ресурс] – 2012. – Режим доступу : http://www.xres.ru/viewpage.php?page_id=53

ІНФОРМАЦІЙНО-АНАЛІТИЧНА ДІЯЛЬНІСТЬ ЯК СКЛАДОВА ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ ОРГАНІВ ВНУТРІШНІХ СПРАВ У ПРОТИДІЇ ОРГАНІЗОВАНИМ ЗЛОЧИННИМ ГРУПАМ

Гула Л.Ф.,
доцент кафедри оперативно-розшукової діяльності та спеціальної техніки ЛьвДУВС, к.ю.н., доцент

Ефективна протидія організованим злочинам у державі потребує підвищення рівня оперативної обізнаності з процесами, які відбуваються в злочинному середовищі, планами й намірами його лідерів та учасників угруповань, уможливлює якісне інформаційне забезпечення виявлення та розкриття замаскованих та організаційно підготовлених особливо тяжких злочинів, створює передумови своєчасному запобіганню насамперед убивствам на замовлення, викраденню людей, протиправним замінам власників стратегічно важливих для держави й суспільства підприємств тощо.

В умовах високого динамізму політичних, соціальних і економічних процесів, ускладнення управління соціальними системами, ефективність організації оперативно-розшукової діяльності підрозділами МВС України у боротьбі з організованими формами злочинності визначається глибиною і всебічністю аналізу оперативної обстановки та прийняттям на її основі відповідних управлінських рішень. У зв'язку з цим результативність діяльності оперативних підрозділів залежить не тільки від особистих ділових якостей і оперативно-технічної оснащеності співробітників, але і ефективності системи інформаційно-аналітичного забезпечення [1, с. 2].

Ми погоджуємося з науковцями стосовно того, що інформаційне забезпечення оперативно-розшукової діяльності підрозділів МВС у боротьбі з організованими групами є циклічним процесом пошуку, збирання, опрацювання, переосмислення, зберігання, видачі інформації та її використання для прийняття оперативно-тактичних та інших управлінських рішень.

Основними завданнями функціонування системи інформаційно-аналітичного забезпечення у боротьбі з організованими злочинними групами є:

- використання можливостей оперативного отримання у повному, автоматизованому та зручному для користування вигляді інформації співробітниками МВС України, для боротьби із злочинними групами;
- збір, обробка та узагальнення оперативної, оперативно-розшукової, оперативно-довідкової, аналітичної, статистичної і контрольної інформації для оцінки ситуацій та прийняття обґрунтованих оптимальних рішень на всіх рівнях діяльності МВС;
- забезпечення динамічної та ефективної інформаційної взаємодії усіх структурних служб МВС, інших правоохоронних органів та державних установ;
- забезпечення захисту інформації.

Організаційно-практична діяльність керівника МВС, ГУВС, УВС України, а також їх оперативних підрозділів щодо боротьби з організованими формами злочинності, значною мірою є інформаційною, оскільки включає отримання повідомлень, необхідних для прийняття рішень, каналами зворотного зв'язку, відомостей про процеси і реалізацію раніше ухвалених рішень. Не випадково фахівці в області теорії управління вважають, що управління у відомому сенсі можна визначити як процес сприйняття, перетворення, накопичення, передачі та використання інформації.

Значення інформації в управлінні оперативними підрозділами у боротьбі з організованими злочинними групами обумовлене її ключовою роллю в системах соціального управління, де інформація є головною умовою і засобом реалізації організаційно-управлінських функцій. З іншого боку, зважаючи на специфіку вирішуваних цими підрозділами завдань, основний зміст їхньої діяльності полягає в добуванні, систематизації і аналізі інформації, необхідної для боротьби з організованими злочинними групами.

Щоб управління було безперервним і ефективним, потрібна певна організація інформаційних процесів. Діяльність, спрямована на створення, функціонування і вдосконалення

інформаційних систем для виконання завдань управління, є функцією органу управління і називається «інформаційним забезпеченням управління». Під інформаційними системами в соціальному управлінні, у тому числі у сфері управління органами внутрішніх справ, розуміються організовані людиною системи збору, зберігання, обробки і видачі інформації, необхідної для успішної роботи суб'єктів і об'єктів управління [2, с. 187–188].

Актуальність проблеми інформаційного забезпечення оперативно-розшукової діяльності МВС, ГУВС, УВС України, спрямованої на боротьбу зі злочинами, здійснюваними організованими злочинними структурами із розширеними міжнародними і міжрегіональними кримінальними зв'язками, характеризуються такими чинниками:

- комплексним характером процесу боротьби з такими злочинами, в якому беруть участь різні служби органів внутрішніх справ, інші правоохоронні органи, а також державні і суспільні організації;
- широкими просторовими масштабами діяльності злочинних структур, мобільністю, технічною оснащеністю;
- необхідністю здійснення оперативно-розшукових заходів щодо боротьби зі злочинними структурами на території різних районів, регіонів, держав;
- жорсткими тимчасовими межами здійснення оперативно-розшукових заходів і слідчих дій, особливо на первинному етапі;
- особливостями оперативно-розшукової характеристики таких злочинів і злочинних структур, що їх здійснюють;
- сучасним станом організованої злочинності у різних сферах.

Суттєво підвищить ефективність боротьби з організованими формами злочинності наявність:

- єдиного інформаційного простору, узагальнення та інтегрування різноманітної інформації, яка надходить від оперативних та інших джерел системи МВС України;
- постійного об'єктивного аналітичного дослідження інформаційних потоків і незалежної від інтересів окремих

служб оцінки для забезпечення розшукової та іншої діяльності галузевих служб МВС України;

- прогнозування ймовірних форм і напрямів розвитку злочинних процесів в економічній та управлінській сферах суспільної та державної діяльності;
- розробки відповідних форм і методів діяльності з нейтралізації злочинних процесів та знешкодження злочинних угруповань.

1. Тищенко В.Н. Теоретические основы и проблемы совершенствования информационного обеспечения аппаратов уголовного розыска оперативно-розыскной информацией / В.Н. Тищенко. – М.: ИМВД РФ, 1980. – 266 с.
2. Захаров В.П. Проблеми інформаційного забезпечення правоохоронних структур: навч.-практ. посібник / В.П. Захаров, В.І. Рудешко. – Львів: ЛьвДУВС, 2007. – 372 с.

ПРАВОВЕ РЕГУЛЮВАННЯ ДОСТУПУ ДО ОКРЕМИХ ВИДІВ ІНФОРМАЦІЇ

Ярема О.Г.,
доцент кафедри конституційного, адміністративного та міжнародного права ЛьвДУВС, к.ю.н.

Накопичення інформаційного потенціалу, розвиток суспільного інтелекту, розширення кола знань, вдосконалення інформаційних технологій та комунікацій свідчать про перехід людства до інформаційного суспільства, яке крім позитивних моментів, несе нові соціальні загрози, особливо якщо інформаційні відносини розвиваються поза цілеспрямованим впливом держави. Це зумовлює актуальність проблеми всебічного регулювання інформаційних правовідносин з боку держави та правового регулювання доступу до окремих видів інформації з метою недопущення обмеження реалізації інформаційних прав особи, суспільства, держави.

У Конституції України (ст. 34) закріплено право кожного вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір; знайомитися в органах державної влади, органах місцевого

самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею. Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя. Однак практика показує, що обмеження даних прав здійснюється не тільки у випадках, передбачених Конституцією та законодавством України. Та й чіткої визначеності стосовно конкретних видів відповідальності за порушення зазначених прав нажаль немає.

Насьогодні актуальним залишається питання обмеження доступу до персональних даних. Порядок обмеження доступу до цього виду інформації визначається Законом України «Про захист персональних даних». Зокрема,

Закон регламентує, що персональні дані за режимом доступу є інформацією з обмеженим доступом (ч. 2 ст. 5). Це означає, зокрема, що особа, яка здійснює оброблення баз персональних даних, повинна забезпечити відповідну охорону таких баз від несанкціонованого доступу третіх осіб, тобто уповноважена обмежити доступ до цього виду інформації. Відповідно до норм цього Закону також встановлюється особливі вимоги оброблення персональних даних – забороняється оброблення персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, а також даних, що стосуються здоров’я чи статевого життя, за винятком встановлених у Законі випадків (ст. 7). Організація баз даних є необхідною передумовою для створення правових інформаційних систем і належного забезпечення правовою інформацією суспільства, але використання таких баз може призводити до нових проблем. Скажімо, нагромадження великого обсягу правової інформації в банку даних може призвести до монополізації, а згодом і до зловживань у вигляді приховування інформації, її незаконного оприлюднення чи використання з корисливою метою. Для запобігання таким зловживанням право

власності на правову інформацію має належати державі, а використання даних регламентуватися законодавством.

З метою законодавчого закріплення ефективних правових механізмів реалізації права кожного на доступ до інформації, зокрема публічної, – тієї, що знаходиться у володінні суб'єктів владних повноважень та інформації, що становить суспільний інтерес 13 січня 2011 р. було прийнято Закон України «Про доступ до публічної інформації», а також нову редакція Закону України «Про інформацію». Закон України «Про доступ до публічної інформації» ввів новий вид інформації з обмеженим доступом – службова інформація на заміну незаконним грифам «ДСК», «не для друку». Можливості застосування статусу службової інформації порівняно з указаними грифами суттєво звужено. Також згідно змін внесених до даного Закону 17 травня 2012 року, не належать до інформації з обмеженим доступом відомості, зазначені у декларації про майно, доходи, витрати і зобов'язання фінансового характеру, оформленої за формою і в порядку, що встановлені Законом України «Про засади запобігання і протидії корупції».

Насьогодні існує й ряд проблем правового регулювання захисту відомостей, що становлять банківську таємницю. Так, згідно Закону України «Про банки і банківську діяльність» до банківської таємниці належить і інформація про клієнтів іншого банку, навіть якщо їх імена зазначені у документах, угодах та операціях клієнта, оскільки частиною 3 статті 62 цього ж Закону банку заборонено надавати таку інформацію. Також банківським установам, відповідно до ч. 4 ст. 62 Закону України «Про банки і банківську діяльність», забороняється надавати інформацію про клієнтів іншого банку, навіть якщо їх імена зазначені у документах, угодах та операціях клієнта. Відповідно, імперативна норма ч. 4 ст. 62 даного закону є основою для відмови в наданні будь-якої інформації стосовно осіб, які є клієнтами іншого банку. Однак існує лист Національного банку України від 19.04.2001 р. № 18-112/1467-2599, який дає роз'яснення, що на запити органів прокуратури України, СБУ, МВС України, державної податкової служби України банки повинні надавати інформацію про рух коштів на рахунку клієнта без зазначення відправника цих коштів та їх одержувача

(які є клієнтами як іншого, так і запитуваного банку). Законом України «Про банки і банківську діяльність» не встановлено порядку та форми надання банками на письмову вимогу зазначених органів інформації, що становить банківську таємницю. Таким чином, системний аналіз чинного законодавства та правозастосовчої практики зумовлює необхідність закріпити в Законі України «Про банки і банківську діяльність» чіткий перелік відомостей, що становлять банківську таємницю.

Звичайно, на сьогодні залишається ще чимало проблем та невирішених питань щодо інформаційної сфери. Причиною цих проблем, на нашу думку, можна вважати недосконале українське інформаційне законодавство, яке перебуває на стадії розвитку, тому існує ще багато невирішених питань, помилок, неврегульованих законодавче прогалин.

На сьогодні є потреба в об'єднанні всіх існуючих нормативно-правових актів, за допомогою яких регулюються відносини в сфері інформації в єдиний кодифікований документ, який би об'єднав (систематизував) правові норми, що регулюють інформаційні правовідносини, встановив режими доступу до окремих видів інформації, відповідальність за їх порушення з метою недопущення як обмеження реалізації інформаційних прав особи, суспільства, держави, так і зловживань такими правами.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ

Галушка Н.В.,
слідчий СВ Городоцького РВ ГУ МВСУ у Львівській області

Удосконалення практики розслідування злочинів неможливе без відповідного інформаційного забезпечення. Інформацію, використовувану при розслідуванні злочинів, можна розглядати як різновид спеціальної і правової інформації, оскільки основним джерелом правової інформації є зведення про право і дотичних до нього явищ. Правова інформація охоплює не тільки чинне право, а й містить у собі все, що пов'язано з практикою реалізації права, з його вивченням і

теоретичною розробкою. Тобто правова інформація охоплює зведення про різні юридичні події, факти, явища і пов'язані з ними процеси.

Функціональним обов'язкам слідчого повинно відповідати його право на те, щоб мати необхідну інформацію, у тому числі інформацію про можливості застосування науково-технічних досягнень при розслідуванні злочинів, тобто при виявленні, закріпленні і дослідженні доказів щодо кожної конкретної справи. Дана вимога диктується зрослим професіоналізмом злочинців, підвищенням рівня злочинності, а отже, – збільшенням навантаження на працівників правоохоронних органів, а також значним зміцненням і суперечливістю показань свідків і інших учасників кримінального процесу.

З метою забезпечення досудового розслідування негласною інформацією проводяться негласні слідчі (розшукові) дії у випадках, якщо відомості про злочин та особу, яка його вчинила тяжкий або особливо тяжкий злочинів, неможливо отримати в інший спосіб [1, с. 103].

Розслідування злочинів як інформаційний процес розпочинається з виявлення необхідної інформації, тобто встановлення конкретних матеріальних об'єктів-носіїв і виявлення в них сигналів інформації. Обсяг даної інформації обробляється слідчим у ході виконання ним професійних обов'язків. За джерелом походження всю інформацію, якою оперує слідчий, поділяють на три види:

- процесуальна, тобто отримана із джерел, названих у кримінально-процесуальному законі;
- отримана органами дізнання за допомогою оперативно-пошукових заходів (оперативно-пошукова інформація);
- інша інформація, отримана слідчим у результаті ознайомлення з навколишнім середовищем [2, с. 40].

Частина цієї інформації увійде до обсягу доказів і іменуватиметься доказовою, інша її частина в доказуванні використовуватися не буде і не матиме процесуального характеру, хоча і має суттєве значення. Можна сказати, що в цілому процес розслідування має два рівні.

Коло джерел кримінально значущої інформації є значно ширшим від кола джерел доказової інформації, вичерпний

перелік якої наведено у кримінально-процесуальному законі. Джерелами можуть бути фізичні особи або об'єкти, які є фрагментами об'єктивної дійсності і взаємопов'язані з обставинами події злочину, вони несуть сигнали інформації про розслідувану подію. Класифікація таких джерел насамперед опосередкована класифікацією матеріальних об'єктів і формами відбитків у неживій і живій природі.

Інформація, одержувана від джерела – людини і від матеріальних слідів відображень, набуває свого доказового значення в процесі її подання у визначеній формі, визначеним способом і за допомогою криміналістичних засобів. У спеціальній літературі виділяють такі форми подання інформації в процесі доказування: вербальна форма (усна, письмова промова тощо); графічна форма; іконічна форма (наочні зразки); комбінована форма [3, с. 347].

Названі форми подання інформації в результаті діяльності суб'єкта, тобто, будучи оформлені відповідним чином (протоколювання, фотографування), набувають статусу доказів. При цьому кінцеві результати діяльності суб'єкта закріплюються в матеріальних формах (криміналістичних засобах), тобто представляють собою відображення об'єктів на будь-якому матеріальному носії у вигляді інформаційної моделі цього об'єкта або явища (фотознімок, гіпсовий зліпок тощо). Криміналістичні засоби забезпечують безпосереднє сприйняття інформації суб'єктом доказування або оперування нею.

Широкі можливості для того, щоб на попередньому слідстві уявити, якою є інформація, дає застосування науково-технічних досягнень, що несуть цінну інформацію, поряд з іншими доказами. Для подання такої інформації використовуються технічні засоби і спеціальні знання. При цьому необхідно чітко розмежовувати компетенцію суб'єкта доказування та особи, яка володіє спеціальними знаннями. Використовувати технічні засоби для подання інформації суб'єкт доказування може тоді, коли він не піддає змінам досліджувані сліди і речові джерела, коли застосовувані прийоми для уявлення інформації доступні розумінню всіх учасників процесу, а подана інформація наочна, очевидна і зрозуміла. Коли ж сигнали інформації недоступні безпосередньому сприйняттю, щоб їх виявити і

пояснити, використовують попереднє дослідження, виконане фахівцем або експертом [4, с. 7].

Зведення, якими доводиться оперувати у процесі розслідування і попередження злочинів, у криміналістичній літературі називають по-різному: одні – просто інформацією, другі – доказовою, інші – криміналістичною або ще повідомляючою. Інформацію, яку використовують у процесі виявлення, розслідування і попередження злочинів, на наш погляд, більш доцільно називати криміналістичною, виходячи з предмета науки криміналістики. Криміналістичну інформацію, по-перше, утворюють дані про розслідувану подію, про всі її елементи і взаємозв'язки між ними. Виявлення такого роду даних і є виявленням інформації, що характеризує подію злочину та окремі його елементи, тобто є виявленням криміналістичної інформації, а виявлення об'єктів, що її містять, є виявленням безпосередніх первинних носіїв і джерела криміналістичної інформації.

Таким чином, інформаційне забезпечення слідчої практики передбачає: підвищену організованість інформаційних процесів, їх упорядкування, узгодженість, злагодженість, регул ярність, закріплення і розвиток демократичних принципів при розслідуванні злочинів та інформаційних процесів, що його забезпечують; захист інтересів і прав суспільства й особистості у правовій державі, оптимізацію інформаційних процесів, добір і закріплення тих прийомів і методів, що відповідають цілям кримінального судочинства.

1. Кримінально-процесуальний кодекс України (текст); – К.: «Центр Учбової літератури», 2012. – 254 с.
2. Кабанов П.П. Процесуальний статус информации, полученной с помощью научно-технических средств при расследовании преступлений // Актуальные вопросы использования достижений науки и техники при расследовании преступлений органами внутренних дел. – М., 1990. – 122 с.
3. Белкин Р.С. Курс криминалистики: Учеб. пособие для вузов. – 3-е изд. допол. – М.: ЮНИТИ ДАНА, Закон и право, 2001. – 837 с.
4. Беляков К.И. Совершенствование информационного обеспечения расследования преступлений на базе АИПС. Автореферат. дис. канд. юрид. наук. – К., 1993. – 20 с.

ВИКОРИСТАННЯ ЕЛЕКТРОННОГО МОНІТОРИНГУ: СВІТОВИЙ ДОСВІД

Кійков В.М.,
викладач кафедри інформаційної безпеки факультету психології, менеджменту, соціальних та інформаційних технологій, Харківський національний університет внутрішніх справ
Рвачов О.М.,
викладач кафедри інформаційної безпеки факультету психології, менеджменту, соціальних та інформаційних технологій, Харківський національний університет внутрішніх справ

Концепція використання електронного моніторингу (далі – ЕМ) злочинців в суспільстві була запропонована американським психологом Робертом Швітцгебелем (Robert Schwitzgebel) у 60-х роках минулого століття. Практичне впровадження даної ідеї у пенітенціарну системі зайняло майже 20 років і ідея була використана з метою зменшення кількості ув'язнених у закладах виконання покарань.

Дана форма покарання, або форма запобіжного заходу має різні назви, так наприклад у Нової Зеландії її називають «домашнім ув'язненням», а у північній Америці найбільш поширеним є термін «електронний моніторинг» [3].

ЕМ можна використовувати для взяття під варту, арешту на стадії досудового слідства, для контролю виконання накладеного судом чи органом досудового слідства обмеження на пересування правопорушника, для спостереження за правопорушником у випадках коли у визначеному законом порядку необхідно знати місце знаходження правопорушника, бути впевненими, що він не перебуває у заборонених зонах та не контактує з забороненими особами та перебуває під безперервним спостереженням [4].

Одним із головних завдань при впровадженні ЕМ в суспільстві є пошук балансу між функцією покарання, яка б задовольняла суспільство в його бажанні покарати правопорушника, та засобу сприяння змінам у поведінці правопорушників, заохочення його до більш соціально-відповідальної поведінки, тобто до реабілітації [5].

До переваг використання програм ЕМ відноситься зменшення бюджетних витрат на порівняно високу ціну тюремного, або традиційного утримання правопорушника та захист засудженого від асоціального впливу тюремного середовища. Перебування засудженого в закладах позбавлення волі руйнує встановлені у нього соціальні зв'язки, призводить до надлому громадянської свідомості засудженого та перегляду ним життєвих цінностей, надає відчуття «клейма засудженого». Програми ЕМ при збереженні функції покарання надають засудженому можливість підтримувати родинні зв'язки, відчувати себе членом суспільства.

Мета усіх програм ЕМ побороти злочинну поведінку шляхом посилення контролю за виконанням умов відбування покарання, збільшення особистої відповідальності правопорушника. ЕМ може розглядатись як фактор забезпечення суспільної безпеки, яка, окрім використання програм ЕМ, досягається традиційною практикою громадського спостереження: звільнення під заставу, умовно-дострокове звільнення, взяття на поруки, умовне засудження. Ряд дослідників [6] вказують, що ЕМ є ефективним у стабільному зменшенні показників рецидивів.

Напрямки використання ЕМ.

З моменту своєї появи, ЕМ був застосований до безлічі злочинців та на різних стадіях правосуддя. Наприклад, багато програм ЕМ застосовувались до правопорушників, що скоїли злочин проти майна або з використанням наркотичних речовин, також доцільність використання цієї технології до правопорушників, що скоїли тяжкі сексуальні злочини та рецидивістів обговорюється в наукових колах [7].

У тактико-технічних прийомах використання ЕМ можливі варіації у відповідності до рівня потенційної небезпеки конкретного правопорушника. У випадку коли, правопорушник вчинив не тяжкий злочин, ЕМ використовується самостійно або в поєднанні з іншими формами контактного моніторингу. Із збільшенням тяжкості складу злочину ЕМ виступає складовою частиною багатогранної виправної програми з посиленими варіантами спостереження за правопорушником.

ЕМ моніторинг різноплановий за впровадженням та охоплює 3 стадії кримінального судочинства: досудова фаза, винесення вироку, фаза відбуття покарання (ув'язнення). Хоча головні цілі усіх програм ЕМ можуть відрізнятися у відповідності до фази застосування, але усі вони націлені на контроль за правопорушником та забезпечення надійної безпеки для суспільства [8].

На стадії досудового слідства ЕМ може використовуватись як умова звільнення затриманого під заставу, коли слідчий суддя визначає можливість застосування такої норми кримінального процесу та дозволяє правопорушнику повернутися до дому і чекати розгляду справи у суді. На цій стадії ЕМ використовують як спосіб спостереження для зменшення ризику втечі правопорушника, для впевненості, що умови звільнення дотримуються та для зменшення вірогідності скоєння ним інших злочинів.

Додатково, на стадії досудового слідства, ЕМ може бути застосований як варіант початкової стадії вироку, як засіб, що накладає певні обмеження щодо прав і свобод правопорушника [9]. Дане застосування ЕМ є основою схем домашнього арешту, що полягає в утриманні правопорушника у його помешканні на визначених судом умовах. У даному випадку ЕМ використовується судом як вид покарання, який передбачає використання помешкання засудженого як засіб для впровадження покарання, враховуючи послаблення спостереження та накладання обмежень на засудженого.

На даний час ЕМ використовується як основна альтернатива традиційному ув'язненню в США, та розглядається як більш м'яке покарання, але розглядається більш ефективним ніж умовний вирок. Як санкція ЕМ має в собі ознаки покарання, та одночасно включає в себе реабілітаційні якості, що підвищує захист суспільства шляхом зменшення вірогідності скоєння нових правопорушень.

Наряду з усіма способами застосування ЕМ, найбільш поширеним є його використання на стадії ув'язнення, а саме як умова при умовно-достроковому звільненні. Звідси і цілі програм ЕМ переважно реінтеграційні та реабілітаційні за суттю.

Говорячи про оцінку ефективності використання програм ЕМ, необхідно зазначити, що деякі дослідження вказують на

зменшення рівню рецидивів серед залучених до програм ЕМ порівняно до тих осіб, у відношенні до яких ЕМ не застосовувався [10].

Технічні аспекти використання ЕМ.

ЕМ є нетаємною формою спостереження, що перевіряє факт наявності особи у певному приміщенні (помешканні) або використовує систему глобальної навігації та передає місце знаходження особи на контрольний пункт спостереження через, наприклад, стільниковий зв'язок.

Залежно від обраного запобіжного заходу використовується та чи інша система контролю: радіочастотна або GPS-системи.

Якщо мова йде про домашній арешт, то в квартирі підозрюваного встановлюється базова станція, а на руку чи ногу йому надягають браслет, що передає сигнал на неї. Якщо заарештований виходить з будинку, то сигнал уривається і станція повідомляє контрольний орган про порушення режиму домашнього арешту. Далі відбувається виїзд працівників міліції та фіксування події на місці.

Другий варіант: коли контроль здійснюється у зв'язку з іншими запобіжними заходами, тоді у браслет вмонтовується GPS-трекер, що дозволяє в режимі он-лайн простежувати не тільки те, в якому місті перебуває суб'єкт, а і яким боком вулиці він іде в даний момент. Комп'ютер контрольного пункту простежуватиме переміщення підконтрольних осіб цілодобово [11].

Прилади спостереження візуально схожі на годинник та мають захист від несанкціонованого зняття, водно резистентні і принципово не відрізняються один від одного. Як приклад, можна навести один із поширених пристроїв модифікації G4S, що встановлюється на щиколотку особи і виглядає як стрічка темного кольору приблизно 2.5 сантиметри ширини та 8 сантиметрів довжини з 3-х сантиметровим робочим елементом – передавачем сірого кольору. По краям стрічки для її посилення вставлені армовані волокна. Додатково і з метою запобігання несанкціонованого зняття пристрою у середині стрічки проходять 10 оптико-волоконних світловодів, по кожному з них пробігає імпульс з періодичністю в 0.5 секунди. При розриві оптичного волокна пристрій випромінює сигнал тривоги. На

пристрої вибитий номер телефону офіцеру підрозділу спостереження, для зв'язку з ним у разі необхідності.

На даний час, пристрої ЕМ можуть бути такими, що безперервного випромінюють сигнал або пристрої, що працюють за певним алгоритмом – програмою.

Перший різновид має 3 основні функціональні частини: передавач, приймач сигналу (пристрій автоматичного набору номеру) та центральний комп'ютер, що знаходиться на пульті спостереження.

GPS системи ЕМ та радіочастотні пристрої.

Використання додаткових способів нагляду та спостереження за правопорушником, що виходять за межі традиційних пенітенціарних заходів нагляду та виконання покарань, не визивають сумніву щодо їх суспільної цінності. Так само і поява GPS технологій дозволила надавати інформацію про пересування особи у реальному часі, що було неможливо у випадку використання радіочастотного устаткування. Як зазначалось вище радіочастотний моніторинг обмежений у визначенні місцезнаходження особи, по відношенню до якої застосовано ЕМ.

GPS системи дозволяють окрім постійного відстеження місцезнаходження правопорушника, визначити зони, що дозволені та заборонені для перебування. Хоча ЕМ моніторинг може надати інформацію про місцезнаходження правопорушника, але не в змозі запобігти кримінальній поведінці.

У випадку активних GPS систем є можливість безпосереднього інформування правопорушника про порушення ним умов електронного моніторингу, знаходження в недозволеній зоні.

Наряду з безперечними перевагами GPS систем порівняно до радіочастотних, вони мають ряд недоліків, такі як значно вища ціна в обслуговуванні. Ціна збільшується за рахунок оплати стільникового зв'язку, більш коштовного обладнання та оплати цілодобової роботи офіцерів служби спостереження і контролю на пульту спостереження.

Пасивні GPS системи збільшують об'єм роботи офіцерів спостереження, коли їм необхідно проаналізувати отриману інформацію, що передав передавач від приладу порушника на приймач пульту, з метою виявлення можливого порушення.

Пасивні GPS системи порівняно до активних у більшості випадків змушують офіцера контролю здійснювати перевірки інцидентів, що згодом виявляються хибними.

Ряд досліджень на заході вказують, що за крітерієм «ціна-ефективність» активні GPS системи випереджають пасивні та припускають, що економічна різниця у більшості залежить від способи обробки інформації та не залежить від самої системи.

Інший недолік, що пов'язаний з стільниковими трекінговими технологіями пов'язаний із залежністю останніх від якості покриття мережі. У стільниковому зв'язку існують так звані «мертві зони», у яких стільникові прилади, що використовуються у якості передавача сигналу, можуть згубити сигнал та ставити під сумнів дотримання правопорушником умов зобов'язання носити ЕЗК. Втрата сигналу викликає сигнал тривоги на пульту спостереження і у випадку активної GPS системи потребує негайного реагування та визначення місця знаходження особи не залежно чи є об'єктивні підстави для цього. У випадку пасивних GPS систем тимчасова втрата сигналу не впливає на хибні виїзди офіцерів охорони.

Тевей (Tewey) запропонував, що у разі спрацювання активної системи доцільно, щоб інформація про місце знаходьження особи продовжувала записуватись на особистий трекінговий пристрій та поновлювала свою роботу у разі відновлення мережевого покриття та надходження сигналу [12].

Висновки.

В цілому, збільшення рівня надзору, що асоціюється з ЕМ та необхідність забезпечення надійного захисту суспільства є раціональним підґрунтям для подальшого наукового дослідження у напрямку технологій ЕМ як вагомого додатку до традиційних способів нагляду за правопорушниками, що використовується у державі.

Додаткові переваги використання GPS обладнання у ЕМ тільки на початковій стадії усвідомлення фахівцями України, але закордоном ця альтернатива радіочастотним сигнальним пристроям вже довела свою більшу ефективність.

Більш того, враховуючи збільшення обсягів використання GPS обладнання та нестримний технологічний розвиток можна прогнозувати зменшення вартості впровадження і використання

GPS систем. Безперечно, з розвитком технічного прогресу та технологій будуть з'являтись нові і більш досконалі програми ЕМ, що спроможні виконувати завдання корекції злочинної поведінки більш ефективніше.

1. Кримінальний процесуальний Кодекс України [Електронний ресурс]: Закон України від 13.04.2012 № 4651-VI, редакція від 15.08.2012. – Режим доступу: http://zakon.rada.gov.ua/go/4651%D0%B1-17.
2. Про затвердження Положення про порядок застосування електронних засобів контролю [Електронний ресурс]: наказ МВС України від 09.08.2012 № 696. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/z1503-12.
3. Rondinelli, V. (1997). Tracking humans: The electronic bracelet in a modern world. Retrieved February 22, 2007, from http://www.criminallawyers.ca/newslett/aug97/rondinelli.htm
4. Black, M., & Smith, R.G. (2003). Electronic monitoring and the criminal justice system. Trends and Issues in Crime and Criminal Justice, 254, pages:1-6.
5. White, E. (2001, May). Electronic surveillance: Where do we draw the line? Paper presented at the Electronic Monitoring and the Ontario Crown Attorneys' Association Conference. Retrieved March 3, 2007, from http://www.stleonards.ca/docs/policy/plelectro.asp
6. Renzema, M., & Mayo-Wilson, E. (2005). Can electronic monitoring reduce crime for moderate to high-risk offenders? Journal of Experimental Criminology, 1, 215-237.
7. Minnesota Department of Corrections. (2006). Electronic monitoring of sex offenders: 2006 report to the legislature. Retrieved March 1, 2007, from http://archive.leg.state.mn.us/docs/2006/Mandated/060146.pdf
8. Albrecht, H. (2005). Electronic monitoring in Europe. A summary and assessment of recent developments in the legal framework and the implementation of electronic monitoring. Retrieved March 6, 2007, from http://www.iuscrim.mpg.de/forsch/onlinepub/albrecht.pdf
9. John Howard Society of Alberta (2006). Electronic (radio frequency) and GPS monitored community based supervision programs. Retrieved February 15, 2007, from http://www.johnhoward.ab.ca/PUB/PDF/monitorupdate.pdf
10. Office of Program Policy Analysis and Government Accountability. (2005). Electronic monitoring should be better targeted to the most dangerous offenders. Research Report No. 05-19. Retrieved February 20, 2007, from http://www.oppaga.state.fl.us/reports/pdf/0519rpt.pdf
11. Богунов, В. Справа техніки [Електронний ресурс] / Валентин Богунов // Закон і бізнес. – 2012. – Вип. № 6 (1045). – Режим доступу:

http://zib.com.ua/ua/7848-zastosuvannya_tehnichnih_zasobiv_u_kriminalnomu_procesi_zgid.html.
12. Tewey, J.F. (2005). Task force to study criminal offender monitoring by global positioning systems: Final report to the Governor and the General Assembly. Retrieved March 1, 2007, from http://www.dpscs.state.md.us

МІСЦЕ ОПЕРАТИВНО-РОЗШУКОВОЇ ІНФОРМАЦІЇ У СИСТЕМІ ДОКАЗІВ В КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Кріль О.В.,
слідчий СВ Теребовлянського РВ УМВСУ у Тернопільській області

Науково-технічна рево–люція і властивий їй інте–гративний характер соціаль–но-економічних зв'язків і від–носин перетворили інформа–цію на одне з найбільш уживаних у різних значеннях понять, зробили її об'єктом серйозних наукових досліджень. Інформа-ційна взаємодія різноманітних сфер громадського життя, окремих індивідів – дуже специфічна і дуже важлива форма соціальної взаємодії. При цьому ступінь налагодженості й ефективності інформаційної взаємодії є одним із найважливіших показників суспільного прогресу.

Але особливий інтерес для нас становить той різновид інформації, який допомагає вирішувати питання боротьби зі злочинністю. Потреба в такій інформації сьогодні надзвичайно велика.

Природа процесу збору, дослідження й оцінки доказів у кримінальному судочинстві за своєю суттю має інформативний характер. Факти, що утворюють подію злочину, після свого виникнення стають об'єктивною реальністю. Щоб пізнати їх, потрібно зібрати про них інформацію, що відтворює їх зміст.

Аналізуючи обсяг понять, не можна не відзначити, що він різний. Наприклад, юридична інформація включає поняття: доказова інформація, криміналістична, кримінально-правова, кримінологічна, оперативно-розшукова та інші значення, які входять в юридичну науку. Тому наведені поняття можна класифікувати і таким чином визначити місце оперативно-розшукової інформації в інформаційній системі доказів. На

вершині класифікації перебуває загальне поняття «юридична інформація», яка поділяється на два види: «правова інформація» (кримінально-правова, кримінально-процесуальна, цивільно-правова, адміністративно-правова…) і «не правова інформація» (криміналістична, кримінологічна, оперативно-розшукова, організаційно-управлінська...), кожна із них поділяється на підвиди (доказова, орієнтовна, профілактична...), а останні – на групи (органолептична, технічна, наукова ...).

Необхідно відзначити, що оперативно-розшукова інформація за своєю суттю є одним із різновидів соціальної інформації. Зміст оперативно-розшукової інформації становлять вміщені в ній дані з приводу злочину і причетних до нього осіб. Суб'єкт використання (застосування) – органи внутрішніх справ, які ведуть боротьбу зі злочинністю. Спосіб отримання – переважно розвідувальний (конспіративний) проводиться за допомогою спеціальних сил, засобів і методів оперативно-розшукової діяльності. Мета, використання – вжиття заходів оперативно-розшукового і правового характеру щодо протиправної діяльності осіб. Цінність – у тому, що вона надає можливість пізнавати факти неочевидних (латентних) злочинів, одержувати відомості про конкретних причетних до них осіб. Вчасне, одержання оперативно-розшукової інформації сприяє правильному вибору необхідних слідчих дій та визначенню раціональних тактичних прийомів їх проведення з метою одержання доказової інформації.

Специфічність методів і тактичних прийомів оперативно-розшукової діяльності, які мають, як правило, потаємний характер, полегшує, з одного боку, встановлення ознак протиправної діяльності, а з другого – ускладнює використання інформації для потреб кримінального процесу [1, с.59].

Проблема співвідношення оперативно-розшукової інформації і судових доказів у кримінально-процесуальній і криміналістичній літературі постає найбільш дискусійною: від повного відкидання доказового значення оперативно-розшукової інформації взагалі (А.Я. Дубінський, А.М. Михайлов, М.С. Строговіч, М.С. Сусло та ін.) – до сприйняття її складової частини процесу доказування і навіть як доказу (А.І. Вінберг, Г.І. Кочаров, Г.М. Міньковський, В.Г. Самойлов, Д.І. Бедняков та інші). Все залежить від способів її одержання і фіксації.

Умовно інформацію, одержану в процесі оперативно-розшукової діяльності, поділяють на три групи .

Першу групу становлять відомості, що вказують на можливі джерела одержання доказів (дані про очевидців злочину, постраждалих осіб, яким відомо про протиправну подію, об'єкти та засоби злочинних дій).

Друга група – це відомості, що зафіксовані у об'єктах-носіях (документи, фотознімки, відео-та фонограми, об'єкти зі слідами злочинних дій, тощо).

Третю групу становлять відомості, що вказують на можливі напрямки і шляхи оперативно-розшукового та кримі–нально-процесуального пошуку судових доказів або конкретних джерел доказів (дані розвідувального опитування, особистого пошуку, повідомлення представників громадськості) [2, с.790-791].

Схожість усіх трьох груп оперативно-розшукової інфор–мації полягає в тому, що вони вміщують відомості про факти і джерела можливих судових доказів, різниця – у способі закріплення цих відомостей.

Заслуговує на увагу нерівнозначність для слідства цих видів оперативно-розшукової інформації.

Інформація, зафіксована в розумовій (образній) формі людини, має важливе, але допоміжне (орієнтовне) значення щодо доказування і не може безпосередньо трансформуватися в докази. Вона сприяє формуванню доказової інформації, визна–чає спрямованість повного, об'єктивного і всебічного одержання фактичних даних у результаті проведення оперативно-слідчих дій.

Стаття 99 КПК України зазначає, що матеріали, в яких зафіксовано фактичні дані про протиправні діяння окремих осіб та груп осіб, зібрані оперативними підрозділами з дотриманням вимог Закону України «Про оперативно-розшукову діяльність», за умови відповідності вимогам цієї статті, є документами та можуть використовуватися в кримінальному провадженні як докази [3, с.42].

О.М. Бандурка зазначає, що використання оперативної інформації здійснюється з метою отримання фактичних даних, які можуть бути доказами у кримінальному провадженні справ [4, с.290].

Із наведеного необхідно підкреслити, що оперативно-розшукова інформація, об'єктивно зафіксована за допомогою

технічних засобів у предметній (речовій) формі, цілком може за певних умов перетворюватись на доказову інформацію, оскільки з моменту фіксації об'єкт (носій інформації) стає документом – джерелом похідних доказів. Вона може використовуватись у процесі доказування при прогнозуванні і проведенні різних прийомів криміналістичної тактики. Завданням слідчого є процесуальне закріплення і використання одержаних матеріалів. На цій стадії виникає проблема так званої легалізації оперативно-розшукової інформації, одержаної за допомогою технічних засобів, тобто введення її у процес доказування.

У теорії і практиці оперативно-розшукової діяльності органів внутрішніх справ один із прийомів виявлення, закріплення і збереження інформаційних даних, які можуть сприяти успішному запобіганню і викриттю злочинів, умовно йменується документуванням протиправних дій розроблюваних осіб. Документування проводиться за справами оперативного обліку з приводу конкретних фактів і стосовно осіб, які обґрунтовано підозрюються у підготовці або здійсненні злочину. Мета документування – виявлення оперативно-розшуковим шляхом фактичних даних, які дозволяють застосовувати до розроблюваних осіб заходи, передбачені законом, а також забезпечення можливості використання цих даних у процесі розслідування.

При безпосередньому використанні таких даних у процесі розслідування до розроблюваних осіб можуть застосовуватись передбачені законом процесуальні заходи примусового характеру (наприклад, порушення справи кримінального провадження, затримання, обшук, огляд, допит та інші) або заходи, в тій чи іншій мірі причетні до особистих прав і інтересів (попередження, вибір міри обмеження тощо). Виходячи з цього, необхідно, щоб дані, одержані з оперативних джерел, були достовірними, дійсними.

Визначаючи можливість використання з метою доказування даних, отриманих оперативно-розшуковим шляхом за допомогою технічних засобів, слід диференційовано підходити до оцінки оперативно-розшукової інформації: за ціллю, джерелами, часом одержання, формою закріплення, тактичною значущістю та інші. Крім того, при виборі варіанту реалізації необхідно враховувати обсяг зібраних даних, ступінь суспільної небезпеки

протиправної дії, достатність даних для викриття підозрюваних осіб у вчиненні злочину. В усіх випадках дані, які одержані за допомогою технічних засобів у процесі оперативної розробки, підлягають обов'язковому контролю на можливість процесуальної перевірки і використання їх при розслідуванні.

1. Овчинский С.С. Оперативно-розыскная информация и процесс доказывания // Оперативно-розыскная информация. / Под ред. А.С. Овчинского и В.С. Овчинского. – М.: ИНФРА-М, 2000. – 367 с.
2. Белкин Р.С. Обнаружения признаков преступления // Курс криминалистики: Учеб. пособие для вузов. – 3-е изд. Допол. – М.: ЮНИТИ ДАНА, Закон и право, 2001. – 837 с.
3. Кримінально-процесуальний кодекс України (текст); – К.: «Центр Учбової літератури», 2012. – 254 с.
4. Бандурка О.М. Оперативно-розшукова діяльності. Частина 1: підручник – Харків: Вид-во ХНУВС, 2002. – 336 с.

ІНФОРМАЦІЙНО-АНАЛІТИЧНА РОБОТА ОПЕРАТИВНИХ ПІДРОЗДІЛІВ ОВС

Сорочинська О.Я.,
оперуповноважений ГКМСД Буського РВ ГУ МВСУ у Львівській області

Інформаційно-аналітична робота є складовою частиною оперативно-розшукової діяльності органів внутрішніх справ. Злочинці, які мають потужні фінансові можливості, систему корупційних зв'язків і контакти із групами, що спроможні до дій терористичного характеру, легалізуючи свою діяльність у сфері економіки тощо, об'єктивно можуть цілеспрямовано впливати на державні органи управління. У них широкі можливості для збирання інформації, злочинці іноді навіть формують систему розвідки та контрозвідки, оперують значними коштами, мають високопоставлених корумпованих осіб, які озброєні найновітнішими технічними засобами і вчиняють активну протидію діяльності правоохоронних органів. Для вжиття ефективних заходів боротьби зі злочинністю правоохоронні органи повинні мати можливість здійснювати систематичне збирання та аналіз інформації з усіх

відповідних джерел, щоб використовувати оперативні дані як у стратегічних, так і тактичних цілях. Отримання оперативних даних передбачає оброблення й аналізу проведення великого обсягу інформації про осіб, які підозрюються у причетності до вчинення злочину. Методи, що застосовуються для отримання і використання такої інформації, мають допускатися і регламентуватися законодавством.

Окремі питання інформаційно-аналітичного забезпечення діяльності оперативних підрозділів ОВС розглядали у своїх працях О.М. Бандурка, В.І. Василинчук, І.П. Козаченко, В.К. Колпаков, Є.Д. Лук'янчиков, Д.Й. Никифорчук, Ю.Ю. Орлов, В.Л. Ортинський, О.Є. Користін, Л.П. Скалозуб, які є представниками різних галузей науки.

Таким чином, існує потреба глибшого аналізу поняття інформаційного забезпечення діяльності оперативних підрозділів ОВС, розкриття його змісту, завдань і місця в теорії та практиці оперативно-розшукової діяльності.

Інформаційне забезпечення являє собою систему пошуку й отримання відомостей, які становлять оперативний інтерес, їх нагромадження, опрацювання, аналіз і використання оперативним підрозділом ОВС для ефективного виконання своїх функцій, у тому числі й за оперативним обслуговуванням об'єктів.

Головним завданням інформаційного забезпечення оперативного обслуговування об'єктів є систематичне і своєчасне надходження в оперативний підрозділ об'єктивної інформації. Систематичність, своєчасність й об'єктивність особливо важливі через те, що оперативні працівники часто володіють інформацією, яка отримана опосередковано, через других осіб. Переломлюючись в їх свідомості, така інформація деформується і потребує певної корекції, тому головними завданнями, що нині виникають перед інформаційно-аналітичним забезпечення, є:

- забезпечити надання на всіх рівнях управлінської інформації про реальне становище оперативної обстановки, можливих напрямів її розвитку і на цій основі підготовка конкретних пропозицій із попередження й оперативного реагування на зміну кримінальної ситуації;
- аналіз об'єктивного оцінення результатів оперативно-службової діяльності оперативних підрозділів ОВС, вико-

ристання аналітичних матеріалів для організації оперативно-службової діяльності підрозділів служби, прогнозування розвитку злочинності й на цій основі розроблення всебічно обґрунтованих управлінських рішень і планування попереджувальних заходів щодо усунення викритих хиб;

- удосконалення системи контролю за виконанням нормативно- правових актів з питань боротьби зі злочинністю та власних рішень підпорядкованими підрозділами;
- підвищення ефективності використання комп'ютерної техніки для своєчасного збирання, нагромадження й оброблення необхідної інформації та поліпшення якості аналітичних документів;
- забезпечення своєчасного надання достовірної інформації до автоматизованого банку даних оперативно-розшукового призначення та ефективного використання в боротьбі зі злочинністю; створення міжвідомчих автоматизованих банків даних в інтересах оперативних підрозділів [1, с. 284-295];
- оперативно-розшукова інформація є важливим складовим елементом інформаційного забезпечення діяльності оперативних підрозділів ОВС. Оперативно-розшукова інформація має низку властивих тільки їй особливостей. Одне з найбільш містких визначень дав Д.В. Гребельський, зазначивши, що оперативно-розшукова інформація являє собою сукупність первинних і перевірених даних про осіб, які причетні до підготовки злочинів, стану оперативно-розшукових сил і засобів, а також умов, у яких здійснюється діяльність органів міліції щодо боротьби зі злочинністю [2, с.34].

Це визначення доповнювали й уточнювали В.І. Лебеденко [3, с. 166], В.О. Лукашов [4, с. 15] та інші вчені. Тому процес збирання інформації оперативними підрозділами ОВС під час оперативного пошуку залежить від особливостей оперативної обстановки, що складається на об'єктах обслуговування внаслідок підготовки та вчинення злочинів. Значну кількість інформаційних потоків, значно частина яких так чи інакше пов'язана з дотриманням режиму законності, формуванням ставлення до нього, забезпеченням його пріоритетів у різних сферах суспіль-

ного життя. Вони складаються з маси відомостей, що мають важливе значення для діяльності оперативних підрозділів ОВС та для ефективного виконання покладених на ці підрозділи завдань. Проте ці відомості перебувають у різних інформаційних системах у хаотичному стані. Для того щоб вони перетворились на інформацію, котра здатна забезпечити потреби оперативних підрозділів ОВС, їх потрібно певним чином систематизувати, впорядкувати, тобто створити з них інформаційний потік, що спеціально призначений для конкретної служби ОВС.

Для цього оперативні працівники ОВС проводять тактичні заходи, суть яких полягає: у здобутті потрібної інформації; її вилученні з інших систем; її надісланні по каналам зв'язку в оперативні підрозділи ОВС.

Джерелами інформації для оперативних підрозділів ОВС являються предмети, документи та люди [5. с.29].

До предметів належать будь-які речові об'єкти, які виникли у зв'язку з подією злочину, або були використані під час його підготовки, вчинення, приховування слідів, або на яких залишились сліди вчинення злочину, тобто предмети, що перебувають у причинно-наслідковому зв'язку з подією злочину. Це може бути сировина, напівфабрикати, готова продукція, викрадені матеріальні цінності, гроші, предмети хабара, штампи, печатки форми, барвники тощо. Інакше кажучи, все, що сприяє відхиленню від передбаченого законом режиму функціонування об'єкта оперативного обслуговування.

Документи – друга група джерел інформації. Це будь-які документи, що містять опис події, яка може стати предметом кримінальної справи (справжні й фіктивні бухгалтерські обліки, чорнові обліки злочинця тощо). Інформація про наявність і місце зберігання зазначених предметів і документів найчастіше надходить негласних співробітників. Вони з найбільшою мірою достовірно відображають процеси й явища, що цікавлять оперативні підрозділи ОВС.

Виходячи з наведеного необхідно зазначити, що система інформаційно-аналітичного забезпечення виявлення та припинення злочинів має об'єктивно виражену предметну сферу, структуру й методичну базу, використовує вживані в криміналістиці (криміналістичній реєстрації) та оперативно-розшу-

ковій діяльності методологічні засади й принципи. Її теоретична будова охоплює широку сферу, пов'язану з теоріями криміналістики, криміналістичної реєстрації, оперативно-розшукової діяльності, судової експертизи та інформатики.

1. Бандурка О.М. Оперативно-розшукова діяльність. Частина 1: підручник – Харків: Вид-во ХНУВС, 2002. – 336 с.
2. Гребельский Д.В. О соотношении криминалистических и оперативно-розыскньїх характеристик / Д.В. Гребельский / Криминалистическая характеристика преступлений : сб. науч. тр. – М. : Акад. МВД СССР, 1984 – С. 17-23.
3. Лебеденко В.І. Застосування інформаційно-аналітичного методу в оперативно-розшукові діяльності оперативних підрозділів правоохоронних органів. Теорія оперативно-розшукової діяльності правоохоронних органів України. – Наукове видання // За гол. ред. проф. В.Л. Регульського. – Львів, ЛІВС НАВСУ, 2000. – С.165-170.
4. Лукашов В.А. Организация и методика аналитической работы в сфере оперативно-розыскной деятельности органов внутренних дел / Лукашов В.А. – Омск : Ом. высш. шк. МВД СССР, 1983. – 32 с.
5. Овчинский А.С. Оперативно-розыскная информация. / Под ред. А.С. Овчинского и В.С. Овчинского. – М. : ИНФРА-М, 2000. – 367 с.

АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЇ У VPN-МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Рудий А.Т.,
військовослужбовець

Останнім часом зафіксовані непоодинокі випадки масованих атак на ІС зі сторони Internet, причому найчастіше об’єктом атак був Web-сервер.Час з'єднання робочої станції корпоративної мережі з Internet – це час, коли безпека трансмісії даних найбільше піддається ризикові [1].

Розглянемо потенційні атаки на прикладному рівні, які поділимо на дві категорії:

- атаки, які експлуатують особливості прикладного протоколу;
- атаки, які використовують помилки в прикладних програмах.

Атаки, які використовують особливості прикладного протоколу. Протокол HTTP (HyperText Transfer Protocol) – прикладний клієнт-серверний протокол типу запит/відповідь, який працює поверх TCP. У ролі HTTP-клієнта виступають Web-броузер або Proxy-сервер, які посилають запит від імені свого клієнта.

Особливо зауважимо, що HTTP є протоколом без збереження стану. Це означає, що кожна пара запит/відповідь є абсолютно самостійною і ніяк не пов'язана ні з попередніми, ні з наступними запитами від цього або іншого клієнтів, навіть якщо серія запитів/відповідей виконується в рамках одного TCP-з'єднання.

Автентифікування в HTTP. HTTP-клієнт для обслуговування свого запиту не повинен подавати ніякого «посвідчення особи» користувача при звертанні на Web-сервери, які містять відкриту інформацію. Зауважимо, що автентифікування жодною мірою не забезпечує захист від прослуховування переданих даних. Для цього треба використовувати протокол SSL.

Proxy-автентифікування. Протокол HTTP підтримує автентифікування користувача на Proxy-сервері. Автентифікування може відбуватися тоді, коли адміністратор Proxy-сервера бажає обслуговувати запити тільки визначених користувачів або вести облік роботи кожного користувача індивідуально.

Proxy-автентифікування виконується аналогічно до автентифікування на кінцевому Web-сервері, але за допомогою заголовка Proxy-Authorization. Якщо потрібне Proxy-автентифікування, але необхідні дані клієнтом не надані, тоді повертається відгук з кодом 407 «Proxy Authentication Required» і заголовком Proxy-Authenticate:, аналогічним за змістом заголовкові WWW-Authenticate:.

Наголосимо, що автентифікування на Web-сервері і Proxy-автентифікування HTTP-запиту – дві не пов'язані між собою процедури, виконувані різними серверами.

Атаки, які використовують помилки в прикладних програмах. Розповсюдженими прикладами додатків прикладного (application) рівня TCP/IP є програми Telnet, FTP, Web-сервери і клієнти (Internet-броузери), програми роботи з E-mail.

На прикладному рівні знаходяться також програми, з якими користувач не взаємодіє безпосередньо.

Результатом атак, які використовують помилки в прикладних програмах, часто є відмова в обслуговуванні (DoS-атаки) або, що гірше, проникнення зловмисника в ОС, часто – із правами повноваженого користувача. Переважна більшість атак на прикладні програми використовують переповнення буферів – надзвичайно розповсюджену помилку. Для виконання атаки зловмисник формує вхідні дані для додатку в обсязі, який перевищує розмір буфера пам'яті виділеного програмою для цих даних.

Багато додатків Internet, особливо серверні, виконуються з повноваженнями адміністратора. Таким чином, використовуючи переповнення буфера, зловмисник віддалено, без введення пароля, може виконувати на робочій станції, на яку спрямована атака, довільний програмний код від імені адміністратора.

Атака через WWW. Відзначимо проблеми з безпекою використовуваних ІТ, таких як під'єднувані модулі (plug-ins), елементи Active, додаток Java, засобу підготування сценаріїв JavaScript, VBScript, PerlScript, Dynamic HTML.

Завдяки підтримці цих ІТ не тільки броузерами, але й поштовими сервісами та наявності помилок у них з'явилася велика кількість поштових вірусів, а також вірусів, які інфікують HTML-файли.

Адміністратор безпеки Web-сервера повинен пильно стежити за командами розробників програмного продукту, які стосуються безпеки, вчасно установлювати обновлення і нові версії.

Безпека серверного програмного забезпечення визначається відсутністю наступних типів помилок:

1. Помилки в серверах:

- помилки, які призводять до втрати конфіденційності;
- помилки, які призводять до атак типу DoS;
- помилки, які призводять до виконання на сервері неавторизованого коду.

2. Помилки у допоміжних програмах.

3. Помилки адміністрування.

Зловмисник, який працює із сервісом WWW, може переслідувати наступні цілі:

- перехоплення переданих даних;

- атака на комп'ютер користувача за допомогою коду, написаного на Javascript, Java або завантаженого за технологією Active;
- інсталювання модифікованої копії Web-сервера з метою ввести користувача в оману і примусити його до розкриття конфіденційної інформації;
- атака на HTTP-сервер через CGI-програми та інші засоби динамічного генерування контента з метою проникнення в його ОС або відмови в обслуговуванні;
- перехоплення паролів і одержання несанкціонованого доступу (НСД) до ресурсів Web-сервера або до послуг Proxy-сервера.

Відзначимо, якщо перехоплені паролі використовуються не тільки в запитах WWW, але і для доступу до інших сервісів, у тому числі і для термінального доступу до ОС, тоді загроза від перехоплення пароля істотно зростає [2].

З огляду на те, що WWW є найпопулярнішим сервісом Internet і поглинає велику частку ресурсів Internet-каналу, для адміністратора безпеки ІС також важливі задачі керування доступом користувачів до WWW. Пропонуємо класифікацію на основі атак на вразливі місця WWW, а не на основі способу реалізування атак.

Атаки на броузери та сервери. Web-сервер – це програмне забезпечення, що здійснює взаємодію за HTTP протоколом з броузерами: прийом запитів, пошук відзначених файлів і передавання їх вмісту, запуск CGI-додатків і передавання клієнтові результатів їхнього виконання.

Безпека Web-сервера є лише невеликим компонентом загальної системи безпеки хосту Internet. Під словами «злам сервера» найчастіше мається на увазі модифікування сторінок Web-сервера – найвидовищніший прояв атаки на сервер, хоча насправді може виявитися лише побічним продуктом захоплення керування усім хостом [3].

У той же час існують проблеми безпеки, притаманні саме для Web-серверів. Скориставшись ними, зловмисник може одержати стартовий майданчик для подальшого проникнення в систему (тому, як і раніше, залишається в силі рекомендація винести Web-сервер, як і всі інші сервіси, які вимагають

зовнішнього доступу, на окремий комп'ютер, бажано ізольований від внутрішньої мережі) [4].

Помилки в серверах. Відзначимо основні класи помилок у серверах:

1. *Помилки, які призводять до втрати конфіденційності* (дають можливість одержати неавторизований доступ до інформації, обійти систему автентифікування, переглянути початковий код додатків тощо).

2. *Помилки, які призводять до атак типу DoS* (носять винятково деструктивний характер, переводять сервер у стан, коли він неспроможний виконувати свої штатні функції, будучи зайнятим обробленням помилкових запитів).

3. *Помилки, які призводять до виконання на сервері неавторизованого коду* (дозволяють запускати на виконання програми, які уже існують на сервері, але не призначені для загального доступу, а також передавати на сервер свій код, який виконується).

Подамо деякі приклади розповсюджених атак на сервери за допомогою спеціальних символів.

Спеціальні символи. «*» запити. Зірочка часто використовується зловмисниками як параметр до системної команди. Приклад:

http://host/index.asp?something=..\..\..\..\WINNT\system32\cmd.exe?/c+DIR+e:\WINNT.txt

Цей запит вимагає щоб були перераховані всі текстові файли в межах каталогу e:\WINNT. Запити подібні до цього можуть використовуватися, щоб зібрати список журналів. Не усі додатки мережі використовують цей символ у допустимому запиті, і тому це змушує зірочку відзначитися у файлах реєстрації.

* http://host/blah.pl?somethingelse=ls%20*.ua

Цей запит вимагає переліку усіх сценаріїв Perl з префіксом .ua у UNIX.

″~″ запити. Символ ″~″ іноді використовується зловмисниками, щоб визначити, хто істинний (допустимий) користувач. Приклад: * http://host/~joe

Цей запит шукає користувача на ім'я «joe» у віддаленій системі. Якщо зловмисник одержить помилку з кодом 403 («Сервер зрозумів запит, але навмисно відмовився його

виконувати») тоді користувач існує. Коли зловмисник має допустиме ім'я користувача, тоді він може пробувати підбирати паролі або здійснювати грубий примус поки він не одержить допустимий пароль.

« ' « запити. Використовувати цей символ можна при SQL атаках. Часто програмні коди можуть бути написані неякісно і це дозволяє зловмисникам вставляти команди SQL у сценарій. Якщо можливо виконати команди, тоді це може призвести до одержання зловмисником адміністративного доступу до системи. Приклад:

* http://host/cgi–bin/lame.asp?name=john;EXEC master.dbo. xp_cmdshell'cmd.exe dir c:'–

На цей запит виконується cmd.exe оболонка на станції Windows NT. Звідси зловмисник має повне панування на віддаленій станції з можливістю додавати користувачів, завантажити trojans і захопити файл паролів.

Безпека CGI-додатків. CGI (Common Gateway Interface, загальний шлюзовий інтерфейс) є компонентом Web-сервера, який забезпечує взаємодію з іншими програмами, виконуваними на цьому сервері.

Нехтуючи тим фактом, що сервери в мережі завжди уразливі, CGI-скрипти погіршують ситуацію, даючи зловмисникам можливість користуватися особливостями CGI. CGI-сценарії – це програми, що знаходяться і виконуються на сервері, які можуть запускатися за запитом від броузера. Подібно тому, як на сервері електронної пошти прихід повідомлення викликає запуск програми агента доставки, запит клієнта до HTTP-сервера може викликати запуск CGI-програми або іншого коду для генерування контенту (для стислості довільний такий код будемо називати CGI-програмою). На вхід цієї програми подаються дані, прислані клієнтом, тобто фактично довільний користувач Internet може якоюсь мірою керувати роботою програми в ОС HTTP-сервера. Отже, CGI-програми можуть бути джерелом поважних проблем, пов'язаних з безпекою.

Відповідальність розробника CGI-додатку нітрохи не менша від відповідальності розробника Web-сервера. Помилка і того, і іншого може призвести до однаково сумних наслідків. Однак мало хто займається написанням Web-серверів для

розваги – це заняття професіоналів, у той час як кількість бажаючих розважитися CGI-програмуванням постійно росте, і з результатами їхньої творчості ми зіштовхуємося усе частіше.

Забезпечення безпеки інформаційної взаємодії приватних мереж спеціального призначення і окремих робочих станцій через відкриті мережі, зокрема через Internet, можливо при ефективному розв'язанні задач ЗІ у процесі її трансмісії відкритими каналами зв'язку, захисту при під'єднанні до відкритих каналів зв'язку локальних мереж і робочих станцій від несанкціонованих дій з боку зовнішнього середовища.

1. Рудий Т.В. Принципи організації системи захисту інформаційних систем підрозділів МВС / Т.В. Рудий, О.В. Захарова, О.І. Зачек., А.Т. Рудий. Науковий вісник ЛьвДУВС. Серія юридична // головний редактор М.М. Цимбалюк. – Львів: ЛьвДУВС. 2012. – Вип. 2 (2). – С. 309-316.
2. Кулешник Я.Ф. Модель системи інформаційної безпеки у Windows / Я.Ф. Кулешник, Т.В. Рудий, А.Т. Рудий / Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами // Матеріали науково-практичного семінару (4 грудня 2009 р.). – Львів: Львівський державний університет внутрішніх справ, 2009. – С.89-93.
3. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації Web-сторінки від несанкціонованого доступу. к.: Держстандарт України. – 2003. – 16 с.
4. Шохін Б.П., Юдін О.М., Мазулевський О.Є. Вдосконалення контролю за станом захищеності ком'ютерної мережі на основі адаптивного моніторингу // Збірник наукових праць військового інституту телекомунікацій та інформатизації національного технічного університету України «КПІ». – 2004. – Вип. 4, – С.208-217.

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ОБІГУ НА РИНКУ УКРАЇНИ НЕБЕЗПЕЧНОЇ ПРОДОВОЛЬЧОЇ ПРОДУКЦІЇ

Оліщук Б.Т.,
здобувач кафедри оперативно-розшукової діяльності та спеціальної техніки ЛьвДУВС

В умовах високого динамізму політичних, соціальних і економічних процесів, ускладнення управління соці-

альними системами, ефективність організації оперативно-розшукового виявлення на ринку України небезпечної продовольчої продукції, значною мірою визначається глибиною і всебічністю аналізу отриманої оперативної інформації в процесі оперативного обслуговування та виробленням на її основі відповідних управлінських рішень. У зв'язку з цим результативність діяльності оперативних підрозділів залежить не тільки від особистих ділових якостей і оперативно-технічної оснащуності співробітників, але і від ефективності налагодженої системи інформаційно-аналітичного забезпечення.

Оптимальна організація боротьби з обігом на ринку України небезпечної продовольчої продукції неможлива без її всебічного, якісного інформаційного забезпечення. Інформаційне забезпечення є одним із основних елементів організації різних напрямків діяльності оперативних підрозділів внутрішніх справ [1].

Значення інформації в управлінні оперативних підрозділами у виявленні та припиненні обігу на ринку України небезпечної продовольчої продукції, обумовлене її ключовою роллю в системах соціального управління, де інформація є головною умовою і засобом реалізації організаційно-управлінських функцій. З іншого боку, зважаючи на специфіку вирішуваних цими підрозділами завдань, основний зміст їхньої діяльності полягає в добуванні, систематизації і аналізі інформації, необхідної для протидії обігу на ринку України небезпечної продовольчої продукції.

В результаті дослідження встановлено, що сфера пошуку і отримання оперативної інформації про обігом на ринку України небезпечної продовольчої продукції необхідно використовувати інформаційні ресурси:

- органів державної реєстрації суб'єктів підприємницької діяльності щодо інформації про фізичних та юридичних осіб, які брали участь у державній реєстрації як засновники суб'єктів господарювання;
- органів державної митної служби країни щодо змісту здійснених операцій;
- органів державної митної служби інших держав щодо змісту здійснених операцій експорту та імпорту конкретним суб'єктом господарювання (як резидентом України, так і нерезидентом);

- органів державної податкової служби України (автоматизовані інформаційно-пошукові системи та автоматизовані робочі місця, банки даних інформації);
- банківських установ щодо відкритих (закритих) розрахункових рахунків та осіб, які мають право розпоряджатися грошовими коштами суб'єкта господарювання. Інформація щодо отриманих та погашених кредитів, дані щодо використання віддаленого доступу до управління грошовими коштами на розрахунковому ра хунку тощо;
- контролюючих органів (санітарно-епідеміологічнії служба, державний нагляд за додержанням правил виготовлення і експлуатації ємностей, що знаходяться під тиском, газова служба) ;
- дані щодо виробництва продукції (товарів) та дотримання умов технологічного процесу їх виготовлення;
- дані обміну оперативною інформацією між оперативними підрозділами органів внутрішніх справ, податкової міліції, Служби безпеки України;
- органів досудового слідства щодо розслідування злочинів, пов'язаних з обігом на ринку України небезпечної продовольчої продукції;
- інформація оперативно-розшукових матеріалів, які знаходяться в провадженні оперативних проділів (податкової міліції, органів внутрішніх справ, Служби безпеки України);
- дані експертних досліджень щодо відповідностей якості товарі (продукції) встановленим вимогам, дотримання технологічного процесу виготовлення продукції, які проведені на запити правоохоронних, контролюючих органів чи окремих громадян;
- дані інформаційних ресурсів органів внутрішніх справ щодо інформації про притягнення конкретних осіб до кримінальної відповідальності, наявності (погашення) судимості;
- відомості щодо отримання дозволів дозвільної системи органів внутрішніх справ на виготовлення печаток;
- інформацію приймальних відділень лікувальних закладів при масові отруєння осіб;

- матеріали прокурорських перевірок щодо фактів масового отруєння громадян, осіб, які харчувалися в закладах громадської харчування, масового отруєння в їдальнях шкіл, таборів відпочинку, інтернатах тощо;
- інформацію лікувальних закладів щодо летальних випадків за результатами споживання недоброякісної, сфальсифікованої продукції;
- інформацію про результати перевірок реалізації товарів, здійснених спеціально створеними комісіями органів виконавчої влади;
- інформацію територіальних підрозділів у справах захисту прав споживачів, Державного комітету України з питань технічного регулювання та споживчої політики (Держспоживстандарт України);
- інформацію правоохоронних та контролюючих органів інших країн щодо діяльності суб'єктів господарювання на їх митній території;
- дані Державної прикордонної служби України щодо перетинання кордону конкретною особою, в т.ч. з використанням транспортних засобів;
- інформаційні ресурси підрозділів Служби безпеки України щодо фактів контрабандного перевезення сировини, обладнання, товарів тощо;
- інформаційні ресурси Державної митної служби України щодо ввезення на митну територію України сировини, обладнання, сировини для виготовлення пакувальних матеріалів, тари тощо;
- інформаційні ресурси мережі Internet щодо пропозицій з реалізації товарів, продукції [2].

Особливе значення інформаційне забезпечення має під час виявлення та розслідування кримінальних справ за злочинами, що здійснюються у сфері обігу на ринку України небезпечної продовольчої продукції в умовах дефіциту відомостей, коли відчувається нестача даних необхідних, як для організації розслідування так і для виявлення слідів злочину, з'ясування механізму злочинної діяльності, встановлення винних у вчинені злочину та ін. [3].

1. Апухтін С.І.. Інформаційно-аналітичне забезпечення аналізу оперативної обстановки. Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. Спеціальний випуск – 2011. № 2. – Ч. 2. – С.52-60.
2. Усманов Р.А. Информационнне основи предварительного расследования [учебн. пособ.] / Р.А. Усманов. – М.:Юрлитинформ, 2006. – 208 с.
3. Цимбал М.І. Інформаційне забезпечення розслідування злочинів: сучасний стан та шляхи удосконалення Вісник Луганського ДУВС ім. Е.О. Дідоренка. Лугарськ.ЛДУВС, 2010. – №1. – С.280-285.

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ У ПРОТИДІЇ РЕЙДЕРСТВУ

Русин А.С.,
здобувач кафедри оперативно-розшукової діяльності та спеціальної техніки ЛьвДУВС

Наукова організація управління у сфері боротьби зі злочинністю органічно пов'язана з інформацією, проходженням інформаційних процесів.

Інформаційне забезпечення оперативно-розшукової діяльності з точки зору теорії інформації є не що інше, як циклічний процес пошуку, збору, опрацювання, переосмислення, зберігання, видачі інформації та її використання для прийняття оперативно-тактичних та інших рішень правоохоронних органів.

Проводячи розвідувально-пошукові заходи, оперативні працівники ДСБЕЗ повинні враховувати інформаційні чинники, які забезпечують ефективну пошукову роботу у виявленні злочинів, пов'язаних протидією законній господарській діяльності.

Особливості оперативного пошуку в будь-якій сфері економічних відносин зумовлюються відповідною специфікою методики отримання первинної інформації. Частково методи, які при цьому застосовуються, збігаються із загальновизнаними методами ОРД – особистим пошуком, негласним методом тощо, але певною мірою вони добираються залежно від своєрідності як безпосереднього процесу поглинання підприємств агресора-

ми, так і наявним у державі адміністративно-правовим механізмом протидії зазначеному суспільно небезпечному явищу.

Однією з умов підвищення рівня організації ОРД підрозділами ДСБЕЗ у виявленні зазначених злочинів є сучасне і повне інформаційне забезпечення їх діяльності з використанням відомостей як негласного, так і негласного характеру, з метою виявлення всіх обставин вчинення злочинів у цій сфері особливо щодо здійснення рейдерства.

Поширення рейдерства, тобто нелегітимного, незаконного заволодіння чужим майном і використання його у власних цілях [1], у сучасних умовах господарювання є найбільшою небезпекою для розвитку корпоративного сектору економіки України.

Недостатня ефективність протидії злочинам в цій сфері значною мірою пояснюється відсутністю її належного інформаційно-аналітичного забезпечення. На сьогодні навіть не ведеться спеціальна статистика рейдерських захватів підприємств, уповноважені органи влади намагаються здійснювати облік корпоративних конфліктів, але застосовувані ними методики лише викривляють реальний стан справ на ринку корпоративного контролю. За цих обставин досить складно проводити моніторинг відповідних господарських процесів і експертизу засобів їх урегулювання, контролювати виконання прийнятих управлінських рішень та прогнозувати їх наслідки. Це актуалізує проблему створення надійної системи інформаційно-аналітичного супроводу державної політики протидії корпоративному рейдерству [2].

Оперативні підрозділи ДСБЕЗ, з метою отримання інформації про підготовку до рейдерський захоплень, необхідно використовувати бази даних державних органів. Так, у сфері державного регулювання відносин перерозподілу корпоративного контролю в Україні виконання цього завдання покладається насамперед на Державну комісію з цінних паперів та фондового ринку (ДКЦПФР). Цей орган виконавчої влади нині здійснює реєстрацію випуску цінних паперів та відомостей про їх випуск, проводить збирання і узагальнення даних про власників великих пакетів (10% і більше) акцій, а також регулярної і особливої інформації про емітентів, реєстраторів і зберігачів цінних паперів тощо [3]. Завдання, пов'язані із збиранням та

обробленням інформації, яка стосується суттєвих характеристик ринку корпоративного контролю в Україні, також виконують:

- фонд державного майна – при веденні реєстру корпоративних прав держави, здійсненні моніторингу ефективності управління ними, аналізу діяльності холдингових компаній, створених за участю держави;
- антимонопольний комітет – у процесі здійснення контролю за економічною концентрацією, запровадження заходів із запобігання та припинення зловживань монопольним становищем, антиконкурентних узгоджених дій;
- державний комітет фінансового моніторингу – при опрацюванні даних про операції, що підлягають обов'язковому фінансовому моніторингу, узагальненні одержаної від правоохоронних та інших державних органів інформації, яка стосується легалізації (відмивання) доходів, одержаних злочинним шляхом;
- національний банк – під час акумулювання інформації про власників істотної участі у банках, проведення моніторингу діяльності банків тощо.

Міністерство промислової політики, Міністерство аграрної політики, Міністерство палива та енергетики, інші міністерства і відомства отримують і обробляють відомості про стан і розвиток ринку корпоративного контролю у відповідних галузях і сферах національної економіки. Крім того, усі господдарські товариства незалежно від їх органі заційно-правової форми зобов'язані надавати інформацію на запити підрозділів Міністерства внутрішніх справ, Служби безпеки, прокуратури. Варто також додати, що всі підприємства періодично подають звіти до:

- органів податкової служби – про доходи і валові витрати господарської діяльності, сплату різноманітних податків, зборів, платежів тощо;органів державної статистики – про заборгованість із заробітної плати, екологічні платежі, виплати за природні ресурси та поточні платежі на охорону природи, зовнішню трудову міграцію тощо;
- державної служби зайнятості – про кількість працівників у товаристві, наявність робочих місць, звільнених та прийнятих на роботу працівників тощо;

- пенсійного фонду – про сплату страхових внесків до пенсійного фонду.

Зауважимо, що всі названі органи не тільки збирають і обробляють зазначену звітність та іншу спеціальну інформацію, а й регулярно проводять перевірки її відповідності безносередньо на підприємствах, що становить базу даних для підрозділів ДСБЕЗ щодо боротьби з рейдерством.

1. Економічна та майнова безпека підприємства і підприємництва. Антирейдерство / Б. М. Андрушків, Ю. Я. Вовк, П. Д. Дудкін та ін.; кер. авт. йол. Б. М. Андрушків. – Тернопіль : Вид-во «Терно-граф», 2008. – 424 с.
2. Сафронова О. Інформаційно-аналітичне забезпечення державної політики протидії рейдерству в корпоративному секторі економіки України. Збірник наукових праць НАДУ при Президентові України / О. Сафронова. 2010,. – № 1. – С. 95-103.
3. Практичні аспекти інформаційно-аналітичної роботи : навч. посіб. / С. О. Телешун. О. Р. Титаренко, 1. В. Рейтерович, С. І. Вировий. – К. : Вид-во НАДУ, 2007. – 44 с.

ОКРЕМІ АСПЕКТИ ОТРИМАННЯ ІНФОРМАЦІЇ ЩОДО ЗЛОЧИНІВ, ЯКІ ВЧИНЯЮТЬСЯ ПІД ЧАС ЗДІЙСНЕННЯ ДЕРЖАВНИХ ЗАКУПІВЕЛЬ ТОВАРІВ, РОБІТ ТА ПОСЛУГ

Нагачевський С.В.,
здобувач кафедри оперативно-розшукової діяльності та спеціальної техніки ЛьвДУВС

Аналіз сучасного стану функціонування системи державних закупівель в Україні свідчить про те, що на сьогодні залишається значна кількість невирішених проблем цієї сфери сучасних відносин, а від того на цьому тлі з'являється велика кількість зловживань. Проведені вивчення та аналіз процедур закупівель, здійснених розпорядниками державних коштів за останні роки, дозволяють зробити висновок, що більшість злочинів та інших правопорушень, які мали місце під час проведення державних закупівель, мають системний характер.

Проводячи розвідувально-пошукові заходи, оперативні працівники ДСБЕЗ повинні враховувати інформаційні чинники,

які забезпечують ефективну пошукову роботу у виявленні злочинів під час здійснення державних закупівель товарів, робіт та послуг.

Однією з умов підвищення рівня організації ОРД підрозділами ДСБЕЗ у виявленні злочинів під час здійснення державних закупівель товарів, робіт та послуг є сучасне і повне інформаційне забезпечення їх діяльності з використанням відомостей як негласного, так і негласного характеру, з метою виявлення всіх обставин вчинення злочинів у цій сфері.

Щодо правопорушень допущених у процесі організації державної закупівлі товарів, робіт і послуг необхідно виявляти інформацію про:

- незаконний поділ замовником предмету закупівлі на частими і метою уникнення тендерної процедури;
- здійснення закупівлі товарів, робіт або послуг, без проведення тендерів (торгів) у разі, якщо сума закупівлі перевищує суму встановлену лену законодавством;
- не здійснення оприлюднення інформації щодо закупівлі товарів, робіт і послуг через спеціальні засоби масової інформації;
- порушення термінів опублікування оголошення про результати відкритих торгів;
- визначення переможцем тендера учасника, який не відповідають кваліфікаційним вимогам, викладеним у тендерній документації;
- проведення оцінки тендерних пропозицій всупереч правил і критеріїв, методиці, визначеній у тендерній документації та визначення на цій основі переможця тендера;
- не проведення перед початком тендерних торгів реєстрації учасників торгів;
- допущення до участі у тендері учасників процедури закуть її що є пов'язаними особами.

Необхідну інформацію про зазначені правопорушення, оперативний працівник ДСБЕЗ може отримувати шляхом перевірки і аналізу наступних документів:

- кошторис проведення державної закупівлі (план використання державних коштів), звіт про його виконання,

довідку про зміни річного розпису бюджету (кошторису), річний план діяльності тендерного змісту щодо організації та проведення процедур державних закупівель, який має бути затверджений замовником у визначений законом термін, після затвердження кошторису (програми, плану використання державних коштів), зміни до нього, оригінали або копії листів щодо погодження окремих процедур закупівлі (інших, ніж відкриті торги);

- рішення та положення про утворення тендерного комітету; наявність сертифікатів чи свідоцтв встановлюного зразка, які підтверджують проходження членами тендерного комітету навчання або підвищення кваліфікації спеціалістів з питань державних закупівель; документ, який затверджує склад тендерного комітету, в якому мають бути визначені функції кожного члена комітету;
- протоколи засідань тендерного комітету, зокрема протоколи вибору процедури закупівлі, розкриття тендерних пропозицій, оцінки та акцепту тендерних (цінових) пропозицій; повідомлення про акцепт тендерної пропозиції (повинно бути розміщено за допомогою інформаційних систем у мережі Інтернет); розміщені в інформаційних системах у мережі Інтернет запити замовника щодо цінових пропозицій (котирувань) – у випадку здійснення процедури запиту цінових пропозицій (котирувань). Перевіряючи протокол оцінки тендерних пропозицій, працівникам ДСБЕЗ слід звернути першочергову увагу на те, щоб зазначена оцінка була здійснена відповідно до визначених критеріїв та методики оцінки тендерних пропозицій;
- журнал реєстрації всіх потенційних учасників тендерних торгів:
- тендерну документацію, в якій можна ознайомитися з таки відомостями:
  - вимоги щодо підготовки тендерних пропозицій; специфікація предмета закупівлі;
  - перелік критеріїв та методика їх оцінки для визначення найкращої тендерної пропозиції, зокрема методика розрахунку ціни тендерної пропозиції;

- перелік основних умов, які мають бути обов'язково включені додоговору про закупівлю;
- спосіб оцінки й порівняння альтернативних тендерних пропозицій інформація про валюту (валюти), в якій (яких) має бути розрахована й зазначена ціна тендерної пропозиції;
- вимоги замовника щодо надання тендерного забезпечений та забезпечення виконання договору про закупівлю;
- спосіб, місце й кінцевий термін подання тендерних пропозицій;
- термін, протягом якого тендерні пропозиції вважаються дійсними;
- місце, дата й час оголошення тендерних пропозицій;
- прізвища, посади та адреси однієї чи кількох службових осіб або інших працівників замовника, уповноважених здійснювати зв'язок з учасниками торгів [1. с12].

Для ефективної протидії злочинам, які вчиняються під час здійснення державних закупівель товарів, робіт та послуг, працівникам ДСБЕЗ необхідно мати відповідну оперативну інформацію щодо діяльності торгів, осіб, які приймають участь та документів, які підтверджують вказану діяльність.

1. Методичні рекомендації щодо запобігання злочинам під час здійснення державних закупівель товарів, робіт та послуг. – К.: ДДСБЕЗ МВС України, 2009. – 23 с.

ОРГАНІЗАЦІЙНІ ОСНОВИ ВНУТРІШНЬОГО УБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПРАВООХОРОННОГО ОРГАНУ

Паславський М.І.,
оперуповноважений ВДСБЕЗ Личаківського РВ ЛМУ ГУ МВС України у Львівській області

Ефективність роботи правоохоронного органу у протидії організованій злочинності напряму залежить від

організаційних заходів по забезпеченню його внутрішньої безпеки та ролі служби внутрішньої безпеки у цьому. Система організаційних заходів у сфері безпеки зобов'язана бути ефективною, а це, в свою чергу, передбачає застосування різних форм правоохоронної та оперативної діяльності, можливих варіантів досягнення мети вищого порядку, визнаних в організаційно-правовому аспекті дієвими. Теперішній державний механізм внутрішнього убезпечення правоохоронних органів вже не відповідає сучасним умовам протидії кримінальному середовищу як у внутрішній, так і зовнішній сферах суспільного життя. Ефективність управління оперативними підсистемами, завданнями яких є боротьба із будь якими проявами злочинності, залежить від ступеню врахування світового досвіду, теорії і практики боротьби із негативними явищами суспільства, національних особливостей держави. Вкрай незадовільне становище в нашій державі в плані дотримання правопорядку в суспільних сферах життя засвідчується не тільки статистичними даними щодо ускладнення оперативної обстановки як в окремих регіонах, так і в державі в цілому, а й загальною соціально-політичною обстановкою, загрозливими тенденціями криміналізації всіх гілок державної влади. Відтак це шкодить безпечному розвитку суспільства, дотриманню соціальних та правових норм, тому активний захист громадянина, його прав і свобод від небезпечних злочинних проявів, є головним завданням держави, насамперед її правоохоронної системи.

Термін «система» означає сукупність якісно визначених елементів, між якими існує закономірний зв'язок чи взаємодія. В залежності від характеру елементів і структури виділяють системи матеріальні (включають в себе системи неорганічної природи – фізичні, хімічні тощо), живі (екологічні, біологічні види) і ідеальні (поняття, гіпотези, теорії, логічні побудови). Особливим класом матеріальних систем являються соціальні (сім'я, колектив, політична система, суспільно-економічна формація)[1, с.195]. Відтак системи, що забезпечують безпеку, за функціональним спрямуванням можна поділити на ті, що забезпечують захист від загальних суспільних загроз; убезпечують від локальних соціальних загроз; убезпечують від невеликої загрози із територіальною чи демографічною складо-

вою. Системи за функціональним призначенням можна поділити на такі, які призначені протидіяти вчиненню насильства проти всіх членів суспільства водночас; протидіють масовому вчиненню насильства всередині нації, а його характер загрожує існуванню держави як цілісної системи; протидіють вчиненню насильства, носій якого знаходиться ззовні.

Держава за своєю суттю не може не протидіяти вчиненню насильства у всіх його проявах як до окремих її членів, так і до всієї системи в цілому, оскільки така бездіяльність означатиме для системи безпеки кінець її існування як державного органу управління. Наявність такої кількості видів систем безпеки викликана різними формами загроз. Відповідно форми управління системами безпеки є неоднакові, але всіх їх поєднує одне головне завдання – безпека.

Зацікавленість держави в особистій безпеці її громадян, сфер її функціонування стає приводом для виникнення зацікавленості у забезпеченні охорони їх прав і свобод, моральних, ідеологічних, економічних, правових, політичних норм суспільства. Правоохоронна функція держави сьогодні напряму залежить від майнового стану носія інтересу. Роль держави у такому випадку убезпечення полягає у наданні дозволу на створення державних і недержавних систем, які б спеціалізувались на охороні як самого носія інтересів, так і самих інтересів, які носій лобіює в своїй діяльності. При вирішенні цих питань держава виходить з того, що у суспільстві є незначна кількість сильних носіїв інтересів, спроможних забезпечувати свою безпеку самостійно, але є і багато відносно слабких, для яких особистий захист від різних форм насильства є нездійсненим.

Державна політика по забезпеченню захисту суб'єктів суспільних відносин від вчинення насильства завжди пов'язана з потребою підтримувати умови загальної безпеки як від зовнішніх, так і внутрішніх загроз, а відтак державі необхідна низка спеціалізованих систем, здатних виконувати саме ці завдання. Згадані системи, виконуючи покладені на них функціональні завдання, з часом, піддаються впливам тих негативних явищ, яким вони покликані протидіяти (організована злочинність, корупція). В цьому випадку важливо відслідковувати згадані впливи, аналізувати ступінь їх небезпеки як для право-

охоронної системи, так і для виконання державної охоронної функції в цілому. Для цього в системі створені підсистеми, покликані її убезпечувати від негативних як зовнішніх, так і внутрішніх впливів. Підсиситеми обов'язково повинні використовувати превентивні заходи для забезпечення необхідного рівня безпеки самої системи.

Служби, які відповідають за внутрішню безпеку правоохоронних органів, в основному, застосовують однакові за характером заходи, що і обумовлює їх організаційну та функціональну подібність. Відрізняє їх лише відомча специфіка.

Внутрішня безпека правоохоронного органу – це система адміністративно-правових, оперативно-розшукових, розвідувальних та контррозвідувальних заходів щодо забезпечення неухильного і стабільного виконання правоохоронним органом покладених на нього державою та суспільством завдань.

За своїм змістом убезпечення діяльності правоохоронного органу полягає у забезпеченні законності і стабільності його функціонування шляхом виявлення та усунення внутрішніх негативних явищ в самому правоохоронному органі (підрозділі) і зовнішніх злочинних впливів.

Досягнення внутрішньої безпеки правоохоронного органу неможливе без реалізації внутрішньовідомчого контролю. Контроль може бути як загальним, так і спеціалізованим. У процесі загального контролю здійснюється галузева оцінка і аналіз адміністративних та соціально-економічних факторів для впровадження перспективних заходів, які б підвищили ефективність діяльності правоохоронного органу як цілісної системи. Результати такого контролю є основою для об'єктивної оцінки управління правоохоронним органом, виявлення його недоліків, умов та причин розвитку негативних тенденцій в його діяльності.

Спеціалізований (внутрішньовідомчий) контроль здійснюється окремим незалежним суб'єктом всередині системи у процесі адміністративної діяльності за законністю прийняття рішень всередині правоохоронного органу.

Беручи до уваги викладене вище, можна зробити наступні висновки.

У сучасних умовах особливого значення набувають проблеми реалізації демократичних принципів державної діяль-

ності, забезпечення прав та свобод людини, тому в нагоді стане міжнародний досвід внутрішнього убезпечення діяльності правоохоронних органів.

Зміст організаційних засад убезпечення діяльності правоохоронного органу полягає у вдосконаленні системи контролю за діяльністю правоохоронних органів; система і механізм контролю повинні бути, комплексними та інтенсивними; в системі контролю за діяльністю правоохоронних органів повинні вводитись нові незалежні суб'єкти контролю.

1. Український Радянський Енциклопедичний Словник: в 3-ьох т. / Редкол.: А.В. Кудріцкій (відпов. ред.) і інші. – К.: 1989 р. Т.3 – 772 с.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ КОНФІДЕНЦІЙНИХ СПІВРОБІТНИКІВ У ПРОТИДІЇ НАРКОЗЛОЧИННОСТІ СЕРЕД НЕПОВНОЛІТНІХ

Рєзников С.Д.,
здобувач кафедри оперативно-розшукової діяльності Одеського державного університету внутрішніх справ

В сучасних умовах незаконний обіг наркотиків активно поширюється серед різних прошарків населення, особливо серед молоді, містить в собі шкоду для здоров'я населення держави, а головне – виступає одним із головних чинників загострення оперативної обстановки в цілому. Велика кількість наркозлочинів вчинюються злочинними наркоугрупованнями з різним рівнем організованості, куди активно залучаються неповнолітні. Оскільки даний вид злочинів має латентний характер, то однією з головних завдань, що стоять перед органами внутрішніх справ, це організація та здійснення оперативно-розшукової діяльності відносно осіб, у тому числі неповнолітніх, які причетні до НОН. Законом України «Про оперативно-розшукову діяльність» визначено сутність (поняття) цієї діяльності, правову основу, принципи, а також відповідні права та обов'язки. Крім того, заслуга прийняття цього нормативного документу полягає в тому, що було нормативно врегульовано питання сприяння осіб здійсненню оперативно-розшукової діяльності. Особи, які співробітни-

чають з оперативними підрозділами отримали законодавчо визначене право на конфіденційність такого співробітництва, отримали відповідні правові та соціальні гарантії. Гуманність (етичність) оперативно-розшукової політики проявилася в забороні залучення до конфіденційного співробітництва «медичних працівників, священнослужителів, адвокатів, якщо особа, щодо якої вони мають здійснювати оперативно-розшукові заходи, є їх пацієнтом чи клієнтом».

Згодом інститут конфіденційного співробітництва поповнювався новими нормами: приймався новий Кримінальний Кодекс України (ст. 43), Закон України «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві», вносилися відповідні зміни до Кримінально-процесуального кодексу (ст. 20, 52-1), приводилися у відповідність до законодавства таємні відомчі нормативні документи тощо. Нажаль більшість норм інституту конфіденційного співробітництва містять істотні прогалини та невизначеності. Згідно ч.2 ст.11 Закону України «Про оперативно-розшукову діяльність» «угоду про сприяння оперативним підрозділам в оперативно-розшуковій діяльності може бути укладено з дієздатною особою». Таке визначенні віку, з якого можливе залучення до співробітництва, не задовольняє сучасних потреб теорії та практики ОРД, законодавець повинен чітко визначити вік. Хотілося б зазначити, що трудова дієздатність (спосібність своїми діями здійснювати права та обов'язки) по загальному правилу наступає з 16 років. В цивільному праві в повному об'ємі дієздатність наступає по досягненню 18-річного віку. Цілком зрозуміло, що стосовно конфіденційного співробітництва необхідно використовувати категорію «трудова дієздатність».

В теорії ОРД визначення віку залучення до негласного співробітництва є дискусійним питанням, що не знаходить узгодженості думок науковців. Деякі науковці (як радянські, так і сучасні українські автори) однією з причин незадовільної негласної роботи, особливо серед неповнолітніх, вбачають заборону залучення до співробітництва осіб, віком до 18 років. Існують також противники точки зору стосовно пониження вікового цензу залучення до негласного співробітництва.

Що стосується кримінального права, то невипадковим, на нашу думку, є встановлення національним законодавством у ч.1

ст. 22 КК України загального віку кримінальної відповідальності саме з 16 років. Саме з 16 років особа у повному обсязі усвідомлює суспільну небезпеку своїх протиправних діянь, неповнолітній володіє достатніми фізичними та психологічними якостями, може у повній мірі усвідомлювати поставлені перед ним завдання в процесі здійснення негласної роботи, правильно вибирати тактичні прийоми, вміло використовувати свої права. На наше переконання, зважаючи на спільні критерії визначення, вік, з якого наступає кримінальна відповідальність, та вік, з якого можливе залучення до негласної співпраці, в нормативно-правових актах повинні йти «пліч-о-пліч».

Не можна не оминути і етичний бік розробки неповнолітніх осіб за допомогою повнолітніх. На нашу думку, таке використання дорослих осіб можна розглядати як своєрідну провокацію та підбурювання неповнолітніх на вчинення протиправних дій. Щоб не казали, неповнолітні особи в силу психологічних особливостей завжди прислухаються до думки старших за віком товаришів, просять поради, допомоги у здійсненні намірів, в тому числі злочинних, тощо. Тобто, таке використання граничить із складом злочину, передбаченого ст. 304 КК України, що передбачає відповідальність за втягнення неповнолітніх у злочинну діяльність, у пияцтво, у заняття жебрацтвом, азартними іграми. У справах про втягнення неповнолітніх у злочинну або іншу антигромадську діяльність згідно Постанови Пленуму Верховного Суду України № 2 від 27.02.2004 р. суди мають перевіряти, чи зазначено чітко й конкретно у постановах про притягнення як обвинуваченого та в обвинувальних висновках, у чому саме полягало втягнення, його форми та способи, а якщо дорослий вчинив злочин у групі з неповнолітнім, – роль кожного з них [5].

Виходячи з вищезазначеного, приймаючи до уваги етичні складові проблематики, потреби практики, вважаємо за необхідне доповнити ст. 11 Закону України «Про оперативно-розшукову діяльність частиною наступного змісту: «Виключно з метою розробки неповнолітніх осіб або їх груп, які готують або вчиняють тяжкі злочини, оперативними підрозділами до негласного співробітництва можуть залучатися особи, віком від 16 років».

ЩОДО ЗАБЕЗПЕЧЕННЯ КРИМІНАЛЬНОГО СУДОЧИНСТВА НА СТАДІЇ СУДОВОГО РОЗГЛЯДУ КРИМІНАЛЬНИХ СПРАВ, ПОВ'ЯЗАНИХ ІЗ ТОРГІВЛЕЮ ЛЮДЬМИ

Мисюра А.М.,
здобувач кафедри оперативно-розшукової діяльності Одеського державного університету внутрішніх справ

Торгівля людьми є найзухвалішою формою порушення основоположних прав людини та громадянина, пов'язаною з цинічним та грубим поводженням, нещадною експлуатацією, обмеженням свободи, приниження честі й гідності особи. Специфіка даного злочину полягає в тому, що йому притаманний організований характер і часто не обмежується територією однієї країни. Тому, нагальним є прийняття усіх можливих заходів, спрямованих на результативне викриття злочинів та притягнення винних до відповідальності.

Відправлення правосуддя в цьому контексті відіграє велику роль. Адже здійснюючи правосуддя, суд остаточно досліджує всі істотні обставини злочину, перевіряє докази, зібрані при провадженні дізнання і досудового слідства, та постановляє виправдувальний чи обвинувальний вирок з призначенням покарання або без призначення покарання. Тому, зважаючи на організований характер злочинів в сфері торгівлі людьми, особливої уваги потребує вирішення питань щодо подолання протидії здійсненню правосуддя по таких справах, необхідністю нейтралізації протиправного впливу на цей процес, забезпеченням безпеки учасників кримінального судочинства та вирішенням інших завдань боротьби зі злочинністю.

У теорії подібні питання взаємодії прийнято розглядати в контексті оперативно-розшукового супроводження кримінального судочинства чи оперативно-розшукового його забезпечення і, головним чином, пов'язувати зі стадією досудового слідства, але снує необхідність здійснювати аналогічну роботу і на стадії судового розгляду. Як свідчить практика боротьби з торгівлею людьми, саме на цій стадії суд має величезну потребу в підтримці оперативних підрозділів і отриманні інформації про

намагання окремих осіб щодо активної протидії передбаченому законом порядку судового розгляду справ, зі встановлення та усунення фактів тиску на потерпілих, свідків, спеціалістів та інших учасників процесу, про причини зміни учасниками процесу своїх показів.

Завдяки недосконалості правового регулювання судового процесу різноманітні перешкоджання нормальному здійсненню правосуддя з боку певних осіб, досить часто не спричиняють жодних негативних правових наслідків для них. Зокрема, це стосується недобросовісних захисників, які нерідко самі безпосередньо здійснюють незаконний вплив на потерпілих і свідків. Сюди слід віднести і недосконаліть правового регулювання діяльності різноманітних приватних детективних та охоронних служб, які за свої послуги кримінальним структурам в організації протидії реально не несуть ніякої юридичної відповідальності.

У справах, пов'язаних із торгівлею людьми, спостерігається енергійна і цілеспрямована протидія з боку зв'язків підсудних, їхніх родичів, друзів, знайомих, співучасників чи інших осіб, зацікавлених у розгляді справи, коли судом можуть бути встановлені небажані для цих осіб обставини. Вибір організаційно-тактичних заходів виявлення і нейтралізації протидії, а також боротьби з нею. залежить від обраних засобів, що застосовують самі злочинці. Їх можна класифікувати за такими напрямами.

1. Вплив на свідків і потерпілих з метою дачі свідчень, потрібних злочинцям. Він може здійснюватися шляхом фізичної розправи, а також погрозою її застосування. У деяких випадках загрожують близьким родичам свідків та потерпілих.

2. Вплив на суддів, прокурорів, що підтримують державне обвинувачення, а також експертів та інших фахівців, що дають на судовому засіданні висновки з тих чи інших питань в економічній сфері.

3. Вплив на співробітників правоохоронних органів, які безпосередньо брали участь у проведенні досудового слідства. Такий вплив полягає в загрозах розправитися з ними або їх близькими, а також знищення їхнього майна.

Вплив може здійснюватись шляхом використання засобів масової інформації, як преса, радіо, телебачення. Крім форму-

вання громадської думки, спрямованої на дискредитацію деяких співробітників правоохоронних органів, злочинці через засоби масової інформації впливають на об'єктивність судового розгляду.

4. Спроби прямого знищення і фальсифікації доказів, що викривають злочинців у вчиненні економічних злочинів. Небезпека цієї форми протидії полягає в тому, що її використовують, у випадках коли не дали позитивного результату інші дії злочинців.

5. Фізичне усунення свідків (як правило, основних свідків обвинувачення). Ця форма хоча і рідко застосовується, проте набуває поширення в умовах зростання професіоналізму організованої злочинності.

У такий спосіб організовані злочинні угрупування, причетні до торгівлі людьми, прагнуть створити систему свого захисту від соціального контролю, засновану на залякуванні, жорстокості, насильстві та широкомасштабній корупції, що становить сутність їх протидії правоохоронній системі.

Звичайно, що це змушує державу посилювати захист суб'єктів судового розгляду кримінальних справ від протиправного впливу на них із боку кримінального середовища. На наш погляд, провідна роль у цьому повинна належати саме оперативному супроводженню судового розгляду кримінальних справ зі сторони оперативних підрозділів, що повинно слугувати інтересам спільного відпрацювання та прийняття відповідних контрзаходів. Так, Закон України «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві» та відповідні підзаконні акти МВС України регламентують заходи фізичного захисту певної категорії осіб, підстави та порядок їх здійснення. До того ж, у структурі МВС України створено спеціальний підрозділ судової міліції «Грифон». Крім основних завдань фізичного захисту, його співробітники також мають право проводити оперативно-розшукову діяльність із метою отримання оперативної та іншої інформації про наявність загрози життю, житлу і майну осіб, які беруть участь у кримінальному судочинстві. Головну ж роль в інформаційному забезпеченні судового розгляду, на нашу думку, повинні відігравати саме ті галузеві оперативні підрозділи, що здійснювали документування протиправних дій фігурантів.

Виходячи з аналізу практики слід визнати, що безпосереднє постійне і комплексне оперативне забезпечення судового розгляду кримінальних справ, пов'язаних із торгівлею людьми, здійснюється рідко. У зв'язку з цим, на наш погляд, нагальною є необхідність нормативно-правового врегулювання цього аспекту діяльності оперативних підрозділів. Зокрема, це можна зробити шляхом видання відомчого нормативно-правового акта, який би визначав механізм в цілому оперативно-розшукового забезпечення судового розгляду і взаємовідносини між судами та відповідними оперативними підрозділами.

ПРОФЕСІОНАЛІЗАЦІЯ КАДРІВ ОВС УКРАЇНИ ЯК ФАКТОР ДЕРЖАВОТВОРЕННЯ

Мельникович В.М.,
здобувач кафедри адміністративного права і процесу, фінансового та інформаційного права ЛьвДУВС

Процеси державотворення молодої незалежної України є найважливішими в усіх сферах життєдіяльності її суспільства. У державі формуються основи громадянського суспільства і сучасного демократичного державного устрою на принципах розподілу влади. Необхідність управлінських перемін в Україні викликана існуючими диспропорціями залишків минулих тоталітарних і сучасних демократичних управлінських систем, неузгодженістю їх з новим соціально-політичним курсом національного державотворення та неконструктивністю щодо переходу на шлях ринкової економіки. Тому поставлено ключове завдання істотного оновлення управлінської еліти і до системи управління мають прийти люди нової генерації. Особливо важливо запобігти новим рецидивам непрофесіоналізму та компетентності при формуванні кадрового потенціалу.

Слід активізувати, розвивати внутрішній духовно-інтелектуальний потенціал державних службовців усіх рівнів. Вони мають стати свідомими провідниками ідеології і політики українського державотворення, каталізаторами національного, економічного, політичного, духовно-культурного розвитку. Люди, які обираються і призначаються на керівні посади,

повинні сприяти консолідації нації, мати відповідні ідейні, моральні, психологічні, фахові якості [1, С.22]. Це має бути авангард української національної еліти, процес формування якої, на думку професора М. Литвина, має бути під опікою держави: «Треба звернути увагу на підтримку талановитих людей і виховувати їх кожного зокрема... Тому, що без інтелекту, без духовності нація приречена бути на узбіччі цивілізації». За його висновком, бажано, «щоб у державні установи прийшли люди, які перебувають в постійному пошуку, треба боятися людей, які керують, не думаючи про Україну» [2]. Надзвичайно важливо, щоб управлінська еліта була глибоко національною за своїми ідейними переконаннями і практичними справами. Щоб рішення, які приймаються управлінцями на місцях, були спрямовані на користь України, працювали на зміцнення економічного, оборонного, соціально-культурного потенціалу. Для цього потрібен високий рівень професіоналізму управлінських кадрів як найважливіша умова державної кадрової політики [3, С.256; 31, С.272; 125].

Нові суспільні умови децентралізації передбачають передачу ряду управлінських функцій у різних галузях гуманітарної, соціальної, економічної, бюджетно-фінансової, інвестиційної сфер, міжнародних відносин з центру на регіональний та місцевий рівні. Тому такі принципово нові підходи до вирішення управлінських проблем перехідного суспільства, зорієнтованого на автономізацію управлінської діяльності в регіонах, вимагають відповідної підготовки управлінських кадрів, які володіють комплексом сучасних знань і навичок управлінського менеджменту. При цьому дуже важливо виробити єдину систему і нормативно-правову базу підготовки, перепідготовки та підвищення кваліфікації співробітників органів внутрішніх справ, забезпечити чітке розмежування їх функцій на основі професійно-кваліфікаційних характеристик, збалансованість у системі взаємних прав, обов'язків і відповідальності, надання гарантованих державних послуг населенню, захисту законних прав і свобод громадян. «Сьогодні, – на думку Володимира Яцуби, – кожен рівень влади повинен мати чітко окреслені повноваження, обов'язки й, головне, рівень відповідальності за управління конкретними сферами суспільного життя» [4].

В умовах побудови правової, демократичної держави, Україна конче потребує такого апарату управління, організаційна побудова якого науково обґрунтована, базується на демократичних засадах і постійному професійному його кадрів. Тому важливо насамперед теоретично і практично визначити суть, структуру і етапи професійного розвитку управлінських кадрів, загалом державних службовців.

На нашу думку, професійний розвиток полягає, перш за все, у формуванні і в постійному збагаченні у правоохоронців якостей, професійно-значимих знань, навиків та умінь, які необхідні їм для ефективного виконання їх посадових функцій, прав і обов'язків. Вони покликані в повній мірі розкрити здібності, талант, потенційні можливості співробітників органів внутрішніх справ. Зазначимо, що професійний розвиток співробітників органів внутрішніх справ є вираженням взаємодії управлінських службових потреб апарату (і створення в ньому умов для їх реалізації) і інтересів, потреб, здібностей кожного співробітника.

Проведені нами соціологічні дослідження дали можливість в певній мірі оцінити професійно-компетенційні характеристики, рівень ефективності управлінської діяльності співробітників органів внутрішніх справ і фактори, що на неї впливають. Зокрема, 73,5% співробітників ГУМВС України областей оцінюють себе як таких, що здатні вирішувати актуальні управлінсько-функціональні проблеми. Але рівень професійної компетентності співробітників органів внутрішніх справ ГУМВС України області становить лише 63,1%, і тільки 61,6% співробітників керівної ланки управління спроможні забезпечити компетентний зворотній зв'язок при реалізації державної соціально-економічної політики. Результати анкетування співробітників органів внутрішніх справ окреслили також причини, які «заважають» цьому. Найголовніші з них: відсутність належної нормативно-правової бази – 21,9%, низька зарплата – 16,5%, мало повноважень – 16,5%, інші проблеми – 13%. У той же час у відповідях майже нівельовані такі важливі особистісно-компетенційні фактори, як слабка організація праці (6,8%), особисті якості працівника (6,3%), низька професійна підготовка (3,0%), некомпетентність (1,8%). На нашу думку,

співробітники органів внутрішніх справ просто замовчують недоліки суб'єктивно-особистісного характеру, посилаючись у своїх службових прорахунках на об'єктивні соціальні обставини, причини виробничого характеру, організаційні збої.

Дослідження окреслили фактори, завдяки яким співробітники досягають поставленої службової мети. Зокрема, 28,5% респондентів вважають, що вони досягають мети службової діяльності, керуючись положенням про свій структурний підрозділ; 27,8 – завдяки власній професійній підготовці; 26% – за дорученням керівництва; 18,7% – через виконання планових завдань. Разом з тим тільки 5,1% співробітників досягали службової мети заради матеріальної зацікавленості, 2,5% – через ідейні мотиви. Лише 2,4% співробітників керівної ланки використовують при цьому новітні технологічні методології, оскільки тільки на 20,6% автоматизовано виконання аналітичних процедур управлінців і на 19,8% забезпечена автоматизація і комп'ютеризація роботи співробітників органів внутрішніх справ. [5, С.37-50].

Тому професійний розвиток співробітників органів внутрішніх справ слід здійснювати у двох напрямах: професійно-кваліфікаційному і професійно-посадовому.

Професійно-кваліфікаційний напрямок в основному пов'язаний з навчанням і самоосвітою, отриманням нових знань, умінь і навичок. Реалізація цього напрямку можлива через низку різноманітних навчальних закладів, курсів підвищення кваліфікації, семінарів, нарад тощо. Особливо це доцільно для співробітників, що вже довгий час займають одну й ту ж посаду, і має враховуватись при проведенні атестації, зарахуванні до резерву на висунення, що має вести до підвищення грошового утримання, просування по службі та ін.

Професійно-посадовий напрямок розвитку в основному пов'язаний з формуванням єдиної ефективно діючої системи функціонування органів внутрішніх справ, де максимально будуть враховуватись можливості і здібності кожного співробітника, його досвід, вік, особисті якості, вміння, знання. Ці зазначені два напрямки професійного росту співробітників внутрішніх справ тісно взаємопов'язані, вони переплітаються між собою, їх неможливо розглядіти окремо, а лише комплексно, у їх

взаємодії з системою професійної підготовки співробітників органів внутрішніх справ.

Важливо не лише визначити стратегію професійного розвитку тої служби, але й бачити різноманітність шляхів і технологій підвищення професіоналізму службовців, передусім на основі:

- вдосконалення, а по суті створення нової системи відбору і приймання співробітників на службу в органи внутрішніх справ, з висуванням уже на цьому етапі конкретних вимог до рівня їх професіоналізму;
- забезпечення системності, послідовності, росту професійного рівня співробітників у ході їх службового просування, стимулювання професійного розвитку в ході атестації, участі в конкурсах і т.д.;
- створення нової системи професійної підготовки, перепідготовки, підвищення кваліфікації співробітників органів внутрішніх справ, визначення за нею важливої складової частини державно-управлінської діяльності;
- створення умов і гарантій для закріплення на державній службі спеціалістів, формування у них зацікавленості у своєму професійно-кваліфікаційному розвиткові, підвищенні якості і ефективності їх праці;
- створення по суті нової нормативно-правової і закріплення матеріально – фінансової бази професійного розвитку персоналу.

І в той же час необхідно не лише визначити державну стратегію професійного розвитку персоналу органів внутрішніх справ, розробити цільові плани і програми професійного розвитку кожного колективу з урахуванням можливої зміни завдань і функцій органу, перспектив розвитку структур його апарату, розширення об'єму роботи, а й розкрити сучасне розуміння професіоналізму співробітника органів внутрішніх справ (структури, характерних якостей, критеріїв та ін.).

З точки зору адміністративного права державний службовець-професіонал – це людина, яка чітко знає, вміє і може робити справу з повнотою ефективного управління та логічною відповідальністю за свою роботу.

«В цілому, – пише В.Ф. Ковалевський, – процес поєднання людини зі службою в органах внутрішніх справ ми окреслюємо поняттям правоохоронної спеціалізації, а науку, яка займається вивченням закономірностей цього процесу, – правоохоронною професіологією» [6, С.35]. Цей підхід найбільше відображає послідовність включення людини в професійну діяльність і дозволяє виявити зміст етапів процесу становлення людини як професіонала і вихід їх чисто за межі психологічного змісту.

Професіоналізм співробітника органів внутрішніх справ – це об'єктивно зумовлена категорія, що розкриває основи механізму трудової і інтелектуально-моральної самореалізації особистості [7, С.37-50].

Професіоналізм діяльності сучасного співробітника органів внутрішніх справ полягає у збагаченні її елементами наукового дослідження з метою контролю і самоконтролю міри продуктивності. А під продуктивністю діяльності розуміється система і послідовність професійно доцільних дій, із розв'язанням службових завдань, що забезпечує досягнення кінцевого результату в процесі розвитку державної служби [6, С.111-120].

Професіоналізм передбачає здатність особи не тільки діяти за алгоритмами, що засвоєні нею у процесі служби в органах внутрішніх справ, а й виробляти нові алгоритми діяльності відповідно до власних індивідуальних особливостей та виробничих умов, які змінюються, процесуального і діалектичного. У стадійних моделях процес розвитку представлено як послідовний ряд якісно різних вікових етапів. У межах цього підходу звичайно досліджуються зміни якого-небудь одного життєвого процесу. У процесуальному підході зміна різних психічних структур розглядається без урахування впливу зовнішніх факторів регуляції життєвого шляху індивіда. Діалектичний підхід відбиває погляд на розвиток людини як на зміну життєвих процесів у їхній єдності, складній організації, на несинхронність і суперечливість цих процесів як джерел розвитку, а також на конкретність характеру розвитку, у тому числі з погляду культурно-історичного контексту.

1. Шпекторенко І.В. Поняття та структура феномену професійної мобільності державного службовця / І.В. Шпекторенко; Універси-

тетські наукові записки // Часопис Хмельницького університету управління і права. – 2007. – № 4, С. 24.
2. Литвин В. М. Повернення не буде // Президент. – 2000. – 21 січня. – №1. – С.24-31.
3. Лефтеров В.О. Професійна кар'єра та психосоціальний розвиток працівників ОВС / В.О. Лефтеров // Вісник Національної академії оборони. – 2010. – № 1(14). – С. 136 – 140.
4. Янюк Н.В. Особливості адміністративно-правового статусу посадової особи / Наталя Володимирівна Янюк // Проблеми державотворення і захисту прав людини в Україні: матеріали III регіон. наук. конф. (Львів, лютий 1997 р.). – 1997. – С. 88.
5. Кісіль З.Р. Професіоналізація – основа державної кадрової політики в Україні / З.Р. Кісіль // Вісник Львівського державного університету внутрішніх справ. – 2011. – № 2. – С. 111–120.
6. Колодкин Л.М. Организация работы с кадрами в органах внутренних дел / Л. М. Колодкин, А.В. Фатула – М.: Академия МВД РФ, 2008. – 113 с.
7. Пєтков С.В. Менеджмент в органах внутрішніх справ України: монографія / С.В. Пєтков. – Дн.: Дніпроп. держ. ун-т внутр. справ; ПП «Ліра ЛТД», 2007. – 280 с.

РОЛЬ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ У ДІЯЛЬНОСТІ ОРГАНІВ ВНУТРІШНІХ СПРАВ

Нагачевська Ю.С.,
доцент кафедри оперативно-розшукової діяльності та спеціальної техніки ЛьвДУВС, к.ю.н.

Сучасний рівень розвитку суспільства характеризується стрімким зростанням потоків і обсягів інформації, ускладненням механізмів управління соціальними процесами та явищами.

У нових умовах роботи органів внутрішніх справ, коли основу їх діяльності складають профілактика та прогнозування правопорушень, розкриття злочинів по гарячих слідах, спостерігається стала тенденція подальшого збільшення обсягів інформації про причини окремих злочинів та умови, що сприяють їх вчиненню, про пошук найбільш ефективних форм і методів їх запобігання і т. ін.

Однією із важливих функцій органів управління будь-якої соціальної системи є інформаційне забезпечення її діяльності.

Ця діяльність спрямована на створення, організацію функціонування та вдосконалення інформаційних систем, які служать успішному виконанню задач управління.

Практика боротьби зі злочинністю переконливо свідчить не тільки про суттєву, а в багатьох випадках пріоритетну роль системи інформаційного забезпечення органів внутрішніх справ як ланки, що значно зумовлює ефективність роботи всієї системи правоохоронних органів. Система інформаційного забезпечення здійснює інформаційну підтримку органів внутрішніх справ у розкритті та попередженні злочинів, установленні й розшуку злочинців, подає багатоцільову статистичну, аналітичну та довідкову інформацію.

Водночас склалася ситуація, що об'єктивно потребує реорганізації та оновлення існуючої системи інформаційного забезпечення органів внутрішніх справ.

Останнім часом набагато загострилась криміногенна обстановка в Україні. У зв'язку з цим надзвичайно збільшився потік інформації, що надходить на адресу правоохоронних органів, зросла кількість оперативних документів, які потребують негайного виконання. Побільшав обсяг ручних довідкових картотек та існуючих банків даних, які досягли тієї межі, коли наявні технічні засоби і технології не дозволяють оперативно та доброякісно обробляти інформацію, що надходить.

Оптимальної організації інформаційних масивів та баз даних можна добитись лише створенням комплексу взаємозв'язаних інформаційних систем у рамках конкретного органу і всієї системи органів. Діяльність же по створенню конкретних інформаційних систем залежно від їх призначення та сфери використання може називатися інформаційним забезпеченням планування, контролю, профілактичної роботи і т. ін.

Необхідність у створенні інформаційних систем виникає при формуванні нових або ж при видозмінюванні колишніх функцій органу управління, а також тоді, коли названі системи переводяться на більш досконалу технічну базу. Дієвість системи інформації, її ефективність у забезпеченні процесів управління силами та засобами органів внутрішніх справ багато в чому залежать від упорядкованості потоків інформації, її обсягу та якості, а також своєчасності проходження як в цілому

в системі управління, так і на конкретних її рівнях. Особливої уваги потребує територіальний рівень (міськрайлінорганів), котрому традиційно в цьому плані приділялось мінімум уваги, хоча значущість інформації, яка формується на цьому рівні, неможливо ігнорувати: саме вона є основою всієї системи інформації в органах внутрішніх справ і тому їй приділяється особлива увага в Концепції розвитку системи інформаційного забезпечення органів внутрішніх справ України. Аналіз реально існуючих умов роботи міськрайлінорганів дає змогу визначити завдання, що мають істотне значення у підвищенні ефективності системи інформаційного забезпечення їх діяльності.

Першим завданням є визначення інформаційних потреб служб, підрозділів та співробітників міськрайлінорган внутрішніх справ. Основою для визначення цих потреб служать функціональні обов'язки служб, підрозділів, співробітників. При розробці функціональних обов'язків треба враховувати реальні інформаційні потреби співробітників, що об'єктивно відповідають їхньому роду діяльності. Саме це дозволить створити в органах внутрішніх справ єдину систему інформації, пристосовану не до структури існуючих зв'язків між підрозділами і співробітниками, а до вимог системного розв'язання завдань, які відповідають цілям та функціям цих органів.

Друге завдання полягає у створенні в міськрайлінорганах внутрішніх справ єдиного центру збирання, збереження і розподілу інформації, тобто інформаційної служби, яка подібна до інформаційного бюро в мініатюрі. На цей підрозділ доцільно покласти такі функції: ведення обліку інформації, яка надходить до міськрайліноргану, її групування, доповідь начальникові органу її квінтесенції, розподіл (видача) її між співробітниками згідно з їхніми функціональними обов'язками, контроль за якістю та строками її реалізації, складання звітних інформаційних документів, оновлен¬ня, фільтрування та систематичне поповнення інформаційного фонду міськрайліноргану. Координацію потоків інформації, контроль за її обробкою та використанням здійснює керівник органу.

Успішний пошук, збирання та відбір необхідної інформації вимагають від співробітників відповідної професійної підготовки, а також знання основ психології сприйняття, запам'ято-

вування та передачі інформації, котрі допомагають їм об'єктивно оцінювати ту чи іншу інформацію.

Крім того, працівники органів внутрішніх справ повинні враховувати те, що люди, які володіють необхідною інформацією, по-різному ставляться до запитів органів внутрішніх справ про видачу цієї інформації. Тому співробітники цих органів повинні здійснювати щодо підвищення ініціативи цих осіб такі заходи, як встановлення тісних ділових контактів, поважне ставлення до них, роз'яснення необхідності здобування відомостей, а також постійну роботу по підвищенню рівня моральної та правової свідомості цих осіб.

Отже, зміст інформаційного забезпечення може відноситись до всього процесу управління, до певних його функцій або стадій управлінського циклу, до діяльності окремих структурних підрозділів або конкретних категорій співробітників.

АНАЛІЗ ЗЛОЧИНІВ, СКОЄНИХ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Рудік В.М.,
к.ю.н., доцент, м. Київ
Рудий Т.В.,
доцент кафедри інформаційних технологій ЛьвДУВС к.т.н., доцент
Фірман В.М.,
доцент кафедри безпеки життєдіяльності, ЛНУ ім. І.Франка, к.т.н., доцент

В умовах перехідної ринкової економіки інформація, за певних обставин, стає об’єктом дій як конкурентів, так і кримінальних структур. У такому разі активи інформаційних систем (ІС) мають бути достатньо захищеними, з тим щоб виключити можливість несанкціонованого доступу (НСД) до них і незаконного використання.

Слід визнати, що сьогодні кримінальні структури володіють досить потужними системами несанкціонованого збору інформації, високоефективними технічними засобами та найголовніше – якісно, у професійному розумінні, підготованими фахівцями. Злочинність з використанням інформаційних технологій (ІТ) перетворюється у цілу індустрію, яка володіє

перспективними методиками і яка проникає практично в усі сфери економічної діяльності.

Зростання рівня злочинності у сфері ІТ пояснюється, у першу чергу, відносною доступністю сучасних ІТ і телекомунікаційних сервісів, розширенням сфери електронного грошового обігу, недосконалістю чинного законодавства у сфері ІТ [1].

Чинне законодавство України досі не передбачає чіткого трактування складових обігу інформаційних ресурсів, не визначені критерії їх належності до категорій державних і недержавних. Розробники законодавства у сфері інформації та інформаційної політики держави не зовсім компетентні у технічному забезпеченні новітніх ІТ і, як наслідок, – орієнтування на зовнішні запозичення, які, у свою чергу, далекі від досконалості.

Розкриваючи злочини з використанням ІТ, аналізуючи наявну інформацію працівники органів внутрішніх справ (ОВС) зустрілися з проблемою, коли зловмисники, з метою приховування злочинних діянь, захищають свою інформацію абсолютно надійною системою криптографічного захисту інформації (КЗІ). Системи КЗІ, програмні продукти та технічні засоби на їх основі набули широкого поширення та стали легкодоступними не тільки для фахівців у галузі ЗІ (СБУ, МО, МВС), але й широкому загалу зацікавлених користувачів, у тому числі і кримінальним структурам. Використання стандартного математичного підходу до розшифрування такої закритої інформації є неефективним.

Щодалі частіше оперативні підрозділи ОВС України звертаються за практичною допомогою до провідних фахівців з проблемами доступу до КЗІ. Хоча проблема не є новою, але ефективні методики і тактика поведінки працівників ОВС при роботі з КЗІ відсутні. На відміну від звичайних "хакерів" працівники правоохоронних органів мають право, згідно з чинним законодавством, застосувати оперативно-розшукові методи, які можуть бути єдиним ефективним методом доступу до такої інформації. [2]

Неможливо обійти увагою банківські електронні платіжні системи та електронну комерцію. За статистичними даними, у промислово розвинених країнах середні збитки від одного злочину в сфері ІТ становлять приблизно $ 450 тис., а щорічні

сумарні втрати в США і Західній Європі сягають $ 100 млрд. і $ 35 млрд., відповідно. В останні десятиріччя зберігалася стійка тенденція до зростання збитків, пов'язаних із злочинністю в сфері ІТ.

В усіх аспектах забезпечення захисту інформації основ.ним елементом є аналіз можливих загроз щодо порушення роботи банківських ІС, тобто дій, що підвищують уразливість інформації, яка обробляється в ІС фінансових установ, призводять до її витоку, випадкового або навмисного модифікування, знищення.

За частотою виявлення загрози можна розташувати в такому порядку:

- копіювання і крадіжка програмного забезпечення;
- несанкціоноване модифікування даних;
- зміна або знищення даних на довільних носіях;
- крадіжка інформації;
- несанкціоноване використання ресурсів ІС;
- несанкціоноване використання банківських ІС;
- НСД до інформації високого рівня таємності.

Одним із найважливіших видів інформації у банку є гроші в електронному вигляді, тому основою інформаційної безпеки у банківських ІС є захист електронного грошового обігу. Крім цього, інформація у банківських ІС становить значний інтерес для великої кількості людей та організацій – клієнтів банку. Ця інформація має обмежений доступ і банк несе відповідальність за забезпечення надійного рівня її захисту перед клієнтами та державою.

Одночасно з розширенням мережі користувачів банківських електронних платіжних систем та спрощенням процедури доступу до них збільшується кількість загроз і кількість НСД. Зростання рівня злочинності у банківсько-кредитній сфері пояснюється дуже просто – адже, власне, у даній сфері зосереджені величезні готівкові кошти, які у першу чергу і цікавлять злочинні угрупування.

У даному випадку злочинні угрупування розв’язують діаметрально протилежну задачу – НСД до закритої інформації з метою нанесення власникам систем електронного грошового обігу матеріальних збитків.

Хочемо відзначити, що правоохоронним органам стають відомі далеко не всі випадки викрадення грошей шляхом

використання банківських електронних платіжних систем. Це можна пояснити декількома обставинами. Серед них і небажання вищого керівництва надавати відповідну інформацію через побоювання «компрометації» фінансової установи та можливості виявлення додаткових правопорушень при проведенні слідчих дій.

Переконані, що значний відсоток несанкціонованого доступу до банківських електронних платіжних систем здійснює персонал, який добре ознайомлений з технологією оброблення та захисту інформації. Найчастіше до числа правопорушників потрапляють особи, які, властиво, повинні відповідати за інформаційну безпеку в фінансовій установі.

Наостанок відзначимо, що високий фаховий рівень підготованості особового складу ОВС у галузі ІТ стане запорукою ефективної протидії і розкриття злочинів, скоєних з використанням ІТ.

1. Рудий Т.В. Специфіка протидії злочинам у сфері інформаційних технологій. / Т.В. Рудий, В.М. Слижук, І.М. Ганич, А.В. Нечепуренко. / Проблеми діяльності кримінальної міліції в умовах розбудови правової держави // Матеріали V звітної науково-практичної конференції факультету кримінальної міліції Львівського державного університету внутрішніх справ 14 квітня 2011 р. – Львів: ЛьвДУВС. 2011, – с. 176-180.
2. Когут В.В. Порядок атестування систем технічного захисту інформації. / В.В. Когут, Т.В. Рудий, Я.Ф. Кулешник. / Проблеми діяльності кримінальної міліції в умовах розбудови правової держави // Матеріали науково-звітної конференції факультету кримінальної міліції Львівського державного університету внутрішніх справ 12 березня 2010 р. – Львів: ЛьвДУВС. 2010, – с. 90-97.

АНАЛІЗ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ ЗА РЕЗУЛЬТАТАМИ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Руда О.І.,
доцент кафедри теоретичної та прикладної економіки ЛьвДУВС, к.е.н.

На поточний момент, коли обсяги інформації, що циркулює, обробляється та накопичується у сучасних ін-

формаційних системах (ІС), стрімко збільшуються, питання захисту інформації стає особливо актуальним. В умовах розвитку та впровадження технології систем з відкритою архітектурою, яка вирізняється складною взаємодією ІС різного походження (інтероперабельність), наявністю проблем перенесення прикладних програм між різними платформами (нобільність) та іншими особливостями, питання захисту інформації набуває все більшої ваги.

З огляду на ці обставини керівництву підрозділів МВС необхідно взяти до уваги проблеми безпеки у спеціалізованих ІС, ймовірність виникнення яких є обов'язковою у процесі функціонування довільної ІС. Доцільним, з пункту бачення захищеності ІС, рішенням у такій ситуації може бути **аудит інформаційної безпеки (ІБ)**, який проведуть фахівці в області інформаційної безпеки.

На сьогодні, у доступних для вільного доступу літературних джерелах, ще не сформовано усталеного визначення аудиту інформаційної безпеки. У подальшому ми пропонуємо під поняттям аудиту інформаційної безпеки розуміти системний процес отримання об'єктивних якісних і кількісних оцінок заходів безпеки, процесів та процедур відповідно до визначених критеріїв та показників безпеки, вимог міжнародних стандартів, чинного законодавства України, відомчих нормативно-правових актів.

Аудит ІБ є обов'язковим механізмом контролю і проводиться незалежними експертами, які мають відповідну кваліфікацію та досвід. Процедура аудиту ІБ дозволяє керівництву отримати об'єктивну інформацію про стан захищеності ІС. Однак, як показує практика, керівництво і особовий склад найчастіше розуміють суть цієї процедури по-різному.

Аудит ІБ є комплексом робіт, що включає дослідження усіх аспектів забезпечення ІБ, проводиться за планом, відповідно до обраної методики і критеріїв. Метою даної публікації є детальне обґрунтування особливостей та головних критеріїв раціонального вибору і застосування різних видів аудиту ІБ.

Основними цілями проведення робіт з аудиту ІБ є:

- ідентифікування загроз та виявлення імовірних каналів витоку службової інформації у ІС;
- розроблення політики безпеки [1] та супровідних документів;

- інвентаризування інформаційних активів ІС та їх подальше категоріювання;
- розроблення та запровадження системи управління ризиками ІБ;
- забезпечення відповідності прийнятих технічних рішень вимогам чинного законодавства та галузевих норм [2];
- незалежне оцінювання поточного стану захищеності інформаційної структури ІС та мінімізування збитків від інцидентів безпеки.

У якості критеріїв процедури аудиту ІБ пропонуємо використовувати:

- міжнародні, національні та галузеві стандарти;
- законодавчі та нормативні акти у галузі безпеки ІС;
- внутрішні організаційно-розпорядчі документи системи МВС;
- вимоги, сформульовані за результатами оцінювання ризиків ІБ.

Одним з найпоширеніших видів аудиту є активний аудит. Це дослідження стану захищеності інформаційної системи (ІС) з точки зору зловмисника, що володіє високою кваліфікацією в області сучасних інформаційних технологій (ІТ). Найчастіше процедуру активного аудиту іменують інструментальним аналізом захищеності ІС, щоб виокремити цей вид аудиту від інших.

Суть активного аудиту полягає у тому, що за допомогою спеціального програмного забезпечення (у тому числі систем аналізу захищеності) і спеціальних методів здійснюється збір інформації про стан системи захисту спеціалізованої ІС.

При здійсненні даного виду аудиту на систему захисту ІС моделюється якомога більша кількість мережевих атак, які може здійснити зловмисник. При цьому аудитор штучно ставиться саме у такі умови, в яких працює зловмисник, – йому надається мінімум інформації, тільки та, яку можна отримати з відкритих джерел.

Активний аудит умовно можна поділити на два види – «зовнішній» і «внутрішній».

При «зовнішньому» активному аудиті фахівці моделюють атаки на зовнішний периметр корпоративної мережі і окремі

вузли спеціалізованої ІС «зовнішнього» зловмисника. У даному випадку проводяться такі процедури:

- визначення доступних з зовнішніх мереж IP-адрес корпоративної мережі спеціалізованої ІС;
- сканування даних адрес з метою визначення працюючих сервісів, а також призначення відсканованих хостів;
- визначення версій сервісів сканованих хостів;
- вивчення трафіку корпоративної мережі;
- збір інформації про систему безпеки ІС з відкритих джерел;
- аналіз отриманих даних з метою реалізування загроз.

Однак, всупереч поширеним уявленням, загрози зовнішньому периметру корпоративної мережі не є найбільш критичними для безпеки інформаційних активів ІС. Інсайдерські загрози (загрози, які виходять від своїх же працівників) є на порядок вищими, ніж загрози зовнішні.

«Внутрішній» активний аудит за складом робіт аналогічний до «зовнішнього» і проводиться з використанням спеціальних програмних засобів моделювання загроз від «внутрішнього» зловмисника.

З огляду на специфіку функціонування спеціалізованих ІС підрозділів МВС у ході активного аудиту необхідно виконувати ряд додаткових досліджень, безпосередньо пов'язаних з оцінюванням стану системи безпеки, зокрема – проведення спеціалізованих досліджень. Це пов’язано з використанням спеціалізованого програмного забезпечення (ПЗ) призначеного для вирішення спеціальних завдань. Подібне ПЗ унікальне, тому готових засобів і технологій для аналізу їх захищеності не існує.

Експертний аудит можна умовно подати як порівняння стану системи захисту ІС з «ідеальним» описом.

Ключовий етап експертного аудиту – аналіз системи захисту проекту ІС, топології корпоративної мережі та технології оброблення інформації, у ході якого виявляються недоліки існуючої системи захисту, які знижують рівень захищеності ІС [3]. За результатами робіт даного етапу пропонуються зміни в існуючій ІС і технології оброблення інформації, спрямовані на усунення виявлених недоліків.

Наступний етап – аналіз інформаційних потоків. На даному етапі визначається критичність інформаційних потоків ІС та використовуються методи забезпечення ІБ, що відтворюють рівень захищеності інформаційного потоку.

На підставі результатів даного етапу робіт пропонується захист або підвищення рівня захищеності тих компонент ІС, які беруть участь в найбільш важливих процесах передавання, зберігання та оброблення інформації. Застосування аналізу рівня критичності інформаційних потоків дає можливість реалізувати систему захисту, яка відповідає принципу розумної достатності.

Особлива увага на етапі аналізу інформаційних потоків надається визначенню повноважень і відповідальності конкретних осіб за забезпечення ІБ різних ділянок ІС. Повноваження і відповідальність повинні бути закріплені положеннями організаційно-розпорядчих документів. Організаційно-розпорядчі документи оцінюються на предмет достатності та несуперечності декларованим цілям і заходам ІБ

У рамках експертного аудиту проводиться аналіз організаційно-розпорядчих документів, таких як політика інформаційної безпеки, план захисту і різних настанов з ІБ.

Аудит на відповідність стандартам. Суть даного виду аудиту найбільш наближена до тих формулювань, які існують у фінансовій сфері. При проведенні даного виду аудиту стан системи захисту ІС порівнюється з якимось абстрактним описом, який подається у стандартах. Офіційний звіт, підготований у результаті проведення даного виду аудиту, включає наступну інформацію:

- ступінь відповідності ІС обраним стандартам;
- ступінь відповідності власним внутрішнім вимогам в області ІБ;
- кількість і категорії отриманих невідповідностей і зауважень;
- рекомендації з побудови або модифікування системи забезпечення ІБ, що дозволяють привести її у відповідність з даним стандартом;
- докладне посилання на основні документи замовника, включаючи політику безпеки, опис процедур забезпечення

ІБ, додаткові обов'язкові і необов'язкові стандарти і норми, які застосовуються до даної компанії.

Далі подано перелік стандартів, на відповідність яким проводиться аудит системи ІБ: ISO/IEC 27002:2005 Інформаційні технології. Методи захисту. Кодекс практики для управління інформаційною безпекою; ISO/IEC 27003:2010 Інформаційні технології. Методи захисту. Керівництво з застосування системи менеджменту захисту інформації; ISO/IEC 27004:2009 Інформаційні технології. Методи захисту. Вимірювання; ISO/IEC 27005:2008 Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки; ISO/IEC 27006:2007 Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікування систем управління інформаційною безпекою.

Спеціалізовані ІС підрозділів МВС, у яких обробляється інформація з обмеженим доступом (ІзОД), відомості, що становлять державну таємницю, відповідно до чинного законодавства обов'язково підлягають атестуванню за участю органу уповноваженого Кабінетом Міністрів України [4].

ЗАПОБІГАННЯ РОЗГОЛОШЕННЮ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ЧЕРЕЗ СОЦІАЛЬНІ МЕРЕЖІ

Цибуляк Б.З.,
доцент кафедри управління інформаційною безпекою ЛДУБЖД к.ф.-м.н.
Шиптицька І.І.,
студент ЛДУБЖД
Любовецька Я.О.,
студент ЛДУБЖД

Використання передових інформаційних технологій та досягнень науково-технічного прогресу дало людям неабиякі можливості для спілкування. Соціальна мережа – це структура, що базується на людських зв'язках або ж взаємних інтересах. В якості інтернет-сервісу соцмережа може розглядатися як платформа, за допомогою люди можуть здійснювати зв'язок між собою та групування за специфічними інтересами. Завдання такого сайту полягає у тому, щоб забезпечити користувачів всіма можливим шляхами для взаємодії один з одним – відео, чати, зображення,

музика, блоги та інше [1]. Сьогодні користувачами соціальних мереж є десятки мільйонів людей. На сторінках цих сервісів користувачі проводять багато годин на день бо соціальні мережі у значній мірі задовольняють потреби у спілкуванні. Але оскільки такі місця згуртовують багатьох людей, тут також полюють кіберзлочинці.

Проте за привабливістю соціальних мереж приховаються деякі небезпеки, про які потрібно знати. Найбільший недолік соціальних мереж – публікація у вільному доступі конфіденційної інформації про людину. Більшість мереж збирають значно більше особистих даних, ніж фактично вимагається для реєстрації. Так, якщо постаратися, через соціальні мережі можна дізнатися про людину практично усе. За допомогою програм, що розпізнають особу по фотографії і дозволяють знайти в Глобальній мережі усі матеріали, з нею пов'язані, ми можемо дізнатися про людину значно більше, ніж вона хоче про себе розповідати. Для прикладу, в США соціальні мережі регулярно використовуються поліцією для пошуку інформації. Абсолютно усе, що ми викладаємо в соціальні мережі, залишається там назавжди. Пошукові машини також зберігають усю інформацію в кеші при індексації, так що бути упевненим в тому, що усі небажані матеріали видалені, не можна. Також існує можливість обману користувача такої мережі. Адже існують шахраї, що усілякими способами намагаються одурити нас та заробити на цьому. Саме тому не слід видавати свою особисту інформацію незнайомцям.

Сьогодні злам аккаунта в «Вконтакті», спустошення вашого електронного гаманця або викрадення пошти стали настільки буденними речами, що на них вже ніхто не звертає уваги. Головною причиною, по якій користувачі стають жертвами шахраїв, дотепер залишається їхня зайва довірливість. Багато людей не розуміють, що інформація, розміщена ними в соціальних мережах, може бути знайдена і використана ким завгодно, у тому числі не обов'язково з добрими намірами. Інформацію про учасників соціальних мереж можуть знайти їхні роботодавці, батьки, діти, колишні або теперішні дружини чи чоловіки, збирачі боргів, злочинці, правоохоронні органи тощо.

Наприклад, наприкінці зими 2012 року десятки користувачів «Одноклассников» зіткнулися з «новим» для себе видом

шахрайства. Зловмисники створювали підроблені профілі родичів або знайомих потенційної жертви, втиралися в довіру і надсилали особисті повідомлення з проханням відправити їм код, що прийшов на телефон жертви. Ці коди використовувалися соціальною мережею для придбання віртуальної валюти. В результаті зловмисники одержували прибуток, а довірливі користувачі розлучалися з реальними грошима зі своїх телефонних рахунків.

Першопричиною такого шахрайства є безпечність самих користувачів соціальних мереж, що залишають про себе дуже багато конфіденційної інформації (контактні дані, адреси, номери телефонів тощо) у відкритому доступі. Зловмисники в будь-який момент можуть використовувати цю інформацію в незаконних цілях.

Інформація про ваше фінансове становище є, мабуть, однією з найбільш секретних. У жодному разі не можна повідомляти про розмір вашої заробітної плати та про те, де ви її отримуєте і зберігайте. Під грифом секретності повинна залишитися й інформація про вашу організацію. Не публікуйте повідомлень особистого характеру на так званій «стіні». Не треба забувати про те, що шедеври на «стіні» бачить не лише одержувач, але й інші користувачі. Тому перед тим, як відправити чергове повідомлення провокаційного змісту, задумайтеся, чи не зашкодить воно адресату.

Для дітей наслідки безконтрольного спілкування з Інтернетом можуть бути найбільш непередбачуваними. У соціальних мережах, як і колись у реальному дворі, можна зустріти і друзів, і ворогів, і хуліганів, і відвертих негідників. Інститут соціології НАН України у 2009 році провів Всеукраїнське соціологічне дослідження, яке виявило тривожні тенденції: понад 28% опитуваних дітей готові надіслати свої фото незнайомцям в Інтернеті; 17% – без вагань діляться інформацією про себе і свою родину (адреса, професія, графік роботи батьків, наявність цінних речей у домі тощо). Близько 14% опитуваних час від часу відправляють платні SMS за бонуси в онлайн-іграх і лише дехто звертає увагу на вартість послуги. Лише у 11% батьків знають про такі онлайн-загрози, як «дорослий» контент, азартні ігри, онлайн-насилля, кіберзлочинність. Спілкуючись у

соціальних мережах, дитина може легко стати жертвою шахраїв та педофілів. Діти, на відміну від дорослих, зовсім інакше реагують на симпатію, проявлену до них незнайомими людьми. І, не відчуваючи небезпеки, можуть відверто розповісти їм про свої захоплення, проблеми, сумніви і тривоги. А досвідчений маніпулятор може легко скористатися цією інформацією зі своєю мерзенною метою.

Ще одною небезпекою є те, що спілкуючись у соціальних мережах тривалий час, діти втрачають здатність до реального спілкування. Як правило, діти спілкуються у мережі зі своїми ж однокласниками або однолітками, тому говорити про абсолютну заміну реального спілкування віртуальним не варто. Найчастіше у мережевому «павутинні» губляться замкнуті, сором'язливі підлітки, яким у реальності складно налагодити будь-які соціальні відносини. Потрапивши у соціальну мережу, дитина відмежовується від батьків, перестає підтримувати з ними відносини. Віддалення від сім'ї – нормальний етап дорослішання. Без цього підліток не зможе збагнути свою унікальність, знайти власне місце під сонцем. Ця стадія розвитку дитини збігається з періодом активної соціалізації, який, як уже зрозуміло, протікає не лише у реальному, а й у віртуальному світі [2].

Тому для підвищення рівня безпеки при роботі в соціальних мережах пропонуємо користувачам дотримуватись ряду нескладних правил.

- розміщення в Інтернеті особистої інформації наражає користувачів на ризик втратити роботу або стати жертвою шахрайства чи знущань;
- вибовкувати все, що лишень прийде в голову – не найкраща ідея, проте мільйони людей саме це щодня й роблять. Більшість з них досі не розуміють, до яких наслідків може призвести також їхня онлайн-поведінка в соціальних мережах на кшталт Facebook, LinkedIn тощо;
- щиро оповідаючи про свої емоції та почуття, ми полегшуємо завдання шахраям, які забажають втертися до нас у довіру та викликати співчуття, а також стаємо зручною мішенню для кібер-знущань та принижень;
- розміщене необережне фото чи коментар здатні зруйнувати репутацію, кар'єру чи навіть привести до суду. Наприклад,

професору з Північної Дакоти вдалося одержати компенсацію в 3 мільйони доларів від свого колишнього студента, який написав, що викладач є педофілом [3];

- думай перед тим, як писати щось у Twitter чи іншу соціальну мережу, адже це може побачити будь-хто;
- не пишіть, де знаходитесь саме зараз. Одна справа зателефонувати вашим друзям і повідомити, що ви спізнюєтесь на зустріч. І зовсім інша – повідомити 47 вашим «друзям», половину з яких ви ніколи не бачили, що повертатиметесь додому пізно й самі;
- не викладайте в мережу інформацію про ваше життя. Викладання подробиць про те, до якої школи ви ходили або ваше дівоче прізвище, може призвести до того, що з часом злодії знатимуть про вас не менше, ніж ваша сім'я;
- бережіть інформацію про інших людей;
- поменше пишіть про дорогі покупки. Злодії вишукують людей, з яких можна поживитися. Коли ви розповідаєте про дорогі подарунки, які накупили до свят, то даєте іншим сигнал, що не завадило б понишпорити у вашому домі чи авто;
- не дайте злодіям дізнатися, що вас немає вдома. Крадіжка – ризикована справа, а тому завжди безпечніше лізти у пустий будинок: можна винести все, що забажаєш, і більш того – піти чистим. Не пишіть про те, що їдете з дому або й взагалі де живете;
- бережіть інформацію про своїх дітей. Чим менше інші люди знають про ваших і чужих дітей, тим краще. Не пишіть про їхнє місцеперебування, звички, уподобання, друзів, гуртки після школи. Безпека дітей – це найважливіша річ;
- ризик стати жертвою переслідування цілком реальний. Зустрічатися особисто зі своїми новими друзями з Twitter варто лише у публічних місцях;
- не розповідайте подробиці, які хулігани можуть використати, щоб підколювати вас у мережі. Дражняться не тільки злі діти;
- не діліться інформацією, що може зашкодити вашій репутації. Невлучними жартам, політичними тирадами, дурни-

ми витівками завдяки сучасним технологіям та соціальним мережам ви можете миттєво знищити свою репутацію;

- не ображайте і не брешіть про ваших рідних, друзів чи колег. Плітки про друзів можуть стати для вас справжньою халепою. Пам'ятайте, за руйнування чужої репутації доведеться відповідати.

Отже, кожен користувач повинен сам дбати про конфіденційність своєї інформації, оскільки від наявності чи відсутності особистих даних соціальна мережа нічого не втрачає, а зловмисникам це лише на руку.

1. Пішковцій С. Що таке соціальні мережі? [Електронний ресурс]. – Доступний з http://blogoreader.org.ua/2008/04/09/about-social-networks/
2. Діти і соціальні мережі. [Електронний ресурс]. – Доступний з http://skola36.ucoz.ru/4_batk.doc
3. Forbes: правила безпеки в соціальних мережах. [Електронний ресурс]. – Доступний з http://life.pravda.com.ua/technology/2010/11/19/65605/

ОРГАНІЗАЦІЯ І ТАКТИКА ПРОТИДІЇ ОРГАНІЗОВАНИМ ЗЛОЧИННИМ УГРУПОВУВАННЯМ У СФЕРІ ЕКОНОМІЧНИХ ВІДНОСИН

Шаранич Р.С.,
курсант ННІПККМ НАВС

Організація ефективної системи протидії організованим злочинним угруповання у сфері економічних відносин є однією з найактуальніших соціальних проблем сучасності, вирішення якої для багатьох країн світу є надзвичайно важливою і складною справою.

Чітка організація, стійкі зв’язки членів угруповання – це саме ті елементи, що дозволяють вчиняти з найбільшою ефективністю економічні злочини, створюючи при цьому складні та заплутані схеми. Тому організована злочинність представляє найбільшу зацікавленість при розробці методик попередження економічної злочинності.

Надмірне державне втручання в економіку неминуче призвело до уповільнення темпів економічних реформ, до корумпованості держапарату.

У свідомості населення втрачено цінність продуктивної праці як джерела благополуччя і головного засобу самореалі-

зації особистості; досить поширеним стало уявлення стосовно можливості легкодосяжного благополуччя шахрайським шляхом через спекулятивні операції, участь у несумлінних фінансових «іграх», кримінальному бізнесі.

Проблема виживання, як і проблема первісного накопичення капіталу, вирішуються сьогодні в Україні за допомогою активного включення населення у різні процеси, що розгортаються в рамках «тіньової» економіки. Люди перестають довіряти державній владі, все більше звертаючи свій погляд у бік «тіньового» капіталу і криміналітету.

Криміналізація банківської сфери містить особливу небезпеку, оскільки, по-перше, є загрозою для стабільності у кредитно-фінансовій системі; по-друге, призводить до підпорядкування злочинним угрупованням ключових сегментів ринку, формування фінансової бази для «зрощування» організованої злочинності з різними органами державної влади за допомогою корупції.

Держава внаслідок існуючих протиріч між галузями влади, проявів сепаратизму, місництва і користолюбства вищих чиновників втратила важливі важелі забезпечення єдиної законності і конституційного правопорядку.

Серед причин низької ефективності протидії цим негативним явищам головними є відсутність системної та скоординованої роботи щодо ліквідації економічного підґрунтя організованої злочинності та корупції, а також недостатня увага профілактичній роботі, насамперед, засобами оперативно-розшукової діяльності.

Через відсутність процесуальних механізмів реалізації багатьох законодавчих положень, зокрема п. 3 ст. 12 та ст. 14 Закону України «Про організаційно-правові основи боротьби з організованою злочинністю», діяльність оперативних підрозділів не має наступального характеру, що є однією з основ в успішної та ефективної боротьби із ОЗУ у сфері економічних відносин.

Не менш важливим є вдосконалення взаємодії державних органів, що здійснюють регуляторні функції в різних галузях економіки, з правоохоронними органами й органами місцевої влади, а пріоритетним напрямом цієї взаємодії повинно стати проведення спільних скоординованих заходів щодо протидії

корупції, перекриття каналів легалізації доходів, одержаних злочинним шляхом, унеможливлення відтоку валютних коштів за кордон, зокрема в офшорні зони, забезпечення реального відшкодування збитків, завданих громадянам, суб'єктам господарювання та державі протиправними діями.

Необхідним елементом у підвищенні ефективності правоохоронних органів є створення інформаційного обміну між суб'єктами взаємодії Єдиної комп'ютерної інформаційної системи правоохоронних органів з питань боротьби зі злочинністю (Постанова Кабінету Міністрів України від 8 квітня 2009 р. № 321 «Про затвердження Державної програми інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов'язана з боротьбою із злочинністю»).

Як одним із заходів організації боротьби доцільно було б встановити кримінальну відповідальність державних службовців за надання ними неправдивих відомостей під час декларування витрат (щодо придбання нерухомості, транспортних засобів, коштовностей, антикваріату та предметів мистецтва, цінних паперів, депозитів у банках тощо).

Слід ужити заходів для запобігання фіктивним банкрутствам, зокрема шляхом уведення представників держави й акціонерів до складу ради кредиторів, що дозволило би безпосередньо працівникам правоохоронних органів здійснювати контроль за даною процедурою щоб унеможливити будь-якого роду порушення.

Важливою складовою є належне наукове супроводження боротьби з організованою злочинністю і тому доцільно створити міжвідомчу аналітичну групу щодо аналізу стану, структури й тенденцій організованої злочинності, факторів, що її детермінують, особливостей поширення в регіонах країни, визначення економічного підґрунтя.

Ефективність протидії організованій економічній злочинності, поряд з іншим, залежить також від належного рівня професійної компетентності працівників правоохоронних органів, опанування сучасних методів виявлення, розслідування та попередження злочинів

Загрозливе становище в фінансово-економічній сфері внаслідок її криміналізації може бути зупинено лише на основі

реалізації демократичних принципів законотворення і подолання тенденції до знецінення норм права не лише підприємницькими структурами, а й державними чиновниками.

Одним із шляхів подолання економічної злочинності як в Україні, так і в інших країнах з розвиненою економікою, є послідовне вдосконалення нормативних законодавчих актів, адже нечітко сформульовані законодавцями терміни і поняття дають можливість їх різнобічної юридичної інтерпретації

Доцільним є також запозичення досвіду роботи правоохоронних органів високо розвинутих економічних країн.

ІІ. СУЧАСНИЙ СТАН, ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У НАВЧАЛЬНОМУ ПРОЦЕСІ

ТЕХНОЛОГІЧНІ ПІДХОДИ В ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЯХ НАВЧАННЯ

Сеник В.В.,
доцент кафедри ОРД та спецтехніки ЛьвДУВС, к.т.н., доцент
Кульчицький І.М.,
професор кафедри інформаційних технологій ЛьвДУВС, к.т.н., доцент
Магеровська Т.В.,
доцент кафедри інформаційних технологій ЛьвДУВС, к.ф.-м.н.

На сучасному етапі розвитку освіти ні для кого не є таємницею, що інформаційні технології навчання необхідно впроваджувати і розвивати у вищих навчальних закладах, оскільки відставання в даному напрямку розвитку науки є втратою технологічних орієнтирів як освіти, так і держави в цілому.

У зв'язку з цим важливо було б провести загальний аналіз теоретичних моделей найпопулярніших технологій навчання, а також аналіз тих властивостей інформатизації, які зумовили надзвичайно широкі можливості проникнення нових інформаційних технологій у сферу освіти.

Одним з основних напрямків, які зумовлюють широке впровадження інформаційних технологій в процес навчання є те, що відтворення копії інформаційного продукту на комп'ютері значно дешевше масового виробництва копій будь-якого іншого товару. Сучасні можливості подання інформації забезпечують якісний і адекватний вплив на всі органи сприйняття, а засоби віддаленої доставки інформації забезпечують всепроникливість і зручний доступ до інформації.

Окрім цього існує значна кількість переваг, які приносять комп'ютерні технології в процес навчання. Серед них:

- велика гнучкість у виборі місця і часу навчання;
- навчальні і тренувальні матеріали можуть легко поновлюватися;
- студенти, а не викладачі, можуть управляти вибором навчального матеріалу, комбінуючи курси різних навчальних закладів;
- здатність стежити за виконанням інструкцій особою, що навчається, запам'ятовувати її відповіді, фіксувати доступ до навчальних матеріалів;
- можливість моделювання аналізу середовища і ситуації взаємодії з тим, хто навчається;
- забезпечення on-line зв'язку між студентом і віддаленим викладачем;
- привабливість для сприйняття мультімедійного представлення інформації;
- можливість організації контролю за порядком і темпом подачі матеріалу, навчальною активністю;
- забезпечення ефекту симуляції складних процесів без ризику і з надзвичайно низькими витратами;
- можливість налагодження сервісу навчання і тренінгу на осіб з різним рівнем здібностей;
- можливість ефективної доставки для користувача широкого діапазону тренувального матеріалу;
- доступ до розподілених банків інформаційних ресурсів, навчальних і контролюючих матеріалів;
- потенціал величезного за діапазоном і глибиною репозитарію змістовної навчальної інформації;
- свобода у пошуку і відборі матеріалу, співзвучного власним цілям і завданням навчання;
- забезпечення більшого контролю з боку студента за процесом;
- надання умов для створення середовища конкуренції навчальних курсів;
- можливість ефективного поширення накопиченого досвіду;
- можливість організації незалежного централізованого і уніфікованого вихідного контролю знань і навичок;

- пристосованість для реалізації моделі безперервної освіти;
- забезпечення ефекту групової співпраці, створення корисного дискусійного середовища і ефективної спеціалізації учасників віртуальних робочих груп;
- симуляція технологічного середовища представлення освітніх послуг, створення віртуальних навчальні закладів [1].

Акцентування уваги на окремих привабливих сторонах організації процесу навчання призвело до проектування декількох моделей нових технологій навчання. Кожна з них, як правило, експлуатує невелике число ідей:

- низьку собівартість надання освітніх послуг;
- розвиток пізнавальної активності студентів;
- зручність доступу до величезних гетерогенних джерел інформаційної підтримки навчальної діяльності;
- безперервний характер навчання;
- групову синергію (системне поєднання) і спеціалізацію;
- відхід від неефективної процедурної моделі організації навчання;
- перехід від моделі навчання, орієнтованої на викладача до студенто-орієнтованої моделі.

На практиці спостерігається тенденція об'єднання фрагментів нових технологій, що добре себе зарекомендували, з метою використання всього кращого в контексті суб'єктивного досвіду і місцевих умов. Проте, вважаємо за важливе дати коротку характеристику найбільш популярних технологічних підходів [1].

Інструктивне дистанційне навчання базується на ідеї дистанційної доставки широкого спектру інструктивних навчальних матеріалів. Навчання, як правило, забезпечується процедурною схемою надання змістовної інформації, повчальних симулюючих програм, ілюстративних і довідкових даних, контрольних завдань і тестів.

Портфель навчальних інструктивних матеріалів може набиратися з різних курсів, підготовлених в різних закладах освіти. Завдяки конкуренції навчальних матеріалів забезпечується необхідний рівень якості. Вихідний контроль проводиться, як правило, централізовано і незалежно від творців навчальних

курсів спеціально організованими сервісними тестовими службами і акредитуючими організаціями. Це виключає необ'єктивну і неузгоджену процедуру оцінювання, передбачає вхідний контроль і індивідуалізацію процесу навчання. Навчання часто супроводжується заздалегідь запланованими сеансами on-line консультацій. Найсильними чинниками розвитку вважаються цінове змагання курсів і модуляризація (або артикуляція) навчальних планів, тобто можливість відбору найкращих модулів з запланованого навчальним планом стандартного сертифікованого набору, які можуть бути підготовлені різними університетами.

Ресурсно-орієнтоване навчання – філософія і методологія навчання, яка забезпечує викладачів цілісним підходом до організації навчального процесу. Воно направлене не лише на засвоєння знань і придбання навичок, але і на тренінг здібностей самостійного і активного перетворення проблемно-інформаційного середовища шляхом розкриття і практичного застосування інформаційних ресурсів. Студенти розвивають навички інформаційної культури завдяки направляючій викладачами практиці вирішення задач, що вимагають інформації з багатьох джерел. Студенти замість готових знань отримують допомогу в тому, щоб поступово розвинути спеціальні навички, що забезпечують своє власне саморозкриття тем курсу, з'єднуючи разом інформаційні нитки для формулювання важливих знань по темі.

Посилення автономії – одна з істотних рис даної технології навчання – виявляється у вмінні студентів того, як взяти на себе відповідальність за визначення того, що вони повинні вчити, де і як знайти інформацію, що найкращим чином розкриває дану тему, яким чином зафіксувати і інтерпретувати інформацію, як її оцінити, як взаємодіяти з колегами по обробці інформації, як організовані інформаційні зв'язки і доступ до інформації, як інформація засвоюється в процесі навчання.

Взаємодія студентів з безліччю ресурсів (книги, журнали, газети, мультимедіа, телебачення, Internet, суспільство, контакти з людьми) мотивує студентів навчатися теми, намагаючись знайти інформацію багатьма шляхами і у всіх місцях, де це тільки можливе. Заохочення студентів у самостійних спробах спрямовувати інформаційні пошуки зміцнює почуття упевненості і самоуправління навчанням, а досягнення інформаційних

цілей сприяє ефективному закріпленню інформаційно-складальних і інформаційно-обробляючих шаблонів.

Ресурсно-орієнтоване навчання – студенто-центроване, воно спирається на посилання, що студенти навчаються в процесі діяльності і індивідуального формування змісту. Такий процес навчання слідує реальному життю, в якому суб'єкт націлюється на постійне полювання за інформацією, на її інтерпретацію і використання, стаючи самокерованим студентом. Накопичений досвід роботи з інформаційними ресурсами дозволяє студенту сформувати репертуар навичок і основ знань, які можуть бути використані в ситуаціях навчання у майбутньому.

Перевагою розглянутої технології вважається те, що навчальна діяльність відбувається на фоні пізнавальних, соціальних, навичкоформуючих і практичних цілей та має тенденцію бути міждисциплінарною.

Ресурсно-орієнтоване навчання, мотивуючи активну і творчу включеність учнів передбачає також використання сил групової взаємодії, дослідження проблем у складі невеликих груп, критичні обговорення, мозкові штурми і т.д.

Діалогічність навчання передбачає створення середовища циркуляції потоків значущих сутностей між учасниками обговорень, кожний з яких відкритий для реконструкції власної моделі знань і переконань. Тут кожний учасник говорить, або готується щось сказати, і кожний захищає свою точку зору, засновану на спостереженні, інтерпретації, припущенні або узагальненні. Ефективне обговорення передбачає підтримку динамічного балансу між відстоюванням своєї точки зору і дослідженням області пов'язаних з нею висновків.

Групова синергія разом з усім пов'язаним з предметом обговорення контекстом – істотна складова навчання через співпрацю. Інформаційні технології можуть тут дати в доступ величезні бази даних та інформаційні ресурси для ідентифікації можливих взаємозв'язків і взаємозалежності між різними елементами знань.

У процесі співпраці колективне навчання може протікати на різних стадіях посилення зв'язків від кооперації до співпраці, супроводжуючись підвищенням складності і конфліктності, які

виступають як каталізатори самооновлення індивідуальної і колективної творчості.

1. http://www.pravo.vuzlib.org/book_z809_page_42.html

ПІДГОТОВКА ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У НАВЧАЛЬНИХ ЗАКЛАДАХ УКРАЇНІ

Грицюк Ю.І.,
завідувач кафедри управління інформаційною безпекою ЛДУ БЖД, д.т.н., професор
Фірман В.Ф.,
ЛДУ БЖД, к.т.н., доцент

Інформаційна безпека (ІБ) займається захистом інформаційних систем. Загалом під інформаційних систем (англ. Information system), як правило, розуміють сукупність організаційних і технічних засобів для збереження та оброблення інформації з метою забезпечення інформаційних потреб користувачів [2]. У таких системах з різних причин відбуваються інциденти – відтік чи втрата інформації, її спотворення, збої роботи системи [3]. Звідси виникає мета захисту інформаційних систем: ІБ – це такий стан системи, при якому інциденти відбуваються відносно рідко, і збиток від них допустимо малий. Тому, головні вимоги до ІБ – цілісність, доступність і конфіденційність інформації на всіх етапах її життєвого циклу.

ІБ недосяжна тільки при застосуванні певного рішення, разової послуги або комплексу заходів. ІБ – це безперервний системний комплексний процес, який інтегровано у всі бізнес-процеси підприємства і вимагає участі всіх користувачів системи, – внутрішніх, зовнішніх і тимчасових. Але навіть в цьому випадку 100%-на ІБ недосяжна. Термін «забезпечення ІБ» застарілий. Зараз прийнято говорити про управління ІБ [1, 4].

Управління ІБ – оптимізаційна задача, основна мета якої полягає в відшукуванні компромісу між рівнем захисту інформації та її вартістю. Причому, ціною ІБ є як разові інвестиції, так і постійні витрати, як прямі, так і опосередковані, зокрема – зниження зручності роботи з інформацією. Оптимізація інвестицій в ІБ часто виконується інтуїтивно, але такий підхід непрозорий для керівництва підприємства [3].

Оптимальність і прозорість інвестицій в ІБ можна досягти шляхом застосування методів управління ризиками. Розумна служба ІБ розподіляє ресурси відповідно до величини ризиків, а не конкретних інцидентів. А мудра служба ще і робить управління ІБ прозорою для керівництва компанії і надає йому інструменти управління та контролю інвестицій і проектів щодо зниження ризиків. Як це робиться – одна з головних проблем ІБ.

Інформаційна безпека держави, як складова національної безпеки [5], визначається складною взаємодією багатьох чинників, серед яких провідне місце займає «чинник людини». Людина є основним носієм і користувачем інформації, вона ж є основним суб'єктом і об'єктом інформаційної боротьби. Тому в інформаційному світі рівень захищеності інформаційного простору держави значною мірою залежить від:

- рівня обізнаності її населення з проблемами інформаційної безпеки особистості, суспільства і держави;
- рівня спеціальної підготовки державного і військового керівництва, особового складу Збройних сил та інших силових міністерств і відомств;
- наявності й рівня фахової підготовки військових і цивільних фахівців відповідних структур інформаційної безпеки, які проводять постійний моніторинг інформаційного простору та здатні на адекватні дії для його захисту.

Таким чином, є актуальною проблема формування відповідної системи (узгоджених систем) підготовки зазначених категорій фахівців, зокрема системи підготовки фахівців у сфері інформаційної безпеки.

Система підготовки фахівців з вищою освітою в Україні [2, 3] базується на певних науково-педагогічних школах, які функціонують в тих чи інших вищих навчальних закладах з відповідною навчально-матеріальною базою, інфраструктурою для забезпечення повсякденної діяльності тощо. Для створення науково-педагогічних шкіл певної спрямованості, як свідчить досвід, необхідно 10-15 і більше років. Для часткової зміни їх завдань у межах традиційної спрямованості, розгортання і введення в навчальний процес нових навчальних комплектів техніки, формування контингенту студентів (слухачів) необхідно 8-4 роки.

Відомо, що наявна в Україні система підготовки фахівців є досить консервативною [3], має певну інерцію, що необхідно враховувати під час проведення реформування системи вищої освіти загалом, в тому числі системи підготовки фахівців з інформаційної безпеки, відповідно до цілей і завдань євроінтеграції України у сфері вищої освіти в контексті Болонського процесу, та переходу на нові Переліки напрямів, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційними рівнями бакалавра і магістра, що передбачено на 2009-2012 роки. Враховуючи те, що підготовка фахівців з вищою освітою у галузі інформаційної безпеки взагалі була розпочата тільки у 1997 році, є найбільш новою і водночас найбільш динамічною за об'єктом діяльності, актуальність розвитку системи підготовки фахівців з інформаційної безпеки є ще більш актуальною.

Проведення порівняльного аналізу систем підготовки фахівців з інформаційної безпеки не може бути повною без врахування, окрім підготовки суто цивільних фахівців, дещо специфічних систем підготовки аналогічних фахівців для силових міністерств і відомств, які були створені першими і зберігають координуючу роль у загальній системі. Досвід показує [2], що обидві категорії фахівців мають переважно споріднену за змістом підготовку і реалізують себе на споріднених об'єктах діяльності.

Для порівняльного аналізу визначимо декілька складових можливої структури системи підготовки фахівців з інформаційної безпеки:

- підготовка фахівців у галузі інформаційної безпеки (як для виявлення і нейтралізації інформаційно-технічних загроз інформаційній сфері машинно-технічних систем, іншим об'єктам інформаційної інфраструктури країни, так і загроз в гуманітарній сфері);
- підготовка фахівців для структур інформаційної безпеки та інформаційної боротьби збройних сил та деяких інших міністерств і відомств;
- спеціальна підготовка (перепідготовка, підвищення кваліфікації) з питань інформаційної безпеки органів державного (військового, корпоративного) управління визначених країн;

- загальна підготовка населення країни (адаптація до умов життя у інформаційному суспільстві).

В Україні на основі значних власних потенційних можливостей за останні роки також створена відповідна система, підготовка фахівців приведена до державних і, певною мірою, до міжнародних стандартів.

Підготовка фахівців з інформаційної безпеки була розпочата відповідно до спільного наказу Державної служби України з питань технічного захисту інформації та Міністерства освіти України від 28 грудня 1995 р., № 66/358 «Про співробітництво між Міністерством освіти України і Державною службою України з питань технічного захисту інформації».

До «Переліку напрямів та спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за відповідними освітньо-кваліфікаційними рівнями», який був затверджений Постановою Кабінету Міністрів України від 24 травня 1997 р., № 507, було внесено напрям 1701 «Інформаційна безпека» у складі п'яти спеціальностей.

З 2007 року і до сьогодні, відповідно до постанови № 787 від 27.08.2010 р. «Про затвердження переліку спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційними рівнями спеціаліста і магістра» система підготовки фахівців з інформаційної безпеки в Україні включає:

- групу стандартів системи вищої освіти галузі знань 1701 «Інформаційна безпека» (напрями: безпека інформаційних і комунікаційних систем; системи технічного захисту інформації; управління інформаційною безпекою);
- групи стандартів системи вищої освіти інших галузей знань, суміжних з 1701:
  - 0501 «Інформатика та обчислювальна техніка (комп'ютерні науки, комп'ютерна інженерія, програмна інженерія)»;
  - 0502 «Автоматика і управління (системна інженерія)»;
  - 0509 «Радіотехніка, радіоелектронні апарати та зв'язок (радіотехніка, телекомунікації)»;

- 0403 «Системні науки та кібернетика (прикладна математика, інформатика)»;

- групи стандартів системи вищої освіти деяких галузей знань та напрямів соціальних наук, бізнесу і права:
  - 0302 «Міжнародні відносини» (міжнародні відносини, міжнародна інформація);
  - 0303 «Журналістика та інформація (журналістика, реклама, зв'язки з громадськістю)»;
  - 0304 «Право» (право);
  - 0301 «Соціально-політичні науки» (соціологія, практична психологія, політологія);
  - 0201 «Культура» (документознавство та інформаційна діяльність);
  - 1601 «Військові науки, національна безпека» та деякі інші;
- ВНЗ різної відомчої приналежності, що здійснюють підготовку фахівців із зазначених напрямів (спеціальностей);
- система відповідних державних та комерційних курсів підвищення кваліфікації;
- профільні наукові організації й установи.

Провідними ВНЗ з підготовки фахівців напряму 1701 «Інформаційна безпека» в Україні є:

- Національний авіаційний університет;
- Національний технічний університет України (НТУУ «КПІ»);
- Національна академія Служби безпеки України;
- Київський національний університет імені Т.Г. Шевченка;
- Державний університет інформаційно-комунікаційних технологій (м. Київ);
- Харківський національний університет радіоелектроніки;
- Національний гірничий університет (м. Дніпропетровськ);
- Запорізький національний технічний університет;
- Національний університет внутрішніх справ (м. Харків) та ін.

Як і за кордоном, обсяги підготовки фахівців з інформаційної безпеки в Україні, порівняно із загальними обсягами підготовки фахівців, недостатні [3]. Особливістю підготовки фахівців з

інформаційної безпеки є динамічний розвиток об'єкта діяльності, а отже, і змісту навчання. Ця проблема має вирішуватись своєчасним оновленням змісту та інтеграцією базової та гнучкої курсової підготовки. З огляду на це негативними чинниками є:

- недостатні обсяги перепідготовки і своєчасного підвищення кваліфікації науково-педагогічних працівників, які забезпечують навчальний процес;
- недостатній рівень модернізації навчально-лабораторної бази ВНЗ за відповідними напрямами і спеціальностями;
- недостатні обсяги залучення до курсової підготовки (перепідготовки і підвищення кваліфікації) з питань інформаційної безпеки державних службовців і фахівців органів державного (корпоративного) управління, особливо середнього і старшого віку;
- недостатній рівень взаємодії між міністерствами і відомствами з питань підготовки фахівців з інформаційної безпеки, обміну програмами підготовки. Практика навчання державних службовців на курсах в Національній академії оборони України на сьогодні призупинена;
- надмірна комерціалізація курсів з інформаційної безпеки. Значна частина комерційного сегмента курсів є фактично представництвами іноземних компаній-виробників програмного продукту, що не зменшує інформаційну залежність України та не сприяє підвищенню ступеня контрольованості запозичених інформаційних технологій, впроваджених у різні сфери державного і корпоративного управління, забезпечення життєдіяльності країни.

Загалом в Україні завершено перший етап – створення системи підготовки фахівців з інформаційної безпеки. Але в контексті світового досвіду, сучасних і перспективних загроз в інформаційній сфері ця система потребує подальшого істотного розвитку в структурному і змістовному плані, а також покращення кадрового та матеріально-технічного забезпечення.

1. Сисоєв Валентин. Аналіз рівня освіти та підготовки фахівців з управління ІТ та інформаційної безпеки в Україні / Валентин Сисоєв // CISM, 23.02.2011 р. – 24 с. [Електронний ресурс]. – Доступний з http://auditagency.com.ua/blog/ISACA_ research_Education.pdf.

2. Бабак В.П. Підготовка фахівців із захисту інформації в Україні / В.П. Бабак, В.В. Козловський, В.О. Хорошко, Д.В. Чирков // Захист інформації. – 2001. – № 4. – С. 57-69.
3. Голубенко О.Л. Особливості підготовки фахівців із інформаційної безпеки / О.Л. Голубенко, О.С. Петров, В.О. Хорошко // Інформаційна безпека. – 2009. – № 2(2). С. 5-17. [Електронний ресурс]. – Доступний з http://www.nbuv.gov.ua/portal/natural/ Ibez/2009_2/1.pdf.
4. Грицюк Ю.І. Проблема підготовки фахівців з інформаційної безпеки структурних підрозділів Міністерства надзвичайних ситуацій України / Ю.І. Грицюк, Т.Є. Рак // Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту : матер. Міжнар. наук. конф. [зб. наук. праць у 2-ох т.], 16-20 травня 2011 р., м. Євпаторія. – Херсон : Вид-во ХНТУ. – 2010. – Т. 2. – С. 272-276.
5. Закон України «Про основи національної безпеки України» від 19.06.2003 р., № 964-IV. Редакція від 13.10.2012, підстава 5286-17. [Електронний ресурс]. – Доступний з http://zakon2.rada.gov.ua/laws/show/964-15.

ПРАВОВІ АСПЕКТИ НАУКОВОЇ ДІЯЛЬНОСТІ СТУДЕНТІВ

Кульчицький І.М.,
професор кафедри інформаційних технологій ЛьвДУВС, к.т.н., доцент
Магеровська Т.В.,
доцент кафедри інформаційних технологій ЛьвДУВС, к.ф.-м.н.
Сеник В.В.,
доцент кафедри ОРД та спецтехніки ЛьвДУВС, к.т.н., доцент
Фірман Л.Ю.,
ст.викладач кафедри природничо-математичних дисциплін Львівського інституту економіки і туризму

Наука – складова загальнолюдської культури. Донедавна розвиток цивілізації не вимагав з такою гостротою наявності наукового стилю мислення від кожної людини. Однак з ростом складності техніки, якою повинні користуватись люди різних професій, розвитком інформаційного суспільства, до кожної людини пред'являють інші вимоги – творчо мислити, бути вільним у виборі, бути відкритим та кмітливим мати справу з невизначеним та неоднозначним. Все це входить в поняття

наукового мислення, формування якого – важлива умова виживання і праці людини в інформаційному суспільстві.

Досягнутий рівень науково-технічного розвитку призвів до якісного стрибка у відносинах між наукою і практикою. Наука почала грати ведучу роль у вдосконаленні практики, рості продуктивних сил, покращенні планування і управління. Складний і достатньо динамічний процес розширення меж перетворювальної діяльності, настійливо вимагають вивчення закономірностей розвитку науки і розробки на цій основі принципів організації, планування і управління наукою в єдиній системі «наука – виробництво». Розробка теоретичних і методологічних основ управління розвитком науки буде сприяти підвищенню ефективності наукової діяльності, а, в кінцевому рахунку, і прискоренню прогресу, досягненню соціальних цілей суспільства.

Як передбачено Законом України «Про вищу освіту», у вищих навчальних закладах наукова та науково-технічна діяльність – невід'ємна інтегруюча складова навчання. Вона передбачає участь всіх учасників навчального-виховного процесу в науковому житті вишу у всіх його формах, чи то у розв'язку складних наукових проблем та упровадження результатів наукових досліджень і розробок, чи то участь у конкурсах, олімпіадах, наукових семінарах та конференціях, чи то просто оволодіння навичками дослідницької та творчої діяльності. Останнє допоможе в майбутньому бакалаврам, спеціалістам та магістрам порівняно легко увійти в професійну діяльність.

Так чи інакше, дослідницькою роботою займаються всі студенти вишів. Обов'язковою для них є та її складова, що входить до навчального процесу. Початком такої діяльності, напевно можна вважати реферування наукових видань та готування оглядів з новинок наукової літератури, що роблять студенти починаючи з першого курсу. Далі йде написання курсових робіт з окремих дисциплін, у яких повинні з'являтися вже перші, нехай прості, але свої ідеї та дослідження, виконання завдань дослідницького характеру в період виробничої та навчальної практик. Завершується навчання виконанням випускної кваліфікаційної роботи, у якій на сьогоднішній день, незалежно від типу – бакалаврська, спеціаліста, магістра, обов'язкова наявність самостійних досліджень. Окрім того при

оцінці кваліфікаційних робіт члени комісії обов'язково вразовують наявність наукових публікацій з теми роботи. Водночас студент має можливість займатись науковою діяльністю і в позанавчальний час. Це і участь у наукових гуртках та у виконанні госпрозрахункових наукових робіт у межах творчої співпраці кафедр і факультетів, і виступи на наукових конференціях, і робота в студентських інформаційно-аналітичних, юридичних консультаціях, туристських фірмах, перекладацьких бюро, і рекламна та лекторська діяльність тощо. Наукові лабораторії і гуртки, студентські наукові товариства і конференції – все це дозволяє студенту почати повноцінну наукову роботу, що є однією з форм самовиразу особистості студента, його прагнення до життєвого самоутвердження, яка розвиває його творче мислення, ініціативність, самостійність, вміння розбиратись у потоках інформації та відбирати необхідну.

З іншої сторони, матеріальне вираження будь-якої наукової діяльності це, в першу чергу, оформлення та оприлюднення своїх наукових результатів у середовищі зацікавлених осіб – публікація наукової роботи чи виступ на семінарі, конференції тощо. Наукова спільнота за час свого існування виробила свої правила і канони написання наукових робіт та участі в наукових зібраннях (сходинах), яких студенти мали б дотримуватись у своїй науковій діяльності.

Таким чином науково-дослідницька робота студентів (НДРС) – одна з важливих форм учбового процесу, мета якої максимально сприяти професійному росту майбутнього спеціаліста та забезпечити тяглість у формуванні наукових і професорсько-викладацьких кадрів. НДРС має такі особливості:

- її цілі підпорядковані навчальним;
- її основні мотиви – пізнавальні;
- її здійснюють під керівництвом викладачів;
- підчас наукової роботи у студента формується професійна самостійність; здатність до творчого вирішення практичних задач від початку трудової діяльності по завершенню навчання;
- вона сприяє розширенню відомостей для успішного вирішення організаційних, виховних та інших проблемних ситуацій, з якими можна зіткнутись у майбутньому;

- при виборі теми дослідження необхідно урахувати той час, який студент зможе виділити на її розробку з урахуванням усього навчального процесу та мають бути враховані всі можливості розробки теми з точки зору витрат матеріальних і фінансових ресурсів.

Таким чином задачі НДРС наступні:

- вивчення основ наукових досліджень, зокрема, поняття науки, наукового методу пізнання;
- освоєння методики наукових досліджень та наукової організації праці при їх виконанні, під час самостійного опрацювання літератури, плануванні та організації наукового експерименту, обробки експериментальних даних тощо;
- розвитку у студентів навичок наукових досліджень, методів та прийомів самостійного вирішення наукових та науково-технічних задач;
- прививанню студентам трудових навиків;
- активізації творчої діяльності студентів;
- розвитку у студентів здатності спілкуватись в колективах при довготривалому контакті з керівником та колегами по праці;
- запровадженню у практику результатів наукових досліджень.

НДРС передбачає:

- включення елементів наукових досліджень в навчальну програму:
  - участь у лекціях з науково-проблемних тем;
  - виступи на семінарських заняттях;
  - виконання лабораторних робіт з елементами наукових досліджень;
  - написання та захист рефератів з наукової проблематики;
  - виконання та захист курсових і випускних кваліфікаційних робіт;
- участь у всіх видах науково-дослідних робіт, олімпіадах, конкурсах;
- за результатами наукових досліджень оформлення звітів та підготовка і публікація наукових статей;

- виступи на конференціях, симпозіумах, наукових семінарах;
- роботу в складі наукових студентських об'єднань, гуртків, що уможливлює не лише ознайомлення з реальними задачами та розробку проектів їх вирішення, але й самим практично реалізовувати свої пропозиції.

Науково-дослідницька робота студентів базована на таких основних регламентуючих документах:

Загальна декларація прав людини (прийнята Генеральною асамблеєю ООН 10.12.1948)

Конституція України.

Закони України:

- «Про освіту» від 23.05.1991 № 1060-XII;
- «Про вищу освіту» із змінами від 19.01.2010 р. № 2984-III;
- «Про наукову і науково-технічну діяльність» із змінами від 19.12.2006 р. №1977-XII;
- «Про науково-технічну інформацію» від 25.06.1993 р. № 3322-XII, із змінами, внесеними згідно із Законами № 762-IV від 15.05.2003 р., № 1294-IV від 20.11.2003 р., 2938-VI від 13.01.2011 р.;

Укази Президента України:

- «Про Національну доктрину розвитку освіти» від 17.04.2002 р. № 347/2002;
- «Про невідкладні заходи щодо забезпечення функціонування та розвитку освіти в Україні» від 04.07.2005 р. № 1013/2005;
- «Про першочергові завдання щодо впровадження новітніх інформаційних технологій» від 20.10.2005 р. № 1497/2005;
- «Про додаткові заходи щодо підвищення якості освіти в Україні» від 20.03.2008 р. № 244/2008;
- «Про заходи щодо забезпечення пріоритетного розвитку освіти в Україні» від 29.09.2010 р. № 926/2010.

Постанови та розпорядження Кабінету Міністрів України:

- Постанова «Про Державну національну програму «Освіта» («Україна XXI століття»)» від 03.11.1993 р. № 896, із змінами, внесеними згідно з Постановою КМ від 29.05.1996 р. № 576;

- Постанова «Про затвердження Положення про державний вищий навчальний заклад» від 05.09.1996 р. № 1074, із змінами, внесеними згідно з Постановою КМ від 13.08.99 р. № 1487;
- Постанова «Про затвердження Положення про освітньо-кваліфікаційні рівні (ступеневу освіту)» від 20.01.1998 р. № 65;
- Постанова «Про затвердження Державної цільової науково-технічної та соціальної програми «Наука в університетах» на 2008-2017 роки» від 19.09.2007 р. № 1155, із змінами, внесеними згідно з Постановами КМ від 23.09.2009 р. № 10000, від 23.11.2011 р. № 1196;
- Постанова «Про затвердження Положення про дослідницький університет» від 17.02.2010 р. № 163, із змінами, внесеними згідно з Постановою КМ від 27.08.2010 р. № 786.

Нормативні документи Міністерства освіти і науки, молоді та спорту України:

- Наказ «Про затвердження Положення про організацію навчального процесу у вищих навчальних закладах» від 02.06.1993 р. № 161;
- Наказ «Про затвердження норм часу для планування і обліку навчальної роботи та переліків основних видів методичної, наукової й організаційної роботи педагогічних і науково-педагогічних працівників вищих навчальних закладів» від 07.08.2002 № 450;
- Наказ «Щодо Положення про організацію наукової, науково-технічної діяльності у вищих навчальних закладах III та IV рівнів акредитації» від 01.06.2006 р. № 422.

Нормативні документи Національного університету «Львівська політехніка».

Міждержавні та міжвідомчі нормативно-правові документи:

- Угода між Міністерством освіти і науки, молоді та спорту України та міністерством освіти і науки Російської Федерації про першочергові заходи з розвитку науково-освітнього співробітництва на 2010-2012 роки від 17 травня 2010;

- Меморандум про взаєморозуміння між Міністерством освіти і науки, молоді та спорту України та Корпорацією Microsoft від 28.10.2003.

Міжнародні та національні стандарти:

- ISO 5966:1982 «Documentation — Presentation of scientific and technical reports»
- ISO 4:1984 «Documentation — Rules for the abbreviation of title words and titles of publications»
- ISO 832:1994 «Information and documentation – Bibliographic description and references – Rules for the abbreviation of bibliographic terms»
- ДСТУ 3008-95 «Документація. Звіти у сфері науки і техніки. Структура і правила оформлення»;
- ДСТУ 3582-97 «Інформація та документація. Скорочення слів в українській мові у бібліографічному описі. Загальні вимоги та правила»;
- ДСТУ ГОСТ 7.1:2006 «Система стандартів з інформації, бібліотечної та видавничої справи. Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання»;
- ДСТУ 6095:2009 «Система стандартів з інформації, бібліотечної та видавничої справи. Правила скорочення заголовків і слів у заголовках публікації» (ГОСТ 7.88-2003, MOD);
- ДСТУ 7093:2009 «Система стандартів з інформації, бібліотечної та видавничої справи. Бібліографічний запис. Скорочення слів і словосполук, поданих іноземними європейськими мовами»;
- ГОСТ 7.12-93 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Сокращение слов на русском языке. Общие требования и правила»;
- ГОСТ 2.004-88. Загальні вимоги до виконання конструкторських і технологічних документів на друкуючих і графічних пристроях виводу ЕОМ.

1. Крушельницька О.В. Методологія та організація наукових досліджень: Навчальний посібник. – К.: Кондор, 2006. – 206 с.
2. Научно – исследовательская работа студентов http://www.csu.ru/main.asp?method=GetPage&p=982&redir=596
3. Основы научных исследований (учебное пособие). Автор: Сафонов А.А., редактор: Александрова Л.И. http://abc.vvsu.ru/Books/u_osnovy_nis/default.asp
4. Папковская П. Я. Методология научных исследований: Курс лекций. – Мн.: ООО «Информпресс», 2002. – 176 с.
5. Попов Г. Х. Техника личной работы.– 4-е изд., доп. и перераб. – М.: Сов. Россия, 1979. – 192 с.
6. Романчиков В. І. Основи наукових досліджень. Навчальний посібник. – К.: Центр учбової літератури, 2007. – 254 с.
7. Сабитов Р. А. Основы научных исследований: Учеб. пособие / Челяб. гос. ун-т. – Челябинск, 2002. – 138 с.
8. Цехмістрова Г.С. Основи наукових досліджень Навчальний посібник / Київ: Видавничий Дім «Слово», 2003. – 240 с.
9. Шейко В.М., Кушнаренко Н.М. Організація та методика науково-дослідницької діяльності: Підручник. – 5-те вид., стер. – К.: Знання, 2006. – 307 с.

ВИКОРИСТАННЯ МОБІЛЬНИХ ПРИСТРОЇВ ТА ТЕХНОЛОГІЙ В ОСВІТІ

Магеровська Т.В.,
доцент кафедри інформаційних технологій ЛьвДУВС, к.ф.-м.н.
Сеник В.В.,
доцент кафедри ОРД та спецтехніки ЛьвДУВС, к.т.н., доцент
Кульчицький І.М.,
професор кафедри інформаційних технологій ЛьвДУВС, к.т.н., доцент

Із стрімким розвитком інформаційних технологій зросла потреба швидкого доступу до інформації, що зумовило багатофункціональність мобільних пристроїв. Мобільні телефони, планшети, «рідери» можуть відтворювати музику, відео, запускати ігри, працювати як телефони, калькулятори, навігатори, точки доступу до мережі Інтернет. Тому особливо актуальним, на сьогоднішній день, є пошук нових підходів до організації навчального процесу і створення навчальних матеріалів, які б враховували можливості мобільних технологій.

Мобільне навчання (m-learning) – навчання, що проходить незалежно від місцезнаходження і відбувається з використанням портативних технологій. Воно являється підвидом дистанційного або електронного (e-leaning) навчання, які реалізуються в умовах віддаленості слухача і викладача на основі використання сучасних педагогічних й інформаційно-комунікаційних технологій, спрямовано на побудову знань з урахуванням індивідуального досвіду, практики і знань учнів.

Типовими ознаками мобільного навчання є:

- використання мобільних пристроїв, а саме телефонів (звичайні мобільні телефони, смартфони, комунікатори), портативних комп'ютерів (ноутбуки, нетбуки, планшети, КПК), пристроїв зберігання і відтворення інформації (електронні «рідери», плеєри);
- взаємодія учасників навчального процесу за допомогою бездротових мереж.

Вибір мобільного пристрою для навчання залежить в першу чергу від віку особи, що навчається. Наприклад, підлітки, як правило, віддають перевагу мобільним телефонам та плеєрам, дорослі – планшетним комп'ютерам та смартфонам. Також неварто забувати про те, що студенти використовують дані пристрої переважно для розваги та спілкування, а не для самоосвіти. Як показують дослідження, студенти найчастіше використовують тільки такі функції мобільних телефонів, як обмін SMS-повідомленнями і калькулятор. Також мало використовується програмне забезпечення мобільних телефонів, виключенням є вихід в Інтернет (68%) за допомогою браузера Opera Mini та використання Java ігр (45%). Отже, не дивлячись на достатньо високий рівень технічного оснащення, студенти не використовують всі функції мобільних пристроїв, які спонукають до самоосвіти і професійного росту.

Однак, більшість сучасних студентів технічно та психологічно вже готові до використання мобільних технологій в освіті, тому необхідно розглядати нові можливості для більш ефективного використання потенціалу мобільного навчання. Розв'язок цієї задачі потребує:

- прийняття нормативно-правових актів, що регламентують впровадження мобільного навчання в навчальний процес ВНЗ;

- розробки методичних рекомендацій щодо створення та наповнення мобільних інформаційних ресурсів і використання мобільних пристроїв у навчальному процесі;
- розробки методичних рекомендації щодо розрахунку навчального навантаження;
- створення дистанційних курсів, електронних підручників, баз і банків даних із врахуванням можливостей мобільних пристроїв;
- впровадження управлінських та інженерних структур, що реалізують стратегію мобільного навчання;
- фінансування розробки та супровіду m-learning.

Найважливішим питанням m-learning є розробка інформаційних ресурсів. Розробники мають враховувати, що мобільні пристрої мають обмежений розмір екрана, менші клавіатури та обмежені пропускною здатністю для мультимедійних файлів. Тому при розробці мобільних версій навчальних сайтів необхідно забезпечувати оптимальні параметри роботи з інформацією за допомогою мобільних пристроїв, а саме

- для підвищення швидкості завантаження інформації не перевантажувати навчальні матеріали мультимедійними об'єктами;
- розробляти мультимедійні матеріали у форматах, що підтримуються мобільними пристроями (PNG, GIFT, 3GP, MP3, MP4);
- враховуючи, що мобільні пристрої використовуються, переважно, у перервах між основними видами діяльності та транспорті, навчальні елементи повинні охоплювати короткі проміжки часу (10–15 хв.);
- розробляти навчальні матеріали з врахуванням анатомічних особливостей людини та якості зору;
- забезпечувати актуальність навчальних матеріалів.

У процесі роботи у мобільних версіях навчальних сайтів курсанти і слухачі повинні мати можливість знайомитися з навчальною інформацією, спілкуватися на форумах, проходити тестування, коментувати навчальний матеріал, розміщувати власний матеріал, коментувати інформацію учасників навчального процесу, спільно створювати документи, робити масове

розсилання повідомлень. Також для них повинні бути розроблені спеціальні програми: словники, калькулятори, перекладачі, спеціальні адаптовані електронні посібники, програми тестування, навчальні фільми, аудіопідручники, озвучені презентації, для роботи яких не потрібний Інтернет, при цьому зв'язок із викладачем відбувається голосовою розмовою та SMS.

Існує велика кількість спеціальних програм для мобільних телефонів:

- *Навчальна платформа для вивчення іноземної мови* http://bit.ly/tlf-mall – дозволяє використовувати телефон для голосових додатків (голосові тести), дає можливість студентам спілкуватися у реальному часі за допомогою голосових або текстових повідомлень, а також приймати участь у рольових іграх-діалогах.

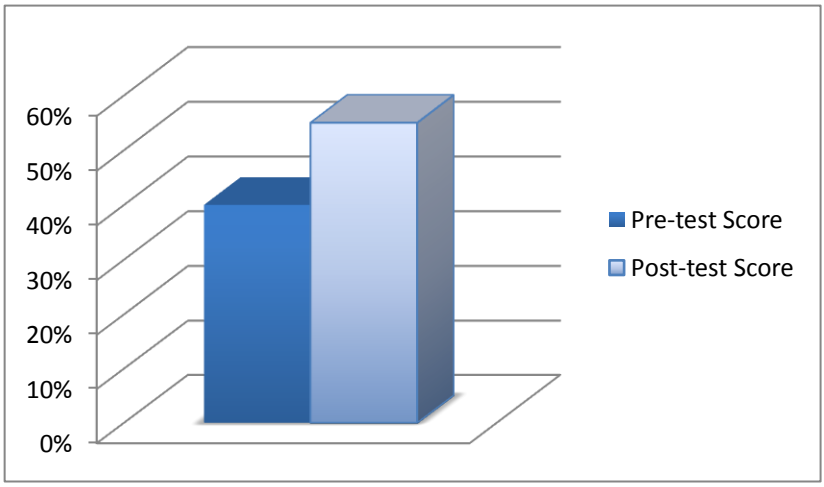


Рис.1. Приріст балів до і після використання системи

- *Bloom* (Bite-sized Learning Opportunities on Mobile Devices) http://www.bloom-eten.org/content/view/7/7/lang,english/ – платформа, створена для підвищення професійної компетенції працівників транспорту, логістики, медицини, може використовуватися для створення різних тестів для вивчення англійської мови, мають мультимедійну підтримку.
- *Mobl21* http://www.mobl21.com/ – програма, що повністю забезпечує учбовий процес, надаючи доступ до навчаль-

ного матеріалу, можливість повторювати пройдений матеріал, отримувати консультацію викладача, спілкуватися з одногрупниками для розробки проектів, мозкового штурму тощо. Викладачі можуть використовувати дане програмне забезпечення для організації роботи студентів поза аудиторією, створюючи тести та пошукові завдання, відеофайли лекцій.

- Програма *iTunesU* дозволяє створювати звукові записи лекцій, семінарів, конференцій, завантажувати цей матеріал на IPod або інший мобільний пристрій *Apple*. Використовується в Стенфордському університеті, Університеті Берклі та ін.
- *MediaBoard http://portal.m-learning.org/mboard.php* програмне забезпечення для зв'язку студент-викладач, а також групова робота над проектом, отримання інструкцій по курсу, проведення наукових досліджень, створення аудіо або відеозаписів.

Отже перевагами використання мобільних пристроїв і технологій є:

- швидкий доступ до навчальних та довідкових ресурсів у будь-який час і у будь-якому місці;
- постійний зв'язок з викладачем;
- врахування індивідуальних особливостей студента: діагностика проблем, індивідуальний темп навчання, тощо;
- підвищення мотивації студентів за рахунок використання знайомих технічних засобів та віртуального оточення;
- створення персоналізованого професійно-орієнтованого навчального простору студента;
- розвиток навиків неперервного навчання протягом життя;
- підвищення кваліфікації викладачів без відриву від роботи.

До негативних аспектів мобільного навчання відносяться:

- складності технічного та фінансового характеру, що зводяться до високої вартості мобільних пристроїв, маленькому екрану та дрібному шрифту;
- складності адміністративно-організаційного характеру. Оскільки мобільні пристрої в навчальних закладах най-

частіше відіграють роль шпаргалки, складно переконати як викладачів так і адміністрацію, що дана форма навчання покращує учбовий процес

- некомпетентність викладацького складу (на відміну від студентів) у питаннях сучасних інформаційних технологій, що не дозволяє їм впроваджувати в традиційну форму завдання на основі мобільних технологій, використовувати існуючі навчальні програми для мобільних пристроїв, забезпечувати інтерактивну підтримку навчального процесу;
- недостатність готових навчальних мобільних ресурсів та програм для студентів різних спеціальностей;
- складності методичного характеру. Відсутність розробленої методичної бази уповільнює використання мобільних пристроїв.

Отже в навчальному процесі нової освітньої моделі повинні використовуватися як нові форми навчальної діяльності (інтерактивні слайд-лекції, вебінари, тренінги та комп'ютерні симуляції, телекомунікаційні дискусії), так і нові типи завдань та вправ (навчально-тренінгові завдання; слайд-презентації; навчальні підкасти; веб-проекти). Мобільне навчання – один із засобів реалізації такої моделі.

Завдання сучасного викладача – перетворити мобільні пристрої та технології із загрози для навчання у допомогу та підтримку.

1. Голицына И.Н. Мобильное обучение как новая технология в образовании [Електронний ресурс] / И.Н. Голицына. – Режим доступу : http://ifets.ieee.org/russian/depository/v14_i1/html/1.htm.
2. Калуга Т.А. Мобильное обучение в дистанционном образовании [Ел. ресурс] / Т.А. Калуга // Вісник ЛНУ імені Тараса Шевченка. – 2011. – № 12 (223), Ч. І. – С. 113–123. – Режим доступу до журн. : http://www.nbuv.gov.ua/portal/Soc_Gum/Vlush/Ped/ 2011_12_1/15.pdf.
3. Мобильное обучение – второе рождение, но те же трудности [Електронний ресурс]. – Режим доступу : http://elearningtime. blogspot.com/2011/01/blog-post_17.html.
4. Мобильное обучение [Електронний ресурс]. – Режим доступу : http://goo.gl/7UdXI.
5. http://ru.wikipedia.org/wiki/
6. http://mobithinking.com

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ – КРОК ДО НОВОЇ ЯКОСТІ НАДАННЯ ОСВІТНІХ ПОСЛУГ

Грицюк М.Ю.,
викладач, магістр ЛДУ БЖД
Грицюк Ю.І.,
завідувач кафедри управління інформаційною безпекою ЛДУ БЖД, д.т.н., професор

Сучасні інформаційні та комунікаційні технології дедалі більше проникають в навчальний процес вищої школи, перетворюючись на головний його системний елемент, який значною мірою визначає характер і напрямок розвитку освіти. Безперечно, ці завдання постають і перед системою вищої освіти МНС України [2], адже науково-педагогічні працівники мають не тільки вміти кваліфіковано обирати і застосовувати саме ті навчальні технології, які повною мірою відповідають змісту і цілям вивчення конкретної дисципліни, але й враховувати індивідуальні особливості курсантів, студентів і слухачів.

Тому мета роботи полягає у тому, щоб показати на прикладі Львівського ДУ БЖД основні причини використання сучасних інформаційних технологій навчання при підготовці курсантів і студентів для потреб структурних підрозділів МНС України.

Використання інформаційних технологій у навчальному процесі. Упродовж останніх кількох років система вищої освіти України зазнає різних концептуальних змін, більшість з яких характеризуються новим розумінням цілей і цінностей освіти, усвідомленням потреби переходу до безперервної освіти, фундаментальними підходами до впровадження нових технологій навчання. Реалізація багатьох із цих завдань, які стоять перед системою вищої освіти, на сьогодні неможлива без використання адекватних методів і досконалих засобів її інформатизації. Зокрема, у Львівському ДУ БЖД набувають все більшої вагомості інформацій-но-комунікаційні технології [3], які забезпечують загальну комп'ютеризацію навчального процесу на такому рівні, який дає змогу вирішувати курсантам, студентам і викладачам щонайменше три основні завдання:

- забезпечує входження в мережу Інтернет кожного учасника навчального процесу у будь-який час і з різних місць перебування;
- розвиває єдиний інформаційний простір освітніх індустрій, які сукупно забезпечують присутність у них у різній час і незалежно один від одного всіх учасників освітнього і творчого процесу;
- створює, удосконалює та ефективно використовує управляючі інформаційно-освітні ресурси – бази даних і банки знань, призначені особисто для курсанта, студента і викладача з можливістю повсюдного доступу для роботи з ними.

Водночас, у багатьох претендентів на освіту, а також постійно охочих до неї зростає розуміння того, що традиційна схема отримання освіти в першій половині життя морально застаріла і потребує заміни на безперервну освіту і навчання протягом всього життя. Для нових форм навчання характерні інтерактивність спілкування та співпраця з викладачами-наставниками в процесі набуття знань. Для цього мають бути розроблені нові методики навчання, які враховуватимуть конструктивізм у поведінці та запитаннях, бажання набути знання студентами з обмеженими можливостями переміщення чи неповносправними, тобто навчання має проходити без часових і просторових меж. Для підвищення якості освіти передбачається також інтенсивно використовувати нові інформаційні технології [4].

Під освітніми технологіями навчання у Львівському ДУ БЖД розуміємо як систему наукових і інженерних знань [5], а також інформаційних методів і засобів, які використовують для створення, збирання, передачі, зберігання та оброблення інформації в системі Міністерства надзвичайних ситуацій. Завдяки цьому формується пряма залежність між ефективністю виконання традиційних навчальних програм і ступенем інтеграції в них відповідних інформаційно-комунікаційних технологій.

Основна мета вирішення проблеми інформатизації навчального процесу у Львівському ДУ БЖД полягає в тому, що внаслідок його запровадження має бути досягнута глобальна раціоналізація інтелектуальної діяльності охочих до навчання курсантів, студентів і навіть викладачів за рахунок використан-

ня сучасних інформаційних технологій з метою підвищення ефективності та якості підготовки різних фахівців до рівня інформаційної культури, досягнутого хоча б у країнах Західної Європи. При цьому має бути забезпечена підготовка кадрів для потреб структурних підрозділів МНС з новим типом мислення, яке відповідатиме сучасним вимогам постіндустріального суспільства.

Сьогодні однією з характерних ознак інформаційно-освітнього середовища навчання у Львівському ДУ БЖД є можливість курсантів, студентів і викладачів звертатися до структурованих навчально-методичних матеріалів [3], до навчально-мультимедійних комплексів всього університету у будь-який час і в будь-якій точці місця перебування. Окрім доступності навчального матеріалу, поступово забезпечується можливість зв'язку курсантів чи студентів з викладачами через мережу Інтернет, отримання консультації в он-лайн або офф-лайн режимах, а також можливість отримання індивідуальної «навігації» в освоєнні того або іншого предмету.

Розробники концепції дистанційного навчання, яку реалізовано у Львівському ДУ БЖД, конкретизують індивідуалізацію освітньої поведінки курсантів і студентів так, що в ній найкраще проявляються ознаки особово-орієнтованого способу навчання [4]:

- *гнучкість* – тобто охочий до навчання має право самостійно планувати час, місце і тривалість проведення занять;
- *модульність* – матеріали для вивчення різних дисциплін пропонуються у вигляді модулів, що дає змогу охочому до навчання генерувати траєкторію свого навчання відповідно до власних запитів і потенційних можливостей;
- *доступність* – незалежність від географічного і тирчасового місця знаходження охочого до навчання, що дає змогу навчальній установі не обмежувати його в освітніх потребах.

Інформаційні технології навчання привносять нові можливості в систему будь-якої освіти, створюють потребу зміни самої моделі навчального процесу: перехід від репродуктивного навчання – «переливання» знань з однієї голови в іншу (тобто від викладача до курсантів чи студентів), до креативної системи

освіти, коли в навчальній аудиторії за допомогою нового технологічного і технічного забезпечення моделюється життєва ситуація або виробничий процес, а курсанти і студенти під керівництвом викладача мають застосувати свої знання, проявляти творчі здібності для аналізу модельованої ситуації та виробляти рішення на підставі отриманого завдання.

Структура сучасного інформаційно-освітнього середовища навчання. Проведений аналіз переваг і недоліків наявних інформаційно-освітніх середовищ навчання (ІОСН), сучасного стану впровадження інформаційних технологій навчання у Львівському ДУ БЖД дає змогу сформулювати такі принципи, на яких мають будуватися інформаційно-освітні середовища:

- *багатокомпонентність* – мають містити навчально-методичні матеріали, навчально-орієнтоване програмне забезпечення, тренінгові навчальні системи, системи контролю знань, технічні засоби аудіо- та відео-відтворення, бази даних і інформаційно-довідкові системи, сховища інформації будь-якого вигляду, які є взаємопов'язані між собою;
- *інтегральність* – інформаційна складова середовища має містити всю необхідну сукупність базових (нормативних) знань в областях освіти і техніки з виходом на світові інформаційні ресурси, які визначено профілями підготов.-ки фахівців з певної області знань;
- *розподіленість* – інформаційна складова середовища має бути оптимально розподілена у сховищах інформації (на серверах) з урахуванням вимог і обмежень сучасних технічних засобів, навчальної доцільності та економічної ефективності;
- *адаптованість* – інформаційно-освітнє середовище навчання має не відторгатися наявною системою освіти, кардинально не порушувати її структури і принципів побудови.

Сформульовані принципи побудови сучасних ІОСН вказують на потребу розглядати їх, з одного боку, як частину традиційної системи освіти, а з іншого боку – як самостійну системи, направлену на розвиток активної творчої діяльності

курсантів чи студентів із застосуванням сучасних інформаційних технологій навчання [5].

Багатьма науковцями [4] вважається, що сьогодні проблема отримання освіти загалом – це проблема не технологій навчання, а, насамперед, проблема людини – викладача. Саме він є слабкою ланкою з погляду сучасних інформаційних технологій навчання. Окрім цього, більшість фахівців з певної області знань, що працюють у вузах, часто взагалі не мають не те що педагогічної освіти, але й мало обізнані з роботою за комп'ютером. Тому головна увага в системі вищої освіти має бути, насамперед, направлена на педагогічну підготовку викладачів-предметників. Водночас, поєднавши педагогічну освіту і освіту в області сучасних інформаційних технологій, можна буде забезпечити прорив у створенні нового інформаційно-освітнього середовища навчання.

Так чи інакше, будь-яке обговорення проблем якості системи вищої освіти сьогодні неминуче торкається атестації, перепідготовки і підтримки викладацького складу старшого віку, які ще претендують на участь в інформаційно-освітньому середовищі навчання. Проте ще й до тепер у традиційному академічному середовищі потенційні викладачі ретельно вибираються за дуже жорсткими критеріями, які, в основному, мають академічний характер з урахуванням супутніх чинників, таких як наявність дослідницьких робіт і публікацій, мають схильність до навчання, педагогічний хист і психологічно урівноважені тощо. Критерії ж підбору викладачів для реалізації програм ІОСН мають бути не тільки академічними, педагогічними та психологічними, але й інформаційними, насамперед, наявністю інформаційно-освітніх навиків навчання.

Висновок. Використання сучасних інформаційно-комунікаційних мереж і комп'ютерних технологій в навчанні поповнює змістову і загальнокультурну складову частину інформаційного навчального середовища освітньої галузі знань, збільшує обсяг і якість професійних знань, впливає на швидкість і оптимальність вирішення навчальних завдань. Достатній рівень інформаційної культури кожного охочого до навчання є однією із складових загальної культури особистості.

1. Грицюк Ю.І. Підготовка фахівців з інформаційної безпеки для потреб Міністерства надзвичайних ситуацій України / Ю.І. Грицюк, Т.Є. Рак // Шоста Міжнародна конференція "Нові інформаційні технології в освіті для всіх: навчальні середовища" : матер. наук.-практ. конф. ITEA-2011, 22-23 листопада 2011 р., м. Київ. – К. : Міжнар. наук.-навч. центр ІТ і систем. – 2011. – С. 123-129.
2. Лаврівська О.З. Використання інформаційних технологій у навчальному процесі Львівського державного університету безпеки життєдіяльності / О.З. Лаврівська, Ю.І. Грицюк // Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : НЛТУ України. – 2010. – Вип. 20.13. – С. 212-221.
3. Федорова Е.Ф. Системное представление дистанционного образования / Е.Ф. Федорова // Педагогические и информационные технологии в образовании. – 2002. – № 5. – С. 123-128.
4. Чудінова Н.В. Формування інформаційно-освітнього середовища навчання у Львівському державному університеті безпеки життєдіяльності / Н.В. Чудінова, Ю.І. Грицюк // Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : НЛТУ України. – 2012. – Вип. 22.2. – С. 384-392.

III. ПРОБЛЕМНІ ПИТАННЯ ЗАСТОСУВАННЯ СПЕЦІАЛЬНИХ ТЕХНІЧНИХ ЗАСОБІВ У ДІЯЛЬНОСТІ МІЛІЦІЇ

СУЧАСНІ СПЕЦІАЛЬНІ ЗАСОБИ ЗАХИСТУ ТІЛА ПРАЦІВНИКА ОВС ПІД ЧАС ПРОВЕДЕННЯ СПЕЦОПЕРАЦІЙ

Цимбалюк М.М.,
ректор ЛьвДУВС, д.ю.н., професор, генерал-лейтенант міліції
Керницький І.С.,
зав. кафедри інформаційних технологій ЛьвДУВС, д.т.н., професор
Гнатюк О.М.,
магістрант ЛьвДУВС

Спеціальні засоби захисту працівників ОВС включають чотири класифікаційні групи:

1) засоби індивідуального захисту (шоломи, бронежилети, щити, комплекти протиударного захисту, захисні щитки, протигази тощо);

2) засоби активної оборони (газова зброя, газові балончики, гумові кийки, наручники, електрошокери тощо);

3) засоби забезпечення спецоперацій (світлошумові пристрої (гранати), газорозпилюючі та димоутворюючі пристрої (гранати), водомети, бронемашини, пристрої для примусової зупинки автотранспорту тощо);

4) пристрої для примусового відкриття заблокованих дверей (малогабаритні підривні пристрої, спеціальні механічні пристрої тощо).

Для безпосереднього захисту працівника ОВС під час виконання службових завдань призначені спеціальні індивідуальні засоби захисту[*].

Захисні шоломи, бронежилети, протигази достатньо широко описані у друкованих працях [1-8]. Додаткового висвітлення

[*] Дана робота не передбачає формування каталожного огляду, а покликана лише навести основні типи і зразки спеціальної техніки з окремої групи засобів індивідуального захисту.

потребують питання, пов'язані з захистом рук, ніг та тулуба правоохоронця. З цією метою використовуються захисні щитки, комплекти протиударного захисту та протиударні і броньові щити.

Найпростішими конструктивно можна вважати наколінники фірми *Paulson International ltd* (США) моделей 1010-ЕВ, 1010-ЕТ, показані на рис. 1.

а *б*

Рис. 1. Наколінники моделей 1010-ЕВ (а) і 1010-ЕТ (б) фірми Paulson

Істотна відмінність їх конструкції полягає у способі кріплення на нозі: модель 1010-ЕВ, окрім пластикових колінних чашок, обладнана пластиковими хомутами з кріпленнями кліпсового типу; модель 1010-ЕТ має еластичні хомути і кріплення на «липучках» типу *Velcro* (Контакт).

Досконалішим засобом індивідуального захисту правоохоронця під час проведення спецоперацій є виріб моделі КЗРН вітчизняного ТОВ «Матеріалознавство» (фірма МАТЕ м. Київ), який, окрім наколінників, включає захисні щитки для гомілок, рук та налокітники (рис. 2).

а

б *в*

Рис. 2. Налокітники (а), наколінники (б) та загальний вигляд (в) захисних щитків моделі КЗРН фірми МАТЕ

Щитки КЗРН забезпечують захист від холодної зброї, а також від ударів, завданих бітами, прутами і камінням. Захисні щитки КЗРН мають незначну массу (1,95 кг), оскільки виготовлені з високоміцного алюмінієвого сплаву, ергономічні, не заважають рухам кінцівок людини, зручні в експлуатації, мають надійне регульоване кріплення типу *Velcro*. Загальна площа захисту становить 27,5 дм^2.

Прототипами комплекту КЗРН послужили показані на рис. 3 протиударні алюмінієві щитки для захисту рук і ніг моделі Ш-308 (спеціальний клас захисту, маса 1,8 кг) та щитки фірми MATE (спеціальний клас захисту, маса 2 кг, товщина алюмінієвих полотен 2 мм).

а *б*

Рис. 3. Налокітники (а) і наколінники (б) фірми MATE з комплекту моделі Ш-308 протиударних щитків для захисту рук та ніг

Однак, комплект КЗРН не передбачає наявності протекторів для захисту передпліч і рамен правоохоронця. Цього недоліку позбавлений комплект захисних протиударних пристроїв моделі Форт-ЗПП українського підприємства Форт (м. Вінниця) (рис. 4).

Щитки з комплекту Форт-ЗПП володіють високими ударостійкими та енергопоглинаючими (амортизуючими) властивостями, оскільки виготовляються з високоміцних полімерних пластмасових матеріалів. Невисока вага та зручні кріплення типу *Velcro* забезпечують можливість довготривалого носіння щитків в умовах, наближених до бойових.

Компанія MATE є дистриб'ютором спецвиробів фірми *Paulson*, зокрема, комплекту протиударного захисту ROBOCOP (рис. 5).

Рис. 4. Комплект захисних протиударних пристроїв моделі Форт-ЗПП фірми Форт

Рис. 5. Комплект протиударного захисту ROBOCOP фірми Paulson

ROBOCOP забезпечує комплексний захист тулуба і кінцівок правоохоронця в бойових умовах. Основна відмінність від попередніх комплектів полягає у наявності пластикового наплічника і нагрудника, при цьому нагрудник обладнаний додатковим щитком для захисту паху. ROBOCOP виготовлений з негорючої високоміцної пластмаси, забезпечує ефективне поглинання ударних навантажень, зокрема, від гострих предметів (завдяки наявності амортизуючих елементів), забезпечує регулювання експлуатаційних розмірів у широкому діапазоні (завдяки використанню кріплень типу *Velcro*), дозволяє довготривале носіння (з огляду на незначну масу – 4,7 кг).

Різновидом комплекту ROBOCOP є комплект протиударного захисту моделі LBA-55 фірми *Paulson*, показаний на рис. 6.

а *б* *в*

Рис. 6. Комплект протиударного захисту LBA-55 фірми Paulson: захист рук моделі AP-100 (а); захист тулуба моделі CP-100 (б); захист ніг моделі LP-100 (в)

Аналізуючи конструктивне виконання комплекту ROBOCOP, видається доцільним зауважити можливість певного обмеження рухомості тулуба правоохоронця за рахунок суцільнолитих нагрудника та наплічника. З урахуванням високих технологічних досягнень у сфері виробництва сучасних бронежилетів, можна вважати за доцільне і раціональне поєднання саме бронежилета із щитками для захисту рук, ніг, колін, ліктів, передпліч та рамен. Однак, даний висновок потребує додаткових експлуатаційних досліджень в реальних умовах несення служби.

1. Інформаційний бюлетень компанії Šestan-Busch «The Power Protection». – Хорватія, Прелог, 2008. – 12 с.
2. Керницький І.С., Керницька М.І., Максимюк С.О., Гнатюк О.М. Світові тенденції у проектуванні високотехнологічних захисних

шоломів // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами. Матеріали наук.-практ. семінару 04.12.2009 р. – Львів, ЛьвДУВС, 2009. – С. 135-139.
3. Керницький І.С., Харабєрюш О.І., Максимюк С.О., Гнатюк О.М. Сучасні та перспективні захисні шоломи, прийняті на озброєння МВС України // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами: наук.-практ. семінар. Львів, 04 грудня 2009. Матеріали семінару – Львів: ЛьвДУВС, 2009. – С. 139-143.
4. Керницький І.С., Керницька М.І., Максимюк С.О., Гнатюк О.М. Новітні розробки кулезахисних шоломів для працівників ОВС // Проблеми діяльності кримінальної міліції в умовах розбудови правової держави. Матеріали науково-звітної конференції факультету кримінальної міліції 12.03.2010 р. Випуск 4. – Львів, ЛьвДУВС, 2010. – С. 71-78.
5. Рудік В.М. Спеціальна техніка в органах внутрішніх справ. Загальна частина / Рудік В.М., Харабєрюш І.Ф., Буханченко А.Г. ; навчальний посібник (у схемах). – Донецьк : Вид-во ДЮІ ЛДУВС, 2009. – 80 с.
6. Спеціальна техніка : посібник – курс лекцій [В.Л. Ортинський, І.С. Керницький, В.М. Слижук та ін.] ; за ред. професора В.Л. Ортинського. – Львів : ЛьвДУВС, 2009. – 197 с.
7. Спеціальна техніка / [Керницький І.С., Щур Б.В., Мовчан А.В., та ін.] ; за ред. професора І.С. Керницького. – Львів : ЛьвДУВС, 2010. – 356 с.
8. Харабєрюш І.Ф. Спеціальна техніка в органах внутрішніх справ. Загальна частина ; навчальний посібник / Харабєрюш І.Ф. – Донецьк : ДЮІ, 2009. – 257 с.

РОЗРОБКА ЖЕЗЛА ІНСПЕКТОРА ДАІ З МЕТАЛОДЕТЕКТОРОМ

Зачек О.І.,
доцент кафедри ОРД та спецтехніки ЛьвДУВС, к.т.н., доцент
Слижук В.М.,
старший викладач кафедри інформаційних технологій ЛьвДУВС

Важливе значення має підвищення ефективності та створення безпечних умов праці для працівників ДАІ під час виконання їх службових обов'язків. Внеском творчого колекти-

ву, що складається з працівників кафедри інформаційних технологій і кафедри ОРД та спецтехніки, у вирішення цієї задачі є модернізація жезла працівника ДАІ. Розробка відноситься до спеціальних технічних засобів Міністерства внутрішніх справ, що використовуються в діяльності ДАІ МВС, і може бути використана для регулювання дорожнього руху як у нічний, так і в денний час доби.

Недоліком відомого жезла працівника ДАІ типу «Зебра-Д» є використання морально застарілих акумуляторів типу Д-0,26 ємністю 260 мА×год., відсутність індикатора заряду акумуляторної батареї і використання малогабаритного світлодіода, що спричиняє недостатню потужність світлового потоку жезла.

Нашим творчим колективом було створено жезл модифікований працівника ДАІ ЖМ-1 (патент України на корисну модель № 55305 «Жезл модифікований працівника ДАІ ЖМ-1», виданий згідно заявки № u201006715 від 31.05.2010 р.). Він позбавлений недоліків жезла «Зебра-Д». Його недоліком є відсутність металодетектора для виявлення зброї чи інших металевих предметів, наприклад, бронежилетів із металевими бронепластинами. Тому подальшою розробкою творчого колективу було створення жезла інспектора ДАІ модернізованого з металодетектором ЖМ-3, який позбавлений вищеназваних недоліків.

В основу розробки поставлено завдання забезпечення можливості використання жезла як ліхтаря для перевірки документів та номерів агрегатів транспортних засобів і як металодетектора для виявлення зброї та інших металевих предметів, а також використання жезла як проблискового маячка; крім того поставлено завдання підвищення потужності світлового потоку жезла, що сприятиме збільшенню рівня безпеки інспекторів ДАІ під час виконання службових завдань; також поставлено завдання збільшення тривалості підсвітки жезла від вбудованої акумуляторної батареї та забезпечення зручності її заряджання.

Поставлені завдання досягаються створенням жезла інспектора ДАІ модернізованого з металодетектором ЖМ-3 (рис. 1), який містить корпус 1, що складається з елементів білого та чорного кольору, і руків'я 2, яке приєднується

посередництвом різьби до корпусу 1. У руків'ї розміщено акумуляторну батарею 3, складену з акумуляторів типорозміру ААА, зарядний пристрій 4 для заряджання акумуляторної батареї 3 із штепсельною вилкою 5 та світлодіодним індикатором заряджання 6, кнопку вмикання ліхтаря 7, перемикач 8 режимів свічення світлодіодів та включення металодетектора, світлодіод збільшеного габариту з високою світловіддачею білого свічення 9 та світлодіод блимаючий червоно-синього свічення 10. Штепсельна вилка закрита різьбовою кришкою 11. У торці корпусу 1 розміщено світлодіод збільшеного габариту з високою світловіддачею білого свічення 12, що використовується як ліхтар, додатковий світлодіод збільшеного габариту з високою світловіддачею білого свічення 13 та світлодіод блимаючий червоно-синього свічення 14, а у елементі корпусу чорного кольору міститься металодетектор 16 з сигналізатором 17. Усі електронні, електричні та електромеханічні елементи з'єднані з руків'ям проводами 15, що укладені спіраллю для уникнення обриву під час від'єднання руків'я 2 від корпусу 1.

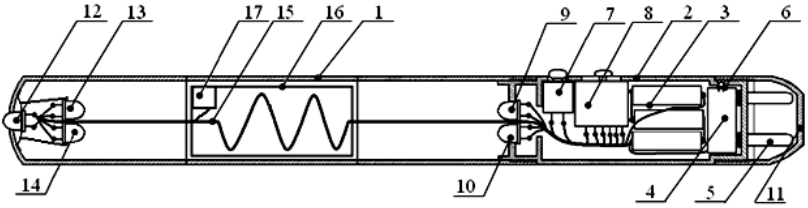


Рис. 1. Жезл інспектора ДАІ модернізований з металодетектором ЖМ-3.

Перед початком роботи необхідно зарядити акумуляторну батарею 3. Процес заряджання візуалізується свіченням індикатора заряджання 6. За необхідності включення підсвітки жезла білого кольору повзунок перемикача 8 пересувається в крайнє ліве положення (див. рис.). За необхідності використання жезла як проблискового маячка повзунок перемикача 8 пересувається на одне положення від крайнього лівого. Підсвітка жезла виключена при знаходженні повзунка перемикача 8 у середньому положенні. За необхідності включення металодетектора 16 повзунок перемикача 8 пересувається в крайнє праве положення (див. рис.); у випадку виявлення метало детектором 16 металевих предметів або зброї спрацьовує сигналізатор 17. За необхід-

ності використання жезла як ліхтаря (за рахунок використання світлодіода 12) натискається кнопка 7. Про розряд акумуляторної батареї 3 свідчить блимання світлодіодів 10 і 14 лише червоним кольором (у режимі проблискового маячка).

На жезл інспектора ДАІ модернізований з металодетектором ЖМ-3 творчим колективом отримано деклараційний патент України на корисну модель. Розробки в даному напрямі є перспективними і будуть продовжуватись.

1. http://www.viva-telecom.ru/SHOP/fullimage.php?id=7323&idfull =4102
2. http://www.viva-telecom.ru/SHOP/fullimage.php?id=7323&idfull =4103
3. http://www.viva-telecom.ru/SHOP/fullimage.php?id=7323&idfull =4104
4. http://www.viva-telecom.ru/SHOP/category.php?curcat=10 &cursubcat =43&makers=%DD%EB%E5%EA%F2
5. Патент України на корисну модель № 55305 «Жезл модифікований працівника ДАІ ЖМ-1», виданий згідно заявки № u 2010 06715 від 31.05.2010 р.
6. Щур Б.В., Керницький І.С., Зачек О.І., Слижук В.М., Сеник В.В. Жезл модифікований працівника ДАІ ЖМ-1 // Промислова власність. Офіційний бюлетень № 23, книга 1, 2010. – Ст. 5.100.
7. Патент України на корисну модель № 64741 «Жезл інспектора ДАІ модернізований з металодетектором ЖМ-3», виданий згідно заявки № u 2011 08335 від 04.07.2011 р. – 6 с.
8. Щур Б.В., Марін О.К., Керницький І.С., Зачек О.І., Слижук В.М., Сеник В.В. Жезл інспектора ДАІ модернізований з металодетектором ЖМ-3 // Промислова власність. Офіційний бюлетень № 21, книга 1, 2011. – Ст. 5.92.

ПРО ДЕЯКІ ОСОБЛИВОСТІ ВИВЧЕННЯ НОВІТНІХ ЗАСОБІВ СПЕЦІАЛЬНОЇ ТЕХНІКИ ОВС В УМОВАХ ІНФОРМАТИЗАЦІЇ СУСПІЛЬСТВА

Губарєв Г.Г.,
доцент кафедри інформаційної безпеки факультету ПМСІТ Харківського національного університету внутрішніх справ, к.т.н.

В умовах інформатизації суспільства інформаційні технології, системи і технічні засоби їх реалізації все частіше стають як об’єктами злочинних посягань, з одного боку, так і знаряддями злочи-

нів, з другого боку. При цьому власне інформація нерідко перетворюється на об'єкт злочину. Саме тому дисципліни, що викладаються в навчальних закладах МВС України повинні враховувати ці тенденції в сучасному інформаційному суспільстві.

Перш за все законодавство і нормативна база в державі повинні давати відповіді на всі питання боротьби зі злочинністю в інформаційній сфері, тому мають оновлюватись випереджаючими темпами в порівнянні з реаліями сьогодення. Відповідно вивчення цих тенденцій і реалій повинно бути предметом дисциплін юридичного спрямування.

По друге, спеціальні фізико-технічні аспекти виникнення і реалізації каналів витоку інформації та протидія злочинам в інформаційній сфері повинні вивчатись в рамках переліку дисциплін за напрямком підготовки 6.170102 – системи технічного захисту інформації.

Третім важливим моментом є своєчасне оновлення змісту традиційних дисциплін правоохоронного спрямування, таких як криміналістика, оперативно-розшукова діяльність, спеціальна техніка та інших. Таке оновлення дисциплін є однією із сторін комплексної проблеми інформатизації спеціальних навчальних дисциплін, розглянутих в [1]. Вирішення останнього завдання на прикладі дисципліни «Спеціальна техніка ОВС» є предметом обговорення в даній публікації, та одночасно є продовженням пошуків шляхів розв'язання проблем, сформульованих в [2].

Можливі підходи до розв'язання проблеми. Оновлення змістовних модулів дисципліни «Спеціальна техніка ОВС» повинно враховувати не тільки появу та вивчення нових зразків техніки в практичній діяльності органів внутрішніх справ, але і відстежувати загальносвітові тенденції в розвитку кримінальної ситуації в інформаційній сфері та рівень технічних засобів боротьби зі злочинами в цій сфері. В цьому зв'язку практично всі змістовні модулі навчальної дисципліни потребують відповідної структуризації та періодичного оновлення.

З урахуванням вказаних особливостей, наприклад, в Харківському національному університеті внутрішніх справ дисципліну «Спеціальна техніка ОВС» поділено на 2 модулі, які у свою чергу поділяються на 8 змістових модулів – тем, один із яких і вивчає особливості попередження та розкриття злочинів в інформаційній сфері:

Модуль 1. Спеціальна техніка органів внутрішніх справ. Засоби загального призначення.

Змістовні модулі:

Спеціальна техніка органів внутрішніх справ.

Засоби зв'язку органів внутрішніх справ.

Технічні засоби охорони об'єктів та системи контролю доступу.

Спеціальні засоби охорони громадського порядку.

Модуль 2. Спеціальна техніка органів внутрішніх справ. Засоби пошуку і фіксації доказів та різних видів інформації.

Змістовні модулі:

Засоби звукозапису. Засоби фотографування і відеозапису. Засоби спостереження.

Пошукова техніка. Спеціальні хімічні речовини.

Способи і засоби дактилоскопування.

Технічні засоби захисту інформації. Способи і засоби зняття інформації та протидія їхньому використанню.

Вказані модулі читаються, відповідно, на 1 курсі, 1 семестр і на 3 курсі, 5 семестр. При цьому на лекціях, практичних і лабораторних заняттях при розгляді всіх змістовних модулів викладачам необхідно підкреслювати можливості технічних засобів, що вивчаються, при виявленні, документуванні та розкритті злочинів в інформаційній сфері. Так, наприклад, при вивченні першого змістовного модуля при розгляді класифікації засобів спеціальної техніки, необхідно види техніки доповнити видом «Засоби технічного захисту інформації обмеженого доступу». При розгляді умов ефективного застосування техніки – вказувати на важливість та особливості документування злочинів в інформаційній сфері.

При вивченні другого змістовного модуля розгляд груп засобів зв’язку проводових та засобів радіозв’язку необхідно доповнити цифровими засобами з світловолоконними лініями, а при розгляді відповідних підгруп зв’язку необхідно акцентувати на можливість їхнього використання як каналів витоку інформації.

При вивченні третього змістовного модуля необхідно підкреслити важливість технічних засобів охорони для протидії і документування злочинів в інформаційній сфері, а також необхідно вказати на можливість виникнення додаткових каналів витоку інформації з приміщень лініями сигналізації та управління.

Аналогічно потребують корегування і змістовні модулі – теми другого модуля курсу дисципліни «Спеціальна техніка ОВС». Не зупиняючись на всіх темах підкреслимо, що для розкриття злочинів в інформаційній сфері особливу складність має документування злочинів та знаходження доказів злочинних дій. Тому величезне значення для успішної боротьби з вказаними злочинами має використання сучасних ефективних засобів пошукової техніки. Вивчення засобів здійснюється шляхом виділення і розгляду в цій темі нової групи засобів пошукової техніки – радіоелектронних засобів. При цьому в цій групі техніки детально необхідно вивчати такі підгрупи засобів, як відеоімпульсні електромагнітні локатори (сканери), детектори електромагнітного поля і випромінювання, універсальні частотоміри, селективні мілі–і мікровольтметри, детектори роботи мобільних телефонів, універсальні засоби пошуку каналів витоку інформації і пристроїв зняття інформації, спектральні корелятори та детектори нелінійних напівпровідникових переходів.

1. Губарєв Г.Г. Проблеми інформатизації спеціальних дисциплін в вищих навчальних закладах МВС України [Текст] / Г.Г. Губарєв, В.В. Тулупов // Матер. науково-практ. конф. «Інформатизація вищих навчальних закладів МВС України», 15-16 травня 2008 р. – Вип.14. Харків: Вид-во ХНУВС, 2008. – С. 65-68.
2. Губарєв Г.Г. Проблеми та шляхи вдосконалення викладання спеціальної техніки у вищих закладах освіти Міністерства внутрішніх справ України [Текст] / Г.Г. Губарєв // Вісник УВС. – 2001. – Вип. 9. – Харків: УВС, 2001. – С. 89-93.

ПРОБЛЕМИ ЗАСТОСУВАННЯ СПЕЦІАЛЬНОЇ ТЕХНІКИ У ПРАКТИЧНІЙ ДІЯЛЬНОСТІ ОВС ПІД ЧАС ДОКАЗУВАННЯ ШАХРАЙСТВА НА ОБ'ЄКТАХ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ

Босак О.О.,
ад'юнкт кафедри кримінального процесу Національної академії внутрішніх справ

З розвитком сучасної кримінально-процесуальної та оперативно-розшукової науки відбувається поступовий перегляд відносини до застосу-

вання спеціальної техніки і її результатів у ході розслідування та розкриття злочинів. Засоби спеціальної техніки поступово перетворюються з допоміжних в основні інструменти протидії злочинності, здобуваючи все більший процесуальний статус і значимість. На сучасному етапі більшість практичних працівників оперативних підрозділів рахують неможливим протидію сучасній злочинності без використання досягнень науково-технічного прогресу [1, с. 55]. У свою чергу досвід інформаційно-технічної протидії злочинності свідчить про збільшення ролі нових методів отримання доказів і перспективності використання сучасних науково-технічних засобів у цій діяльності [2].

Спеціальна техніка – це сукупність технічних засобів, спеціальних пристроїв, речовин і відповідних тактичних прийомів, що використовуються ОВС, із суворим дотриманням законності під час здійснення оперативно-службових заходів з метою профілактики та розкриття злочинів, охорони громадського порядку та забезпечення охорони окремих установ. Зазначимо, що в поняття спеціальної техніки включено, не лише технічні засоби та прилади, але й відповідні тактико-технічні прийоми, які також мають свою специфіку, наприклад, використання засобів активної оборони під час охорони громадського порядку та забезпечення громадської безпеки [3, с. 204].

Під час розслідування злочинів СТЗ використовуються гласно для збирання і дослідження доказів. Методика та прийоми застосування цих засобів розробляються криміналістикою. Ці технічні засоби, прилади та прийоми охоплюються поняттям «криміналістична техніка». Ці питання розглядалися також при застосуванні знарядь і приладів пошукової техніки [4, с. 76], приладів спостереження [5, с. 44]. Застосування криміналістичної техніки регулюється нормами кримінально-процесуального закону.

Практика доводить, що за допомогою низки оперативно-технічних засобів (ОТЗ) можна швидко та надійно отримати і зафіксувати відомості про конкретних осіб, які замислюють чи готують злочини, а після цього вжити заходу щодо їхнього недопущення. Прикладами застосування таких засобів можуть бути апаратура звуко- та відеозапису, прилади спостереження і т. ін.; припиненні групових порушень громадського порядку та

хуліганських проявів. Це може бути досягнуто через застосування спецзасобів захисту особового складу та проведення спеціальних операцій; виявленні причин вчинення злочинів та умов, що цьому сприяють.

Для виконання окремих слідчих дій зазначені технічні засоби комплектують і створюють спеціальні набори: слідчі портфелі, спеціальні криміналістичні набори, комплекти НТЗ для прокурора-криміналіста, оперативний і експертний «чемодан» (сумка), службовий «чемодан» автоінспектора, пересувна криміналістична лабораторія.

При провадженні слідчих дій з використанням найважливіших НТЗ – звукозапису, кінозйомки і відеозапису – порядок їх застосування детально врегульований в законі (ст. 851 і 852 КПК України) [6, с. 383-389]. Про це повідомляються учасники слідчої дії. Звуко- і відеозапис відтворюються після закінчення слідчої дії, кіноплівка також демонструється всім учасникам. Виготовлені під час провадження слідчої дії фотознімки, матеріали звуко- і відеозапису, кінозйомок, плани, схеми та інші матеріали додаються до протоколу цієї дії як такі, що пояснюють його зміст (ч. 4 ст. 85 КПК України). Але в дійсності ці матеріали мають більш широке і самостійне доказове значення, тому доцільно було б визначити їх самостійним джерелом доказів, а зліпки й відбитки – похідними речовими доказами.

У КПК України досить докладно регулюється застосування лише трьох НТЗ (статті 851 і 852), а це є не зовсім ефективним, бо з появою кожного нового технічного засобу виникає питання про допустимість і правомірність його використання для фіксування доказів, обставин кримінальної справи. Тому цілком слушними є пропозиції сформулювати в КПК України загальні норми про умови допустимості використання науково-технічних засобів і в широкому плані – досягнень науки і техніки в кримінальному процесі. Однак не слід виключати уже наявні в КПК України норми, які регулюють порядок застосування окремих технічних засобів і охорону прав особи при цьому, оскільки саме конкретні вказівки закону є важливими й реальними гарантіями додержання принципів кримінального судочинства [7, с. 94].

Для ефективного застосування НТЗ працівники органів слідства мають самостійно набувати навичок їх використання, а

за потреби запрошувати спеціаліста до участі у проведенні слідчої дії, мати вичерпну інформацію про можливості існуючих експертних установ. Нехтування цими вимогами призводить на практиці до того, що слідчий не вміє відшуковувати матеріальні сліди злочину, правильно їх вилучати й оформляти, внаслідок чого докази назавжди втрачаються. Поряд з тим слід зазначити, що відображувані у протоколах оглядів, обшуків, впізнань та багатьох інших дій фактичні дані засвідчуються підписами понятих. Існує суперечність між необхідністю фіксування у протоколах слідчих дій всієї отриманої інформації та реальною можливістю її засвідчення. Зумовлено це тим, що дослідження матеріальних слідів злочину можуть проводитися з використанням фахових знань за методикою, яка не завжди може бути зрозумілою понятим, а результати таких досліджень іноді потребують спеціальної розшифровки. Перебіг досліджень, під час яких застосовуються спеціальні знання та різноманітні сучасні науково-технічні засоби, не завжди можна контролювати, а результати таких досліджень іноді недоступні для безносереднього сприйняття. Нарешті, перешкодою для засвідчення за допомогою понятих може бути також небезпека для здоров'я через безпосереднє сприйняття матеріального джерела інформації (отруйні речовини, радіоактивні ізотопи тощо). Тому такого роду дослідження, на думку В.М. Тертишника, не можуть здійснюватися в рамках слідчих дій, де беруть участь поняті. У протоколах слідчих дій, можуть фіксуватися перебіг та результати досліджень, які проводяться без залучення фахових знань.

У протоколах слідчих дій можуть і повинні фіксуватися перебіг та результати досліджень, які виконуються із застосуванням і без застосування фахових знань [8, с. 573].

Усі дії, які сприймаються та усвідомлюються при провадженні слідчої дії, мають контролюватися та перевірятися слідчим, що відображається у протоколі та засвідчуються підписами всіх учасників слідчої дії.

Ураховуючи те, що всі технічні засоби, які використовуються для розкриття злочинів, розроблені тільки на науковій підставі, і використовуються для виявлення, збирання, наочної демонстрації, підвищення ефективності провадження слідчих дій, спираючись на законодавче підґрунтя особливостей

застосування та експлуатації, документального оформлення і використання результатів, отриманих внаслідок застосування технічних засобів.

Суд, дослідивши джерела інформації, отримані із застосуванням спеціальних технічних засобів, дає їм оцінку та можливість їх використання як доказів.

При вчиненні шахрайств відносно власності осіб злочинці використовують різноманітні способи в залежності від наявних у них індивідуально-психологічних особливостей, навичок та вмінь у конкретній сфері людської діяльності. Від обраного шахраєм способу залежить вибір засобів вчинення шахрайства, при застосуванні яких виникають певні зміни в оточуючому середовищі, що відображаються у слідах, предметах та об'єктах, дослідження яких потребує призначення та проведення відповідних судових експертиз.

Зупинимося на тих судових експертизах, які є важливими для викриття шахраїв, однак не завжди призначаються на досудовому слідстві. При вчиненні шахрайства щодо власності осіб, злочинці нерідко використовують речовини, матеріали та вироби, наприклад продають потерпілому виріб з міді чи латуні під виглядом виробу з золота, тобто дорогоцінного металу. В цих випадках виникає потреба в проведенні фізико-хімічної експертизи, яка відноситься до низки найбільш складних та трудомістких експертиз. Однією із задач криміналістичної експертизи матеріалів, речовин та виробів, об'єкти якої виступають як елементи матеріальної обстановки злочину є встановлення тотожності, що аналогічно завданням традиційних криміналістичних експертиз (судово-почеркознавчої, техніко-криміналістичної експертизи документів, судово-трасологічної, судово-портретної). У справах про шахрайство методи цих експертиз використовують при дослідженні підроблених грошей, документів, металів, сплавів та виробів з них, а також різних речовин невідомого походження. Наукову підтримку фізико-хімічні дослідження отримали у 30-ті роки минулого століття з появою різних приборів у хімічних лабораторіях, що дало можливість реєструвати матеріальну інформацію, недоступну людському сприйняттю, виявляти речовини мінімальних концентрацій. Фізико-хімічне дослідження дає можливість встановити приро-

ду та склад фальшивих дорогоцінних каменів та виробів з металів, реалізованих потерпілому під видом благородних металів.

Нерідко шахрай використовує грошову або речову «ляльку», обгорнуту у фрагмент тканини, паперу, тощо. Вилучена під час обшуку частина обгортки дозволить вирішити питання про наявність єдиного джерела походження. У таких ситуаціях необхідно призначати *судово-трасологічні експертизи,* в ході проведення яких вирішується питання про встановлення цілого за частиною. Експертизою цілого по частинах встановлюється, чи мають частини предмета (знайдені уламки, шматки, осколки тощо) спільну лінію розділення, тобто чи становили вони раніше одне ціле. Основними питаннями, що вирішуються у даному випадку, є: чи становили знайдені частини єдине ціле (чи є осколки скла частинами розсіювача фар даного автомобіля, чи відколота дана тріска від певного поліна та ін.); яким способом відокремлено від предмета його частину; до якого виду належить предмет, частина якого вилучена з місця події. Основними об'єктами криміналістичного дослідження у справах про шахрайство є документи (88%). Серед досліджуваних об'єктів можна виділити документи, що: 1) засвідчують особу; 2) підтверджують статус суб'єкта підприємницької діяльності, державного службовця; 3) мають відомості про господарські угоди; 4) підтверджують споживчі властивості та якість товарів; 5) вміщують відомості, що мають значення для справи, але не відносяться до перерахованих (чорнові записи, листи, тощо).

Техніко-криміналістична експертиза документів є дієвим засобом встановлення фактичних обставин вчинення шахрайств. Цей вид експертиз сприяє викриттю злочинів, встановленню способів вчинення злочину. Передумови для призначення цієї експертизи виникають при появі у справі документа – речового доказу, відносно якого є сумнів у достовірності чи припущення про його підробку.

---

1. Використання оперативно-технічних засобів у протидії злочинам, що вчиняються у сфері нових інформаційних технологій: монографія / [І.Ф. Хараберюш, В.Я. Мацюк, В.А. Некрасов, О.І. Хараберюш]. – К. : КНТ, 2007. – 196 с. – (Сер.: Проблеми оперативно-розшукової діяльності).

2. Мещеряков В.А. Криминалистический аналіз противоправного использования ботнетов / В.А. Мещеряков // Воронежские криминалистические чтения: сб. науч. трудов. – 2009. – Вып. 11. – 252-266.
3. Тертишник В.М. Науково-практичний коментар до Кримінально-процесуального кодексу України. – К. : А.С.К., 2002.
4. Гончар В.К., Золотар О.В. Знаряддя та прилади пошукової техніки: Навч. посіб. – К.: Нац. акад. внутр. справ України, 2001.
5. Гончар В.К., Золотар О.В. Прилади спостереження в екстремальних умовах : Навч. посіб. – К. : Нац. акад. внутр. справ України, 2003.
6. Белкин Р.С. Криминалистическая энциклопедия. – М. : БЕК, 1997.
7. Гончаренко В.И. Использование данных естественных и технических наук в уголовном судопроизводстве. – К., 1980.
8. Коваленко Є.Г. Кримінальний процес України: Навч. посіб. – К. : Юрінком Інтер, 2004.

СУЧАСНІ ВІТЧИЗНЯНІ ТЕХНІЧНІ ЗАСОБИ ПРОВЕДЕННЯ СПЕЦІАЛЬНИХ ОПЕРАЦІЙ ПІДРОЗДІЛАМИ ОВС.

Прокопов С.О.,
старший викладач кафедри спеціальної техніки та інформаційних технологій Дніпропетровського державного університету внутрішніх справ

За останні роки у світових тенденціях розвитку озброєння та спеціальної техніки, що, зокрема, використовується правоохоронними структурами в антитерористичних цілях, боротьбі з організованою злочинністю та підтриманні громадського порядку, відбулися значні зміни.

Більшість зразків озброєння та боєприпасів для потреб спеціальних підрозділів ОВС, крім виробів КП НВО «Форт» і карабіна КС-23, розроблялися у 50-70 рр. XX ст., тому нині вони вже не задовольняють вимог до спеціальної так званої «поліцейської» зброї.

На замовлення МВС України розроблені й виготовлені наступні спеціальні засоби:

- світлозвукові пристрої «Терен-7», «Терен-7М», «Терен-7Е»;
- пристрої миттєвого розпилення сльозоточивого аерозолю «Терен-2000», «Терен-1000»;

- газові гранати «Терен-6»;
- водомети.

Розглянемо деякі з названих вище вітчизняних розробок спеціальної техніки, призначеної для охорони громадського порядку та припинення масових безладів більш детально.

Світлозвукові пристрої сімейства ТЕРЕН-7

Пристрої світлозвукові (гранати) сімейства ТЕРЕН-7 призначені для використання з метою припинення протиправних дій шляхом тимчасового придушення психовольової стійкості світловим і звуковим імпульсами високої інтенсивності. ТЕРЕН-7, ТЕРЕН-7М, ТЕРЕН-7ЕМ є однофункціональними, невідновлюваними, неремонтованими виробами. Спосіб застосування – метання убік цілі вручну. Мінімальна припустима дистанція застосування не менш 1,5 м до людини.

Кожний пристрій ТЕРЕН-7, ТЕРЕН-7М складається з корпусу, елемента світлозвукового, запобіжно-пускового пристрою (ЗПП). Пристрої ТЕРЕН-7ЕМ складається з корпусу, елемента світлозвукового та електрозапалювача ЕВ-МБ-2Н чи РИШБ.773924.005-13.

Сталевий корпус ТЕРЕН-7М після спрацьовування й переспорядження може багаторазово використовуватися з метою навчання й тренування.

Технічні характеристики ТЕРЕН-7М

Сила світла, створювана пристроєм при спрацьовуванні, кд	(10±2)х106
Сила звуку, створювана пристроєм при спрацьовуванні на відстані 1,5м ,дБ	165±10
Мінімальна дальність застосування, м, не менш	1,5
Час із (ВЗ) спрацьовування пристрою	2±0,5 3,5±1
Застосування при температурі (^{0}C)	від-25 до +40
Габаритні розміри довжина мм:	130±5
Габаритні розміри діаметр мм:	50±5
Маса, г	680±50

Газова граната ТЕРЕН-6

Пристрій миттєвого розпилення сльозоточивого аерозолю із препаратом БМ-4 (гранати) ТЕРЕН-6 призначені для використання з метою припинення протиправних дій окремих осіб і масових безладь шляхом тимчасового придушення психовольової стійкості.

ТЕРЕН-6 є однофункціональним, невідновлюваним, неремонтованим виробом. Спосіб застосування – метання убік цілі вручну. Мінімальна припустима дистанція застосування не менш 2 м до людини. Після приведення в дію ТЕРЕН-6 повинен створювати хмару з нестерпною концентрацією препарату в межах 150-180 м^3.

Кожний пристрій складається з корпуса, спорядженого препаратом БМ-4, піротехнічного елемента, запобіжно-пускового пристрою (ЗПП).

Конструктивне виконання гранат дозволяє робити їхнє зберігання й транспортування в неостаточно спорядженому виді, що забезпечує їхню безпеку для навколишніх. ЗПП, забезпечує два ступеня запобігання від ймовірного спрацьовування, установлюється перед видачею гранат.

ТЕРЕН-6 має модифікацію ТЕРЕН-6Д для відстрілу з рушниці Форт-500 за допомогою спеціальної насадки й вишибного патрону.

Характеристики гранати ТЕРЕН-6

Мінімальна дальність застосування від людини, м., не менш	2
Час затримки спрацьовування пристрою	3...4…4
Застосування при температурі (^{0}C)	від-10 до +40
Габаритні розміри довжина мм.	185±2
Габаритні розміри діаметр мм.	63±2
Маса, г.	158±15
Обсяг хмари з нестерпною концентрацією препарату, м^3	150-180

Пристрої миттєвого розпилення сльозоточивого аерозолю «Терен-2000», «Терен-1000»

Вироби призначені для застосування правоохоронними органами при припиненні протиправних дій, пов'язаних з масовим безладдям з метою придушення активності порушників дією аерозольної хмари сльозоточивих і дратівних речовин на дальність до 12м.

Вироби є мобільними пристроями багаторазового використання (з можливістю перезаряджения на підприємстві-виготовлювачі або заміни) з контролем подачі й витрати використовуваної речовини ємністю балона 1 л (Терен-1000, маса в спорядженому стані до 2,9 кг), 2 л (Терен-2000, маса в спорядженому стані до 3,7 кг). Для оперативного реагування на зміну обстановки передбачені різні конструкції управління пускового важеля.

Тактико-технічні характеристики Терен-1000

Ємність, л	1,0
Дальність ураження, до, м	12
Час безперервного використання, з	28
Споряджена маса, кг	2,9
Діюча речовина	МПК+CS

Де МПК – це морфолід пеларгонової кислоти,
CS – це ортохлорбензальмалонітріл.

Для створення неможливої для перебування в закритому приміщенні концентрації газу (квартира, тюремна камера й т.п.) необхідно, наприклад, для приміщення 150...180 $м^3$ (площа 50...60 $м^2$) подача діючої речовини протягом 4...5 с.

Спеціальні автомобілі сімейства торнадо «Торнадо»

Завдяки своїй здатності швидко, ефективно розосереджувати натовп без загрози для життя людей і без насильства, протидіяти масовим безладдям, спеціальні водометні машини давно стали популярними серед засобів, призначених для охорони громадського порядку. Нещодавно на українських теренах з'явилися перші зразки вітчизняних спеціальних водометних автомобілів серії «Торнадо».

Науково-дослідний інститут спеціальної техніки разом із ГУВВ і ДРЗ МВС України та ЗАТ «Енергосоюз» взяли участь у створенні двох спеціальних водометних автомобілів під назвою «Торнадо» на базі автомобіля КрАЗ-63221. Ці машини пройшли дослідну експлуатацію в одному з підрозділів внутрішніх військ МВС України, призначені для використання підрозділами ОВС під час масових безладь або, за наявності підстав, для припинення масових заворушень. Протидія групам осіб, які порушують громадський порядок, здійснюється шляхом впливу на них струменями води.

Система розпилення активної суміші призначена для захисту персоналу у разі нападу на автомобіль шляхом розпилення по периметру (через 10 форсунок) 60 л активної суміші.

Система керування та контролю забезпечує спрацьовування системи окремо по кожній із сторін спецавтомобіля – спереду, справа, зліва, ззаду.

Система відео- та аудіозапису призначена для фіксування відеозображення (на відстані до 80 м) та звуків (на відстані до 30 м). Має в своєму складі відео камеру, мікрофон та пульт управління.

Система зв'язку забезпечує радіозв'язок екіпажу з іншими радіостанціями УКВ в діапазонах (137-180 МГц; 320-480 МГц), що знаходяться ззовні, та радіозв'язок між членами екіпажу.

Система протипожежного захисту. Передбачено дві системи протипожежного захисту (вуглекислотна та водопійна) для усунення загрози загоряння моторного відсіку та коліс. Колеса оснащено пристроєм для подачі піни з протипожежної установки.

Крім того, спецавтомобіль обладнано відвалом, прожектором, сигнально-гучномовною установкою та проблисковими маяками.

Насамкінець зазначимо, що підрозділи МВС України можуть забезпечуватись необхідним мінімумом спецзасобів для ефективного виконання завдань по охороні громадського порядку лише за умови виділення необхідних коштів на їхню закупівлю, а також проведення відповідних науково-дослідних і дослідно-конструкторських робіт, запланованих Державною програмою розвитку озброєння та військової техніки.

ОЦІНЮВАННЯ ТА СПЕЦІАЛЬНІ ТЕХНІЧНІ ЗАСОБИ ДОСЛІДЖЕННЯ НАВАНТАЖЕНЬ ЛЮДИНИ ПІД ЧАС ДТП

Когут В.М.,
викладач кафедри організації контролю за безпекою дорожньо руху ЛьвДУВС
Керницький І.С.,
завідувач кафедри інформаційни технологій ЛьвДУВС, д.т.н., професор
Горбай О.З.,
доцент кафедри експлуатації автомобілів НУ «Львівська політехніка» к.т.н.
Копитко М.І.,
доцент кафедри менеджменту ЛьвДУВС, к.е.н.

Під час ДТП на людину діють, головним чином, локальні навантаження, пов'язані із взаємодією різних частин тіла з елементами кузова та з утримуючими системами, до яких у першу чергу відносяться ремені безпеки. Тривалість дії навантаження – надзвичайно важливий чинник при співударянні.

Короткочасні навантаження, які характеризуються малою амплітудою переміщень, сприймаються організмом людини аналогічно до вібрацій. Такі навантаження людський організм переносить відносно легко, але починаючи з деякої тривалості, пошкодження від ударних навантажень стають непереборними. Останніми роками набули поширення випробування на пасивну безпеку, що проводяться незалежними від виробників організаціями (такими як EURONCAP, IIHS, NHTSA, LATINNCAP, NASVA, ANCAP, KNCAP, C-NCAP) [1-12].

Якщо не враховувати американських стандартів (де NHTSA є сертифікаційним органом), то результати більшості таких випробувань не є обов'язковими для виробників, але вони широко висвітлюються в пресі. На відміну від сертифікаційних випробувань (де перевіряється тільки відповідність Правилам ЄЕК ООН) щодо результатів випробувань незалежні експерти виставляють оцінювальні бали за безпеку автомобіля. Критерії травмування і сама процедура незалежних випробувань, як правило, не обмежуються, але переважно базуються на методиці Правил ЄЕК ООН.

Під час фронтального удару вимірюють показники за трьома критеріями:

- Head Injury Criteria (HIC);
- Chest deceleration (сповільнення на рівні грудної клітки);
- Femur load (навантаження на стегно).
- Для бокового удару використовують додаткові показники:
- Thoracic Trauma Index (TTI) – індекс травмування грудної клітки;
- Lateral Pelvic Acceleration (LPA) – бокове пришвидшення тазу.

В Україні надалі використовують стандарт для двох- і трьохвимірних манекенів [4] (рис. 1), який відповідає стандартам СТ РЕВ 4016-83, ІСО 6549, Правилам ЄЕК ООН № 12, 14, 17, 21, 25, 29, 32, 33, 35, 43 і 46, але вже морально застарів.

Рівень репрезентативності, %	А, мм	В, мм
10	391	406
50	417	432
95	605	454

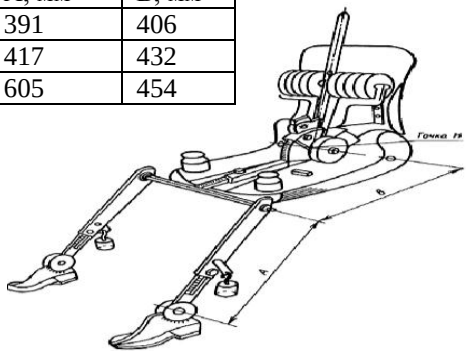


Рис. 1. Трьохвимірний посадочний манекен

Сучасні манекени мають давачі інерції в центрі мас голови, давачі згину, розтягування і зсуву шиї, давачі прогину грудної клітки, вимірювач осьової сили стегнової кістки, сил і моментів у колінному і гомілковостопному суглобах та деякі інші давачі (всього може встановлюватися біля 30 давачів). При навантаженнях у поздовжньому напрямі, а саме – при фронтальному ударі використовують манекен HYBRID III, а для бокового удару – манекен Eurosid-1, котрий, аналогічно як і HYBRID III, має давачі інерції в центрі мас голови, проте немає

давачів у шиї, грудині і на ногах, натомість передбачені давачі на ребрах, у черевній порожнині і тазі.

Розглянемо і проаналізуємо критерій травмобезпеки голови (як один з основних показників безпеки людини на транспорті).

Критерій травмування голови HPC/HIC (Head Performance/Injury Criterion) використовується у цілому світі як один з основних показників травмобезпеки автотранспортного засобу (АТЗ) для голови пасажира і фактично показує «дозу поглиненого сповільнення». Фізичний зміст критерію HIC полягає у визначенні максимального інтегралу сповільнення на небезпечній ділянці.

У сучасній світовій практиці оцінювання травмозахищеності голови від перевантажень базується на аналізі кривої Уейн-Стейта, яка графічно відображає порогове значення перевантаження у залежності від тривалості удару, при якому ще не настає струс мозку. У процесі аналізу вибирається відрізок часу, на якому сумарні перевантаження, що діяли, були максимальними. Розглянемо, для прикладу, значення (що згадується в Правилах пасивної безпеки № 12 і 21 ЄЕК ООН [6, 7]) перевантаження у 80 g. яке діяло на людину протягом 3 мс. Відклавши 3 мс на осі абсцис кривої Уейн-Стейта і 80 g – на осі ординат, отримаємо значення, що лежить нижче від кривої порогового навантаження і є безпечним (рис. 1).

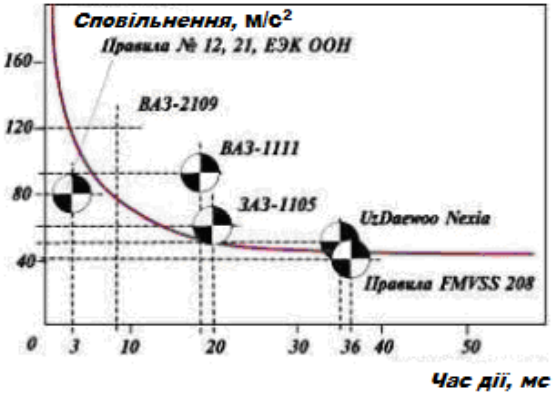


Рис. 1. Крива Уейн-Стейта з нормами згідно правил № 12, 21, FMVSS 208 для різних моделей легкових автомобілів

Досліджено, що із зростанням «інтенсивності» удару швидкість фронтального удару (безпечна для людини) зменшується, а під час удару голови об жорстку перешкоду з великою швидкістю наростання перевантаження порогова величина швидкості, втраченої під час удару, при якій відбувається втрата свідомості, складає 3 м/с (11 км/год.) [9]. Таким чином під час ударів із швидкостями, що перевищують порогову, ступінь важкості травм значно зростає. Важкість черепно-мозкових травм у значній мірі залежить і від напрямку удару, що показано на рис. 2 [10].

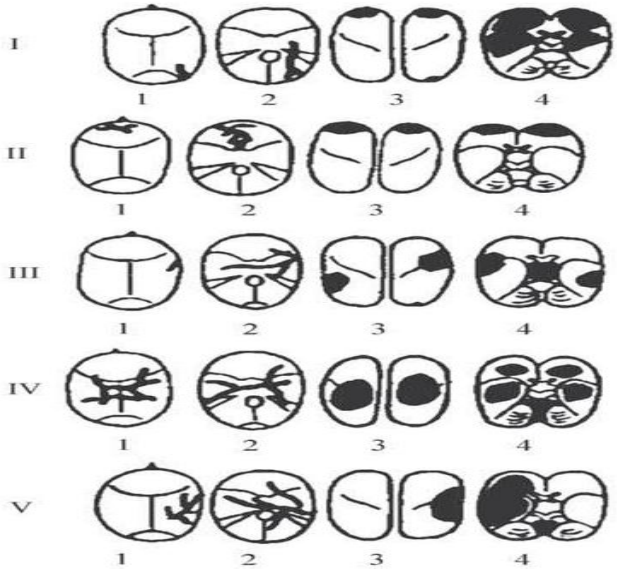


Рис. 2. Результати аналізу пошкоджень головного мозку і кісток черепа при черепномозковій травмі в залежності від напряму удару: I – удар по потилиці; II – удар спереду; III –бічний удар; IV – удар зверху вниз; V – дотичні удари зверху вниз (1 – склепіння черепа; 2 – основа черепа; 3 – поверхня мозку в зоні склепіння черепа; 4 – базальна поверхня мозку; жирні лінії – лінії переломів; зачорнені ділянки – зона контузії)

Під час сертифікаційних випробуваннях АТЗ на пасивну безпеку прийнято, що якщо голова манекена не торкнулася елементів інтер'єру, то випробування пройдено. Якщо відбувся контакт з будь-якою деталлю, то обчислюється критерій травмування голови під час удару:

$$HPC = (t_2 - t_1) \cdot \left[\frac{1}{t_2 - t_1} \int_{t_1}^{t_2} a \cdot dt \right]^{2.5},$$

де t_1, t_2 – час від початку до закінчення контакту голови з перешкодою, с; a – навантаження в долях g; dt – крок інтегрування (не більший ніж $1{,}25 \times 10^{-4}$ с).

Критерій HIC не повинен перевищити значення 1000 і обчислюється для кожного з кількох ударів. Сертифікаційні випробування АТЗ вважаються позитивними, коли виконані наступні вимоги до «травмування» голови манекена: пришвидшення центру мас голови манекена не перевищило 80 g протягом 3 мс і в разі удару голови об будь-яку перешкоду критерій HIC не перевищив значення 1000 [11]. Вважається також, що значення HIC до 1250 – безпечні, від 1250 до 1500 – відносяться до травм середньої важкості і понад 1500 – спричинюють небезпечно смертельні травми. За даними зарубіжних дослідників для високобезпечних автомобілів цей показник знаходиться у діапазоні 300-600, для звичайних автомобілів – 600-1000. Однак не можна однозначно констатувати, що автомобіль з меншим значенням HIC безпечніший при фронтальному зіткненні, ніж автомобіль, у якого значення HIC більше. І це не лише тому, що під час аварії важливі інші небезпечні ситуації – наприклад, удар по потилиці під час відхилення голови назад або пошкодження шийних хребців при різких обертальних рухах голови після ударів у деталь інтер'єру. Справа в тому, що HIC, як і крива Уейн-Стейта, носить статистичний характер і відображає лише ймовірну оцінку можливої травми голови. Отже критерій HIC потрібно розглядати разом з іншими критеріями.

Критерій травмування шиї NIC (Neck Injury Criteria). Якщо людину посадити в анатомічне крісло і міцно закріпити разом з головою великою кількістю широких і досить жорстких ременів, то сповільнення її тіла не перевищить 40 g. Оскільки в реальних умовах жодна людина не погодиться сидіти в такому кріслі більше декількох хвилин то переміщення корпуса тіла людини обмежують (але не фіксують) ременями безпеки різного типу. Тому під час лобового зіткнення корпус людини під дією інерційних навантажень нахиляється вперед, а ремені витягу-

ються. При цьому шия піддається розтягуючій дії сили, яка визначається добутком маси голови на пришвидшення. Якщо сила розтягування шиї перевищить деяку величину, що змінюється залежно від тривалості дії навантаження, то травма шиї неминуча [1]. Під час удару голови об перешкоду контролюється сила, що спричинює переміщення голови відносно першого шийного хребця шиї в напрямі спереду назад. Ця сила не повинна перевищувати відповідну граничну величину, а згинний момент на шийних хребцях не повинен перевищувати 57 Нм.

Критерій травмування грудної клітки THCC (Thorax Compression Criterion) визначається на основі абсолютного значення деформації грудної клітки між грудиною і хребтом, вимірюється в мм (стискування грудної клітки не повинне перевищувати 50 мм).

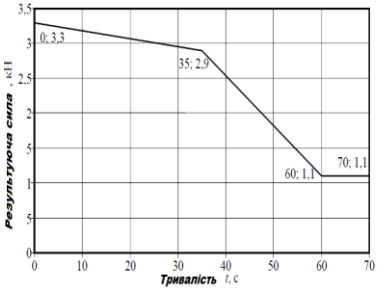
Показник по м'яких тканинах VC (Viscous Criterion) розраховується як добуток миттєвого значення деформації грудної клітки і миттєвої швидкості її деформації за формулою

$$VC = max\left[\frac{D}{0{,}229}\cdot\frac{dD}{dt}\right],$$

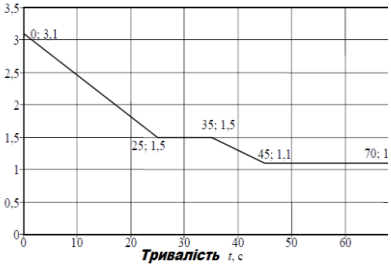
де D – зміщення грудної клітки, м; 0,229 м – стандартна ширина грудної клітки (по осі *x*).

Величина критерію VC по м'яких тканинах для грудної клітки не повинна перевищувати 1,0 м/с.

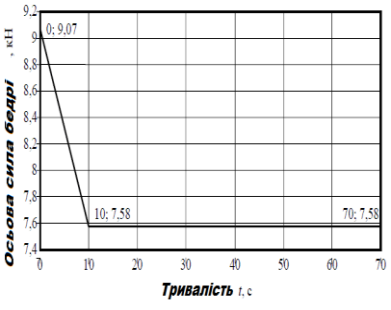
Критерій травмування стегна FFC (Femur Force Criterion) визначається на основі стискуючого навантаження, що передається по осі до кожного стегна манекена і вимірюється в кН (рис. 3).



а



б



в

Рис. 3. Залежності тривалості дії навантаження при гранично допустимих: а –силі, що розтягує шию; б – силі зсуву, в – осьовій силі на стегні

Критерій стискуючого зусилля на гомілці TCFC (Tibia Compressive Force Criterion) визначається на основі стискуючого навантаження (F_z), прикладеного по осі до кожної гомілки манекена, яке не повинно перевищувати 8 кН.

Показник травмування гомілки TI (Tibia Index) розраховується на основі моментів згину (M_X і M_Y) за наступними формулами:

$$TI = \left|\frac{M_R}{(M_C)_R}\right| + \left|\frac{F_Z}{(F_C)_Z}\right|;\ M_R = \sqrt{M_X^2 + M_Y^2}\ ,$$

де M_X – момент згину по осі *x*; M_Y – момент згину по осі *y*; $(M_C)_R$ – критичний згинний момент рівний 225 Нм; F_Z – осьове стискуюче зусилля по напряму *z*; $(F_C)_Z$ – критичне стискуюче зусилля по осі *z* величиною 35,9 кН.

Показник травмування гомілки TI розраховується для верхньої та нижньої точки кожної гомілки окремо, при цьому в кожній точці показник TI не повинен перевищувати 1,3 одиниць при зміщенні колінних шарнірів не більш ніж на 15 мм. Основні параметри травмонебезпечності, визначені за методикою EURONCAP, наведені в таблиці.

Параметри травмонебезпечності, визначені за методикою EURONCAP [12]

.	Максимально допустиме значення	Травмонебезпечна межа (ймовірність серйозної травми 50 %)
Сумарні перевантатаження голови HIC (Head Injury Criteria)	650	1000
Згинний момент шиї, Нм	42	57
Стиск грудної клітки, мм	22	50
Навантаження на стегні, кН	3,8	9,07
Критерій травми гомілки TI	0,4	1,3

Висновки

1. Заходи щодо пасивної безпеки АТЗ під час ДТП повинні бути скеровані на:
   - зниження рівня перевантажень, що діють на тіло людини з демпфуванням енергії удару за рахунок формування енергопоглинаючих елементів та зон деформації каркасу кузова;
   - розробку сучасних утримуючих систем (ременів безпеки);
   - зниження тривалості перевантажень шляхом створення систем перерозподілу енергії удару.
2. Система пасивної безпеки АТЗ повинна проектуватися, виходячи з науково обґрунтованих гранично допустимих фізіологічних можливостей людини щодо переносимості аварійних перевантажень.
3. Для забезпечення об'єктивності результатів випробувань АТЗ на пасивну безпеку доцільно проводити дослідження з метою уточнення граничних значень критеріїв, які традиційно використовуються в теоретичних і експериментальних дослідженнях з даної проблеми.

1. Безопасность автомобиля, анализ концепции. Рабинович Б.А. Журнал автомобильных инженеров. № 1 (54). 2009. С. 18-23.
2. Проект розпорядження Кабінету Міністрів України «Про схвалення Концепції Державної цільової програми підвищення безпеки дорожнього руху в Україні на 2012-2016 роки». www.sai.gov.ua/ua/law/38.htm.

3. Нурналиев Р.Г. Второй Международный конгресс «Безопасность на дорогах ради безопасности жизни». С.-Петербург. 17-19.09.08. www.gibdd.ru.
4. ГОСТ 20304-90. Манекены посадочные трехмерный и двухмерный. Конструкция, основные параметры и размеры. М., 1990.
5. Как измеряют безопасность автокресел? Что такое HIC? Posted on 11.07.2012 by Adminka. http://yut.kiev.ua/wordpress/?p=333.
6. ДСТУ UN/ECE R 12-03:2004. Єдині технічні приписи щодо офіційного затвердження колісних транспортних засобів стосовно захисту водія від удару об механізм кермування (UN/ECE R 12-03:1994, IDT).
7. Правила проведения краш-тестов в Европе. http://cartest.omega.kz/euro.html.
8. ДСТУ UN/ECE R 80-00:2002. Єдині технічні приписи щодо офіційного затвердження сидінь великогабаритних пасажирських дорожніх транспортних засобів і офіційного затвердження цих дорожніх транспортних засобів стосовно міцності сидінь та їхніх кріплень.
9. Рабинович Б.А. Безопасность человека при ускорениях (биомеханический анализ). М., 2007. 208с. илл.
10. Курме Д.А. Купч А.Я. Черепно-мозговые повреждения в зависимости от пусковых механизмов. Тр. Рижск. НИИ травматол. и ортопедии. Вып. 13. Рига. 1975.
11. Хусаинов А.Ш. Пассивная безопасность автомобиля : учебное пособие для студентов направлений 190100.62 «Наземные транспортно-технологические комплексы» по профилю – Автомобиле- и тракторостроение и 190109.65 «Наземные транспортно-технологические средства» по специализации «Автомобили и тракторы» / А.Ш. Хусаинов, Ю.А. Кузьмин – Ульяновск : УлГТУ, 2011. – 89 с.
12. Допускаемые нагрузки на различные части тела человека http://www.spacioclub.ru/ZE121/about/safety/person/.

IV. ДЕЯКІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ОРГАНАМИ ДЕРЖАВНОЇ ТА ВИКОНАВЧОЇ ВЛАДИ, ІНШИХ МІНІСТЕРСТВ ТА ВІДОМСТВ, КОМЕРЦІЙНИХ УСТАНОВ

ЧИСЛОВЕ ДОСЛІДЖЕННЯ НЕСТАЦІОНАРНОЇ ПРОСТОРОВОЇ ЗАДАЧІ ПРО ТЕРМОПРУЖНО-ПЛАСТИЧНУ ДЕФОРМАЦІЮ СТВОЛІВ ЗБРОЇ ПІД ВНУТРІШНІМ ТЕПЛОВИМ НАВАНТАЖЕННЯМ

Керницький І.С.,
завідувач кафедри інформаційних технологій ЛьвДУВС, д.т.н., професор
Неспляк Д.М.,
викладач кафедри інформаційних технологій ЛьвДУВС
Магеровська Т.В.,
доцент кафедри інформаційних технологій ЛьвДУВС, к.ф.-м.н.
Шишко В.Й.,
старший викладач кафедри інформаційних технологій ЛьвДУВС
Бичинюк І.В.,
викладач кафедри інформаційних технологій ЛьвДУВС

Розглянемо термопружне і термопружнопластичне деформування просторового ствола зброї із внутрішнім та зовнішнім радіусами $\alpha_{3b}=0,28$ м і $\alpha_{3e}=0,32$ м, значеннями осьової координати $\alpha_1 \in [\alpha_{1b};\alpha_{1e}]$ ($\alpha_{1b}=1$, $\alpha_{1e}=1,04$) і значеннями колової координати $\alpha_2 \in [\alpha_{2b};\alpha_{2e}]$ ($\alpha_{2b}=1,48$, $\alpha_{2e}=1,52$) під дією внутрішнього теплового навантаження (рис. 1)

$$T_{sur}=\left(-2500\cdot 473\cdot\left(\alpha_2-1,5\right)^2+473\right)\cdot\left(-2500\cdot\left(\alpha_1-\alpha_1^*\right)^2+1\right),$$

де

$$\alpha_1^*=1+\frac{\tau}{600}\cdot\left(1,04-1\right)\cdot$$

Числове знаходження термопружного і термопружнопластичного напружено – деформівних станів здійснюється за числовою схемою, описаною у роботах [1-4]. Механічні та теплофізичні характеристики такі:

- модуль пружності $E = 2 \cdot 10^5$ МПа,
- коефіцієнт Пуасона $\nu = 0,3$,
- межа пластичного течіння $\sigma_* = 160$ МПа,
- густина тіла $\rho = 7820$ кг/m^3,
- теплоємність одиниці маси матеріалу при сталому об'ємі $c_v = 565,47$ Дж/(кг·К),
- коефіцієнт теплопровідності $\lambda = 30,9542$ Дж/(m·К·с),
- коефіцієнт теплообміну на поверхні $\alpha = 3496,988$ Дж/(m^2·К·с).
- точність $\varepsilon = 1,0e-3$.

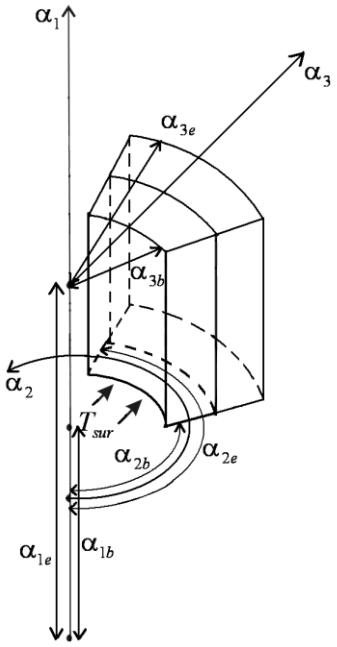


Рис. 1. Частина стволу зброї під внутрішнім тепловим навантаженням

Навантаження будемо здійснювати рівномірно на часовому інтервалі $\tau \in [0,600]$ з кроком $\Delta\tau = 20$ с.

Для числового розв'язування задачі побудуємо 16 скінченних елементи першого порядку за коловою, осьовою координатами і товщиною.

На рис. 2 – 4 зображений розподіл термопружних (1) і термопружнопластичних (2) колових напружень σ_{22} при значеннях осьової координати $\alpha_1 = 1,00053$, $\alpha_1 = 1,02053$ та $\alpha_1 = 1,03803$ відповідно і значенні радіальної координати $\alpha_3 = 0,28053$ у момент часу $\tau = 600$ с. Як видно із наведених рисунків найбільші відхилення значень термопружних і термопружнопластичних деформацій спостерігаються при $\alpha_2 = 1,5$, де колові напруження є найбільшими, і становлять ~ 75 % при $\alpha_1 = 1,00053$, ~ 30 % при $\alpha_1 = 1,02053$ та ~ 70 % при $\alpha_1 = 1,03803$.

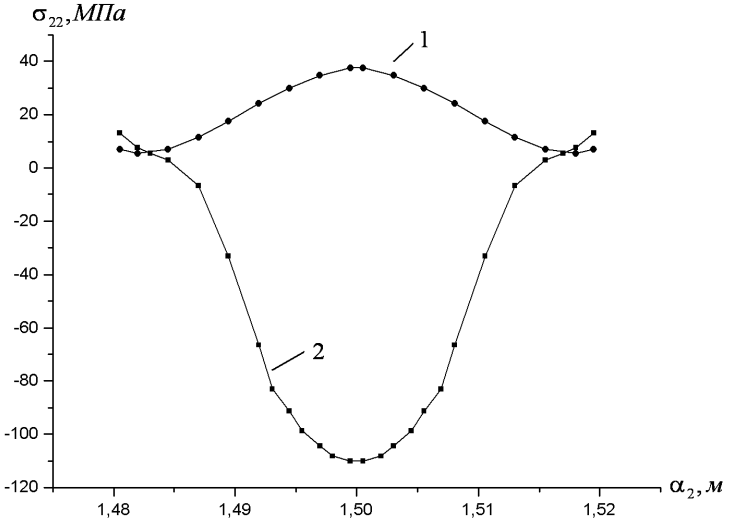


Рис. 2. Термопружні (1) і термопружнопластичні (2) колові напруження σ_{22} *при* $\alpha_1 = 1,00053$ *та* $\alpha_3 = 0,28053$ *у момент часу* $\tau = 600$ *с.*

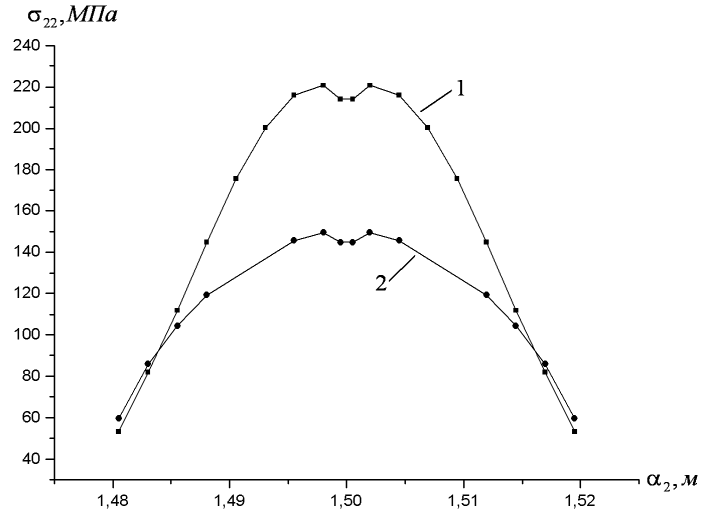


Рис. 3. Термопружні (1) і термопружнопластичні (2) колові напруження σ_{22} *при* $\alpha_1 = 1,02053$ *та* $\alpha_3 = 0,28053$ *у момент часу* $\tau = 600$ *с.*

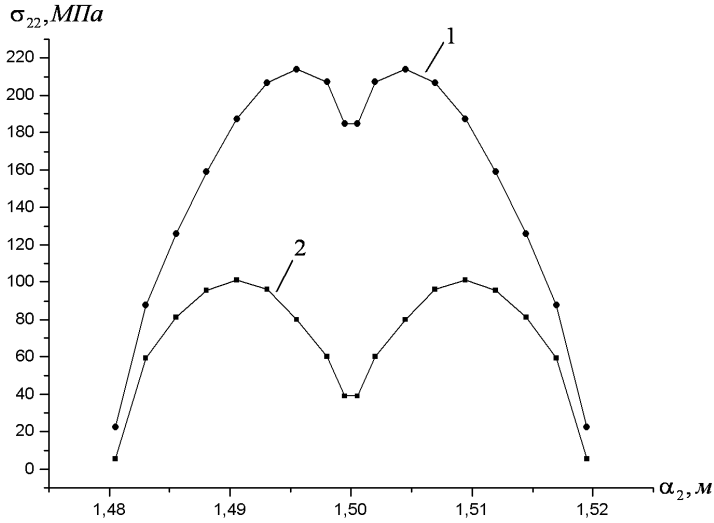


Рис. 4. Термопружні (1) і термопружнопластичні (2) колові напруження σ_{22} *при* $\alpha_1 = 1,03803$ *та* $\alpha_3 = 0,28053$ *у момент часу* $\tau = 600$ *с.*

На рис. 5 зображений розподіл інтенсивності пластичних деформацій ε_{int} при значеннях колової координати $\sigma_2 = 1,50053$ та радіальної координати $\alpha_3 = 0,28053$ у момент часу $\tau = 600$ с. Найбільші інтенсивності пластичних деформацій спостерігається при $\alpha_1 \in [1,02;1,03]$, а також на частині, близькій до межі при $\alpha_1 = 1,04$. Найбільший градієнт інтенсивності пластичних деформацій спостерігається на частині, близькій до межі при $\alpha_1 = 1,04$.

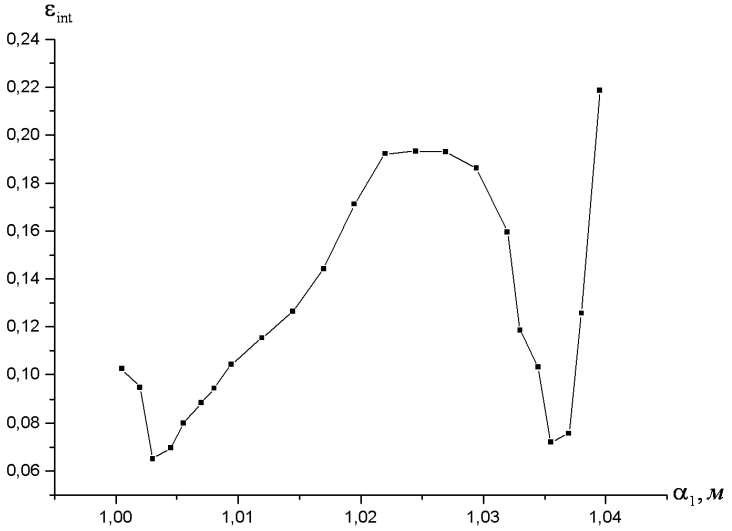


Рис. 5. Інтенсивність пластичних деформацій ε_{int} *при заченнях колової координати* $\sigma_2 = 1,50053$ *та радіальної координати* $\alpha_3 = 0,28053$ *у момент часу* $\tau = 600$ *с.*

На рис. 6 зображений розподіл інтенсивності пластичних деформацій ε_{int} при значеннях осьової координати $\alpha_1 = 1,00053$ (1), $\alpha_1 = 1,02053$ (2) та $\alpha_1 = 1,03803$ (3) відповідно і значенні радіальної координати $\alpha_3 = 0,28053$ у момент часу $\tau = 600$ с. На частині, близькій до границь при $\alpha_2 = 1,48$ та $\alpha_2 = 1,52$, пластичні деформації відсутні при $\alpha_1 = 1,00053$ (1) та $\alpha_1 = 1,03803$ (3), а інтенсивність пластичних деформацій при $\alpha_1 = 1,02053$ (2) є найбільшою.

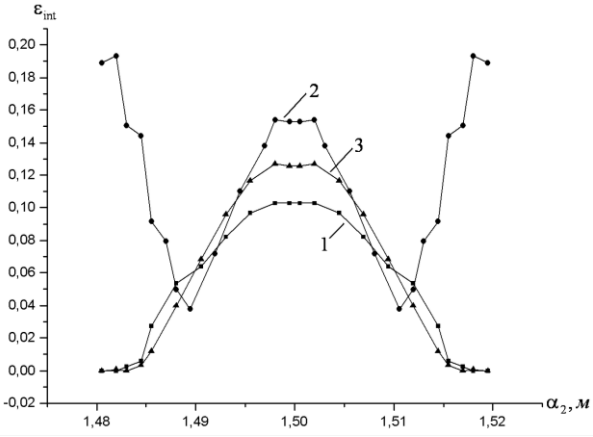


Рис. 6. Розподіл інтенсивності пластичних деформацій ε_{int} *при* $\alpha_1 = 1,00053$ *(1),* $\alpha_1 = 1,02053$ *(2) та* $\alpha_1 = 1,03803$ *(3) відповідно і* $\alpha_3 = 0,28053$ *у момент часу* $\tau = 600$ *с.*

На рис. 7 зображено термопружні (1) і термопружнопластичні (2) колові напруження σ_{22} при $\alpha_1 = 1,02053$ та $\alpha_2 = 1,50053$ у момент часу $\tau = 600$ с. На частині, близькій до межі при $\alpha_3 = 0,28$ різниця між термопружнопластичними і термопружними коловими напруженнями становить до 32 %.

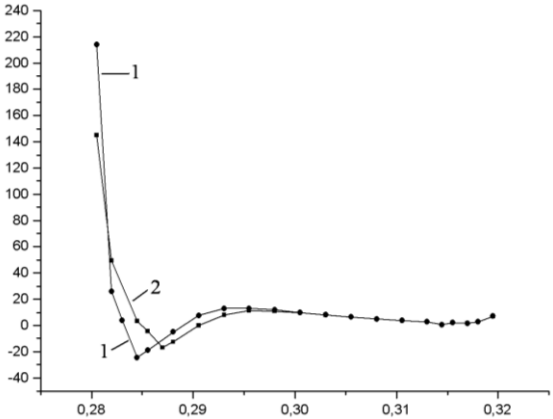


Рис. 7. Термопружні (1) і термопружнопластичні (2) колові напруження σ_{22} *при* $\alpha_1 = 1,02053$ *та* $\alpha_2 = 1,50053$ *у момент часу* $\tau = 600$ *с.*

Отже, урахування пластичних деформацій якісно і кількісно впливає на напружено – деформівний стан стволів зброї, що знаходяться під дією внутрішнього теплового навантаження.

1. Муха І. С. Числове дослідження процесів термопластичного деформування осесиметричних тіл з урахуванням розвантаження / І. С. Муха, Д. М. Неспляк // Математичні методи і фізико – механічні поля. – 2010. – 53, № 4. – С. 117-126.
2. Неспляк Д. М. Дослідження процесів нелінійної теплопровідності у товстостінних складових тілах / Д. М. Неспляк, І. С. Муха // Математичні методи і фізико – механічні поля. – 2007. – 50, № 2. – С. 176-182.
3. Неспляк Д. М. Числове дослідження термопластичності у роторі парової тербіни за теорією пластичного течіння / Д. М. Неспляк, І. С. Муха // Прикладні проблеми механіки і математики. – Львів: Інститут прикладних проблем механіки і математики ім. Я. С. Підстригача НАН України, 2010. – С. 125-132.
4. Mukha I. S. Numerical analysis of processes of thermoplastic deformation of axisymmetric bodies with regard for unloading / Mukha I. S., Nespliak D. M. // Journal of Mathematical Sciences. – Vol. 181, No 4, March, 2012. – P. 438-449.

ІНФОРМАЦІЙНІ ВПЛИВИ ЯК ПСИХОЛОГІЧНИЙ ЧИННИК ВЗАЄМОВІДНОСИН

Чистоклетов Л.Г.,
доцент кафедри конституційного, адміністративного та міжнародного права к.ю.н., доцент ЛьвДУВС
Шишко В.В.,
професор кафедри теорії та історії держави і права ЛьвДУВС, доцент
Шишко В.Й.,
старший викладач кафедри інформаційних технологій ЛьвДУВС

Сучасні можливості науки і техніки, засобів масової інформації спричинили кардинальні зміни в інформаційно-психологічній війні. Вони стали невід'ємною рисою війн і збройних конфліктів другої половини XX ст. і початку XXI ст. Аналіз їх підготовки і проведення однозначно засвідчує, що хід і результати військових дій будь-якого масштабу в сучасному світі кардинальним

чином залежать від мистецтва і технологій ведення інформаційно-психологічної війни.

Зважуючи на роль інформації в сучасному світі, американський дослідник М.Маклюен виводить цікаву тезу: «Істинно тотальна війна – це війна за допомогою інформації. Її непомітно ведуть електронні засоби комунікації – це постійна і жорстока війна, у ній беруть участь буквально всі» [2].

У книзі В.Ф. Прокоф'єва «Тайное оружие информационной войны: атака на подсознание» визначається: інформаційна війна – це дії, початі для досягнення інформаційної переваги шляхом завдання шкоди інформації, процесам, що базуються на інформації та інформаційних системах супротивника при одночасному захисті власної інформації, процесів, що базуються на інформації і інформаційних системах [3, с. 19].

Слушно і справедливо В.Б. Толубко зазначає, що засоби масової інформації є найбільш ефективними засобами для здійснення інформаційно-психологічного впливу на великі групи людей і тому їх слід вважати складовою частиною стратегічних сил інформаційної війни [4, с. 51].

Перевага будь-якої країни або групи країн дозволяє з достатньо високим ступенем достовірності моделювати поведінку «противника» і здійснювати на нього у явній чи прихованій формі вигідний для себе вплив. Можна стверджувати, що держави, які програли інформаційну війну, програють її назавжди, оскільки їх можливі кроки щодо зміни ситуації потребують колосальних матеріальних і інтелектуальних витрат, будуть контролюватися і нейтралізуватися стороною, що перемогла.

Вперше термін «інформаційна війна» (information war) вживається в американських військових колах у 1991 році. Першим офіційним документом з цієї проблематики були директива міністра оборони ЗША від 21 грудня 1992 р. під назвою «Інформаційна війна». В подальшому, в звіті американської корпорації «Ренд» MR-661-0SD «Strategic Information Warfare. A new face of War» (1996 р) вперше з'явився термін – «стратегічна інформаційна війна (інформаційне протиборство)». Вона визначалася як війна з використанням державного глобального інформаційного простору й інфраструктури для проведення стратегічних військових операцій і зміцнення впливу на власний інформаційний ресурс. [5].

Різниця в перекладі слова «warfare», що може бути перекладене і як війна, і як боротьба, спричинила паралельне вживання понять «інформаційна війна» та «інформаційна боротьба (протиборство)». Друге поняття є широковживаним в Росії, де воно означає «суперництво соціальних систем в інформаційно-психологічній сфері з приводу впливу на ті чи інші сфери соціальних відносин і встановлення контролю над джерелами стратегічних ресурсів, в результаті якого одні учасники суперництва отримують переваги, необхідні їм для подальшого розвитку, а інші їх втрачають»[6].

Аналізуючи вище вказане, слід констатувати, що Україна дедалі частіше стає об'єктом інформаційних атак з боку інших держав, зокрема – Росії. Проте надійно захистити свій інформаційний простір самотужки держава поки що не здатна. Таких висновків дійшли експерти Інституту Євроатлантичного співробітництва та фонду «Демократичні ініціативи». З цього приводу Борис Тарасюк зазначав: «Було прикро читати на сторінках українських часописів передруки на дуже делікатні теми, які здійснювалися з російської ініціативи. Інформація подавалася без жодного осмислення та аналізу, в російській «упаковці», і виглядала вона як відверта агресія проти України» [7].

Досліджуючи інформаційно-психологічні впливи як невід'ємної складової парадигми інформаційної безпеки, ми вважаємо, що на думку багатьох спеціалістів, інформаційний вплив на психологію слід поділити на такі види: інформаційно-психологічний, психогенний; психоаналітичний; нейролінгвістичний; психотропний.

Інформаційно-психологічний вплив – вплив словом, інформацією, психологічний вплив такого виду ставить своєю основною метою пропаганду певних світоглядних ідей, поглядів, уявлень, переконань, з одночасним формуванням у людей позитивних або негативних емоцій, почуттів, масових психічних реакцій.

Психогенний вплив здійснюється в результаті фізичного впливу на мозок людини в результаті травми голови або впливу фізичних факторів (звуку, освітлення, температури і ін.), а також шокового впливу умов середовища і певних подій (наприклад, картин масових руйнувань, великої кількості жертв

тощо). Внаслідок психогенного впливу людина вже не в стані раціонально діяти, втрачає орієнтацію в просторі, відчуває афект або депресію, впадає в паніку, в стан ступору. У зв'язку з чим і з'явилось таке поняття, як психогенні втрати особового складу.

Психоаналітичний вплив – це вплив на підсвідомість людини терапевтичними засобами, особливо в стані гіпнозу або глибокого сну.

Нейролінгвістичний – вид психологічного впливу, що змінює мотивацію людей шляхом введення в їхню свідомість спеціальних лінгвістичних програм.

Психотронний вплив – вплив на психіку людини за допомогою лікарських препаратів, хімічних або біологічних речовин.

Психотропний – вплив на людей, що здійснюється шляхом передачі інформації через позачуттєве (неусвідомлене) сприйняття.

Для інформаційно-психологічного впливу характерні певні закономірності, а саме:

- якщо він спрямований на емоційну сферу людей, їх потреби, то його результати відчуваються, передовсім, на спрямованості й силі спонукань, бажань і прагнень людей;
- коли під впливом виявляється емоційна сфера психіки, то це відображається на внутрішніх переживаннях, на міжособистісних відношеннях людей;
- поєднання впливів на обидві названі сфери дозволяє впливати на вольову активність людей і таким чином керувати їх поведінкою;
- вплив на комунікативно-поведінкову сферу, специфіку взаємовідношень і спілкування дозволяє створювати соціально-психологічний комфорт і дискомфорт, змушує людей співробітничати чи конфліктувати з оточуючими;
- в результаті психологічного впливу на інтелектуально-пізнавальну сферу людини змінюються в необхідну сторону її уявлення, характер сприйняття нової інформації і, як підсумок, «картина світу людини» [8, с.297].

Відомо, що потужні інформаційні технології, які отримали назву інформаційних війн, мають тисячолітню історію. Уже в біблійній легенді згадано Гедеона, який під час війн регулярно

вдавався до залякування ворога. Одного разу він так залякав супротивника, що той розгубився і завдав удару своїм військам. Як показує аналіз дослідження зазначеної проблематики, прикладів інформаційного впливу на моральну, духовну стійкість супротивника можна знайти чимало і в стародавньому Римі, і в епоху феодалізму (боротьба з «єрессю», за «істинну віру» тощо), і в подальшому. Особливого значення інформаційні війни набули в XX столітті, коли газети, радіо, а потім і телебачення стали справді засобами масової інформації, а поширювана через них інформація – справді масовою. Уже в 20-х роках США вели радіопередачі на регіони своїх «традиційних інтересів» – країни Латинської Америки, Великобританія – на свої колонії. Німеччина, яка домагалася перегляду умов Версальського миру, – на німців Померанії та Верхньої Сілезії в Польщі, Судетів – у Чехії. У 30-ті роки, на думку американського соціолога Сіпмана, «жодна з політичних криз не обходилася без акомпанементу радіо. Громадянська війна в Іспанії, боротьба Китаю з Японією, мюнхенська криза – усе це було відображено в нових, скрипучих симфоніях на коротких хвилях». Тоді ж, у 30-х роках, інформаційні війни перестають бути додатком до збройних і перетворюються в самостійне явище, зокрема, німецько-австрійська радіовійна 1933-1934 рр. з приводу приєднання Австрії до рейху. Саме тоді з'явилося і набуло поширення поняття «інформаційний агресор». Мета інформаційної війни – послабити моральні й матеріальні сили супротивника, посилити власні. Вона передбачає заходи пропагандистського впливу на свідомість людини в ідеологічній та емоційній галузях. Очевидно, що інформаційна війна – складова частина ідеологічної боротьби. Здавалось б з розпадом комуністичної системи мали б зникнути й інформаційні війни як явище, але цього не трапилося. Лише за офіційними даними, 120 країн здійснюють чи закінчили акції впливу на інформаційний ресурс супротивника. І цьому є щонайменше два пояснення. По-перше, національні інтереси країн світового співтовариства відрізняються не тільки в ідеологічній сфері. По-друге, важливою є псевдогуманність інформаційних війн. Вони не призводять безпосередньо до кровопролиття, руйнувань, при їх веденні немає жертв, ніхто не позбавляється їжі, даху над головою. І це

породжує небезпечну безпечність у ставленні до них. Тим часом, руйнування, яких завдають інформаційні війни в суспільній психології, психології особи за масштабами і за значенням цілком співмірні, а часом і перевищують наслідки збройних війн [9, с. 75].

Батьком вітчизняного досвіду ведення інформаційних війн вважають Богдана Хмельницького. За допомогою розвідувальної та контррозвідувальної служби Богдан Хмельницький шляхом поширення дезінформації прагнув посіяти у ворожому війську непевність у власних силах, панічний настрій. У своїх універсалах до населення та інструкціях до розвідників гетьман наполягав на необхідності створення в стані противника відчуття приреченості, напруги та непевності. Отже, вперше в практиці вітчизняного воєнного мистецтва застосовувалися принципи ведення так званої психологічної війни. Такі методи використовував український гетьман у вирішальних битвах з ворогом під Корсунем, Пилявцями та Берестечком.

Так, перед Корсунською битвою, що завершилася перемогою українців наприкінці травня 1648 р., Б.Хмельницький зумів блокувати інформацію про реальний стан речей у своєму таборі й поширив неправдиві свідчення про кількість козацького війська. Внаслідок цього командувач польською армією М. Потоцький почав ухилятися від бою, втратив стратегічну ініціативу і вже задовго до безпосередньої битви зазнав психологічної поразки.

Психологічний чинник був визначальним і під час перемоги української армії над поляками під Пилявцями у вересні того ж року. Вдалими маневровими діями Б. Хмельницький створив несприятливі умови для розташування оборонного табору польських військ. Це натомість викликало невпевненість коронного командування у своїх діях, яка поширилася й на особовий склад. Учасник тих подій з польського боку занотував у своєму щоденнику: «...У таборі ніякої дисципліни, ніякого авторитету вождів. Вночі після паролю стріляли, кричали, і ніхто за це не одержував догани, бо однаковий страх охоплював усіх, так що не було абсолютно ніякого порядку». Окрім того, на другий день битви, 22 вересня, за наказом гетьмана до ворожого табору потрапляє полонений козак, переодягнений священиком.

Незважаючи на тортури, він повідомляє про прихід на допомогу Хмельницькому кількох десятків тисяч татар. Насправді ж союзницькі війська налічували до п'яти тисяч вояків. Проте хитрий гетьман організував їм надзвичайно гучну зустріч: було дано салют з гармат і мушкетів. Цей факт та попередня дезінформація мужнього козака спричинили те, що серед поляків поповзла страхітлива чутка: до Хмельницького надійшла тридцятитисячна кримська орда! Можливо, саме відтоді пішла відома народна приказка: «У страху очі великі».

Засилання до противника «підставних» полонених відбувалося неодноразово й під час подальшого ведення бойових дій. Це стало важливим складовим елементом «психологічної війни» Б.Хмельницького. Адже ворог не сподівався, що козацькі «язики», мужньо витримуючи жорстокі тортури, будуть давати наперед запрограмовані й вигідні для українців свідчення. Коли під час Збаразько-Зборівської кампанії та боротьби з полками Данила Нечая польський воєначальник С. Лянцкоронський отримав від захоплених «язиків» відомості про підхід на допомогу козацькому полковнику начебто основних козацьких сил на чолі з самим Хмельницьким, він наказав відвести свої сили від Старокостянтинова. Зрозуміло, що це було простою дезінформацією, але завдяки їй Д.Нечай отримав оперативний простір для подальших дій. Так само вчинив полковник Станіслав-Михайло Кричевський під Лоєвим, коли заслав козаків-«смертників» у табір литовського князя Януша Радзивілла й тим самим ввів його в оману щодо напряму свого просування [10, с. 34-38].

Переводячи свою увагу у вектор банківської діяльності, слід зазначити що починаючи ще з 2008 року – початку чергової фінансової кризи, яка охопила більшість країн світу і закінчуючи сьогоденням, застосування інформаційно-психологічного впливу набрало особливо великого розмаху. Тепер про це явище говорять як про доконану реальність, не забуваючи спекулювати ним у певних цілях, сіючи паніку і поглиблюючи хаос.

З цього приводу, слід констатувати, що найстрашнішим для будь-якого банку є інформаційна війна. Цьому свідчать багато прикладів, як вилив компромату може негативно вплинути на роботу банківської установи. Поява хоча б дрібних

сумнівів у стабільності банку призводить лише до одного: з нього починають тікати вкладники. Одночасна втрата 5% депозитів означає серйозну проблему, а 10% – майже гарантоване призупинення платежів.

Так, у 2004 році був конфлікт між акціонерами «Надра Банку». Одним з них були тодішні власники Укрсиббанку. Вони не хотіли вносити нові кошти до статутного капіталу і намагалися захистити свою частку акцій від розмивання.

Коли конфлікт досяг піку, «Українська металургійна компанія» оголосила про намір ліквідувати «Надра банк». Вкладники миттєво почали забирати з «Надр» гроші, і власники дуже скоро домовилися.

Тоді ж відбулася відома інформаційна атака на банк «Мрія». З нього також почався відтік вкладників, який ледь вдалося припинити. Також відомі конфлікти навколо Промінвестбанку і «Родоводу» [11].

Все це говорить про негативні наслідки, які настають в результаті ведення інформаційно-психологічних впливу в сфері банківської діяльності. Україна отримала чергову банківську інформаційну війну. І в будь якому випадку банківській сфері довелося докласти чималих зусиль, щоб повернути проблемні кредити та одночасно заспокоїти вкладників.

В наш час інформаційно-психологічна війна розглядає інформацію як окремий об’єкт або як потенційну зброю та вигідну ціль. Інформаційну війну можна розглядати як якісно новий вид бойових дій, активну протидію в інформаційному просторі. Інформаційна війна – це атака інформаційної функції незалежно від засобів, які застосовуються.

У веденні стратегічних інформаційних війн застосовується специфічна зброя. Ця зброя не завдає фізичної шкоди, але може призвести до справжньої війни. За визначенням В.Ф Прокофьева, інформаційна зброя – сукупність спеціалізованих (фізичних, інформаційних, програмних, радіоелектронних) методів і засобів тимчасового або безповоротного виводу з ладу функцій або служб інформаційної інфраструктури в цілому або окремих її елементів. Основна дія інформаційної зброї – блокування або спотворення інформаційних потоків та процесів прийняття рішень супротивника [3, с. 29].

Як слушно зауважує вітчизняна дослідниця Д.Прокоф'єва, сучасні війни ведуться перш за все в інформаційній сфері, яка випереджає й безперервно супроводжує так званий «прямий контакт» протиборчих сторін. Як повідомлялося, для боротьби з потенціальним супротивником в експортне мережене обладнання США встановлюються чипи з логічними вірусами, які можуть бути активізовані в потрібний момент. Для боротьби з певними особами є комп'ютерні програми обнуління банківських рахунків. І мабуть, багато є такого, про що ми не знаємо і можемо тільки здогадуватись [12, с. 123-128, с. 127].

Таким чином, аналіз термінологічних понять «інформаційно-психологічний вплив», «інформаційна зброя», «інформаційна війна» дає змогу зробити висновок, що вони пов'язані з такими факторами:

- інформаційно-комунікаційними – конвергенцією нових інформаційних технологій та їхнім впливом на різноманітні сфери діяльності і механізми функціонування суспільства;
- впливом масової культури на свідомість і поведінку людей за допомогою широкодоступних каналів передачі інформації;
- стандартизацією способу життя більшості населення;
- удосконаленням засобів маніпулювання людьми, тобто створенням на стан останніх таких регуляторних механізмів інформаційного впливу, які б допомогли протягом тривалого проміжку часу зберігати й підтримувати його для досягнення поставлених цілей [13, с. 43].

Результатом інформаційних взаємодій, як зазначають О.Т. Лебедєв, А.Р. Каньковська, може бути одержання інформації з метою власного розвитку й створення умов для розширення власного життєвого простору, а також навмисного (прямого) або ненавмисного впливу на цю інформацію з метою її перекручування та впливу на інформаційну інфраструктуру одного із суб'єктів інформаційної взаємодії (іншого об'єкта). Результат інформаційної взаємодії – це інформаційна війна, це завдання збитків інформаційній інфраструктурі супротивника шляхом порушення діяльності або функціонування певних її підсистем (елементів) чи зв'язків між ними [14, с. 121].

Висновки. У природі людського співжиття існують різноманітні впливи, котрі мають особливу структуру, закони, принципи. Відомо, що одні спричиняють певні зміни у формах людської активності (поведінці, діяльності, спілкуванні, вчинках), інші – у мотивації, пізнавальних процесах, ще інші – в емоційно-вольовій сфері особистості. Тому ключове значення у поліпшенні теоретичної і практичної складових суспільного буття має вивчення закономірностей, технологій, засобів і прийомів психологічного впливу на осіб, професійні громади, малі і великі соціальні спільноти.

Стрімкий розвиток процесу інформатизації світу веде до непередбачуваних наслідків, вже сьогодні ми бачимо, що інформаційно-психологічний вплив відіграє роль своєрідного інструментарію або так званої нелегальної зброї, за допомогою якої в мирний час, без війни, у звичайному розумінні цього явища здійснюється агресія в соціальні, політичні, економічні, військові та інші сфери суспільного буття інших держав із метою скерувати розвиток тієї чи іншої країни.

1. Бабенко Ю. Інформаційна війна – зброя масового знищення! / Ю. Бабенко // Інститут Масової Інформації. – 2006. – 322 с.
2. Маршал Маклюэн и информационные войны [Електронний ресурс]. – Режим доступу : www.smi.ru/2000/01/ 14/947797776.html
3. Прокофьев В.Ф. Тайное оружие информационной войны: атака на подсознание / В.Ф. Прокофьев. – 2-е изд., расшир. и доработ. – М. : Синтег, 2003. – 395 с.
4. Толубко В.Б. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти) / Толубко В.Б. – К.: НАОУ, 2003. – 320 с.
5. Присяжнюк М., Жарков Я. Аналіз засобів ведення інформаційної боротьби з використанням інформаційних технологій, форм і способів їх застосування // Центр воєнної політики та політики безпеки: http://defpol.org.ua.
6. Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно-психологической войны. – Монография, с ил.. – М.: Горячая линия – Телеком, 2003. – 541 с.
7. Євген Солонина. Інформаційні війни: у пошуках українського шляху до перемоги. – Режим доступу : http://www.radiosvoboda.org/content /article/1752190.html.
8. Методы и приемы психологической войны / Сост. – ред. .Е.Тарас. – Мн.: Харвест, 2006. – 352 с.).

9. Крилова О. Всі секрети по кишенях / О.Крилова. [Електронний ресурс]. – Режим доступу : www.rdwmedia.ru.
10. Таємниці, казуси і курйози української історії. Козацька доба / В.Горобець, Т.Чухліб. – Київ : «Наукова думка», 2004. – 310 с.
11. Сергій Лямець, Сергій Щербина, Як витримає «Форум» інформаційну війну? [Електронний ресурс]. – Режим доступу : http://www.epravda.com.ua/publications/2012/05/30/325064//
12. Прокоф'єва Д.М. Підприємницьке шпигунство в системі інформаційних злочинів / Д.М. Прокоф'єва // Український центр інформаційної безпеки, 2008. – С. 123-128, с. 127
13. Рейтер Г. Легальне промислове шпигунство [Електронний ресурс] / Г.Рейтер. – Режим доступу : http://www.agentura.ru
14. Лебедев О.Т. Основы менеджмента / О.Т. Лебедев, А.Р. Каньковская. – СПб. : ИД «МИМ», 1998. – 192 с.

ЦИФРОВА МОДЕЛЬ ДЛЯ АНАЛІЗУ НАПРУЖЕНО-ДЕФОРМОВАНОГО СТАНУ Г-ПОДІБНОЇ ПРОМІЖНОЇ ОПОРИ КАНАТНОЇ ТРАНСПОРТНОЇ УСТАНОВКИ

Бичинюк І.В.,
викладач кафедри інформаційних технологій ЛьвДУВС
Рудий Т.В.,
доцент кафедри інформаційних технологій ЛьвДУВС, к.т.н., доцент
Кулешник Я.Ф.,
доцент кафедри інформаційних технологій ЛьвДУВС, к.т.н., доцент
Неспляк Д.М.,
викладач кафедри інформаційних технологій ЛьвДУВС

Багатопрогонні канатні установки є одним із ефективних, а часом і єдиним, засобом транспортування спеціального обладнання, службовців МНС, МВС, людей, які постраждали внаслідок техногенних та природних катастроф у важкодоступних гірських умовах, умовах бездоріжжя, болотистій місцевості [1, 2, 3].

При обмеженні термінів проведення конструкторсько-проектувальних та випробувальних робіт і розрахунку конструкційних параметрів опор доцільно використовувати просторове цифрове моделювання з використанням прикладних програм MathCAD Professional, SolidWorks, CAD/CAM/CAE/ PDM/TDM-системи, MSC/NASTRAN for Windows [4].

Суттєво підвищити ефективність канатних багатопрогонних транспортних установок можна використавши проміжні опори, конструкція яких розроблена і описана у [5]. Більш простими з точки зору монтажу та надійності в експлуатації є Г-подібні опори. Схема такої опри подана на рис.1.

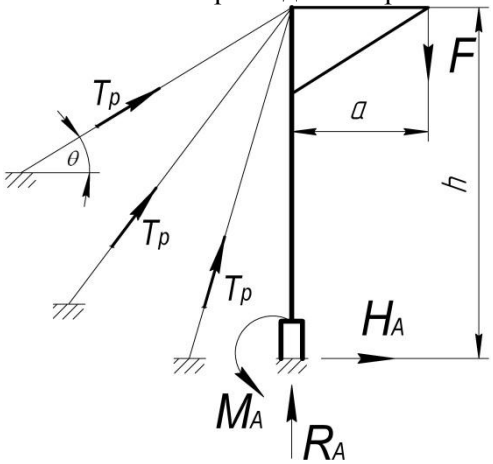


Рис. 1. Розрахункова схема Г-подібної опори

Зусилля F, що діє на опору залежить від параметрів суміжних прогонів установки. Це зусилля буде максимальним, коли вантаж знаходиться на башмаку. При цьому максимальний монтажний натяг складе $T_0 = 0{,}8T_{\max}$, [2], тобто можна записати:

$$F = Q\left(1 + 0{,}8\frac{l \cdot \cos\gamma}{4f \cdot \cos\alpha}\right), \qquad (1)$$

де Q – вага вантажу і каретки; l – довжина більшого прогону, який примикає до проміжної опори; f – стрілка провисання канату; α – кут ухилу хорди прогону до горизонту; γ – кут перелому несучого канату на опорі. Якщо прийняти $f/l = 1/20$, формулу (1) можна подати в наступному вигляді:

$$F = Q\left(1 + 0{,}01 \cdot l \frac{\cos\gamma}{\cos\alpha}\right). \qquad (2)$$

Вираз в дужках назвемо коефіцієнтом перевантаження опори k_n, тобто:

$$k_n = 1 + 0{,}01 \cdot l \frac{\cos\gamma}{\cos\alpha}. \qquad (3)$$

Тоді:

$$F = k_n \cdot Q. \qquad (4)$$

Щоб визначити F величину k_n можна отримати з графічних залежностей (рис. 2.), які побудовано для випадку, коли $\gamma = 5^0$.

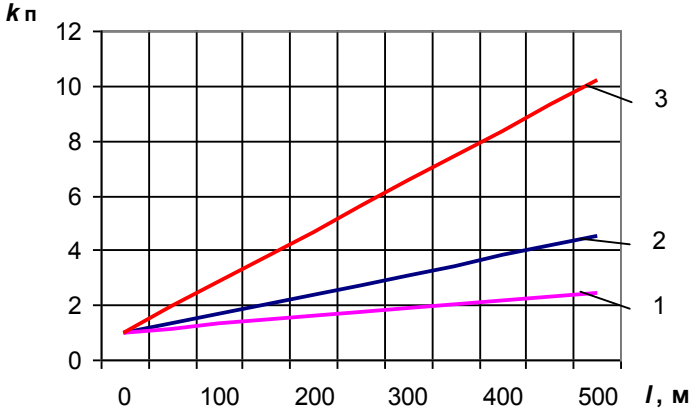


Рис. 2. Графічні залежності коефіцієнта перевантаження опори від величини прогону установки: 1 – при $\alpha = 20^0$; 2 – при $\alpha = 25^0$; 3 – при $\alpha = 30^0$

Для визначення зусиль, які діють на щоглу розглянуто рівняння рівноваги статики. Для симетричної системи, що оснащена трьома розтяжками вони приймуть наступний вигляд:

$$\left.\begin{aligned} R_A &= F + T_\partial \cdot \cos\theta + 2T_\partial \cdot \cos^2\theta = F + T_\partial \cdot \cos\theta\left(1 + 2\cos\theta\right); \\ H_A &= T_\partial \cdot \sin\theta + 2T_\partial \cdot \sin^2\theta = T_\partial \cdot si\theta\left(1 + 2\sin\theta\right); \\ M_A &= F \cdot a - H \cdot h = 0. \end{aligned}\right\} \qquad (5)$$

де R_A; H_A; M_A – опорні реакції стояка опори; T_p – натяг, який виникає в розтяжках; F – вертикальне зусилля, яке діє на башмак опори; θ – кут нахилу розтяжок до горизонту; h – висота опори; a – довжина поперечини опори.

Із третього рівняння системи (5), отримаємо:

$$H = \frac{F \cdot a}{h},$$

або:

$$T_p = \frac{F \cdot a}{h \cdot \sin\theta \cdot (1 + 2\sin\theta)}. \quad (6)$$

Тоді зусилля, яке діє на стояк щогли $F_{cm} = R_A$ можна обчислити з залежності:

$$F_{ñò} = R_A = F + \frac{F \cdot a \cdot \cos\theta \cdot (1 + 2\cos\theta)}{h \cdot \sin\theta \cdot (1 + 2\sin\theta)} = F\left(1 + \frac{a \cdot ctg\theta \cdot (1 + 2\cos\theta)}{h \cdot (1 + 2\sin\theta)}\right). \quad (7)$$

Якщо прийняти $\theta = 45^0$ рівняння (7) прийме наступний вигляд:

$$F_{ñò} = F \cdot \left(1 + \frac{a}{h}\right), \quad (8)$$

тоді зусилля для визначення натягу в розтяжках можна обчислити з залежності:

$$T_p = \frac{F \cdot a}{1{,}71 \cdot h}. \quad (9)$$

Введемо поняття коефіцієнта зміни натягу розтяжок k_p, який дорівнює:

$$k_p = \frac{a}{1{,}71 \cdot h}, \quad (10)$$

та коефіцієнт зміни зусилля у стояку, k_{cm}:

$$k_{cm} = 1 + \frac{a}{h}. \quad (11)$$

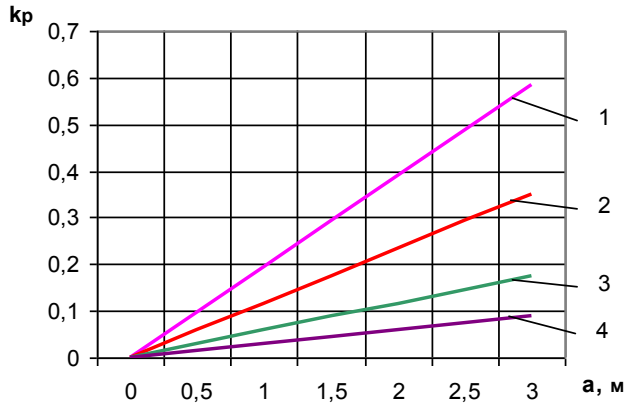
Тоді, відповідно:

$$F_{ñò} = k_{ñò} \cdot F \ ; \qquad (12)$$

$$T_p = k_p \cdot F \ . \qquad (13)$$

Для обчислення відповідних коефіцієнтів побудуємо графічні залежності $k_{ст} = f(a)$ та $k_p = f(a)$ для різних значень висоти стояка опори (рис. 3)

а)



б)

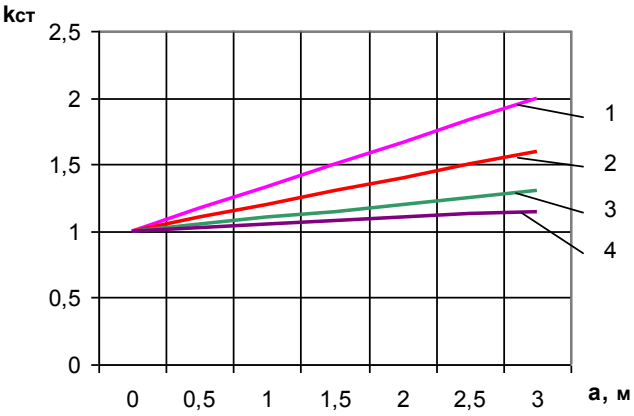


Рис. 3. Графічні залежності коефіцієнтів зусиль від довжини поперечини опори: 1 – при $h = 3$*м; 2 – при* $h = 5$*м; 3 – при* $h = 10$*м; 4 – при* $h = 20$*м. а)* $k_p = f(a)$*; б)* $k_{ст} = f(a)$

Внутрішні зусилля, з урахуванням динамічних навантажень, які виникають в елементах опор можна обчислити за рахунок аналізу міцності їх просторових структур шляхом підбору різних профілів та альтернативних сполучень їх у вузли.

Для проведення цифрового моделювання використано систему MSC/NASTRAN for Windows [6]. Для прикладу розглянемо розрахунок просторової конструкції проміжної опори (рис. 4). Просторова конструкція опори складається з вертикальної щогли висотою 10 м; консольного кронштейну довжиною 1,7 м з модулем канатної підвіски вантажу; трьох натяжних канатів-розтяжок, розташованих в плані під кутом 45° одна відносно іншої (рис.4). До кінця консольного кронштейну прикладається вертикальне навантаження 15 кН з коефіцієнтом динамічності $k_{\partial} = 2{,}0$. Таким чином активне навантаження складає F =30 кН.

Для компенсування дії моменту згину, який виникає у щоглі від активного навантаження, до кожної з трьох розтяжок прикладений попередній натяг 10000 Н. Таке рішення дозволяє покращити прямолінійність щогли, частково розвантажити консольний кронштейн, а також зменшити провисання розтяжок.

В рамках даного міцнісного аналізу щогли транспортної установки розрахункова модель (рис.4) подана у вигляді стрижневої конструкції. Механічні характеристики матеріалів елементів опори прийнято згідно з рекомендаціями поданими в [7]. Для використання методу кінцевих елементів проведена нумерація стрижнів та вузлів опори.

Розв’язок нелінійної задачі не може бути отриманий з одноразового розв’язання матричного рівняння кінцевих елементів $Kx = f$, оскільки матриця жорсткості залежить від переміщень. З умови рівності зовнішньої і внутрішньої робіт отримуємо нелінійне матричне рівняння, яке може бути розв’язане ітераційним методом Ньютона-Рафсона. До складу рівняння входить матриця початкового напруження, яка використовується у розрахунках на початкову стійкість, і матриця великих переміщень. Кількість ітерацій при розрахунку досліджуваної моделі щогли транспортної установки склала 4, що забезпечило точність 0,0001.

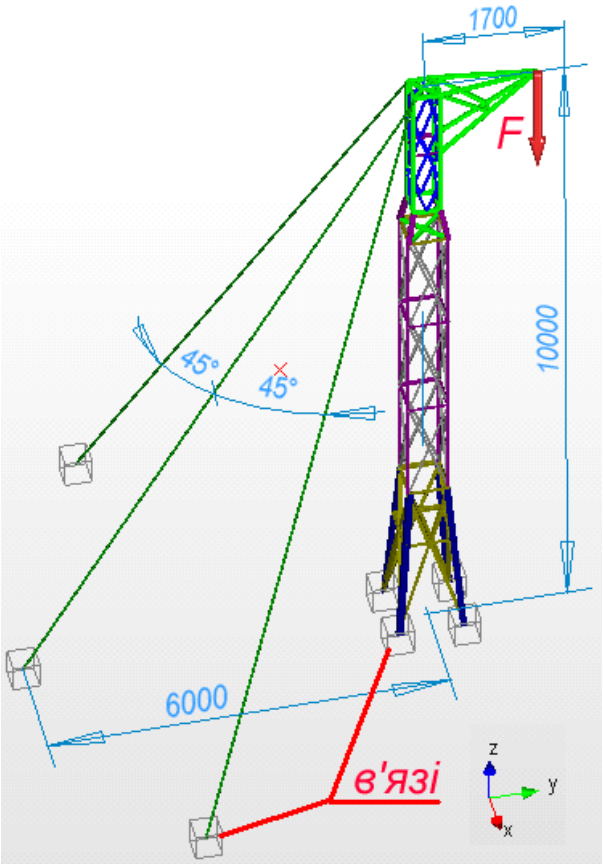


Рис. 4. Схема Г-подібної опори канатної транспортної установки (габаритні розміри)

Ключовою умовою виконання вимог щодо статичного навантаження досліджуваної конструкції є поглинання необхідних навантажень з урахуванням коефіцієнту динамічності $k_{\partial} = 2{,}0$ та забезпечення запасу міцності за межею текучості матеріалу виготовлення (Сталь 10): рівень зафіксованих напружень у результаті числового експерименту не повинен перевищувати 205 МПа.

Аналіз напружено-деформованого стану щогли транспортної установки методом кінцевих елементів дозволив обчислити

максимальне напруження на рівні 191,1 МПа. Дане значення зафіксовано в усіченій піраміді звуження щогли у її верхній частині (рис. 5). На рис. 5 подано напружено-деформований стан каркасу щогли.

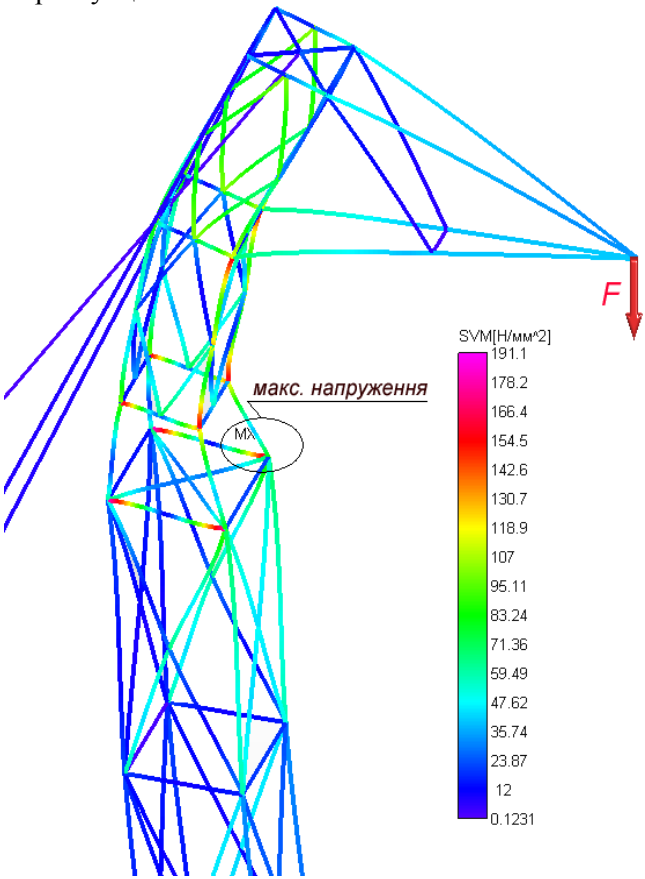


Рис. 5. Напружено-деформований стан каркасу щогли транспортної установки: стрижневе подання моделі (на карті відзначена область максимальних напружень)

Враховуючи той факт, що межа текучості матеріалу виготовлення щогли транспортної установки (Сталь 10) складає 205 МПа, а максимальне обчислене значення напружень – 191,1 МПа, можемо стверджувати про достатній запас міцності конструкції у даній стрижневій конфігурації. Рівень напружень

основи щогли знаходиться в межах 30÷25 МПа; центральної частини 35÷85 МПа; верхньої разом з консольним кронштейном – 85÷191,1 МПа. Аналізуючи розподіл напружень за довжиною консольного кронштейну (рис. 5), необхідно зауважити, що завдяки застосованому сортаменту (60×3мм) значення напружень залишились у межах 67,1 МПа (рис. 6).

а)

б)

Рис. 6. Графічні залежності розподілу напружень за довжиною стрижнів консольного кронштейну: а) стрижні № 1, 2; б) стрижні № 3, 4

На основі поданих на рис. 6 залежностей розподілу напружень за довжиною відповідних стрижнів консольного кронштейну робимо висновок про рівноміцність конструкції. Враховуючи обчислене максимальне значення у 67,1 МПа, досліджуваний кронштейн характеризується потрійним запасом міцності відносно межі текучості матеріалу виготовлення (Сталь 10), що дозволяє стверджувати про допустимість експлуатації кронштейну в умовах прикладання навантажень з коефіцієнтом динамічності $k_д$ (початково в крайові умови розрахунку було закладено значення $k_д = 2{,}0$). Значення осьової сили (режим розтягу) центрального канату дорівнює 6286 Н, а крайніх канатів – 8482 Н. Як бачимо, отримані значення є меншими за початково закладений попередній натяг (10000 Н). Це свідчить про те, що, володіючи власною жорсткістю та піддаючись активному навантаженню (F =30000 Н), щогла поглинула частину осьових зусиль від канатів, частково розвантаживши їх.

Значення реакцій та моментів згину в опорах (в'язях консольного типу) канатної транспортної установки дозволяє, за необхідності, продовжити розрахунки у напрямку несеної здатності ґрунту.

Моделювання роботи опор дало можливість не тільки визначити внутрішні силові фактори, які виникають в перерізах елементів, а оцінити їх напружений стан залежно від розмірів та форм поперечного перерізу. Це дасть можливість вибрати раціональні опори канатних установок залежно від схем навішування несучого канату.

1. Бичинюк І.В. Визначення довговічності канатів підвісних транспортних установок, які призначені для потреб спецпідрозділів МВС та МНС / І.В. Бичинюк, Я.Ф. Кулешник, В.В. Хлистун / Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами // Матеріали науково-практичної конференції 14 грудня 2011 р. – Львів: Львівський державний університет внутрішніх справ, 2011. – С. 267–267.
2. Мартинців М.П. Розрахунок основних елементів підвісних канатних лісотранспортних установок / Мартинців М.П. – К.: Ясмина, 1996. – 175 с.

3. Бичинюк І.В. Математична модель для дослідження впливу коливань несучих канатів на режими роботи підвісних транспортних канатних установок / І.В. Бичинюк, Т.В. Рудий, Д.М. Неспляк, В.Я. Гурільов / Актуальні проблеми діяльності кримінальної міліції та підготовки фахівців для її підрозділів // Матеріали VI звітної науково-практичної конференції факультету з підготовки фахівців для підрозділів кримінальної міліції Львівського державного університету внутрішніх справ (Львів,6 квітня 2012р.) – Львів: ЛьвДУВС, 2012. – С. 233–242.
4. Соломенцев О.Ю. Автоматизированное проектирование и производство в машиностроении / О.Ю. Соломенцев, В.Г. Митрофанова. – М.: Машиностроение, 1986. – 254с.
5. Патент на корисну модель UA 48067 U, МПК B61B 7/00. Проміжна щогла підвісної канатної установки / Мартинців М.П., Бичинюк І.В., Сологуб Б.В.; заявник і власник патенту Національний лісотехнічний університет України. – № u200907889. – Заявл. 27.07.2009. – Опубл. 10.03.2010. – Бюл. № 5. – 4 с.
6. Шимкович Д.Г. Расчёт конструкций в MSC/NASTRAN for Windows / Д.Г. Шимкович. – М.: ДМК Пресс, 2001. – 448 с.
7. Павлище В.Т. Основи конструювання та розрахунок деталей машин / В. Т. Павлище. – Львів: Афіша, 2003. – 558 с.

МАТЕМАТИЧНА МОДЕЛЬ ФУНКЦІОНУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ У СТРУКТУРНИХ ПІДРОЗДІЛАХ МНС УКРАЇНИ

Сташевський З.П.,
ст. лейтенант служби цивільного захисту, ад'юнкт
Грицюк Ю.І.,
завідувач кафедри управління інформаційною безпекою ЛДУ БЖД, д.т.н., професор

Проблема захисту інформації актуальна зараз не тільки для спеціальних служб, але й для всіх організацій, так чи інакше пов'язаних зі збереженням і розробленням нових виробів разом з технологіями їх виготовлення. Ефективна робота систем захисту інформації (СЗІ) в інформаційній структурі МНС України полягає в тому, що вона унеможливлює спотворення інформації, яка надходить, втрату секретної інформації, та забезпечує збереження державної таємниці. Проте на сьогодні виникає проблема в постановці задачі синтезу

ефективних засобів захисту інформації в інформаційних системах МНС України. Для розв'язання такої задачі необхідно передусім побудувати математичну модель ефективності функціонування СЗІ в структурних підрозділах МНС України [4].

Відомо, що інформаційна система (ІС) будь-якого структурного підрозділу може піддаватися різним загрозам, кількість яких нехай буде обмеженою

$$\tilde{Z}^{\text{дз}} = f(\tilde{P}^{\text{заг}}, \Delta\tilde{Q}^{\text{заг}}),$$

де: $\tilde{P}^{\text{заг}} = \{p_i^{\text{заг}}, i = \overline{1,m}\}$ – ймовірністю появи i-ої загрози; $\Delta\tilde{Q}^{\text{заг}} = \{\Delta q_i^{\text{заг}}, i = \overline{1,m}\}$ – обсяг збитку ІС, який наноситься i-ою загрозою. СЗІ виконує функцію повної або часткової ліквідації загроз для ІС. Основною характеристикою СЗІ є ймовірність усунення дії i-ої загрози з наявної множини $\tilde{P}^{\text{усун}} = \{p_i^{\text{усун}}, i = \overline{1,m}\}$. За рахунок функціонування СЗІ забезпечується зменшення збитку, що наноситься ІС під впливом джерел загроз.

Нехай ΣW – загальний попереджений збиток ІС, а $\tilde{W} = \{\omega_i, i = \overline{1,m}\}$ – попереджений збиток за рахунок ліквідації дії i-ої загрози. Тоді постановка задачі синтезу системи захисту інформації в ІС має такий вигляд: необхідно вибрати такий варіант реалізації СЗІ, яка забезпечить максимальне попередження збитку, що може виникнути під впливом різних загроз, при обмежених витратах на її функціонування. Формальна постановка задачі має такий вигляд:

знайти $\tilde{T}^0 = \arg\tilde{W}(\tilde{T}) \to \max : \tilde{T}^0 \in \tilde{T}^+$, (1)

при обмеженні $C(\tilde{T}^0) \le C^{\text{доп}}$, (2)

де: $\tilde{T} = \{t_j, j = \overline{1,n}\}$ – множина параметрів технічної реалізації СЗІ; $\tilde{T}^+ = \{t_j^+, j = \overline{1,n}\}$, $\tilde{T}^0 = \{t_j^0, j = \overline{1,n}\}$ – множина допустимих і оптимальних значень параметрів технічної реалізації СЗІ; $C^{\text{доп}}$ – сума допустимих витрати на функціонування СЗІ [1].

Для розв'язання цієї задачі необхідно насамперед сформулювати показник якості функціонування СЗІ, тобто $\tilde{W}(\tilde{T})$. Очевидно, попереджений збиток у загальному вигляді виражатиметься таким співвідношенням:

$$\widetilde{W} = F(\tilde{P}^{\text{заг}}, \Delta\tilde{Q}^{\text{заг}}, \tilde{P}^{\text{усун}}) \to F(\tilde{p}^{\text{заг}}, \Delta\tilde{q}^{\text{заг}}, \tilde{p}^{\text{усун}}, i = \overline{1,m}) \quad (3)$$

Попереджений збиток за рахунок ліквідації дії *i*-ої загрози:

$$\widetilde{W} = \{\omega_i = p_i^{\text{заг}} \cdot \Delta q_i^{\text{заг}} \cdot p_i^{\text{усун}}, i = \overline{1,m}\}. \quad (4)$$

За умови незалежності загроз і адитивності їх наслідків отримуємо

$$\sum W = \sum_{i=1}^{n} \omega_i = \sum_{i=1}^{m} p_i^{\text{заг}} \cdot \Delta q_i^{\text{заг}} \cdot p_i^{\text{усун}}. \quad (5)$$

Ймовірність появи *i*-ої загрози ($p_i^{\text{заг}}$) визначається статистично і відповідає відносній частоті її появи:

$$\tilde{P}^{\text{заг}} = \left\{ p_i^{\text{заг}} = {\lambda_i}\Big/{\sum_{j=1}^{m} \lambda_j' = \lambda_i', i = \overline{1,m}} \right\}, \quad (6)$$

де: λ_i – частота появи *i*-ої загрози; λ_i' – нормоване значення частоти появи *i*-ої загрози.

Збиток ($\Delta\tilde{q}^{\text{заг}}$), що виникає від впливу *i*-ої загрози, може визначатися в абсолютних одиницях: фінансових чи матеріальних втратах на відновлення СЗІ, тимчасових витратах, обсязі знищеної або «зіпсованої» інформації і т.д. Проте, практично це зробити дуже складно, особливо на ранніх етапах функціонування СЗІ. Тому доцільно замість абсолютного збитку використовувати відносний збиток, який, по суті, є ступенем небезпеки *i*-ої загрози для ІС. Ступінь небезпеки здебільшого визначається експертним шляхом в припущенні, що усі загрози для ІС становлять повну групу подій [2], тобто:

$$0 \le \Delta\tilde{Q}^{\text{заг}} \le 1 \to \{0 \le \Delta\tilde{q}^{\text{заг}} \le 1, i = \overline{1,m}\}; \sum_{i=1}^{m} \Delta q_i^{\text{заг}} = 1.$$

Найбільш складним питанням є визначення ймовірності усунення *i*-ої загрози ($p_i^{\text{усун}}$) при функціонуванні СЗІ. Зробимо звичайне припущення, що ця ймовірність визначається тим, наскільки повно враховані кількісних і якісних вимог до СЗІ при її проектуванні, тобто:

$$\tilde{P}^{\text{усун}} = \{p_i^{\text{усун}} = f_i(\tilde{X}_i), i = \overline{1,m}\}, \quad (7)$$

де $\tilde{\tilde{X}} = \left\{ \tilde{X}_i = \{x_{ij}, j = \overline{1,n}\}, i = \overline{1,m} \right\}$ – ступінь виконання *j*-ої вимоги до СЗІ для усунення *i*-ої загрози.

Нехай перші "*k*" вимог будуть кількісними ($j=\overline{1,k}$) інші $j=\overline{k+1,n}$ – якісними вимогами. Ступінь виконання *j*-ої кількісної вимоги визначається її наближенням до потрібного (оптимального) значення. Для оцінювання ступеня виконання *j*-ої кількісної вимоги до СЗІ найзручніше використовувати її нормоване значення:

$$\tilde{\tilde{X}}' = \left\{ \tilde{X}'_i = \left\{ x'_{ij} = \frac{x_{ij} - x_{ij}^{\text{í}\tilde{a}}}{x_{ij}^{\text{í}\hat{e}} - x_{ij}^{\text{í}\tilde{a}}}, j = \overline{1,k} \right\}, i = \overline{1,m} : 0 \le x'_{ij} < 1 \right\}, \quad (8)$$

де: x'_{ij} – нормоване значення *j*-ої вимоги до СЗІ для усунення *i*-ої загрози, визначається за [3]; $x_{ij}^{\text{íê}}$, $x_{ij}^{\text{íã}}$ – найкраще і найгірше значення.

З урахуванням формули (8) отримаємо такі співвідношення:

при $x_{ij}^{\text{íê}} = x_{ij}^{\max}; x_{ij}^{\text{íã}} = x_{ij}^{\min}$, (9)

$$\tilde{\tilde{X}}' = \left\{ \tilde{X}'_i = \left\{ x'_{ij} = \frac{x_{ij} - x_{ij}^{\min}}{x_{ij}^{\max} - x_{ij}^{\min}}, j = \overline{1,k} \right\}, i = \overline{1,m} \right\},$$

при $x_{ij}^{\text{íê}} = x_{ij}^{\min}; x_{ij}^{\text{íã}} = x_{ij}^{\max}$, (10)

$$\tilde{\tilde{X}}' = \left\{ \tilde{X}'_i = \left\{ x'_{ij} = \frac{x_{ij}^{\max} - x_{ij}}{x_{ij}^{\max} - x_{ij}^{\min}}, j = \overline{1,k} \right\}, i = \overline{1,m} \right\}, \quad (11)$$

$$x'_{ij} = \begin{cases} 0, & \text{якщо} \quad x_{ij} < x_{ij}^{\min}; x_{ij} > x_{ij}^{\max}; \\ 1, & \text{якщо} \quad x_{ij} = x_{ij}^{opt}; \\ \dfrac{x_{ij} - x_{ij}^{\min}}{x_{ij}^{opt} - x_{ij}^{\min}}, & \text{якщо} \quad x_{ij}^{\min} \le x_{ij} \le x_{ij}^{opt}; \\ \dfrac{x_{ij}^{\max} - x_{ij}}{x_{ij}^{\max} - x_{ij}^{opt}}, & \text{якщо} \quad x_{ij}^{opt} \le x_{ij} \le x_{ij}^{\max}. \end{cases}$$

Ступінь виконання якісної вимоги визначається функцією належності до найкращого значення $\mu(x_{ij})$.

Розклавши функцію (7) в ряд Маклорена і обмежившись тільки першими членами ряду, отримаємо

$$\tilde{P}^{\text{усун}} = \left\{ p_i^{\text{усун}} = p_i^{\text{усун}}(0) + \sum_{i=k+1}^{n} \frac{\partial p_i^{\text{усун}}}{\partial x_{ij}} \cdot x_{ij} + \sum_{i=k+1}^{n} \frac{\partial^2 p_i^{\text{усун}}}{\partial x_{ij}^2} \cdot x_{ij}^2 + \cdots \ , i = \overline{1,m} \right\}, \quad (12)$$

де: $p_i^{\text{усун}}(0) = 0$ – ймовірність усунення *i*-ої загрози при не виконанні вимог lj СЗІ; $\frac{\partial p_i^{\text{усун}}}{\partial x_{ij}} = \alpha_{ij}$ – величина, яка характеризує ступінь впливу *j*-ої вимоги на ймовірність усунення *i*-ої загрози (важливість виконання *j*-ої вимоги для усунення *i*-ої загрози). Очевидно, що $0 \le \alpha_{ij} \le 1; \sum_{j=k+1}^{n} \alpha_{ij} = 1, i=\overline{1,m}$.

Після підстановки в (12) відповідних значень отримаємо:

$$\tilde{P}^{\text{усун}} = \left\{ p_i^{\text{усун}} = \sum_{j=1}^{k} \alpha_{ij} \cdot x'_{ij} + \sum_{j=k+1}^{n} \alpha_{ij} \cdot \mu(x_{ij}) + \cdots \ , i = \overline{1,m} \right\} \quad (13)$$

Остаточно формула (5) для оцінювання загальної величини ΣW попередженого збитку набирає такого вигляду:

$$\sum W = \sum_{i=1}^{m} \lambda'_i \cdot \Delta\tilde{q}^{\text{заг}} \left(\sum_{j=1}^{k} \alpha_{ij} \cdot x'_{ij} + \sum_{j=k+1}^{n} \alpha_{ij} \cdot \mu(x_{ij}) \right). \quad (14)$$

Таким чином, задача синтезу СЗІ у вигляді (1) і (2) зводиться до оптимального обґрунтування кількісних і якісних вимог до СЗІ при допустимих витратах на її функціонування, тобто набуває такого вигляду:

знайти $$\tilde{W}\left(\tilde{\tilde{X}}'\right) \to \max \quad , \quad (15)$$

при обмеженні $$C(\tilde{\tilde{X}}') \le C^{\text{äîï}}.$$

Згідно з формулюванням задачі (15), основними етапами її розв'язання є:

- збирання та оброблення експертної інформації про характеристики загроз: частоту появи *i*-ої загрози λ'_i і збитку $\Delta\tilde{q}^{\text{заг}}, i = \overline{1,m}$;

- збирання та оброблення експертної інформації для визначення важливості виконання *j*-ої якісної вимоги до СЗІ для усунення *i*-ої загрози α_{ij} і функції належності $\mu(x_{ij}),\ j=\overline{1,n},\ i=\overline{1,m}$;
- оцінювання вартості СЗІ для конкретного варіанту її реалізації залежно від ступеня виконання вимог $C(x'_{ij},\ j=\overline{1,n};\ i=\overline{1,m})$;
- розроблення математичної моделі та алгоритму вибору раціонального варіанту побудови СЗІ (раціонального завдання щодо вимог) відповідно до постановки (15) як задачі нечіткого математичного програмування.

За відсутності інформації про джерела загроз ІС, для розв'язання задачі (15) можна використати показник такого вигляду:

$$\Sigma W = \sum_{i=1}^{m}\left(\sum_{i=1}^{k}\alpha_{ij}\cdot x'_{ij} + \sum_{j=k+1}^{n}\alpha_{ij}\cdot\mu(x_{ij})\right). \qquad (16)$$

Таким чином, ефективний захист інформації є одним з найголовніших аспектів при побудові надійної ІС будь-яких структурних підрозділів МНС України. Наведена математична модель функціонування СЗІ в ІС структурного підрозділу МНС України дає змогу вибору такого її варіанта реалізації, який може забезпечити максимум попередженого збитку, отриманого внаслідок дії загроз при доступних витратах на цю систему. Це забезпечить безперебійне і вчасне реагування рятувальної служби МНС на будь-які надзвичайні ситуації.

1. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О.М. Новіков. – К. : Вид. група BHV, 2009. – 608 с.
2. Грицюк Ю.І. Проблеми захисту інформації у структурних підрозділах МНС України / Ю.І. Грицюк, Т.Є. Рак // Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2011. – Вип. 21.12. – С. 330-346.
3. Комплексна система захисту інформації. [Електронний ресурс]. – Доступний з http://uk.wikipedia.org/wiki/Комплексна_система_захисту_інформації.

4. Сташевський З.П. Особливості проблеми синтезу систем захисту інформації у структурних підрозділах МНС України / З.П. Сташевський, Ю.І. Грицюк // Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2012. – Вип. 22.10. – С. 79-96.

ШЛЯХИ НАЛАГОДЖЕННЯ ОХОРОНИ КОМЕРЦІЙНОЇ ТАЄМНИЦІ НА ПРОМИСЛОВИХ ПІДПРИЄМСТВАХ

Копитко М.І.,
доцент кафедри менеджменту Львівського державного університету внутрішніх справ, к.е.н.

Важливим завданням у процесі діяльності промислових підприємств є вміння надійно перекрити канали просочування конфіденційної інформації. Коли на підприємстві визначено перелік відомостей, що становлять комерційну таємницю, то потрібно передбачити джерела витоку цієї конфіденційної інформації [3]. Потенційними джерелами витоку комерційної таємниці можуть бути [1, 2]:

1. *Документація підприємства або просто документи (накази, бізнес-плани, ділове листування тощо)*. Це найпоширеніша форма обміну інформацією, її накопичення та зберігання. Важливою особливістю документів є те, що вони іноді є єдиним джерелом найважливішої інформації (наприклад, контракт, боргова розписка та ін.), а отже, їх втрата, викрадання, знищення можуть завдати непоправного збитку. Структура документів промислового підприємства є предметом окремого розгляду, оскільки документи можуть мати не тільки різний зміст, а й різні фізичні форми – матеріальні носії. Різноманітність форм і змісту документів за призначенням, спрямованістю, характером руху і використанням є вельми принадним джерелом для зловмисників, що, природно, привертає їх увагу до можливості отримання інформації, яка їх цікавить.

2. *Персонал підприємства (усі, хто працює на підприємстві, у тому числі й керівник)*. У деяких джерелах конфіденційної інформації люди відіграють особливу роль, оскільки здатні виступати не тільки джерелом, а й суб'єктом зловмисних дій. Вони не тільки володіють і розповсюджують інформацію в

рамках своїх функціональних обов'язків, а й можуть аналізувати, узагальнювати її, робити певні висновки, а також за певних умов приховувати, продавати її та вчиняти інші кримінальні дії, аж до злочинних зв'язків із зловмисниками.

3. *Партнери, контрагенти або клієнти*, що користуються або користувалися послугами підприємства, найбільш обізнані із джерелами найважливіших секретів фірми. Тому вони заслуговують ретельної уваги під час аналізу системи захисту.

4. *Вироблена продукція або надані послуги*. Продукція в промисловості є особливим джерелом інформації, за характеристиками якої активно полюють конкуренти. Заслуговує на увагу нова або така, яку готують для виробництва, продукція. Враховують етапи її «життєвого циклу»: задум, макет, дослідний зразок, випробування, серійне виробництво, експлуатація, модернізація і зняття з виробництва. Кожен із цих етапів супроводжується специфічною інформацією, що виявляється різними фізичними ефектами, які у вигляді демаскувальних ознак можуть розкрити відомості, що охороняються.

5. *Технічні засоби забезпечення виробничої діяльності.* Ці засоби є широкою і ємкою групою джерел конфіденційної інформації. До групи засобів забезпечення виробничої діяльності належать, зокрема, телефони і телефонний зв'язок, телевізори і промислові телевізійні установки, радіоприймачі, радіотрансляційні системи, системи гучномовного зв'язку, підсилювальні системи, кіносистеми, охоронні й пожежні системи та інші, які за своїми параметрами можуть бути джерелами перетворення акустичної інформації в електричні й електромагнітні поля, здатні утворювати електромагнітні канали просочування конфіденційної інформації.

6. *Непрямі джерела (відходи виробництва, реклама, публікації у пресі).* Більшість інформації можна отримати саме з непрямих джерел. Професійно проведена аналітична робота іноді дає чудовий результат. Зазвичай цьому джерелу не надають особливої уваги, тому воно є найбільш доступним. Наприклад, відходи виробництва, які називають непотрібом, можуть багато про що розповісти щодо використовуваних матеріалів, їх складу, особливостей виробництва, технології. І отримати їх можна майже безпечним і законним шляхом на

звалищах, смітниках, у місцях збору металобрухту, в корзинах для сміття в робочих кабінетах. Умілий аналіз цих відходів може багато що розповісти про секрети виробництва. У публікаціях – книгах, статтях, монографіях, оглядах, повідомленнях, рекламних проспектах, доповідях, тезах та ін.: можна мимовільно розкрити всі виробничі таємниці.

Із джерел конфіденційної інформації можна мати дані про склад, зміст і напрям діяльності промислового підприємства, що цікавить конкурентів. Природно, що така інформація їм украй потрібна, і вони знайдуть способи отримати її. Тому грамотна система захисту, розроблена з урахуванням усіх її особливостей, дасть змогу запобігти багатьом проблемам.

1. Економічна безпека підприємств: Підручник / Ортинський В.Л., Керницький І.С., Живко З.Б. та ін..; – К.: Алерта, 2011. – 704 с.
2. Живко З.Б. Конкурентна (ділова) розвідка в системі економічної безпеки. Монографія / З.Б. Живко. – Львів: АПРІОРІ, 2008. – 192 с.
3. Артур Вайс. Краткое руководство по конкурентной разведке: как собирать и использовать информацию о конкурентах. [Електронний ресурс] – Джерело доступу: http://ci-razvedka.narod.ru/Arthur_Weiss_Brief_Guide_CI.html

СУТНІСТЬ ПОНЯТТЯ «СИСТЕМА ЕКОНОМІЧНОЇ БЕЗПЕКИ» ПІДПРИЄМСТВА

Живко З.Б.,
професор кафедри менеджменту ЛьвДУВС, к.е.н., доцент

Для тлумачення суті поняття «система економічної безпеки», перш за все розглянемо поняття «безпека» та «економічна безпека». Безпека – властивість будь-якої системи, що виражається у здатності предмета, явища чи процесу зберігати свої основні характеристики, сутнісні параметри патологічних, руйнівних впливів [1]. Щодо поняття «економічна безпека», то Л. Коженьовскі виокремлює такі стани:

- відчуття безпеки (свідомість існування, відсутності чи можливості протидії небезпеці) у визначенні загальному, місцевому чи індивідуальному [2, с. 147];

- об'єктивний стан безпеки (наявність чи відсутність загрози) у загальному вимірі, місцевому чи індивідуальному.

Слід погодитися з авторами [3], які стверджують, що у найбільш загальному розумінні, поняття «безпека» – це стан захищеності від будь-чого. Воно є прикладним як для загальних речей, так і конкретних ситуацій, пов'язаних з особистістю, підприємством, державою [3]. Зокрема, З.С. Варналія [4, с.13], систематизовано міждисциплінарний підхід до визначення поняття безпека (рис. 1):

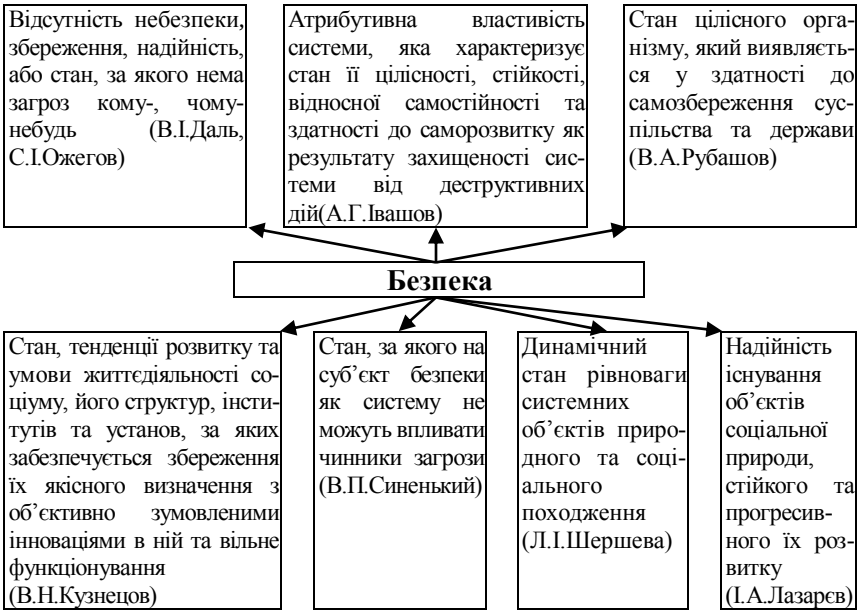


*Рис.1. Міждисциплінарні підходи до визначення поняття безпека (*складено автором за [4])*

З огляду на представлені визначення категорії «безпека», слід відзначити такі положення:

- безпека – це стан;
- безпека – це здатність протидії;
- ключовими для існуючих визначень безпеки є терміни «захищеність», «відсутність небезпеки», «спокій», «незалежність», «стабільність»,«допустимі межі», «безпечні та

контрольовані умови», «збереження», «надійність», «захист від небезпеки (загроз)», «механізм запобігання загрозам», «зменшення впливу загроз»;

- опосередкованими категоріями є «прогресивний розвиток», «існування», «цілісність», «життєдіяльність соціуму та його структур», «розвиток», «впевненість», «рівновага», «самозбереження».

Виокремивши основні характеристики безпеки в розрізі багатоманітності наведених тлумачень категорії «безпека», зупинимося на сутності категорії «економічна безпека», враховуючи її широку спектральність та уточнення на макрорівні. Зокрема, В. Забродський трактує економічну безпеку підприємства як сукупність факторів, які визначають стійкість, незалежність, забезпечення економічних інтересів тощо [5, с. 35]. Розуміння такого підходу зближується із поняттям адаптації та стійкості підприємства. Стрімкому дослідженню проблематики економічної безпеки підприємства сприяла розбудова ринкових відносин, тому низка науковців враховують вплив умов зовнішнього середовища підприємства. Так, Д. Ковальов і Т. Сухорукова визначали економічну безпеку підприємства як захищеність його діяльності від негативного впливу зовнішнього середовища та здатність швидко усувати різноманітні загрози або пристосуватись до умов, які не впливають негативно на його діяльність [6, с. 48].

Сьогодні серед науковців як вітчизняних, так і поширено трактування сутності економічної безпеки господарюючих суб'єктів за видами їх професійної діяльності (банківські установи, страхові компанії, сільськогосподарські підприємства, підприємства харчової промисловості, торгівлі тощо), та за формою власності і наявністю капіталу (крупні компанії, холдинги, акціонерні товариства, підприємства малого і середнього бізнесу тощо). Так, О.А.Кириченко, В.В. Коваленко, С.І. Мельник вивчали економічну безпеку комерційних банків; О.А.Кириченко та Т.В. Сусуловська досліджували економічну безпеку діяльності кредитних спілок; Т.В. Яворська, О.Й. Жабинець – страхових компаній; В.І.Франчук, Є.М.Палига, М.Я.Рупняк – економічну безпеку акціонерних товариств; З.С.Варналій, І.І.Мазур, А.І.Сухоруков, С.Г.Дрига, О.М.Сумець,

М.Б.Тумар – економічну безпеку підприємства, малого та середнього бізнесу.

На нашу думку, економічна безпека підприємства – це такий стан підприємства, який дозволяє зберігати стійкість до внутрішніх і зовнішніх загроз, забезпечує стабільність розвитку та здатність локалізувати і протидіяти загрозам, забезпечивши потреби і захищенність особи, підприємства, держави.

Надійний захист економічної безпеки підприємства можливий лише за комплексного та системного підходу до його організації, тому повинна бути розроблена дієва система економічної безпеки підприємства(СЕБП).

Сьогодні поширилась тенденція щодо захисту інформації, як найціннішого ресурсу підприємства, який покладено в основу економічної безпеки, яку розглядають як систему захисту інформації. Однак, система економічної безпеки підприємства – це комплекс організаційно-управлінських, режимних, охоронних, технічних, профілактичних, рекламних та пропагандистських заходів, спрямованих на кількісну реалізацію захисту інтересів підприємства від зовнішніх та внутрішніх загроз.

Вчені [6] визначають СЕБП, як сукупність заходів (спрямованих на досягнення визначених цілей) розглянутих з точки зору їх генерування та їх взаємозв'язку один з одним [6], однак не вказано спрямованість системи.

Більш повним є визначення СЕБП Ярочкіна В.І., що СЕБП – це організована сукупність спеціальних органів, служб,засобів, методів і заходів, забезпечуючи захист важливих інтересів особистості, підприємства і країни від зовнішніх і внутрішніх загроз [7].

Загалом система економічної безпеки розділяється відповідно до трактування економічної безпеки. Існують два концептуальні підходи до трактування безпеки: статистичний (безпека як стан) і діяльнісний (безпека як діяльність). Із врахуванням основних завдань, умов конкурентної боротьби, специфіки бізнесу формується механізм забезпечення економічної безпеки. Логічно, що схема побудови є індивідуальною для кожного підприємства, її повнота та ефективність багато в чому залежить від законодавчої бази держави, матеріально-технічної та фінансової бази підприємства.

На нашу думку, СЕБП – комплекс постійно діючої взаємоузгодженої сукупності заходів, засобів та принципів, які за допомогою механізму дії яких забезпечується стан безпеки підприємства.

1. Матеріали сайту. Система. Вікіпедія. [Електронний ресурс]. – Режим доступу: http://ru.wikipedia.org.
2. Коженьовскі Л. Управління безпекою / Л. Коженьовскі // Актуальні проблеми економіки. – 2004. –№ 1 (31). – С. 147.
3. Кузенко Т.Б. Управління фінансовою безпекою підприємства: методичний аспект / Т.Б. Кузенко, Н.В. Сабліна, О.Ю. Литовченко // Вісник економіки транспорту і промисловості, 2010. – № 29. – С. 119 – 123.
4. Варналій З.С. Економічна безпека України: проблеми та пріоритети зміцнення : [монографія] / З.С. Варналій, Д.Д. Буркальцева, О.С. Саєнко. – К. : Знання України, 2011. – 299 с. – Бібліогр. в кінці розд.
5. Забродский В.А. Современные методы организации и управления промышленным производством / В.А. Забродский, Н.А. Кизим, Л.И. Янов. – Харьков : АО «Бизнес-Информ», 1997. – 64с.
6. Ковалев Д. Экономическая безопасность предприятия / Д. Ковалев, Т. Сухорукова // Экономика Украины. – 1998. – № 10. – С. 48–51.
7. Сумець О.М. Стратегії сучасного підприємства та його економічна безпека: Навч.посіб. / О.М.Сумець, М.Б.Тумар. – К.: Хай-Тек Прес, 2008р. – 400с.
8. Ярочкин В.І. «Система безопасности фирмы»/ В.І.Ярочкин. – М.: – Ось-89, 2003р. – С. 5-36.

ПРОБЛЕМИ ВЗАЄМОДІЇ ОРГАНІВ ВНУТРІШНІХ СПРАВ ТА ПОДАТКОВОЇ МІЛІЦІЇ ПРИ ЗАПОБІГАННІ ЗЛОЧИНАМ, ЩО ПОРУШУЮТЬ ПОРЯДОК ЗДІЙСНЕННЯ ОПЕРАЦІЙ З МЕТАЛОБРУХТОМ

Сисоєва В.П.,
ад'юнкт кафедри кримінології та кримінально-виконавчого права Національної академії внутрішніх справ

Розвиток важкої промисловості в нашій державі ще до становлення незалежності підкреслив важливість металобрухту для металургійної галузі. Адже металобрухт є важливою сировинною базою для багатьох металургійних комбінатів. Після розпаду СРСР та переходу від командно-

адміністративної системи господарювання до ринкової, з розривом міжгалузевих зв'язків, значення металобрухту збільшилося. Це пов'язане з тим, що переробка металобрухту – це не тільки економічно вигідна справа, а й важливий компонент збереження природних ресурсів, що не відновлюються.

У зв'язку з інтенсивною криміналізацію, ринок обігу металобрухту вже не перший рік перебуває у зоні посиленого контролю з боку правоохоронних органів. Про це говорить постійне збільшення зареєстрованих злочинів, підвищення кількості осіб, які притягуються до відповідальності за порушення законодавства в сфері забезпечення порядку здійснення операцій з металобрухтом.

Основні зусилля правоохоронних органів, як правило, спрямовуються на виявлення незаконних пунктів прийому металобрухту; затримання автотранспорту з металобрухтом, на який відсутні документи про походження; виявлення та припинення порушень юридичними і фізичними особами чинного законодавства, що регулює операції з металобрухтом; притягнення до кримінальної та адміністративної відповідальності осіб, причетних до таких злочинів та правопорушень. Такі заходи проводяться з метою захисту економічних інтересів держави, недопущення незаконного обігу металобрухту, попередження фактів крадіжок, розкрадань, розукомплектування обладнання об'єктів і підприємств енергетики, транспорту, зв'язку та сільського господарства.

Якщо розглядати виявлення, розкриття та розслідування злочинів в сфері обігу металобрухту, кримінально-процесуальний кодекс України 1960р. визначав, що досудове слідство за фактами вчинення злочинів, що порушують порядок здійснення операцій з металобрухтом, провадиться органами внутрішніх справ та податкової міліції. Відповідно до ст.ст.112, 425 КПК України редакції 1960р., провадження досудового слідства по даній категорії справ здійснюється лише за умови наявності кваліфікованого складу злочину (тобто ч.2 ст.213 КК України) та належить до компетенції органів внутрішніх справ. У випадках некваліфікованого складу (ч.1 ст.213 КК України) законодавством була передбачена протокольна форма досудової підготовки матеріалів. Крім того, ч.4 ст.112 Кримінально-

процесуального кодексу України 1960р. визначала випадки, коли досудове слідство в справах, порушених за аналізованою статтею, ведеться слідчими органами податкової міліції.

Що стосується Кримінального процесуального кодексу України 2012р., стаття 216 «Підслідність» не містить вказівки на те, що слідчі органів, які здійснюють контроль за додержанням податкового законодавства, мають право розслідувати злочини, передбачені ст.213 КК України. Це означає, що за загальним правилом досудове розслідування кримінально караних порушень порядку здійснення операцій з металобрухтом здійснюється виключно слідчими органів внутрішніх справ.

Варто відзначити, що найбільше таких злочинів виявляється та реєструється під час проведення профілактичних операцій, які в органах внутрішніх справ мають умовну назву «метал», а в органах податкової міліції – «металобрухт». Так, тільки в 2012 році за 20 днів відпрацювання міліцією на території Донецької області було виявлено понад півтисячі злочинів на ринку металобрухту. На території цієї області проходило оперативно-профілактичне відпрацювання, мета якого – викриття злочинів, пов'язаних із збором, переробкою, продажем брухту чорних і кольорових металів, виявлення зловживань, пов'язаних з його експортом, розкриття крадіжок металу, а також припинення діяльності незаконних пунктів прийому металобрухту і промислових майданчиків. Як зазначається в аналітичному огляді результатів, було порушено 40 кримінальних справ за фактами порушення порядку здійснення операцій з металобрухтом [1].

Податкова міліція Державної податкової служби також регулярно звітує в засобах масової інформації стосовно результатів проведення своїх профілактичних заходів. Так, у тій самій Донецькій області органами податкової міліції було порушено 24 кримінальні справи проти власників пунктів прийому брухту чорних та кольорових металів під час проведення операції «металобрухт» [2].

Як ми бачимо, ці профілактичні заходи проводяться незалежно один від одного, хоча, враховуючи комплексність протиправної діяльності при незаконних операціях з металобрухтом, тобто можливість вчинення багатьох інших злочинів,

дії оперативних підрозділів щодо запобігання порушенням порядку здійснення операцій з металобрухтом повинні мати комплексний характер, а для підвищення ефективності в запобіжній діяльності потрібна взаємодія між різними підрозділами правоохоронних органів [3, с. 22].

Під час проведення анкетування серед працівників правоохоронних органів з метою отримання емпіричних даних для дослідження, нами було поставлене запитання правоохоронцям стосовно їх думок щодо визначення порядку взаємодії підрозділів правоохоронних органів з метою підвищення ефективності запобігання злочинам, що порушують порядок здійснення операцій з металобрухтом. В результаті виявилося, що більше половини респондентів не знають, якими документами визначається цей порядок. Крім того, 60% опитаних співробітників взагалі не мали досвіду взаємодії з підрозділами інших правоохоронних структур у попередженні злочинів в сфері обігу металобрухту, а серед тих, хто мав такий досвід, переважає взаємодія у формі обміну інформацією, а не прийняття участі в комплексних заходах запобігання.

Аналіз сучасного стану нормативно-правового забезпечення запобіжної діяльності дозволяє дійти висновку, що рівень цього забезпечення залишається низьким. Існує декілька нормативно-правових актів, які регулюють цю сферу діяльності правоохоронних органів. Насамперед, це Рішення Ради національної безпеки і оборони України «Про стан злочинності у державі та координацію діяльності органів державної влади у протидії злочинним проявам та корупції», яке введене в дію Указом Президента України від 27.10.2009 № 870. На виконання вимог цього Указу в адміністративних одиницях розроблені комплексні програми профілактики злочинності та охорони громадського порядку. Проте, вони також не містять нормативного закріплення порядку взаємодії підрозділів правоохоронних органів з метою запобігання як економічним злочинам взагалі, так і злочинам, що порушують порядок здійснення операцій з металобрухтом, зокрема. Для підвищення ефективності запобігання порушенням порядку здійснення операцій з металобрухтом необхідно розробити порядок такої взаємодії, визначити комплекс заходів, при реалізації яких будуть залу-

чатися різні правоохоронні органи. Це забезпечить результативне та плідне виявлення та усунення обставин, які створюють умови для вчинення таких злочинів.

1. Коментарі, статті, нариси [електронний ресурс] // Офіційний сайт ГУМВС України в Донецькій області – режим доступу: http://doneck-mvs.gov.ua/body.php?year=2012&lang=ukr&m=02&id=09_06-12.01&act=st
2. Регіональні новини ПМ ДПС України [електронний ресурс] // Офіційний портал Державної податкової служби України – режим доступу: http://sts.gov.ua/media-tsentr/regionalni-novini/58620.html
3. Ніколаюк С.І., Никифорчук Д.Й., Тихонов В.О., Тихонова О.В. Протидія незаконним операціям з металобрухтом: Науково-практичний посібник. – К.: КНТ, 2006. – 104 с.

МЕТОДИКИ ТЕСТУВАННЯ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

Мандрона М.М.,
викладач кафедри управління інформаційною безпекою ЛДУБЖД

Визначення якості та надійності генераторів випадкових та псевдовипадкових послідовностей – одна з основних задач сучасної прикладної та теоретичної криптографії, тому що вони використовуються для генерації ключів та інших випадкових параметрів криптосистем. Існують спеціальні методики тестування для оцінки якості випадкових послідовностей. На сьогоднішній день розглядаються групи тестів, які використовуються для аналізу рівня безпеки генераторів псевдовипадкових чисел (ПВЧ), а також різні методики інтерпретації отриманих результатів.

Для дослідження якості генераторів псевдовипадкових чисел використовують дві групи тестів [1]:

- графічні тести;
- статистичні тести.

На рис. 1 запропонована класифікація методик тестування генераторів псевдовипадкових чисел.

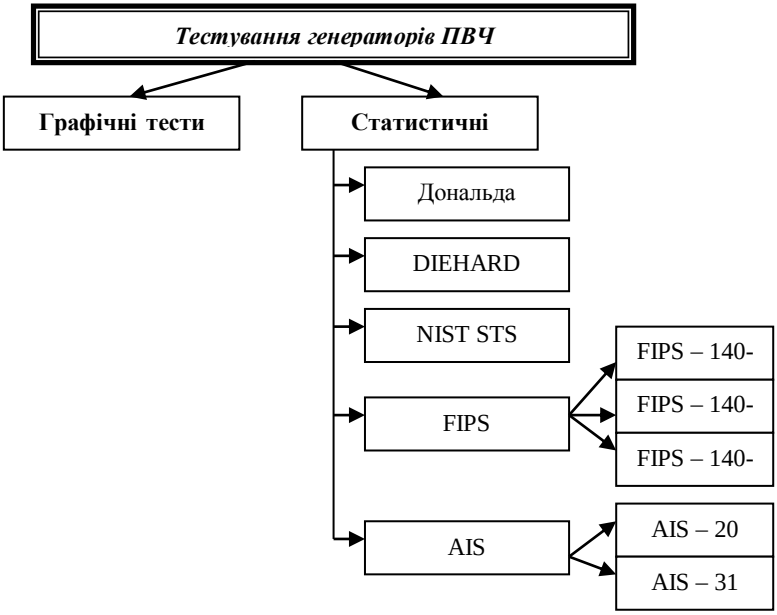


Рис. 1. Класифікація методик тестування генераторів ПВЧ

При графічному тестуванні статистичні властивості послідовностей відображаються у виді графічних залежностей, за виглядом яких роблять висновки про властивості досліджуваної послідовності. До даної категорії відносяться такі тести: гістограма розподілу елементів послідовності, розподіл на площині, перевірка серій, перевірка на монотонність, автокореляційна функція, профіль лінійної складності, графічний спектральний тест. Результати графічних тестів інтерпретуються людиною, тому висновки можуть бути неоднозначними.

Статистичні тести використовуються для перевірки певної нульової гіпотези H0 щодо випадковості сформованої послідовності. З цією нульовою гіпотезою пов'язана альтернативна гіпотеза На про те, що послідовність не випадкова. Для кожного тесту, що застосовується, можна зробити висновок щодо прийняття чи відхилення нульової гіпотези, виходячи із сформованої генератором послідовності. При цьому для кожного тесту має бути вибрана адекватна статистика випадковості, на основі якої може бути прийнята або відхилена нульова гіпотеза.

Теоретично для нульової гіпотези розподілення статистики визначається математичними методами. Під час проведення тесту розраховується значення тестової статистики, яке порівнюється з критичним. Якщо значення тестової статистики перевищує критичне значення, нульова гіпотеза для випадковості відхиляється, інакше – приймається [2].

Статистичні тести, на відміну від графічних тестів (результати інтерпретуються користувачами, внаслідок чого можливі відмінності у трактуванні результатів), характеризуються тим, що вони видають чисельну характеристику, яка дозволяє однозначно сказати, пройдено тест чи ні.

Нижче описано короткий огляд найбільш відомих на сьогоднішній день методик тестування.

Методика тестів Дональда Кнута заснована на статистичному критерії $\chi 2$. Обчислюване значення статистики $\chi 2$ порівнюється з табличними результатами, і залежно від імовірності появи такої статистики робиться висновок про її ефективність. Серед переваг цих тестів – легкий та швидкий алгоритм виконання. Недолік – невизначеність у трактуванні результатів. Перелік тестів: перевірка незчіплених серій, перевірка інтервалів, перевірка комбінацій, тест збирача купонів, перевірка перестановок, перевірка на монотонність та перевірка кореляції [1].

Система статистичного тестування DIEHARD була запропонована Джорджем Марсалі для дослідження статистичних властивостей розроблених ним же конгруентних генераторів. Недоліки системи – параметри тестування жорстко фіксовані, неточність у трактуванні результатів обробки, деякі тести не мають змістовного обґрунтування. У систему входять такі тести: перевірка проміжків між «днями народження», перевірка перестановок, що перетинаються, перевірка рангів матриць 32x32; 31x31; 6x8, літерні тести – перевірка потоку бітів, перевірка розріджених пар, що перетинаються, тест підрахунок одиниць в потоці байт [1,2].

Методика FIPS – дана методика використовується для технологічного аналізу вихідних послідовностей генераторів ПВЧ. Вона є стандартом для контролю криптографічних модулів. Складається з 4-х статистичних тестів: монобітний,

«покер-тест», тест серій, тест довжини серій. Для цих тестів, задаються межі для задовільних значень статистичних параметрів. Якщо який-небудь з тестів не пройдений, то вважається, що генератор не пройшов весь комплекс перевірок [2,3].

Методика AIS – застосовується для тестування псевдовипадкових послідовностей. Може використовуватись як у процесі формування послідовності, так і в процесі дослідження, а також для технологічного тестування. Основна ідея полягає в тому, що придатність генераторів псевдовипадкових чисел має бути оцінена з урахуванням криптографічних застосувань, у яких вони використовуються. Система AIS складається з 4-х функціональних класів К1, К2, К3, К4. Ці класи описують набір ієрархічних вимог до генераторів ПВЧ. Аналіз показав, що методика AIS 31 за своєю ефективністю забезпечує такі ж результати тестування як NIST STS. Перевагою AIS 31 є те, що він забезпечує тестування як у реальному часі, так і в процесі досліджень [2].

Методика NIST STS – використовується як засіб комплексного контролю. Статистичні тести NIST призначені для перевірки послідовності, сформованої генератором, на випадковість. Для кожного тесту отримують висновок про прийняття або відхилення нульової гіпотези, ґрунтуючись на сформованій досліджуваним генератором послідовності. Кожен тест заснований на обчисленні значення тестової статистики, яка є функцією даних. Ця статистика використовує обчисленні значення P-value, за допомогою якого і визначається чи дана послідовність є випадковою. Для тесту слід вибрати рівень значущості α. Якщо значення P-value $\geq \alpha$, то приймається нульова гіпотеза H0, тобто послідовність є випадковою. Якщо значення P-value $< \alpha$, то нульова гіпотеза відхиляється, тобто послідовність не є випадковою. Як правило, значення α вибирається в інтервалі [0.001, 0.01].

До складу пакету NIST входять 15 статистичних тестів, метою яких є визначення міри випадковості двійкових послідовностей, сформованих апаратними або програмними генераторами псевдовипадкових чисел: частотний монобітний, частотний блоковий, тест перевірки серій, найдовшої серії з одиниць, перевірки рангу двійкових матриць, тест на основі дискретного

перетворення Фур'є, тест на співпадіння з шаблоном без перекриття, тест шаблонів з перекриттям, універсальний тест Мауера, тест лінійної складності, тест серій, тест на основі апроксимації ентропії, тест накопичених сум, тест випадкових відхилень та тест випадкових відхилень-2 [3].

Описані у статті методики перевірки послідовності чисел на випадковість, дають змогу визначити якість та надійність генераторів ПВЧ, і зробити висновки, чи варто використовувати такі генератори у системі захисту чи ні.

1. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков – М.: Изд-во «КУДИЦ-ОБРАЗ», 2003. – 240 с.
2. Горбенко І.Д. Прикладна криптологія: Теорія. Практика. Застосування: монографія / І.Д. Горбенко, Ю.І. Горбенко. – Харків.: Вид-во «Форт», 2012. – 880 с.
3. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. [Електронний ресурс]. – Доступний з http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf

ІНФОРМАЦІЙНА БЕЗПЕКА У СИСТЕМІ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

Сулятицький П.Р.,
курсант ЛДУ БЖД
Жвалюк Ю.А.,
курсант ЛДУ БЖД
Грицюк Ю.І.,
ЛДУ БЖД, д.т.н., професор

Розвиток і впровадження практично у всі сфери людської діяльності інформаційних технологій істотно впливає на свідомість суспільства, а також змінює міжнародні відносини. Одним з найважливіших напрямів цієї зміни стає реалізація безпеки життєдіяльності його (суспільства) громадян, що загалом забезпечує національну безпеку держави. Її важливою складовою є інформаційна безпека, яка в сучасному світі набирає щодалі більшого значення. Наприклад, інформація про місце проживання, про номери особистих телефонів і банківських рахунків, про стан здоров'я і приватне життя часто використовують опоненти як

засіб тиску і шантажу, що порушує безпеку не тільки громадян, але й суспільства загалом. Вочевидь і суспільний прогрес, і розвиток кожної людини зокрема супроводжуються і навіть визначаються розвитком їх інформаційної безпеки.

Сьогодні інформація стала чинником, який може призвести до значних технологічних аварій, військових конфліктів і поразок у них, і може дезорганізувати державне управління та стійкість фінансової системи, а також звести нанівець роботу наукових центрів. Чим вищий рівень інтелектуалізації та інформатизації суспільства, тим потрібнішою стає надійна інформаційна безпека її громадян, оскільки реалізація їх інтересів окремо та держави загалом все більше здійснюється за допомогою інформаційних технологій.

Інформаційна безпека громадян, суспільства та держави загалом характеризується ступенем їх захищеності, та, як наслідок, стійкістю головних сфер життєдіяльності у відношенні до небезпечних інформаційних впливів. Наприклад, під впливом цілеспрямованих інформаційних атак може поступово змінюватися кругозір та мораль як окремих осіб, так і всього суспільства, можуть нав'язуватись чужі інтереси, мотиви, спосіб життя та інше. Інформаційна безпека визначається здатністю відповідних державних служб нейтралізувати такі впливи.

На сьогодні більшість країн світу вважає функціонування інформаційних технологій та телекомунікаційних систем питанням державного значення. Передові держави вже давно зрозуміли, що інформаційні технології є рушієм далекосяжних структурних змін, що забезпечують швидкий і, водночас, гуманістичний прогрес країни, її політики та економіки, розвиток суспільства і добробут його громадян.

За останні роки розвиток інформаційних і телекомунікаційних технологій стає найбільшим сектором прибуткового бізнесу України, що значно випереджає інші галузі господарства. Цей сектор є основною рушійною силою зростання нової економіки, засобом вирішення бюджетних проблем, зокрема величезних витрат на утримання адміністративних апаратів, на забезпечення процесу функціонування владних державних структур.

Держава безпосередньо зацікавлена у розвиткові інформаційних технологій на своїй території, поза як вони також несуть

велике позитивне соціальне навантаження: сприяють стабілізації суспільної думки, підвищенню життєвого рівня громадян та, як наслідок, підвищенню популярності влади серед населення. Це особливо важливо при виробленні владними структурами власної позиції щодо швидкого впровадження інформаційних технологій та формування інформаційної політики держави загалом.

Розвиток і застосування інформаційних технологій значно спрощує вирішення проблеми безробіття та зайнятості населення, збільшує можливості для самоосвіти, набуття додаткових спеціальностей, обміну корисними відомостями щодо діяльності у будь-якій сфері народного господарства.

З урахуванням майбутнього розвитку інформатизації суспільства, проникнення інформаційних технологій у найважливіші сфери життєдіяльності його громадян виникає проблема надійного захисту інформації. Розгляд інформаційної безпеки з позицій системного підходу дає змогу побачити відмінність наукового розуміння цієї проблеми від повсякденного. В повсякденному житті інформаційна безпека розуміється лише як необхідність боротьби з витоком закритої (таємної) інформації, а також з розповсюдженням хибної та ворожої інформацій.

На сьогодні стосовно національної безпеки існує чимала кількість потенційних загроз в інформаційній сфері: незбалансованість державної політики та відсутність необхідної інфраструктури засобів масової інформації; повільне входження України до світового інформаційного простору; відсутність у міжнародного співтовариства об'єктивного уявлення про життя та побут громадян України, а також їх менталітет та суспільну свідомість; інформаційна експансія з боку інших країн-сусідів, імперські залишки яких з кожним роком набирають все більших обертів; відтік інформації, що містить державну таємницю, а також конфіденційну інформацію, що є власністю держави.

Наведений перелік можливих загроз інформаційній безпеці країни і засобів їх реалізації завжди буде неповним, оскільки зміни в суспільних відносинах, розвиток інформаційних технологій та їх технічних засобів сприяє не стільки усуненню наявних загроз, скільки виникненню нових. Водночас джерела загроз інформаційній безпеці, як складовій національної безпеки дер-

жави, залишаються достатньо стабільним протягом тривалого періоду часу, а саме:

- недружня політика сусідніх держав у галузі глобального інформаційного моніторингу, поширення неправдивої інформації та новітніх піар-технологій;
- планомірна та цілеспрямована діяльність іноземних спецслужб, політичних партій і економічних структур;
- злочинна діяльність міжнародних угруповань, військових формувань та окремих високопоставлених осіб;
- неправомірна чи протиправна діяльність посадових осіб державних органів влади і політичних партій, спрямована проти інтересів України;
- стихійні лиха, природні та техногенні катастрофи, збройні конфлікти, які негативно впливають на моральну стійкість окремих громадян і суспільства загалом;
- некерований характер процесу створення інформаційної інфраструктури України, яка здебільшого покриває тільки індустріально розвинену її територію;
- недосконалість технічних і програмних засобів, а також недостатній рівень кваліфікації управлінського персоналу служб інформаційної безпеки;
- недосконалість, неповнота і неузгодженість з відповідними міжнародними правовими актами чинного законодавства України в сфері управління інформаційною безпекою;
- небажання владних структур розвивати лексикографічну базу української мови і національного лінгвістичного забезпечення інформаційних систем;
- низькі темпи науково-технічного і культурного розвитку суспільства внаслідок появи економічних криз та неадекватної внутрішньої політики держави в сфері управління інформаційною безпекою;
- низька правова законодавча база, організаційна та програмно-технічна забезпеченість в галузі інформаційної безпеки.

Особливо складною на сьогодні є проблема своєчасного створення технічних засобів, необхідних для ефективного про-

тиборства інформаційній війні. Її основна мета – послабити моральні сили та впевненість у майбутньому супротивника або конкурента та, водночас, посилити власні позиції у подальшій конкурентній боротьбі. Вона передбачає заходи пропагандистського впливу на свідомість людини в ідеологічній та емоційній галузях. Загалом інформаційна війна – складова частина ідеологічної боротьби. Вони не призводять безпосередньо до кровопролиття чи масових руйнувань, при їх веденні немає людських жертв, ніхто не позбавляється харчів чи даху над головою. І це породжує часто спокій значної кількості громадян відносно власної безпечності у ставленні до них. Тим часом, руйнування, яких завдають інформаційні війни у суспільній психології та свідомості громадян, за економічними масштабами і моральними збитками цілком співвимірні, а часом і перевищують наслідки збройних конфліктів.

Серед нових, найбільш поширених засобів інформаційної війни сьогодні називають математично досконалі різні програмні засоби типу «вірусів» і «закладок», засоби дистанційного знищення інформації, яка записана на магнітних носіях, генераторів шкідливих електромагнітних імпульсів, засобів неконтрольованого під'єднання до закритих інформаційних мереж та ін. У більш вузькому розумінні "інформаційна війна" стає реалізацією однією із різновидів інформаційних піар-технологій, або важливою фазою безпосередньої підготовки до інформаційних дій, спрямованих на послаблення економічної чи моральної стійкості.

Як свідчать наукові дослідження, система забезпечення інформаційної безпеки України не виконує окремих важливих функцій. Зокрема, неефективними є управління її діяльністю, організаційні зміни, що здійснюються в рамках адміністративної реформи, мають несистемний характер, проводяться без попереднього функціонального дослідження органів державної влади. Негативні тенденції розвитку національного інформаційного простору, кризовий стан економіки України та інші чинники зумовлюють нагнітання загроз, що часто призводить до значних втрат політичного, економічного, воєнного та іншого характеру, завдають шкоди як юридичним, так і фізичним особам.

Тому життєво важливою на сьогодні проблемою є забезпечення інформаційної безпеки не тільки громадян України, але й всього світу. Під такою інформаційною безпекою розуміється здатність держави, суспільства, соціальної групи чи місцевого населення, а також окремої особи зберегти з певною імовірністю надійні та захищені інформаційні ресурси та потоки інформації для підтримки своєї життєдіяльності, які забезпечують стійке функціонування, розвиток та протистояння інформаційним небезпекам і загрозам, негативним інформаційним впливам на індивідуальну й суспільну свідомість та психіку людей, а також на комп'ютерні мережі та інші технічні джерела інформації, виробляти особисті та групові навички й уміння безпечної поведінки, підтримувати постійну готовність до застосування адекватних заходів у інформаційному протистоянні, ким би воно не було нав'язане.

Щоб реалізувати переваги функціонування інформаційних технологій і домогтися надійного захисту інформаційного простору держави, суспільство має навчитися застосовувати передові технології, а це означає передовсім визначення державою свого ставлення до них, тобто – виробити законодавчі основи для їх чіткого функціонування та розробити стратегію надійного захисту інформації.

1. Ансофф И. Стратегическое управление : сокр. пер. с англ. / И. Ансофф. – М. : Изд-во «Экономика», 1989. – 520 с.
2. Бегма В.М. Стратегічне управління військово-технічним співробітництвом в інтересах застосування воєнної безпеки України : монографія / В.М. Бегма, О.М. Загорка, В.О. Косевцов, В.М. Шемаєв / за заг. ред. І.С. Руснака. – К. : ПІНБ; НАОУ, 2005. – 228 с.
3. Богданович В.Ю. Теоретические основы анализа проблем национальной безопасности государства в военной сфере : монография / В.Ю. Богданович. – К. : Изд-во «Основы», 2006. – 296 с.
4. Богданович В.Ю. Методичний підхід до формалізації стратегічного планування у сфері державного управління забезпеченням національної безпеки держави України / В.Ю. Богданович, А.І. Семенченко // Вісник НАДУ. – 2006. – № 4. – С. 123-128.
5. Брайсон Джон М. Стратегічне планування для державних та неприбуткових організацій : пер. з англ. А. Кам'янець / Джон М. Брайсон. – Львів : Вид-во «Літопис», 2004. – 352 с.

6. Горбулін В.П. Методологічні засади розробки стратегії національної безпеки / В.П. Горбулін, А.Б. Качинський // Стратегічна панорама. – 2004. – № 3. – С. 15-24.

СТРУКТУРА ЗАВДАНЬ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Муж П.О.,
студент групи МО-22
економічного факультету
ЛьвДУВС

Безпека як система корінних, типових властивостей будь-якої країни втілює в собі усі сфери різних галузей життєдіяльності й розвитку людини, суспільства, держави і природи. В цілому, безпеку можна визначати як якісну характеристику об'єкта (системи), здатність об'єкта до існування і розвитку та його захищеність від внутрішніх та зовнішніх загроз.

Економічна безпека підприємства – це такий стан суб'єкта господарювання, за якого він при найбільш ефективному використанні корпоративних ресурсів досягає запобігання, послаблення чи захисту від існуючих небезпек та загроз чи інших непередбачуваних обставин та в основному забезпечує досягнення цілей бізнесу в умовах конкуренції та господарського ризику [1]. Економічна безпека підприємства – це стан найбільш ефективного використання корпоративних ресурсів для запобігання загрозам та забезпечення стабільного функціонування підприємства в даний час і в майбутньому [2]. Отже, економічна безпека підприємства – це стан та здатність протидії загрозам, система заходів, спрямованих на найбільш ефективне використання ресурсів та підприємницьких можливостей для активної протидії небажаним змінам.

Захист економічної безпеки підприємства можливий лише при комплексному та системному підході до її організації. Система економічної безпеки підприємства – це комплекс організаційно-управлінських, режимних, технічних, профілактичних и пропагандистських заходів, спрямованих на кількісну реалізацію захисту інтересів підприємства від зовнішніх та внутрішніх загроз.

До основних завдань системи економічної безпеки підприємства відносять наступні:

- захист законних прав і інтересів підприємства і його співробітників;
- збір, аналіз, оцінка даних і прогнозування розвитку;
- вивчення партнерів, клієнтів, конкурентів, кандидатів на роботу в підприємстві;
- недопущення проникнення на підприємство структур економічної розвідки конкурентів, організованої злочинності й окремих осіб із протиправними намірами;
- протидія технічному проникненню в злочинних цілях;
- виявлення, попередження й припинення можливої протиправної й іншої негативної діяльності співробітників підприємства на шкоду його безпеки;
- захист співробітників підприємства від насильницьких зазіхань;
- забезпечення схоронності матеріальних цінностей і відомостей, що становлять комерційну таємницю підприємства;
- добування необхідної інформації для вироблення найбільш оптимальних управлінських рішень із питань стратегії й тактики економічної діяльності підприємства;
- формування серед населення й ділових партнерів сприятливої думки про підприємство, що сприяє реалізації планів економічної діяльності й статутних цілей;
- контроль за ефективністю функціонування системи безпеки, удосконалювання її елементів.

Після урахування основних завдань, специфіки бізнесу, конкурентного середовища будуємо систему економічної безпеки, яка є цілком індивідуальною для кожної виробничої чи комерційної одиниці (рис. 1.).

Слід зауважити, що формування завдань для кожного структурного елементу системи необхідно якомога конкретніше. Основний зміст подібної системи полягає попередженні, послабленні загроз, а основними критеріями оцінки її надійності й ефективності є:

- забезпечення стабільної роботи підприємства, збереження і збільшення фінансів і матеріальних цінностей;
- попередження кризових ситуацій, у тому числі різних надзвичайних подій, пов'язаних з діяльністю зовнішніх та внутрішніх загроз.

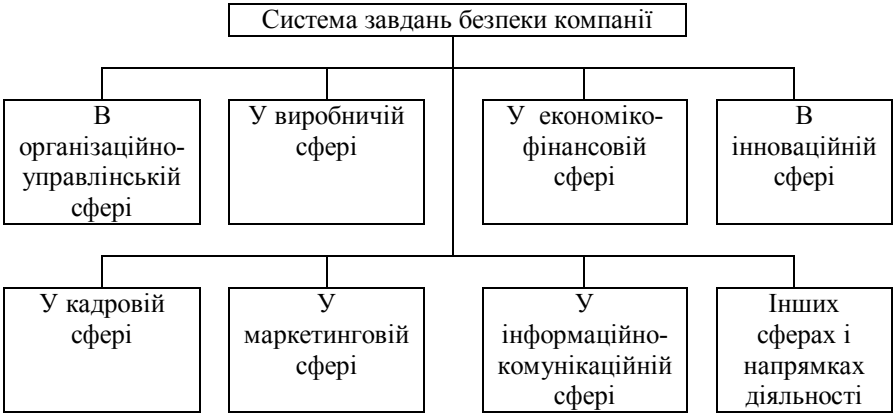


Рис. 1. Схема структури завдань системи економічної безпеки компанії

1. Грунин О.А. Экономическая безопасность организации / О.А. Грунин, С.О. Грунин. – СПб. : Изд-во «Питер», 2002. – 160 с.
2. Основы экономической безопасности (Государство, регион, предприятие, личность) / под ред. Е.Л. Олейникова. – М. : Изд-во «Интел-Синтез», 1997. – 138 с.
3. Колпаков П.А. Концептуальные основы экономической безопасности фирмы: автореф. дис. канд. екон. наук / П.А. Колпаков. – М., 2007.
4. Лянной Г. Система экономической безопасности предпритяия / Г.Лянной // BOS – журнал о личной и коммерческой безопасности. – 2006. –№7.
5. Шевченко І. Особливості формування економічної безпеки підприємства / І. Шевченко // Наука молода. – 2010. – №10.

Зміст

І. НАУКОВО-МЕТОДИЧНІ, НОРМАТИВНО-ПРАВОВІ ТА ПРОГРАМНО-ТЕХНІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОПЕРАТИВНІЙ ДІЯЛЬНОСТІ ОРГАНІВ ВНУТРІШНІХ СПРАВ

ІІІ. ПРОБЛЕМНІ ПИТАННЯ ЗАСТОСУВАННЯ СПЕЦІАЛЬНИХ ТЕХНІЧНИХ ЗАСОБІВ У ДІЯЛЬНОСТІ МІЛІЦІЇ

IV. ДЕЯКІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ОРГАНАМИ ДЕРЖАВНОЇ ТА ВИКОНАВЧОЇ ВЛАДИ, ІНШИХ МІНІСТЕРСТВ ТА ВІДОМСТВ, КОМЕРЦІЙНИХ УСТАНОВ

НАУКОВЕ ВИДАННЯ

ПРОБЛЕМИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ, СПЕЦІАЛЬНИХ ТЕХНІЧНИХ ЗАСОБІВ У ДІЯЛЬНОСТІ ОВС, НАВЧАЛЬНОМУ ПРОЦЕСІ, ВЗАЄМОДІЇ З ІНШИМИ СЛУЖБАМИ

Збірник наукових статей
за матеріалами доповідей
науково-практичної конференції
14 грудня 2012 р.

Відповідальний за випуск І.С. Керницький
Упорядник Т.В. Магеровська
Комп'ютерна верстка Т.В. Магеровська
Загальне редагування І.С. Керницький

Матеріали видано в авторській редакції

Формат 60×84/16. Папір офсетний.
Гарнітура Times. Умов.друк.арк.14,0 Умов.Фарбовід. 17,5
Тираж 100 прим. Зам. 173.

Друк СПДФО Марусич М.М.
М.Львів, пл.Осмомисла, 5/11
тел./факс: (032)261-51-31.
e-mail:interprint-m@rambler.ru

233