ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ПРОБЛЕМИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ, СПЕЦІАЛЬНИХ ТЕХНІЧНИХ ЗАСОБІВ У ДІЯЛЬНОСТІ ОВС ТА НАВЧАЛЬНОМУ ПРОЦЕСІ

Збірник наукових статей за матеріалами доповідей учасників науково-практичної конференції

26 грудня 2014 р.

Львів
2014

ББК 32.973
П 78

Рекомендовано до друку Вченою радою
Львівського державного університету внутрішніх справ
(протокол № 5 від 24.12.2014р.)

П 78 Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та навчальному процесі. Збірник наукових статей за матеріалами доповідей науково-практичної конференції 26 грудня 2014 року. – Львів: ЛьвДУВС, 2014. – 249 с.

У збірнику вміщено наукові статті за матеріалами доповідей, підготовлених учасниками науково-практичної конференції «Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та навчальному процесі», що проводилася 26 грудня 2014 р. у Львівському державному університеті внутрішніх справ.

ББК 32.973

ВІТАЛЬНЕ СЛОВО

РОЛЬ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У РЕФОРМУВАННІ СИСТЕМИ ПРОФЕСІЙНОЇ ПІДГОТОВКИ СПІВРОБІТНИКІВ ОВС

Шановні учасники конференції, радий вітати Вас на цьому науково-практичному заході!

Інформаційні технології посіли чільне місце в усіх сферах нашої життєдіяльності. З огляду на посилені тенденції реформування української міліції, без активного застосування інформаційних технологій в оптимізації діяльності правоохоронців нині не обійтися.

Завдяки правильному розумінню пріоритетних напрямів розвитку інформатизації суспільства з'явилася можливість підняти технологічний рівень обігу інформації в державі загалом і в ОВС зокрема на належний рівень. Інакше, відсутність спільної стратегії тактики та ефективного оперативного управління процесами інформатизації ізолюють нашу державу на фоні розвинутих країн Європи та світу.

Водночас для ухвалення правильних і своєчасних кадрових, методичних та організаційно-правових рішень оперативним підрозділам ОВС необхідна різнопланова та достовірна інформація, збір і надання якої ґрунтуються на сучасних спеціалізованих базах даних із використанням відповідного програмно-технічного забезпечення для захисту інформаційних активів.

Зауважу, що науковці університету в тісній взаємодії з практичними підрозділами ОВС успішно працюють над удосконаленням існуючих та розробкою і запровадженням

нових інформаційно-пошукових систем, аналітичних систем пошуку інформації, гарантуванням інформаційної безпеки спеціалізованих баз даних тощо.

У рамках сьогоднішньої науково-практичної конференції ***«Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та навчальному процесі»*** *пропонується продовжити наукові напрацювання у сфері інформатизації ОВС, спрямовані на забезпечення практичних потреб оперативних підрозділів, розробку та впровадження якісно нових програмно-технічних комплексів у діяльність ОВС, удосконалення використання сучасних інформаційних систем у навчальному процесі, застосування аналітичних систем ухвалення оптимальних рішень у спеціалізованих інформаційно-пошукових системах з урахуванням міжнародного досвіду.*

Впевнений, що конференція дасть поштовх до подальших творчих розробок, розвитку нових ідей та втілення їх у практичну діяльність органів і підрозділів внутрішніх справ.

Щиро бажаю успішного діалогу!

Ректор Львівського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент,
генерал-майор міліції ***В. В. Середа***

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

ДО ПИТАННЯ БЕЗПЕКИ СПЕЦІАЛІЗОВАНИХ КОМП'ЮТЕРНИХ МЕРЕЖ ПІДРОЗДІЛІВ МВС

Рудік Володимир Михайлович,
начальник управління АП України, к.ю.н., доцент
Рудий Тарас Володимирович,
доцент кафедри інформатики ЛьвДУВС, к.т.н., доцент
Фірман Володимир Михайлович,
доцент кафедри безпеки життєдіяльності ЛНУ ім. І. Франка, к.т.н., доцент

З огляду на вимоги сучасного підходу до побудови системи захисту інформаційних активів спеціалізованих комп'ютерних мереж (СКМ) актуальним залишається розроблення ефективних механізмів захисту.

Автори пропонують використати адаптивний підхід до захисту інформаційних активів СКМ, який дає можливість пристосовуватися до зовнішніх змін середовища функціонування, компенсуючи небажані впливи й дозволяючи оптимізувати свою роботу відповідно до встановлених критеріїв, і навіть змінити ціль функціонування, якщо цього вимагають нові умови.

При розгляді питань захисту інформації (ЗІ) в СКМ завжди говорять про наявність деяких бажаних станів усієї інформаційної системи (ІС). Ці бажані стани описують захищеність ІС.

Особливістю поняття захищеність є його тісний зв'язок з поняттям загроза (те, що може бути причиною виведення ІС із захищеного стану). Отже, виокремимо три компоненти, які безпосередньо пов'язані з порушенням безпеки СКМ: загроза – зовнішнє, відносно СКМ, джерело порушення властивості захищеності; об'єкт атаки – частина СКМ, на яку спрямована загроза; канал дії – середовище перенесення зловмисної дії.

Інтегральною характеристикою, яка об'єднує всі ці компоненти, є політика інформаційної безпеки (ПІБ) – якісно-кількісний вираз властивостей захищеності СКМ. Опис ПІБ повинен включати або враховувати властивості загроз, об'єкта атаки та каналу дії.

Для СКМ існує своя типова архітектура, структурні компоненти якої розв’язують свої специфічні задачі. У загальному випадку архітектура СКМ включає чотири рівні: рівень прикладного програмного забезпечення (ППЗ) – рівень взаємодії з користувачем; рівень системи управління базами даних (СУБД) та Web-сервери – рівень збереження і оброблення даних; рівень операційної системи (ОС) – рівень обслуговування СУБД і ППЗ; мережевий рівень – рівень взаємодії вузлів СКМ. Можливості порушення безпеки СКМ можуть бути реалізовані на всіх чотирьох рівнях архітектури СКМ. Найбільш видовищним проявом порушення безпеки СКМ є блокування або модифікування вмісту Web-порталу підрозділу МВС [1].

У більшості випадків для вирішення існуючих проблем ЗІ використовуються часткові підходи, обумовлені рівнем доступних ресурсів. Тільки суворий поточний контроль захищеності СКМ і адаптивний підхід, який забезпечує єдину ПІБ стосовно усієї ІС [2], дозволять істотно знизити ризики безпеки.

Адаптивний підхід до ЗІ дозволяє виявляти, контролювати ризики і реагувати на них у режимі реального часу використовуючи правильно спроектовані і керовані процеси і засоби. Такий підхід потребує проведення аналізу ризиків, розроблення ПІБ, використання традиційних засобів ЗІ, постійного аудиту безпеки та моніторингу стану системи, що передбачає оперативне реагування на ризики безпеки та впровадження технологій аналізу захищеності, виявлення атак, управління ризиками.

Технології аналізу захищеності – це технології пошуку вразливих місць у мережевому оточенні. Структурні компоненти СКМ потребують як оцінки ефективності їх захисту, так і виявлення невідомих уразливостей. Технології аналізу захищеності є дієвим методом реалізування ПІБ у СКМ перш, ніж здійсниться спроба її порушення ззовні або з середини. Засоби аналізу захищеності працюють на першому етапі здійснення атаки.

Технології виявлення атак – технології оцінювання процесів, які відбуваються в СКМ. Компоненти виявлення атак, розміщені у вузлах або сегментах СКМ. Виявлення атак реалізується за допомогою аналізу журналів реєстрації ОС і додатків та мережевого трафіку у реальному часі.

Технології управління інформаційними ризиками – технології виявлення, аналізу та зменшення ризиків безпеки. Завдання управління ризиками включає у себе створення набору заходів (засобів контролю), які дозволяють знизити рівень ризиків до допустимого рівня. Процес управління ризиками дозволить виявити і мінімізувати інформаційні ризики, а також: гарантувати ЗІ в агресивному динамічному середовищі ризиків; оптимізувати витрати на реалізування системи ЗІ; забезпечити визначеність у тому, наскільки потрібно захищати інформаційні активи; забезпечити визначеність у тому, як досягти прийнятного рівня безпеки, і який рівень можна вважати прийнятним; керівництво зможе приймати правильні стратегічні рішення; інтегрувати функції безпеки в усі аспекти управління.

Оцінювання ризиків полягає у виявленні і ранжуванні уразливостей СКМ за ступенем критичності, небезпеки потенційних дій, вірогідності реалізування загроз, що дає можливість визначитися з пріоритетами реакції на події безпеки, які на сьогодні задаються статично і не реалізовують адаптивні підлоди до управління ЗІ у СКМ та випереджувальні дії. З оцінювання ризиків необхідно розпочинати побудову системи ЗІ усієї ІС.

Висновки. Розв’язання проблем безпеки СКМ передбачає застосування адаптивного механізму, що працює у режимі реального часу і володіє високою чутливістю до змін в інформаційній інфраструктурі.

Ефективність захисту СКМ залежить від прийняття правильних рішень, адаптуючи його до постійно змінюваних умов функціонування мережевого оточення.

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. Рудий Т.В. Політика інформаційної безпеки в інформаційних системах спеціального призначення / Т.В. Рудий, О.В. Захарова, А.Т. Рудий / Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та навчальному процесі: збірник наукових статей за матеріалами доповідей науково-практичної конференції 27 грудня 2013 року. Львів: ЛьвДУВС, 2014. – С. 21-26.

МОЖЛИВОСТІ ТА ПЕРСПЕКТИВИ НОВІТНІХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В РЕГУЛЮВАННІ МІГРАЦІЙНОЇ ПОЛІТИКИ

Ковалів Мирослав Володимирович,
завідувач кафедри адміністративно-правових дисциплін ЛьвДУВС, к.ю.н., професор

В останні десятиліття проблема міграції стає ще актуальнішою у зв'язку з феноменом глобалізації. Поняття всесвітньої глобалізації виступає як складний багатоаспектний процес, що припускає розширення світової взаємозалежності і взаємопов'язаності більшості сучасних держав між собою, що виражається в тісному економічному, соціальному, культурному та політичному співробітництві. У даний час глобалізація та міграція стають нероздільними процесами. Багато в чому завдяки глобалізації, розвитку комунікації і нерозривно з нею пов'язаної інформатизації, сучасні міграційні процеси стають загальносвітовим явищем, яке впливає на політику, економіку та демографію.

Беручи до уваги демографічний дисбаланс в сучасному світі, який характеризується стрімкою зменшенням населення в

деяких розвинених країнах і перенаселенням в ряді країн, що розвиваються, можна з високою ймовірністю припустити, що міграційні потоки з часом будуть тільки наростати. Україна відчуває дефіцит трудових ресурсів через демографічну кризу, низький рівень народжуваності та старіюче населення.

За останні два десятиліття міграційний приріст в значній мірі компенсував більше половини природного спаду населення. Амбітні завдання, згідно з якими Україна повинна увійти до Європейського Союзу, дуже складно реалізувати без адаптації національного імміграційного законодавства [1].

Водночас міграція породжує цілий ряд проблем: політичних, культурних, соціальних, економічних, вирішення яких потребують визначення вектора подальшого розвитку міграційного законодавства.

Згідно Концепції державної міграційної політики України визнається доцільним забезпечити відкритість і доступність інформації про міграційні процеси, а також розширити використання інформаційних технологій для аналізу міграційної ситуації та забезпечення державної міграційної політики України [2].

Сучасні технології відіграють все більш значиму роль в міграційних процесах. Доступність інформації сприяє розвитку обміну трудовими ресурсами між країнами та континентами. Вдосконалення технологій і механізмів збору, зберігання, обробки та розповсюдження інформації у сфері міграції за допомогою новітніх інформаційних технологій надає можливість підвищення ефективності подальшого управління та регулювання міграційних процесів.

У сучасних реаліях глобалізації, всесвітньої інформатизації, фінансового, культурного і трудового обміну між країнами змінюються підходи, модернізуються інструменти і засоби вивчення багатьох проблем.

Можливість застосування мігрантами новітніх інформаційних технологій також сприяє розвитку не тільки трудового обміну між країнами, а й відкритості, доступності інформації, необхідної для ефективного державного регулювання. Створення єдиних баз даних, інформації про вакансії, доступ до актуальної інформації про ринок праці та нормативним документам, які регулюють

суспільні відносини у міграційній сфері, здатні вплинути на загальну обізнаність потенційних працівників. Розвиваючи інформаційно-аналітичні бази, держава зможе в перспективі отримувати оперативну інформацію про процеси, що йдуть в країні, виявляючи проблеми і контролюючи ефективність проведеної політики.

Всесвітня мережа Інтернет дає можливість вивчити проблеми міграції зсередини, роблячи доступними відгуки та коментарі самих мігрантів. Вивчення настроїв, що переважають у соціальних мережах, в блогах і на форумах стає можливим за допомогою спеціальних програмних продуктів, зокрема програми для моніторингу соціальних медіа що дозволяє оцінити соціально-політичну кон'юнктуру в суспільстві і ефективність адміністративно-правового регулювання процесів у сфері міграції.

Аналіз загальної картини міграції в сучасній України за останні десятиліття вказує на серйозні проблеми в даній сфері. У 90-і роки минулого століття пішли хвилі неконтрольованої міграції, зниження рівня народжуваності, зростання старіючого населення, демографічна криза, яка, згідно з численними прогнозами, буде тільки наростати. Тим не менш, деякі процеси вже не зупинити, ними потрібно навчитися ефективно управляти.

У даний час в епоху комп'ютеризації та розвитку комунікаційних і інформаційних технологій, у держави з'явилися нові можливості та реальні перспективи щодо вдосконалення методів моніторингу нормативно-правового регулювання міграційних процесів в Україні. Розвиток новітніх Інтернет технологій справив великий вплив на модернізацію інструментів регулювання багатьох процесів, у тому числі і міграційних. Поява революційно нових підходів щодо збору та зберігання інформації дає можливість не тільки детально вивчити специфіку міграційних процесів в України, а й прогнозувати можливі труднощі, пов'язані з регулюванням міграційної політики надалі.

Зниження чисельності працездатного населення спричинить за собою ряд проблем, пов'язаних із соціальним забезпеченням пенсіонерів, підвищення віку виходу на пенсію. Нестача працівників позначиться і на економічному розвитку країни в цілому, сповільнюючи його темпи. Зазначене опосередковано впливає на нормативно-правове регулювання у сфері економіки та

соціального забезпечення населення. Разом з тим, на сьогоднішній день нормативно не врегульовані процедури збору, аналізу, порівняння та оцінки правової інформації про стан законодавства у сфері імміграції, використання результатів моніторингу правозахисних організацій. Моніторинг правозастосування, в контексті діяльності Державної міграційної служби України, не забезпечує повноту, об'єктивність і актуальність інформації. Відсутність єдиного офіційного банку даних правової інформації, що містить нормативні, правозастосовні акти, а також аналітичну інформацію про них, є недоліком і не сприяє ефективній правотворчості у сфері яка розглядається. Зазначене не дає можливість визначити, якою мірою проведена міграційна політика відповідає цілям і завданням розвитку країни в цілому та чи є ефективними діючі інструменти регулювання міграційних процесів в даний час.

Жорсткість вимог до мігрантів, обмеження кількості квот, посилення контролю з боку силових структур і багато інших застосовуваних державою заходи, спрямовані на жорстке регулювання, можуть призвести лише до того, що частина мігрантів перейде в нелегальний, тіньовий сектор економіки. Спостерігається зростання інтересу до міграційних процесів, управління якими перестало бути винятковою прерогативою держави. В умовах євро інтеграції збільшується кількість суб'єктів, здатних впливати на міграційні процеси – роботодавці, профспілки, агентства з працевлаштування, туристичні і інші фірми, що займаються наданням послуг з організації пересування, працевлаштування та подальшої адаптації мігранта. Серйозною перешкодою у підвищенні ефективної міграційної політики стає проблема адаптації мігрантів у України, яка на даний момент далека від вирішення, але держава поступово приходить до розуміння необхідності пошуку способів її регулювання. Головною перешкодою успішної адаптації мігрантів у України є недостатня нормативно-правова база що знайшло своє відображення у плані заходів з реалізації Концепції державної міграційної політики [3]. Але зазначений план не передбачає розвиток інформаційного забезпечення дослідження міграційних процесів та моніторингу законодавства на підставі інформаційних технологій.

Всі більший вплив на законодавство України надають процеси зв'язані з Асоціацією України до Європейського Союзу. Нова

міграційна ситуація вимагає вироблення комплексу заходів на державних, регіональних та місцевих рівнях. Слід мати на увазі, що дослідження Інтернет простору українськими соціологами та політологами показують, що значна частина суспільства демонструє сприйняття ідеї відкритості українського суспільства. Разом з тим є і крайні точки зору але вони не є домінуючими в Інтернет.

Концепція реформування місцевого самоврядування та територіальної організації влади в Україні передбачає прийняття нормативно-правової бази щодо створення у регіонах міграційних інфраструктур, які могли б надати комплекс послуг з працевлаштування, навчання українській мові, забезпечення житлом і наданням інформаційно-консультаційних послуг, що стане одним з перших кроків до ефективного регулювання міграційними процесами [4].

Інтернет стає барометром ставлення до різних процесів і подій, що відбуваються в країні в цілому і за певними напрямами соціального розвитку зокрема. Розвиваючи інформаційно-аналітичні бази, держава зможе в перспективі отримувати оперативну інформацію про процеси, що йдуть в країні, виявляючи проблеми, контролюючи ефективність законодавства у міграційній сфері. Це представляє нові можливості та перспективи в регулюванні міграційної політики. Вміле використання благ розвитку людської цивілізації може призвести до процвітання країни, а небажання чи невміння їх застосування призведе до відсталості і не конкурентоспроможності держави. Будемо сподіватися, що Україна скористається можливостями, які дають новітні інформаційні технології для вдосконалення міграційної законодавства.

1. Про імміграцію: Закон України від 07.06.2001 № 2491-III // Відомості Верховної Ради. – 2001. – № 41. – Ст. 197.
2. Указ Президента України від 30.05.2011 № 622/2011 «Про Концепцію державної міграційної політики». [Електронний ресурс]. – Режим доступ: http://zakon4.rada.gov.ua/laws/show/622/2011
3. Розпорядження Кабінету Міністрів України від 12.10.2011 №1058-р «Про затвердження плану заходів з реалізації Концепції державної міграційної політики». [Електронний ресурс]. – Режим доступ: http://zakon4.rada.gov.ua/laws/show/1058-2011-%D1%80

4. Розпорядження Кабінету Міністрів України від 01.04.2014 № 333-р «Про схвалення Концепції реформування місцевого самоврядування та територіальної організації влади в Україні». [Електронний ресурс]. – Режим доступ: http://zakon2.rada.gov.ua/laws/show/333-2014-%D1%80

ПРОБЛЕМИ ЗАСТОСУВАННЯ МЕТОДИКИ ЕКСПЕРТНОЇ ОЦІНКИ РІВНІВ ЗАХИЩЕНОСТІ ІНТЕГРОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОПЕРАТИВНОГО ІНФОРМУВАННЯ МВС УКРАЇНИ ДЛЯ РІЗНОМАНІТНИХ ІНТЕГРОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ОРГАНІВ ВНУТРІШНІХ СПРАВ УКРАЇНИ

Кудінов Вадим Анатолійович,
начальник кафедри інформаційних технологій
Національної академії внутрішніх справ, к.ф.-м.н., доцент

Від початку процесу інформатизації органів і підрозділів внутрішніх справ (ОВС) України минуло вже більше 40 років. За цей час накопичений чималий досвід використання різноманітних інформаційних та інформаційно-телекомунікаційних систем оперативно-розшукового та інформаційно-довідкового призначення. За час їх існування в них неодноразово відбувалися зміни інформаційних процесів у зв'язку з періодичним оновленням засобів оргтехніки й інформаційних технологій [1].

Протягом останніх років в ОВС України вживаються заходи щодо створення та впровадження різноманітних інтегрованих інформаційних систем (ІІС). Так, зокрема, наказом МВС України від 12.10.2009 № 436 було затверджено Положення про Інтегровану інформаційно-пошукову систему ОВС України [2]. У зв'язку з набранням чинності новим Кримінальним процесуальним кодексом України 20.11.2012 наказами МВС України від 22.10.2012 № 940 та від 19.11.2012 № 1050 було передбачено створення та впровадження Єдиного обліку всіх звернень громадян до міліції про вчинені кримінальні правопорушення та інші події [3-5].

Необхідність створення ІІС стосується не тільки МВС України. Указом Президента України від 31.01.2006 № 80 та постановою

Кабінету Міністрів України (КМУ) від 08.04.2009 № 321 передбачено створення Єдиної комп'ютерної інформаційної системи правоохоронних органів з питань боротьби зі злочинністю.

Процес створення інтегрованих інформаційних систем нерозривно пов'язаний з необхідністю вирішення проблеми захисту в них інформації та ресурсів з її обробки. Цього вимагають різноманітні нормативно-правові акти, зокрема: Закони України від 31.05.2005 «Про захист інформації в інформаційно-телекомунікаційних системах» та від 09.01.2007 «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», Укази Президента України від 12.02.2007 № 105 «Про Стратегію національної безпеки України» та від 08.07.2009 № 514 «Про Доктрину інформаційної безпеки України», постанови КМУ України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» та від 16.11.2002 № 1772 «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах».

Таким чином, виникає актуальна і важлива для ОВС України науково-технічна проблема щодо створення методології оцінки рівнів захищеності інтегрованих інформаційних систем [6-8].

В роботі [9] наведено методику експертної оцінки рівнів захищеності інтегрованої інформаційної системи оперативного інформування МВС України, яку взагалі можна застосувати для оцінки рівнів захищеності різноманітних ІІС. Розглянемо проблеми, які необхідно буде вирішити при цьому.

По-перше, застосування зазначеної методики передбачає виділення найбільш вірогідних об'єктів обробки інформації в ІІС ОВС України з порушенням її цілісності, доступності та конфіденційності.

По-друге, застосування зазначеної методики передбачає створення моделі ймовірного порушника безпеки для вибраних об'єктів захисту, яка оцінює не тільки самого порушника, але також визначає загрози цим об'єктам.

По-третє, застосування зазначеної методики передбачає виділення всіх існуючих засобів та заходів захисту для вибраних об'єктів захисту.

По-четверте, застосування зазначеної методики передбачає здійснити на основі досвіду фахівців з захисту інформації експертну оцінку ймовірності подолання існуючих засобів та заходів захисту $P_{под}$ для вибраних об'єктів захисту, значення якої визначається в межах від 0 до 1. При цьому: а) якщо для об'єкту захисту є низка шляхів подолання існуючих засобів та заходів захисту з різними значеннями $P_{под}$, то у підсумковій експертній оцінці необхідно брати її найбільше значення; б) якщо для об'єкту захисту є низка засобів та заходів захисту від конкретного впливу порушника безпеки з різними значеннями $P_{под}$, то у підсумковій експертній оцінці необхідно брати її найменше значення.

Таким чином, вирішення наведених проблем дозволить застосувати методику експертної оцінки рівнів захищеності інтегрованої інформаційної системи оперативного інформування МВС України [9] для оцінки рівнів захищеності різноманітних інтегрованих інформаційних систем ОВС України у вигляді цифрових даних, на підставі яких можна буде виявити слабкі ланки комплексної системи захисту інформації ІІС з метою їх подальшого удосконалення.

1. Від арифмометра до високих технологій. До 40-ї річниці створення інформаційної служби МВС України. Том 1 / С. П. Черних, О. М. Іщенко, І. А. Аршинов. – З.: Видавництво «Просвіта», 2012. – 472 с.
2. Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України: Наказ МВС України від 12 жовтня 2009 року № 436.
3. Кримінальний процесуальний кодекс України (із змінами, внесеними згідно із Законами 2013-2014 років) // Відомості Верховної Ради України. – 2013. – № 9-10, № 11-12, № 13. – ст. 88.
4. Про організацію реагування на повідомлення про кримінальні правопорушення, інші правопорушення, надзвичайні ситуації та інші події, та забезпечення оперативного інформування в органах і підрозділах внутрішніх справ України: Наказ МВС України від 22 жовтня 2012 року № 940.
5. Про затвердження Інструкції про порядок ведення єдиного обліку в органах і підрозділах внутрішніх справ України заяв і повідомлень про вчинені кримінальні правопорушення та інші події та положень про комісії: Наказ МВС України від 19 листопада 2012 року № 1050.

6. 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.
7. Кудінов В. А. Аналіз загальних особливостей функціонування основних об'єктів інформаційної безпеки інтегрованих інформаційних систем органів внутрішніх справ України / В. А. Кудінов // Сучасна спеціальна техніка. – 2012. – № 1. – С. 91–96.
8. Кудінов В. А. Оцінка коефіцієнта оперативної готовності організаційних заходів до захисту типового вузла Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України з обробки інформації / В. А. Кудінов // Сучасна спеціальна техніка. – 2013. – № 2. – С. 58–63.
9. Кудінов В. А. Методика експертної оцінки рівнів захищеності інтегрованої інформаційної системи оперативного інформування МВС України / В. А. Кудінов // Сучасна спеціальна техніка. – 2014. – № 2. – С. 116–120.

ОРГАНІЗАЦІЙНО-ПРАВОВІ ПРИНЦИПИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ЗАСАДАХ ПОЛІТИКИ БЕЗПЕКИ

Рудий Тарас Володимирвич,
доцент кафедри інформатики ЛьвДУВС, к.т.н., доцент
Кулешник Ярко Федорович,
доцент кафедри інформатики ЛьвДУВС, к.т.н., доцент
Захарова Олександра Василівна,
доцент кафедри кримінального процесу та криміналістики ЛьвДУВС, к.ю.н.
Фірман Ігор Володимирович,
старший оперуповноважений з особливо важливих справ ДБЕЗ МВС України

Система управління інформаційною безпекою (СУІБ) повинна забезпечувати безпечність та надійність функціонування інформаційних систем (ІС) підрозділів ОВС і, на переконання

авторів, розробляється, впроваджується, функціонує на засадничих принципах політики інформаційної безпеки (ПІБ). ПІБ документально описує і регламентує СУІБ у ІС підрозділів ОВС, відповідає вимогам законодавства України та міжнародних угод, рекомендаціям міжнародних стандартів ISO/IEC 27001:2005, ISO/IEC 17799/2005.

Аналіз наявних матеріалів стосовно проблеми безпеки інформаційних активів ІС дає змогу виявити недоліки у методології розроблення ПІБ і, як наслідок, СУІБ, які суттєво впливають на ефективність функціонування усієї системи безпеки. Серед них відзначимо: ПІБ системи захисту інформаційних активів ІС не враховує динаміки зміни загроз; не забезпечує достатній рівень стійкості системи захисту ІС до відмов та відновлення після збоїв; відсутність ефективних методик попереднього оцінювання ефективності СУІБ; ігнорування законодавчими аспектами та вимогами міжнародних стандартів у галузі ЗІ при проектуванні надійної СУІБ.

Мета дослідження полягає у тому, щоб означити організаційно-правові принципи менеджменту ІБ у ІС підрозділів ОВС на засадах ПІБ, що дозволить створити ефективну СУІБ. СУІБ призначена виявляти, реагувати й аналізувати колізії та інциденти ІБ. Без реалізування цих процесів неможливо забезпечити рівень захищеності з урахуванням динаміки зміни загроз, який є адекватним до вимог міжнародних стандартів і галузевих норм.

Автори пропонують розробляти організаційно-правову структуру і впроваджувати СУІБ у відповідності до настанов міжнародних стандартів та чинного законодавства України [1]. У відповідності до вимог міжнародних стандартів процес розроблення СУІБ повинен містити такі етапи: планування – етап планування забезпечує правильне завдання контексту і масштаббу СУІБ, оцінюються ризики, пропонується відповідний план оброблення цих ризиків; реалізування – етап реалізування впроваджує ухвалені рішення, які були визначені на етапі планування; аналіз захищеності – етап оцінювання ефективності та надійності функціонування створеної СУІБ, проведення аудиту ІБ, виявлення недоліків; реагування – етап виконання коригувальних дій з покращення функціонування СУІБ, реагування вимагає

первісного інвестування, документування діяльності, формалізування підходу до управління ризиками, визначення методів аналізу.

У процесі розроблення і впровадження СУІБ необхідно виконати: ухвалити рішення про створення СУІБ і визначити межі відповідальності посадових осіб; провести інвентаризування активів ІС, які пов'язані з інформаційним простором СУІБ; виконати категоріювання активів ІС; виконати аудит захищеності ІС з виявленням загроз; оцінити інформаційні ризики; розробити систему управління інформаційними ризиками; розробити новітні бази нормативних документів з ІБ і домогтися їх виконання у повному обсязі.

Для процесів СУІБ застосована модель циклічного процесу з використанням принципів реалізування управління ІБ, ядро якого становить централізоване адміністрування (враховує специфіку функціонування ІС підрозділів ОВС):

1. Встановлення централізованого адміністрування.
2. Автентифікування об’єктів, суб’єктів та інформаційних активів ІС.
3. Авторизування об’єктів, суб’єктів та інформаційних активів ІС.
4. Аналіз ризиків і формування керуючих впливів.
5. Досягнення необхідного рівня підготованості працівників.

Підставою для розроблення і впровадження ПІБ та вибору необхідних засобів контролю є оцінювання ризиків. Ефективність засобів контролю полягає в оцінюванні шляхом аудиторських перевірок. Отримані результати забезпечують підхід до подальшого оцінювання ризиків і визначають необхідні зміни у ПІБ і засобах контролю. Всі ці дії централізовано адмініструються і координуються. Організаційні принципи реалізування системи управління інформаційною безпекою подано на рис. 1.

Аналіз і оцінювання ризиків, на думку авторів, провадитися за чотирма основними критеріями безпеки:

- доступність – забезпечення безперервного доступу до інформаційних та апаратних активів ІС, сервісів згідно з наданими працівникам повноваженнями у мінімально необхідному обсязі;

- цілісність – захист точності/коректності та повноти інформаційних активів ІС і методів оброблення інформації;
- конфіденційність –доступність інформаційних активів винятково для офіційно авторизованих працівників у мінімально необхідному обсязі;
- спостережність –забезпечення принципу невідмови від вчинених дій. Тобто, у СУІБ ІС реалізоване жорстке адміністративне керування доступом.

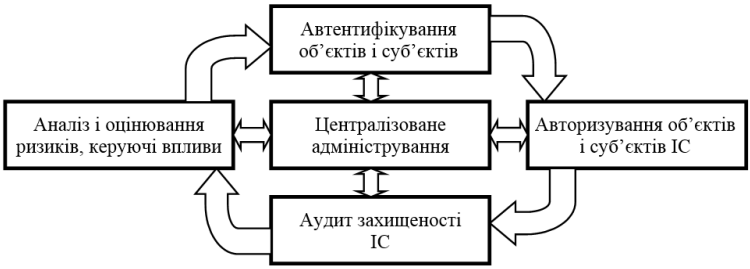


Рис. 1. Організаційні принципи реалізування системи управління інформаційною безпекою

Це означає, що керування інформаційними потоками між користувачами, процесами, об'єктами та суб'єктами ІС здійнюють тільки спеціально авторизовані користувачі. Звичайні користувачі змінювати права доступу користувачів, а також виконувати довільні інші функції керування засобами СУІБ не можуть.

При категоріюванні інформаційних активів основною складністю є те, що важко визначити їх цінність. Фахівцям з ІБ потрібно розробити ефективні методики і критерії категоріювання інформаційних активів. Відзначимо, що визначення цінності активів дійсно дуже складний процес [2].

Сформульовані правила фіксуються у відповідних документах (документування процедур – одне з основних вимог стандарту ISO 27001). Наголосимо, що основним документом є ПІБ, у якій перераховані всі процедури, визначено ступінь відповідальності посадових осіб за забезпечення ІБ, а також позиція керівництва [3]. Автори вважають, що ПІБ у ІС підрозділів ОВС є багаторівневою системою документів, які визначають вимоги безпеки, систему заходів, відповідальність персоналу та механізми контролю задля забезпечення захисту інформації у ІС. 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.

Для зменшення ризиків виникнення інцидентів ІБ, пов'язаних з зовнішніми і внутрішніми, навмисними та ненавмисними впливами, елементарною необізнаністю працівників у галузі ІТ необхідно розробити та запровадити систему управління інцидентами інформаційної безпеки (СУІБ), яка є базовою частиною загальної СУІБ. 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.

Усі процедури забезпечення СУІБ повинні бути адресними, тобто, для кожної процедури повинен бути визначений перелік користувачів, виконавців, а також перелік інформаційних активів ІС, для яких потрібне їх застосування.

Висновки. СУІБ дозволяє виявляти, враховувати, реагувати й аналізувати загрози та інциденти ІБ. Без реалізування цих процесів неможливо забезпечити рівень ІБ, який є адекватним до вимог сучасних стандартів і галузевих норм.

Впровадження СУІБ дозволить зменшити інформаційні ризики, порушення роботи ІС за рахунок розмежування фізичного доступу та впровадження механізму моніторингу (аудиту) стану ІБ.

Наостанок 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 захисту ІС.

1. Рудий Т.В. Управління безпекою в інформаційних системах МВС / Т.В. Рудий, Я.Ф. Кулешник, І.М. Ганич, І.В. Бичинюк / Науковий вісник Львівського державного університету внутрішніх справ, №1(47). – Львів: ЛьвДУВС, 2011. – С. 382-392.
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: Львівський державний університет внутрішніх справ, 2010. – С.90-97.
3. Рудий Т.В. Політика інформаційної безпеки в інформаційних системах спеціального призначення / Т.В. Рудий, О.В. Захарова, А.Т. Рудий / Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та навчальному процесі: збірник наукових статей за матеріалами доповідей науково-практичної конференції 27 грудня 2013 року. Львів: ЛьвДУВС, 2014. – С. 21-26.

ІНФОРМАЦІЙНІ ТЕХНОЛГІЇ В ДОСЛІДЖЕННІ ІНДИКАТОРІВ ДЕМОГРАФІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Хомин Оксана Йосипівна,
професор кафедри інформаційних технологій у діяльності ОВС та економічної безпеки ЛьвДУВС, к.е.н., доцент

Для дослідження демографічної безпеки держави необхідна велика кількість інформації про чисельність населення, його статево-вікову структуру, розміщення населення, його зайнятість за галузями, кількість працездатного, безробітного населення, їх соціальний захист, чисельність безробітного населення та його соціальні гарантії, чисельність бідного населення, стан здоров'я населення, інвалідизація населення, кількість мігрантів, емігрантів, чисельність освітніх закладів та якість надання освітніх

послуг, кількість продуктів споживання та їх якість, стан екологічної ситуації в різних регіонах країни, наявність чи відсутність якісної води для споживання та чисельність кримінальних правопорушень на певній території.

Для опрацювання значної кількості статистичної інформації, що надає не лише кількісну, але і якісну характеристику усім процесам, задіяним в системі забезпечення демографічної безпеки необхідно ставити великі вимоги до інформаційного забезпечення.

Статистична інформація окрім її накопичення повинна певним чином опрацьовуватися, аналізуватися, систематизуватися та узагальнювати інформацію, що дозволить в найкоротші терміни її дослідити та в перспективі визначити прогноз стану демографічної безпеки держави.

Велику кількість статистичної інформації отримують різними шляхами:

- статистична інформація;
- переписи населення;
- різного роду дослідження;
- статистична інформація з місць проживання;
- галузева інформація;
- статистична інформація міністерств та відомств та інші джерела.

Для дослідження системи демографічної безпеки необхідна певна кількість індикаторів демографічної безпеки. Для визначення самих індикаторів необхідно:

- зібрати всю інформацію, що потрібна для аналізу системи демографічної безпеки;
- визначити особливості формування та розвитку складових демографічної безпеки;
- систематизувати індикатори;
- окреслити індикативні ознаки;
- сформувати комплекс індикаторів демографічної безпеки (Рис. 1).

Базуючись на відкритій базі та міжнародній і національній нормативній базі даних потрібно провести моніторинг складових демографічної безпеки. Дану інформацію порівняти зданими усіх

регіонів України. Досягнуті результати потрібно зіставити з встановленими стандартами усіх сфер суспільного життя держав Європейського союзу. На основі отриманих результатів необхідно описати виявлені небезпеки та загрози демографічної безпеки та охарактеризувати їх передумови. На основі проведеного дослідження необхідно розробити необхідні мінімізуючі та нівелюючі заходи, що допоможуть забезпечити демографічну безпеку держави.

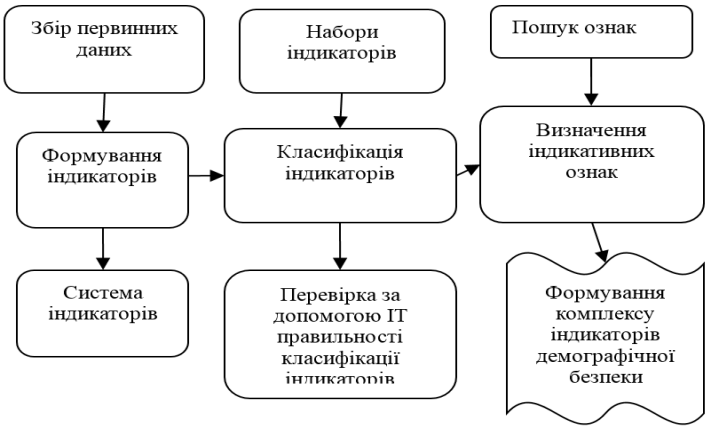


Рис. 1. Формування комплексу індикаторів демографічної безпеки (розробка автора)

Висновок. Увесь комплекс аналітичних дій враховуючи всю складність аналітичних операцій неможливо швидко і якісно провести без застосування інформаційних технологій.

ІСТОРИЧНІ АСПЕКТИ РОЗВИТКУ СИСТЕМ ІДЕНТИФІКАЦІЇ ОСОБИ НА ПРИКЛАДІ ФРАНЦІЇ

Керницький Іван Степанович,
професор кафедри інформатики ЛьвДУВС, д.т.н., професор
Когут Володимир Михайлович,
викладач ЛьвДУВС
Максимюк Софія Орестівна,
студент ЛьвДУВС

Сучасний світ сповідує принципи конституційності, демократії та всестороннього захисту і розвитку особи. Такі глобальні

задачі неможливо вирішити без високорозвинутих поліційних служб у цілому та різноманітних спеціалізованих підрозділів органів внутрішніх справ (ОВС) зокрема, оскільки саме вони повинні стояти на передовому рубежі захисту прав і свобод громадянського суспільства. Проблеми реформування та вдосконалення сучасних сил правопорядку особливо гостро відчутні у державах, що стали на шлях демократичного розвитку і поступово асоціюються до міжнародної спільноти. Україна в цьому переліку займає чільне місце за своєю відкритістю до нововведень, сучасних методів роботи, прагнення до міжнародної співпраці. МВС України займає активну позицію у царині впровадження сучасних методів боротьби із злочинністю та застосування новітніх технологій для розкриття і попередження злочинів.

Керівництво МВС України прикладає значні зусилля для забезпечення ОВС сучасними засобами протидії злочинному світу. При цьому до уваги приймаються не лише практичні підрозділи, а й освітянські заклади системи МВС, покликані готувати висококласних фахівців для нашої держави (а в майбутньому і для інших держав).

Яскравим прикладом дбайливого ставлення до освіти може слугувати Львівський державний університет внутрішніх справ (ЛьвДУВС), який за свою 70-літню історію пройшов усі віхи розвитку – від школи міліції до провідного університету МВС, стратегія розвитку якого базується на формуванні колективу науково-педагогічних працівників найвищої кваліфікації, невпинному розвитку матеріально-технічної бази, впровадженні передових освітянських та інформаційних технологій навчання, а також на вихованні курсантів і студентів на кращих традиціях, закладених попередніми поколіннями.

Особливу увагу у ЛьвДУВС приділяється вивченню інформаційних дисциплін. З цією метою у 2000 р. була створена кафедра інформатики та інформаційних технологій в діяльності ОВС, науковий та навчально-методичний досвід роботи якої підтверджує доцільність поділу інформаційних дисциплін на два етапи вивчення:

- на першому курсі (вивчення загальноужиткового опрограмування);

- на старших курсах (наприклад, на четвертому – вивчення спеціалізованих «міліцейських» програм).

З цією метою у ЛьвДУВС створена спеціалізована комп'ютерна лабораторія інформаційно-пошукових систем (ІПС) ОВС, кожне робоче місце якої обладнане сучасним комп'ютером, сканером, друкаркою та ксероксом. У лабораторії ІПС ОВС передбачене навчання курсантів і студентів наступних програм:

- АРМОР;
- дактилоскопічна ідентифікація особи;
- фоторобот.

З огляду на актуальність теми дактилоскопії пропонуємо реферований огляд історії розвитку систем ідентифікації особи від їх зародження до часів становлення і глобального використання.

На запитання – як найдостовірніше і найпростіше можна ідентифікувати особу – сучасна людина без зволікань відповість – за відбитками пальців. Відповідь настільки очевидна, що навіть важко уявити, який складний і тернистий шлях пройшла дактилоскопія та скільки десятиліть необхідно було для досягнення переконання про однозначність і безпомилковість цієї системи ідентифікації.

Становлення поліції Франції. Перша у світі чітко структурована кримінальна поліція була створена у 1810 р. у Франції під назвою «Сюрте» («Безпека») [1]. Її до 1833 р. очолював Ежен Франсуа Відок (1775–1857 рр.), який до 35-річного віку був пов'язаний з кримінальним світом, чудово знав його особливості і сповідував принцип – «перемогти злочинність може лише злочинець». Е.Ф. Відок, маючи феноменальну пам'ять, запровадив у тюрмах «паради засуджених» і заснував архів Сюрте, який до 1879 р. містив 80 тис. фотографій (вперше фотографування запровадили у брюссельській тюрмі в 40-х роках XIX ст.) і 5 млн карт з описами злочинців. Це була перша систематизована картотека, яка стала підсумком ефективної роботи Сюрте, шеф котрої Е.Ф. Відок лише за рік роботи разом з 12 оперативниками заарештував 812 вбивць, грабіжників, фальшивомонетників, злодіїв та шахраїв.

Однак, перша науково обґрунтована система ідентифікації особи була розроблена та запроваджена у практичну діяльність

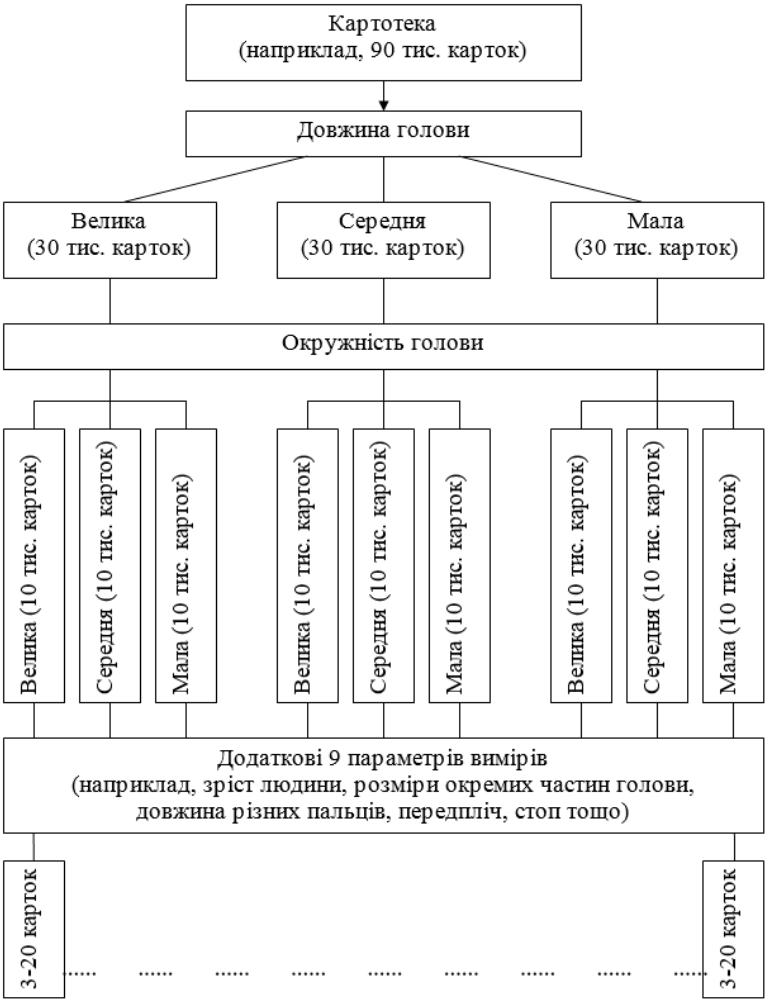
французької поліції Альфонсом Бертільоном (1853–1914 рр.) і базувалась на антропометричних вимірах людини.

Хворобливий, з дуже складним характером А. Бертільон (син віце-президента Паризького антропологічного товариства д-ра Луї Адольфа Бертільона і внук знаного математика Ахілла Гітара) у березні 1879 р. був призначений на посаду помічника писаря у префектуру поліції Парижа. Успадкована допитливість розуму, поглиблене вивчення праць бельгійського статистика Адольфа Кєтлє (який досліджував соціальні аспекти злочинності) та італійського психіатра Чезаре Ламброзо (який стверджував наявність атавізмів і спорідненість злочинців з тваринами) дали змогу А. Бертільону розпочати розробку системи ідентифікації особи за розмірами окремих частин її тіла (хоча ще у 1860 р. в Бельгії начальник Лувенської тюрми Стевенс пропонував, хоча і безуспішно, виміряти зріст, окружність голови, довжину вух, стоп, ширину грудної клітки для ідентифікації злочинців).

У липні 1879 р. А. Бертільон у тюрмі Санте почав вимірювати зріст, окружність і довжину голови, довжину рук, пальців, стоп і переконався, що ніколи не співпадають розміри 4 або 5 частин тіла одночасно.

1 жовтня 1879 р. А. Бертільон дістав підвищення і отримав посаду писаря. Маючи більше повноважень, А. Бертільон пише доповідну записку на ім'я префекта поліції Луї Андріє та шефа Сюрте Гюстава Масе, в якій з посиланням на закон Кєтлє (вірогідність співпадіння зросту різних людей становить 1:4, при цьому розміри кісток дорослої людини не змінюються усе життя), засвідчив, що врахування хоча б двох розмірних параметрів тіла людини зменшує вірогідність співпадіння до 1:16, 11 параметрів – до 1:4 191 304, 16 параметрів – до 1:286 435 456.

На основі показаної на схемі розробленої класифікації А. Бертільон хотів кардинально вдосконалити (систематизувати) картотеку Сюрте, яка на той час в силу своєї масовості (5 млн. карт) перетворилась у хаос несистематизованих документів. Однак, Луї Андре не зрозумів цінності запропонованої методики і жорстко відмовив у її впровадженні.



Структурна схема антропометричної класифікації людей Альберта Бертільона (жовтень 1879 р.)

1. Торвальд, Юрген. Век криминалистики : пер. с нем. / Юрген Торвальд ; Вступ.ст., пер. И.С. Власов ; Пер. Л.А. Пэк ; Под ред. Ф.М. Решетников . – Москва : Проспект, 2009 . – 326 с. : ил. – Библиография в подстрочных примечаниях . – На рус. яз. – ISBN 978-5-392-00764-6

ОКРЕМІ АСПЕКТИ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ НОТАРІУСА

Магеровська Тетяна Валеріївна,
доцент кафедри інформатики ЛьвДУВС, к.ф.-м.н., доцент
Скоробогата Ольга Євгенівна,
магістр ЛьвДУВС
Сеник Святослав Володимирович,
студент ЛьвДУВС

Стрімкий розвиток науки і техніки у світі, призвів до широкого використання електронних засобів зв'язку та інформаційно-комунікаційних технологій (ІКТ), за допомогою яких відбувається оперативне поширення інформації в різних сферах правовідносин в Україні. Більша частина обороту інформації і документів нотаріату сьогодні здійснюється саме в електронному вигляді, а сучасні інформаційні технології використовуються з метою здійснення цивільних правочинів через мережу Інтернет.

Метою даної статті є визначення окремих проблем використання сучасних інформаційних технологій в діяльності нотаріуса у сучасних умовах.

Широке використання електронного документообігу було б не можливим, якби не було б запроваджено електронний підпис. Вперше про електронний підпис заговорили ще у 80-х рр. минулого століття, хоча ані технічних умов, ані організаційних структур для повноцінного посвідчення особи автора електронного документа у тих роках ще не існувало. Під «електронним підписом» розуміли певну послідовність символів. Сучасний електронний цифровий підпис (ЕЦП) – це вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. І тут виникає таке питання: який взаємозв'язок між інформаційно-комунікаційними технологіями,

що дозволяють ідентифікувати особу, організацію в електронному спілкуванні, та нотаріусом?

Згідно ст.1 Закону України «Про нотаріат» [1] Нотаріат в Україні – це система органів і посадових осіб, на які покладено обов'язок посвідчувати права, а також факти, що мають юридичне значення, та вчиняти інші нотаріальні дії, передбачені законодавством, з метою надання їм юридичної вірогідності. Сучасні інформаційно-комунікаційні технології, а також інструменти, розроблені з їх використанням, такі, наприклад, як електронний цифровий підпис, вирішують проблеми, пов'язані із зіставленням інформації в електронній формі про особу, підприємства, установи, організації різної форми власності, їх ідентифікацію, забезпечують цілісність та захист такої інформації і надають користувачам можливість продемонструвати наявність у них законних права чи дозволу на доступ до послуг або джерел інформації.

Для проведення паралелей між «паперовими» діями нотаріуса і завданнями та функціональними призначеннями окремих продуктів і рішень, які базуються на останніх результатах інформаційних технологій, виділяючи при цьому електронний цифровий підпис, можливо стверджувати про тотожність досягнутого результату. Нотаріус надає юридичної значущості певним діям – волевиявленню фізичних і юридичних осіб, – як на папері, так і, у разі дотримання певних правил, встановлених законодавством, в електронних документах, що скріплюються електронним цифровим підписом і є рівнозначними за юридичною силою власноручному підпису. Не зупиняючись і не заглиблюючись у технічні аспекти, можна відзначити, що згадані правила визнання ЕЦП юридично значущим визначено в ст. 3 Закону України «Про електронний цифровий підпис» [2]. Водночас, і Закон України «Про електронні документи і електронний документообіг» [3] підкреслює необхідність визнання дійсності електронного документа за наявності в його структурі електронного цифрового підпису.

Різноманітні проекти із впровадження та реалізації інформаційних технологій в усі сфери суспільних правовідносин підтверджують необхідність використання електронних засобів зв'язку, а також сучасних інформаційних технологій. Можливість використання електронних засобів зв'язку, інструментів інформаційно-комунікаційних технологій під час здійснення правових

операцій закріплені як у міжнародних угодах, так і в національному законодавстві.

На жаль, можливості використання електронних засобів зв'язку, інструментів інформаційно-комунікаційних технологій під час здійснення правових операцій мають обмежений характер, отож існує велика необхідність у перегляді чинної нормативно-правової бази України з метою як деталізації та удосконалення, регламентації проведення процесів, так і визначення самої можливості їх здійснення, участі у цих процесах нотаріуса. Особливо це питання актуалізується, коли йдеться про міжнародні економічні та правові зв'язки. У цій сфері потрібна не тільки декларація про можливість визнання договорів, укладених за допомогою електронного підпису, а й встановлення конкретних шляхів їх нотаріального посвідчення. На підтвердження необхідності подібних кроків можна навести приклади з міжнародної практики. Спираючись на матеріали, підготовлені ЮНСІТРАЛ (Комісії ООН з права міжнародної торгівлі) «Сприяння зміцненню довіри до електронної торгівлі: правові питання міжнародного використання електронних методів посвідчення достовірності і підписання» (2009), і проаналізувавши практику використання електронних засобів зв'язку, інструментів ІКТ у нотаріальній діяльності, можна виділити наступні напрями розвитку: використання сучасних інформаційних технологій (електронний документообіг, електронний цифровий підпис, інформаційні та інформаційно-реєстраційні систем) для організації нотаріальної діяльності; надання окремих видів нотаріальних дій в електронному вигляді, у тому числі посвідчення: авторства, інформації, відправки електронних листів (е-контент), електронний апостиль.

На сьогодні українські нотаріуси під час здійсненні своєї діяльності мають доступ і користуються відомостями відповідних державних реєстрів, в яких враховуються майнові права, а саме: Єдиного реєстру заборон відчуження об'єктів нерухомого майна, Державного реєстру іпотек, Державного реєстру операцій, Державного реєстру обмеження прав на рухоме майно, Спадкового реєстру, Єдиного реєстру доручень; Державного реєстру прав на нерухоме майно (нотаріуси також є і реєстраторами цього реєстру з 1 січня 2013 р.); Державного земельного кадастру (розпочав

свою роботу 1 січня 2013 року). Доступ нотаріусів до вище перелічених реєстрів здійснюється за допомогою ЕЦП.

Стратегія розвитку інформаційних технології у діяльності нотаріуса повинна враховувати:

- поетапну комп'ютеризацію нотаріусів;
- встановлення системи комунікацій, встановлюючи використання електронної пошти;
- розвиток ідеї об'єднання, щоб надати можливість комунікації між органами та громадянами;
- координація інформації в необхідних межах;
- встановлення об'єднаної системи для збору інформації і статистики;
- встановлення єдиної інформаційної системи;
- встановлення єдиних внутрішніх інформаційних реєстрів;
- розробка стандартного програмного забезпечення для баз даних.

Розглянемо приклад Республіки Грузія, де починаючи з 2009 року функціонує Електронний реєстр нотаріальних дій Нотаріальної Палати Грузії. Кожен громадянин Грузії може знайти тут і перевірити інформацію про всі виконані нотаріальні дії. Зокрема, доступні для перевірки: факти реєстрації в електронному нотаріальному реєстрі нотаріальних дій, виконаних за участі громадянина; факти реєстрації в електронному нотаріальному реєстрі представленого громадянином нотаріального акта або виконаного за його участі. Пошук інформації здійснюється за певними параметрами. Вказана програма забезпечує конфіденційність інформації про виконані нотаріальні дії. Варто відмітити, що пошук інформації можна здійснити лише в разі повного володіння реквізитами нотаріального акта (індивідуальний унікальний номер і номер реєстрації в електронному реєстрі)»

У Республіці Казахстан у жовтні 2010 року також розпочато впровадження Єдиної нотаріальної інформаційної системи, так званої системи Е-нотаріат. Ця програма надає нотаріусам он-лайн доступ до баз даних органів юстиції: «Реєстр нерухомості», «Юридичні особи», «Фізичні особи» і «РАЦС». Існує також можливість надання окремих видів нотаріальних дій в електронному вигляді, у тому числі, фіксація і посвідчення: авторства, інформації, яка

міститься на інтернет-сторінках, відправки електронного листа (е-контент). Розвиток електронних держпослуг в Казахстані не стоїть на місці – за рівнем можливості он-лайн-спілкування громадян з державними органами ця країна змагається з Сінгапуром.

Слід зазначити і той факт, що не лише міжнародний досвід і практика інших держав свідчить про необхідність залучення ІТ у нотаріальну діяльність України (зокрема, використання електронного підпису як невід'ємного елементу електронного документа), але й діяльність міжнародних організацій, учасником яких є Україна, також активно закликає використовувати можливості електронних засобів зв'язку, інструментів ІКТ у нотаріальній практиці.

Розвиток електронних засобів зв'язку, інструментів ІКТ (електронного документообігу, ЕЦП) у діяльності нотаріуса дозволяє зробити взаємодію нотаріуса з фізичними і юридичними особами ефективнішою і зручнішою, а також створює умови для продуктивної взаємодії нотаріату з державними органами та органами місцевого самоврядування відносно багатьох конфліктних питань, зокрема, таких як посвідчення операцій та реєстрація права фізичної чи юридичної особи, реєстрація юридичних осіб надання запиту.

На нашу думку сьогодні побудова системи е-нотаріату в Україні сприятиме переходу на якісно новий рівень правовідносин між громадянами і державою.

1. http://kodeksy.com.ua/pro_notariat.htm
2. http://kodeksy.com.ua/pro_elektronnij_tsifrovij_pidpis.htm
3. http://kodeksy.com.ua/pro_elektronni_dokumenti_ta_elektronnij_dokumentoobig.htm

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Зачек Олег Ігорович,
доцент кафедри інформаційних технологій у діяльності ОВС та економічної безпеки ЛьвДУВС, к.т.н., доцент

Злочинці в своїй діяльності використовують найновіші технології і тому для ефективної протидії злочинності правоохоронні

органи повинні використовувати останні досягнення науки та техніки. Найбільш сучасним напрямком розробок є використання біометричних технологій. Біометричні технології мають ряд переваг порівняно з традиційними методами ідентифікації осіб з метою надання їм права доступу до інформації.

До 11 вересня 2001 року біометричні системи доступу використовувалися в основному тільки для захисту військових секретів та найважливішої комерційної інформації [1, с. 7]. Але після теракту в Нью-Йорку ситуація різко змінилася. Так наприклад, серед громадян США всього 10% підтримувало ідею біометричної паспортизації до 11 вересня 2001 року і вже понад 75% – після теракту, коли відстеження потенційно небезпечних особистостей стало першорядним завданням [2]. На даний час попит на системи, які використовують біометричні технології, значно зріс, зросла кількість галузей їх використання та вдосконалилися технології. Відбулося зниження вартості елементів таких систем, що позитивно впливає на подальший розвиток. Наприклад, до недавнього часу вартість дактилоскопічних систем становила $ 2000-5000 США, а після створення мініатюрного мікроелектронного дактилосканера вартість біометричного захисту комп'ютерів знижена до $ 50 – 100 США [2]. Тому запровадження в практичну діяльність новітніх біометричних технологій, навіть таких, які зараз є незвичними та перебувають в зародковому стані, є справою недалекого майбутнього.

З точки зору поширеності біометричних методик виділяють «три великі біометрики»: ідентифікація за відбитками пальців, за геометрією обличчя та за райдужною оболонкою ока. Як вважають деякі автори, системи ідентифікації за відбитками пальців займають більше половини ринку біометричних технологій, системи на основі технології розпізнавання за геометрією обличчя – 13-18 %, а системи на основі ідентифікації за райдужною оболонкою ока – 6-9 %. Надійність способів ідентифікації оцінюється за допомогою таких понять як FAR (False Acceptance Rate – характеризує можливість помилкового пропуску особи, яка не має на це права) и FRR(False Rejection Rate – визначає вірогідність

помилкової заборони доступу). Для методу ідентифікації за геометрією обличчя з використанням двох вимірів FAR становить 0.1-0.001%, FRR – 2.5-9.0 %, а з використанням трьох вимірів FAR становить 0.0047%, FRR – 0.103 % (що порівняно зі статистичною надійністю методу ідентифікації за відбитками пальців). Для методу ідентифікації за відбитками пальців FAR становить 0.1-0.001%, а FRR – 0.3-0.9 %. Для методу ідентифікації за райдужною оболонкою ока FAR становить 0.00001%, а FRR – 0.13 % [3].

Згідно огляду зарубіжного досвіду застосування методу біометричної аутентифікації людини Укрбюро Інтерполу в країнах Євросоюзу, США та в Ізраїлі використовують переважно способи біометричної автентифікації за відбитками пальців та за двовимірним зображенням обличчя. Але перевірка за двовимірним зображенням обличчя здійснюється, як правило, без використання спеціальних приладів, шляхом візуального порівняння обличчя особи з цифровим зображенням, що міститься в біометричному паспорті [4].

В біометричних паспортах, які видаватимуть в Україні, буде міститися чіп з оцифрованими відбитками пальців і оцифрованим фото для визначення овалу обличчя. Згідно інформації гендиректора консорціуму ЄДАПС Олександра Дранікова, планувалося використання також відсканованої райдужної оболонки ока, але вирішили, що на даний час найнадійніше – це відбитки пальців [5].

Найбільш широко вживаним на даний час є використання систем розпізнавання за відбитками пальців. Ця біометрична технологія на сьогодні має найбільшу кількість напрямків використання та застосувань з усіх біометричних технологій. Це обумовлено невисокою вартістю порівняно з іншими методами біометричної ідентифікації, а також високою точністю у зв'язку з незмінністю біометричної ознаки.

Використання біометричних технологій на основі дактилоскопії є дуже популярним для забезпечення контролю доступу до комп'ютера та комп'ютерних мереж, внаслідок чого користувачу не потрібно запам'ятовувати пароль, досить зісканувати відбиток пальця. Дуже перспективним є використання вищеназваних технологій в системах контролю та управління доступом, що дозволяє підвищити рівень безпеки.

Але біометричні технології, які базуються на використанні відбитків пальців, мають і недоліки. Неодноразово в засобах масової інформації з'являлися повідомлення про успішні спроби фальсифікації відбитків пальців для зламу систем захисту на основі дактилоскопії [6].

Для розпізнавання осіб в системах відеоспостереження придатний лише метод ідентифікації за геометрією обличчя, оскільки це єдиний метод, який дозволяє здійснювати ідентифікацію на значній відстані. У процесі ідентифікації виділяються та обробляються найбільш характерні параметри обличчя: форма носа, губ, брів, відстань між ними, на основі яких формуються цифрові моделі. Для точної ідентифікації достатньо 40 точок обличчя [1, с. 99-102].

У зарубіжних країнах вже є неодноразові спроби використання методу ідентифікації по обличчю в системах відеоспостереження. Наприклад, практично вся територія м. Лондона вкрита системою відеоспостереження, для запобігання та розкриття правопорушень. І, згідно повідомлення на сайті Dokumentika.org від 12.09.2012, в Лондоні за допомогою системи розпізнання облич, яка була розроблена до лондонської Олімпіади, заарештовано біля 2 тисяч осіб, причетних до мародерства під час масових безпорядків. Згідно даних цього ж сайту ФБР розпочинає використання нової системи розпізнавання за обличчям, розробка якої коштувала $1 млрд, що дозволяє шукати злочинців за матеріалами відеонагляду на основі бази даних фотографій з використанням 3-D моделі голови особи [7].

Значно рідше в системах захисту інформації використовуються такі методики, як ідентифікація за сітківкою ока, за ДНК, за зображенням кисті руки, за малюнком вен долоні або пальця руки, за термограмою обличчя, за формами вушних раковин, за запахом, за голосом, за підписом, за клавіатурним почерком та шляхом аналізу біоелектричної активності мозку.

Найбільш надійним з практично реалізованих методів вважається метод сканування сітківки ока. Тому він використовується в системах контролю доступу на особливо секретні об'єкти. Із-за низького рівня поширення таких систем малою є вірогідність реалізації спроб зламу. Але недоліком є висока вартість систем з використанням цього методу.

Сьогодні в правоохоронних органах України практично не використовуються біометричні технології. Лише в процесі проведення криміналістичних досліджень та під час зіставлення за допомогою автоматизованих дактилоскопічних ідентифікаційних систем відбувається ідентифікація особи за наявними відбитками пальців.

Для забезпечення достатнього рівня захисту інформації доцільним є застосування біометричних технологій для контролю доступу до комп'ютерів, комп'ютерних мереж та в приміщення. З метою запобігання зламу таких систем доцільним є використання мультибіометричних систем, тобто таких, де здійснюється ідентифікація за двома та більше біометричними параметрами.

Для збільшення ефективності використання систем відеоспостереження в діяльності правоохоронних органів доцільно використовувати біометричний метод ідентифікації за геометрією обличчя. Тим більше, що на біометричному ринку вже є достатня кількість пропозицій програмного забезпечення для таких систем. Необхідним є держзамовлення на розробку програмного забезпечення для систем ідентифікації за обличчям, оскільки рівень підготовки програмістів в науково-дослідних установах України є достатнім для такої розробки.

Якщо ж розглядати методи ідентифікації особи, які не входять в «три великі біометрики», то для практичного використання в правоохоронних органах України сьогодні можна рекомендувати ідентифікацію за геометрією кисті, за венами руки та пальців і за голосом. Ці методи не вимагають дорогого обладнання і програмного забезпечення, які до того ж є у продажу. Також доцільною є розробка такого обладнання і програмного забезпечення в Україні, оскільки науковий та промисловий потенціал нашої держави це дозволяє.

1. Захаров В.П., Рудешко В.І. Використання біометричних технологій правоохоронними органами у XXI столітті: науково-практичний посібник / В.П. Захаров, В.І. Рудешко. – Львів: ЛьвДУВС, 2009. – 440 с.
2. Барсуков В.С. Біоключ – шлях до безпеки // http://kvartir-remont.com.ua/biokljuch-shljah-do-bezpeki.
3. Современные биометрические методы идентификации. Хабрахабр від 11.08.2011. [Електронний ресурс] – Режим доступу: http:// habrahabr.ru/post/ 126144.

4. Огляд зарубіжного досвіду застосування методу біометричної аутентифікації людини Укрбюро Інтерполу від 29.06.2010. [Електронний ресурс] – Режим доступу: http://42827.ncbint00.web.hosting-test.net/?p=270.
5. Біометричний паспорт зовні такий самий, як звичайний. ZAXID.NET від 9.12.2014. [Електронний ресурс] – Режим доступу: http://zaxid.net/news/showNews.do?biometrichniy_pasport_zovni_takiy_samiy_yak_zvichayniy_foto&objectId=1286931.
6. Соя О. Chaos Computer Club зламують Touch ID. Гаджети українською від 23.09.2013р. //http://vinsee.com.ua/chaos-computer-club-zlamuyut-touch-id.
7. Участников беспорядков полиция «вычисляет» с помощью компьютерной технологии распознавания лиц. Dokumentika.org від 12.09.2012. [Електронний ресурс] – Режим доступу: http://dokumentika.org/spetssluzhbi/uchastnikov-besporyadkov-v-londone-politsiya-vichislyaet-s-pomoschiu-kompiuternoy-technologii-raspoznavaniya-lits.

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ ПІДГОТОВКИ ПРАЦІВНИКІВ ПРАВООХОРОННИХ ОРГАНІВ В УКРАЇНІ

Гаврильців Марія Теодорівна,
доцент кафедри адміністративно-правових дисциплін ЛьвДУВС, к.ю.н.

Стрімкий та динамічний розвиток інформаційних відносин у XXI ст. щораз більше впливає на трансформацію різних сфер життя людини у всіх країнах світу. Широке впровадження інформаційно-комп'ютерних технологій та систем, удосконалення технологічних засобів збирання, зберігання, використання та поширення інформації призвели до стрімкого розвитку інформаційних відносин, розбудови інформаційного суспільства та формування світового інформаційного простору. В усіх сферах життєдіяльності все частіше використовуються категорії, пов'язані з поняттям «інформація», як-от: «інформаційні технології», «інформаційна війна», «кіберпростір», «кіберзлочинність», «електронне урядування» тощо.

За таких умов дедалі актуальнішими стають проблеми формування нормативно-правової бази у галузі інформаційних

відносин та її подальшого розвитку і удосконалення в умовах європейських інтеграційних пріоритетів України, імплементації норм міжнародного права в інформаційне законодавство України, а також проблема систематизації національного законодавства у сфері застосування інформаційних технологій.

Після проголошення державної незалежності України розпочалося активне формування системи національного законодавства у сфері інформації та інформаційних технологій. З 90-х рр. XX ст. і до сьогодні прийнято значну кількість законів та інших нормативно-правових актів, що дозволило врегулювати найбільш важливі норми інформаційних відносин та інформаційної діяльності.

Нормативно-правовою основою інформаційних відносини в Україні є ціла низка нормативно-правових актів: Конституція України, закони України «Про інформацію», «Про науково-технічну інформацію», «Про телебачення і радіомовлення», «Про друковані засоби масової інформації (пресу) в Україні», «Про бібліотеки і бібліотечну справу», «Про Національний архівний фонд і архівні установи», «Про інформаційні агентства», «Про телекомунікації», «Про Національну програму інформатизації», «Про концепцію національної програми інформатизації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», «Про авторське право і суміжні права», «Про державну таємницю», «Про державну статистику», «Про доступ до судових рішень», «Про електронні документи та електронний документообіг», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації», «Про рекламу», «Про засади державної мовної політики», «Про Суспільне телебачення і радіомовлення України», «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» тощо.

Інформаційно-комунікаційні технології істотно змінили практично всі види суспільних відносин (у науці під цим терміном розуміють всі технології, пов'язані із застосуванням та експлуатацією комп'ютерних систем, використовуваних для збереження, перетворення, захисту, обробки, передачі й одержання інформації). Усі сучасні зазначені технології зорієнтовані на об'єднання в

мережі з єдиним програмним забезпеченням, що носить характер глобальної інформатизації.

Початок третього тисячоліття позначився оновленими поглядами світової спільноти в майбуття, визначенням ціннісних властивостей суспільного життя, які характеризують його якість. Світ визнав, що добробут, освіта та здоров'я людини є головними чинниками якості її життя, а якість освіти – основною метою, пріоритетом розвитку суспільства XXI ст. [1, с. 4].

Особливої уваги потребує належна професійна підготовка майбутніх працівників правоохоронних органів України, адже сучасний стан застосування інформаційних технологій у всіх галузях права потребує розширення їх впровадження у правоохоронній діяльності.

Сьогодні неможливо уявити собі ефективну роботу правоохоронних органів з попередження, розкриття та розслідування злочинів, встановлення осіб, які їх вчинили без використання сучасних інформаційних технологій. Величезна кількість статистичної, аналітичної та довідкової інформації використовується в діяльності судових органів, прокуратури, нотаріальних та адвокатських організацій, а також в оперативно-розшуковій, слідчій та експертній роботі органів внутрішніх справ. Для цього широко застосовуються інформаційні технології та відповідне спеціальне програмне забезпечення.

Стрімкий розвиток інформаційно-комунікаційних технологій створив об'єктивні передумови щодо використання сучасної комп'ютерної техніки в процесі професійної підготовки. На сьогодні комп'ютер та інформаційні технології є не лише предметом вивчення цілої низки навчальних дисциплін, а й засобом здійснення навчальної, наукової і професійної діяльності фахівця, який виконує свої професійні обов'язки в умовах інформаційного суспільства, в якому інформація й технології її опрацювання перетворюються на стратегічний ресурс. Саме тому комп'ютерно-інформаційна підготовка випускника вищого юридичного навчального закладу займає одне з пріоритетних місць у процесі визначення професійної компетентності випускника та його та здатності до здійснення певної професійної діяльності [2, с. 15].

Юрист-правоохоронець – це професіонал, який має фундаментальні та спеціальні юридичні знання, глибоко переконаний у винятковому призначенні права, верховенства права і законності для суспільства, кваліфіковано користується юридичним інструментарієм при розв'язанні юридичних проблем в ім’я захисту прав і законних інтересів громадян.

Безперечно, професійна діяльність юриста пов’язана з опрацюванням значних обсягів нормативно-правової бази з різних галузей права для аналізу різноманітних нестандартних конфліктів, кваліфікації правопорушень, тих чи інших суперечливих з точки зору чинного законодавства ситуацій. На сьогодні обсяг правової матерії настільки великий, що для оперативного доступу до неї, систематизації, а також своєчасного і коректного використання все більш актуальним стає застосування спеціалізованих інформаційно-технічних і програмних засобів.

Саме для цього призначені комп’ютерні правові системи із законодавства, що знайшли широке розповсюдження у науковій, методичній, навчальній роботі провідних юридичних вищих навчальних закладів та у практичній професійній діяльності фахівців у галузі права. Напрацювання майбутніми правниками стійких навичок роботи з правовими інформаційно-пошуковими системами стало складовою їхньої комп’ютерно-інформаційної підготовки, що дозволяє майбутньому юристу впевнено орієнтуватися у мінливому правовому полі, адекватно реагувати на зміни і доповнення у чинному законодавстві [3, с. 46].

Фахівець-правоохоронець має досконало орієнтуватися в пошукових системах Інтернету, мати здатність швидко знайти необхідну для роботи нормативну базу, а також навички швидкої адаптації до незнайомих йому програм. Також фахівець у сфері юриспруденції має володіти навичками роботи з правовими базами та їх пошуковими системами (наприклад, «Ліга», «НАУ», «Експерт» та ін.). Такі навички є складовими інформаційної культури юриста, тобто такого рівня інформаційної підготовки, який дозволяє не тільки вільно орієнтуватися йому в потрібному інформаційному середовищі, а й брати участь у його формуванні та перетворенні.

Категоріями інформаційної культури особи можна вважати також її вміння формулювати свою потребу в інформації, ефективно здійснювати пошук необхідної інформації в усій сукупності інформаційних ресурсів, переробляти і створювати якісно нову інформацію, вести індивідуальні інформаційно-пошукові системи, відбирати та оцінювати інформацію, а також здатність до інформаційного спілкування і комп'ютерну грамотність.

Коректне і впевнене володіння комп'ютерними засобами пошуку і зберігання правових матеріалів, навички аналізу нормативно-правових актів на предмет відповідності і придатності для кваліфікації фабул правових задач, підготовка власних документів з використанням знайдених правових інформаційних матеріалів стають невід'ємною складовою професійної діяльності правознавця в умовах інформаційного суспільства.

1. Забезпечення якості вищої освіти: європейський досвід та реалії українського класичного університету: навч. посіб./укл. : Р.І. Петришин, О.Г. Ущенко, М.Г. Іванчук та ін. – Чернівці: Чернівецький нац. ун-т, 2013. – 208 с.
2. Співаковський О.В. Інформаційні технології в юридичній діяльності: базовий курс: [навч. посібн.] / О.В. Співаковський, М.І. Шерман, В.М. Стратонов, В.В. Лапінський. – Херсон: ХДУ, 2012. – 220 с.
3. Шерман М.І. Правова інформаційно-пошукова система «ЛІГА: ЗАКОН. Юрист» як засіб комп'ютерної підтримки навчання правових дисциплін / М.І. Шерман // Науковий часопис Національного педагогічного університету ім. М.П. Драгоманова.: Збірник наукових праць. – 2011. – Вип. 11 (18). – С. 46–51.

ПРОБЛЕМИ І КОНЦЕПЦІЯ РОЗВИТКУ ІНФОРМАЦІЙНИХ СИСТЕМ ОВС УКРАЇНИ

Нагачевський Сергій Володимирович,
доцент кафедри кримінально-правових дисциплін факультету психології, права і економіки ЛьвДУВС, к.ю.н.

Засоби обчислювальної техніки почали активно використовуватись в органах внутрішніх справ (ОВС) з 1960-х років. Здебільшого сфера їх застосування обмежувалась аналізом статистичної інформації, веденням криміналістичних та інших обліків і

контролем за станом розгляду заяв і повідомлень про злочини. Принципи побудови інформаційних систем ОВС відображали притаманний для того часу рівень розвитку технічних засобів і досягнень технології. Переважала централізована обробка інформації, за умов якої безпосередній доступ споживачів інформації (практичних працівників ОВС) до банків даних був неможливий або незручний. При цьому практично для кожної нової задачі розроблялись окремі проектні рішення, що призводило до дублювання інформаційних масивів, неузгодженості між ними і нераціональної організації інформаційної системи в цілому. Ефективність використання інформаційних систем знижувалась через відсутність зв'язку між базами даних різних регіонів і несумісність форматів зберігання даних.

Поступово склалася ситуація, коли програмно-технічна база інформаційних систем ОВС застаріла і перестала відповідати вимогам користувачів. Крім зазначених вище можна назвати такі важливі недоліки:

- дублювання процесів збирання та оброблення даних різними галузевими службами і на різних рівнях;
- недостатні повнота, вірогідність і захищеність даних;
- численність і недосконалість первинних облікових документів;
- слабкий інформаційний зв'язок між обліково-реєстраційними, оперативно-розшуковими та довідковими фондами різних служб;
- недосконалість організаційно-кадрового забезпечення інформаційних підрозділів МВС, ГУМВС, УМВС та галузевих служб;
- нераціональне використання фінансових коштів на підтримку і розвиток інформаційних систем;
- недосконалість нормативно-правової бази.

Водночас загострення оперативного стану в Україні, збільшення обсягів інформації, що надходить і переробляється, зумовило гостру потребу в підвищенні ефективності всіх служб МВС на основі новітніх інформаційних технологій. Це підтверджується і нормативними документами, зокрема програмою боротьби з організованою злочинністю (Указ Президента України від

17.01997 р. № 837). Уже сьогодні в цьому напрямку спостерігаються певні позитивні тенденції, серед яких загальне підвищення комп'ютерної грамотності працівників міліції; збільшення переліку комп'ютерних інформаційних обліків; поширення використання сучасних засобів комп'ютерної техніки в діяльності всіх ланок ОВС; впровадження безпаперових технологій оброблення інформації; створення комп'ютерної мережі обміну інформацією.

Головною метою робіт, що проводяться, є забезпечення інформаційної підтримки діяльності ОВС:

- оперативне отримання працівниками та підрозділами ОВС повної інформації, необхідної для розкриття, розслідування, попередження злочинів і розшуку злочинців у систематизованому та зручному для користування вигляді;
- збирання та оброблення оперативної, оперативно-розшукової, оперативно-довідкової, аналітичної, статистичної і контрольної інформації для оцінювання ситуації та прийняття обґрунтованих оптимальних рішень на всіх рівнях діяльності ОВС;
- ефективна інформаційна взаємодія з іншими правоохоронними органами і державними установами.

У 1997 році інформаційні системи Держкомкордону та МВС України було інтегровано в єдиний інформаційний простір. Основу ІС прикордонних військ України складає комплекс автоматизованого паспортного контролю «Кордон», який було адаптовано до нових пристроїв зчитування паспортів. Інформаційна система МВС України здійснює інформаційну підтримку в розкриванні та попередженні злочинів, установленні та розшуку злочинців, надає статистичні, аналітичні та довідкові дані. У результаті нова система прикордонного контролю дає змогу за лічені секунди одержувати інформацію про будь-який суб'єкт, який перетинає кордон України. У Німеччині час реакції подібної системи на запит оператора складає всього 1,5с.

У сфері управлінської та контрольно-методичної роботи виконуються такі завдання комп'ютеризації:

- збирання і нагромадження даних про скоєні злочини;
- аналіз статистичної звітності за встановленими формами;
- контроль за дотриманням процесуальних строків, розглядом заяв громадян, виконанням планових заходів;

- складання управлінських документів;
- створення і використання баз даних (знань) та автоматизованих інформаційно-пошукових систем для одержання інформації про нормативні акти, наукову літературу, методичні розробки, матеріали передового досвіду слідчої та судової практики;
- нагромадження інформації про експертні установи, їх можливості, види експертиз, приблизні питання експертам та ін.;
- аналіз робіт з профілактики злочинів та оцінювання їх ефективності;
- аналіз інформації щодо нерозкритих злочинів минулих років, розробка рекомендацій щодо їх розкриття та використання типових ознак і ситуацій;
- формування моделей процесуальних дій зі збільшенням обсягу стандартної інформації стосовно розслідування різних видів злочинів;
- розробка методик розслідування кримінальних справ з комп'ютерних та інших видів злочинів.

У сфері розслідування злочинів автоматизації підлягають:

- процес слідчого виробництва з використанням баз процесуальних та інших документів, що оформляються на стадії попереднього розслідування;
- планування заходів по конкретних кримінальних злочинах;
- створення календарних планів і мережних графів розслідування;
- складання слідчих та інших документів (у першу чергу, постанов щодо притягнення як обвинуваченого та висновків з обвинувачення) на основі даних, занесених у базу;
- передача до суду протоколів допитів, постанов та інших процесуальних документів на магнітних носіях та по каналах зв'язку;
- вибір та передача необхідної інформації для проведення відповідних заходів у ході оперативно-розшукової діяльності, її оформлення згідно з кримінально-процесуальним кодексом;
- організація та проведення бухгалтерських ревізій та експертиз, різноманітні розрахунки з кримінальних проваджень по економічних злочинах;

- контроль з боку керівників підрозділів за розслідуванням кримінальних проваджень на всіх етапах;
- використання у ході розслідування програм з методиками розслідування злочинів різних видів.

У цілому ІС МВС має структуру, адекватну адміністративно-територіальному розподілу і складається з підсистем відповідно до напрямків діяльності міністерства. Комплекс технічних засобів підтримує всі функції архітектури «клієнт-сервер» та «термінал-сервер» з урахуванням специфіки завдань, що виконуються на кожному рівні системи. Усі рівні комплектуються серверами баз даних і АРМ кінцевих користувачів. Для інформаційного забезпечення ОВС України створюються дві категорії ІС за функціональним призначенням – загальновідомчі та галузеві. До **загальновідомчих ІС** належать:

- ІС оперативно-розшукового призначення, які містять дані, безпосередньо пов'язані з кримінальним провадженням або оперативно-розшуковою справою і використовуються багаторазово;
- спеціалізовані ІС оперативного оброблення інформації;
- ІС оперативно-довідкового призначення, які містять фактографічну інформацію про осіб, об'єкти та речі, що становлять оперативний інтерес;
- ІС кримінальної статистики, що містять інформацію про стан злочинності та результати боротьби з нею;
- адміністративно-управлінські ІС, які містять інформацію загальнодержавного та загальнослужбового використання.

До категорії **галузевих ІС** належать такі, що не містять загальновідомчої інформації.

Доступ до ІС ОВС України здійснюється з відповідних АРМ безпосередньо або за допомогою засобів закритої відомчої електронної пошти через комутовані телефонні канали міжміської телефонної мережі, телефонної мережі «Іскра-2», телефонної мережі «Укрзалізниця», по виділених каналах зв'язку. Мережа має топологію типу «зірка» з Головним поштамтом в УОІ МВСУ і регіональними поштамтами в областях, до яких підключаються віддалені поштові відділення (абоненти). Абонентами електронної пошти ОВС України є підрозділи та окремі працівники органів внутрішніх справ.

Об'єднання АРМ у мережу дає змогу не тільки поєднати всі інформаційні ресурси, створити єдину розподілену базу даних, а й забезпечити за допомогою засобів комунікації пошук і одержання необхідної фактографічної та документальної інформації з баз даних Інтерполу та інших структур.

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ У КОНТЕКСТІ ПРОЕКТУ ДОКТРИНИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Єсімов Сергій Сергійович,
доцент кафедри адміністративно-правових дисциплін ЛьвДУВС, к.ю.н., доцент

Політичні реалії розвитку держави у 2014 році показали неадекватність системи національної безпеки реально існуючим загрозам життєво важливих інтересів України. Очевидно, що загроза стабільності державного життя, яка розглядається як загроза сталого функціонування всіх існуючих у ньому інститутів, є основною в числі існуючих загроз, а її запобігання має ґрунтуватися на створенні сукупності економічних, політичних, правових та інших умов реалізації інтересів особи, суспільства і держави.

Система національної безпеки функціонує як результат нормативної дії самих різних правових інститутів. Одним з таких інститутів є інформаційна безпека, яка в умовах демократичних перетворень є важливим чинником забезпечення політичної стабільності. Можна виділити три обставини, що обумовлюють необхідність правових досліджень інформаційної безпеки: по-перше, концептуальна недооцінка значення інформаційної безпеки для захисту життєво важливих інтересів особи, суспільства і держави; по-друге, неадекватність правового забезпечення інформаційної безпеки завданням, що стоять в сфері інформатизації, розвитку інформаційного суспільства; по-третє, невідповідність інституційно-правового поля функціонування інформаційної безпеки обсягом завдань, що стоять у цій сфері.

Розроблені проекти Доктрина інформаційної безпеки України та Стратегії розвитку інформаційного простору України на період до 2020 року мають позитивний вплив на процес формування системи національної безпеки [1; 2]. Найважливіше значення для інформаційної безпеки має концептуальна оцінка ролі інформатизації, визначення інтересів України та напрямів їх реалізації. Однак, враховуючи сучасні реалії, слід відзначити і важливий недолік цих документів – у них немає чіткої оцінки правових засобів у забезпеченні безпеки інформаційної сфери, а Стратегія національної безпеки не вводить інформаційну безпеку в число пріоритетів. Очевидно, що це робить істотний вплив на розвиток інформаційної безпеки, що відбивається на правовому регулюванні даної сфери. Наслідком цього є комплекс проблем правового забезпечення захисту інформаційних інтересів, пов'язаних з державним регулюванням цієї сфери, які полягають як у суперечливості, так і в неузгодженості деяких діючих нормативних правових актів, правових прогалинах, низькому рівні відповідальності за порушення інформаційного законодавства, що не відповідає рівню вимог які існують в Європейському Союзі. Як приклад, доцільно привести рішення Окружного адміністративного суду м. Києва від 23 березня 2014 р. і Національної ради України з питань телебачення і радіомовлення від 17.07.2014 № 292 щодо заборони програм окремих телеканалів Російської Федерації у місцях масового відпочинку та скупчення людей, баз відпочинку, розважальних закладів [3].

Інформаційні відносини – це сукупність зв'язків між людьми, які виникають у процесі створення, збору, обробки, накопичення, зберігання, пошуку, розповсюдження та споживання інформації. Інформаційні відносини є частиною системи суспільних відносин, обумовлені змістом економічних, політичних, правових і культурних зв'язків, що характеризують суспільну і правову системи. Учасниками інформаційних відносин виступають людина, органи державної влади та громадського самоврядування, громадські, міжнародні та міжурядові організації. Суб'єктом інформаційних відносин є особистість, суспільство і держава, об'єктом – свобода шукати, одержувати та поширювати інформацію. Інформаційні відносини є основою інформаційного процесу,

який являє собою діяльність суб'єктів інформаційних відносин, засновану на пріоритетах економічного, соціального та культурного розвитку, спрямовану на формування відповідного інформаційного порядку суспільства.

У зазначеному контексті інформаційну безпеку доцільно розглядати як правову категорію, що виражає зв'язок між інтересами особи, суспільства і держави у сфері інформації та правовим забезпеченням захисту. Тобто це можна розглядати як стан захищеності особи, суспільства та держави в інформаційному просторі, захист інформації та інформаційних ресурсів, а також інформаційно-телекомунікаційної інфраструктури від можливих внутрішніх і зовнішніх загроз. Зазначено чітко визначено змістом наказу МВС України від 19.08.2014 № 840 «Про деякі питання інформаційної безпеки України» [4]. Правова природа інформаційної безпеки забезпечує її функціонування як виду національної безпеки у контексті інституційної, організаційної та правової системи забезпечення направленої на збереження інформаційних ресурсів держави, захищеності прав особистості в даній сфері. З погляду юриспруденції інформаційна безпека виступає як важлива частини інформаційних правовідносин, що доведено українськими вченими. Правові засоби забезпечення інформаційної безпеки є провідним фактором захисту національних інтересів у даній сфері, а їх застосування визначається: оптимізацією балансу відносин між правом суб'єктів інформаційних відносин на вільне отримання інформації та правом на встановлення обмежень даних відносин з боку інших осіб щодо відомостей, власниками яких вони є; розробкою та реалізацією правових заходів захисту інформації, доступ до якої повинен обмежуватися правовими підставами в процесі захисту інформаційних ресурсів. Стан інформаційної безпеки визначається правовою політикою органів державної влади спрямованої на нормативно-правове регулювання інформаційних відносин. Мета регулювання полягає у впливі на формування бажаного для суспільства режиму створення, збору, обробки, накопичення, зберігання, пошуку, розповсюдження та споживання інформації включає законотворчу, правозастосовну та правозахисну діяльність що охоплюється Стратегією розвитку інформаційного суспільства в Україні. Водночас правове

регулювання інформаційних процесів представляє собою обумовлену нормативно-правовим регулюванням діяльність суб'єктів інформаційної сфери, спрямовану на їх моделювання та проектування; яка визначається правовими принципами, що виражають пріоритети державних зобов'язань з реалізації та дотримання прав і свобод людини; конституційним закріпленням права громадянина та людини на пошук, отримання та поширення інформації. Зазначене повинно знайти правову інституціоналізацію інтересів України в інформаційній сфері у проектах Доктрини інформаційної безпеки України, Стратегії розвитку інформаційного простору України на період до 2020 р.

Правове забезпечення ліквідації загроз і ризиків у сфері інформаційної безпеки є основним чинником її структурування, формування і розглядається як законотворча діяльність, спрямована на запобігання нанесення шкоди інтересам особи, суспільства і держави в інформаційній сфері. Сукупність потенційних загроз інформаційної безпеки України поширюється на сферу конституційних права і свобод громадян, духовного життя суспільства, інформаційних інфраструктури та ресурсів. На думку Підюкова П.П., кіберзлочинність, як одна із загроз інформаційній безпеці, є суттєвою перепоною євроінтеграції України та серйозна загроза її економічній безпеці, як складової частини національної безпеки, правам і законним інтересам громадянського суспільства, що теж повинно бути відображено у Доктрині [5].

Відзначаючи те, що в України в цілому склалася законодавча база забезпечення інформаційної безпеки, слід констатувати цілий ряд недоліків до яких доцільно віднести: правову невизначеність статусу окремих категорій суб'єктів інформаційних відносин; проблеми розмежування повноважень регулювання інформаційних процесів між органами державної влади та органами місцевого самоврядування у контексті Концепції реформування місцевого самоврядування та територіальної організації влади в Україні; невирішеність проблеми наділення повноваженнями органів місцевого самоврядування у сфері забезпечення інформаційної безпеки; суперечності між нормами законодавства, які найчастіше зустрічаються між нормами законів і підзаконних актів. Зазначене не у повній мірі визначено у проекті Доктрини інформаційної безпеки України.

Подальший розвиток правового забезпечення інформаційної безпеки, пов'язаний з розробкою Доктрини інформаційної безпеки України, повинен сформулювати правові основи інформаційної безпеки України, визначити її структуру та соціальні функції, систему суб'єктів, сил і засобів забезпечення; закріпити систему правових норм загального характеру, що регулюють формування та використання інформаційних ресурсів, збір, зберігання, обробку, розповсюдження інформації, створення та використання інформаційних технологій, засобів їх забезпечення у контексті нормативно-правового регулювання інформаційної безпеки прийнятому у Європейському Союзі, але з урахуванням постійної протидії інформаційній експансії Росії. Нормативно-правове регулювання інформаційної безпеки повинно бути спрямоване на підтримку динамічної рівноваги в суспільстві за рахунок розвитку інститутів демократії, правового регулювання суспільних процесів. Зазначені аспекти відіграють вирішальну роль у побудові системи інформаційної безпеки, яка вимагає подальшого інституційного розвитку та вдосконалення.

1. Проект Указу Президента України «Про Доктрину інформаційної безпеки України». [Електронний ресурс]. – Режим доступу: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat_id=61025
2. Проект Указу Президента України «Про затвердження Стратегії розвитку інформаційного простору України на період до 2020 року». [Електронний ресурс]. – Режим доступу: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113102&cat_id=61025
3. Протокол спільної наради МВС України і Національної ради України з питань телебачення і радіомовлення від 30.08.2014 р.
4. Наказ МВС України від 19.08.2014 № 840 «Про деякі питання інформаційної безпеки України».
5. Підюков П.П. Кіберзлочинність як суттєва перепона євроінтеграції України та серйозна загроза її економічній безпеці, правам і законним інтересам громадянського суспільства: психолого-юридична характеристика / [Підюков П.П., Устименко Т.П., Дронова О.С. та ін.] / Інформаційно-популярний та наук.-практ журнал «Міліція України». – 2014. – № 9-10 (207-208). – С. 23-26.

АДМІНІСТРАТИВНО-ПРАВОВІ ЗАХОДИ ЯК ЧИННИК ЗАХИСТУ ІНФОРМАЦІЇ

Дідик Наталія Іванівна,
доцент кафедри адміністративного права та адміністративного процесу ЛьвДУВС, к.ю.н, доцент
Шишко Валерій Валерійович,
доцент кафедри теорії держави і права ЛьвДУВС, к.ю.н, доцент
Шишко Валерій Йосипович,
старший викладач кафедри інформатики ЛьвДУВС

Стан захисту державного інформаційного простору є одним із показників ефективності роботи держави щодо захисту власних інформаційних ресурсів від протиправних посягань. Інформаційна безпека має велике значення для забезпечення життєво важливих інтересів будь-якої держави. Створення розвиненого і захищеного середовища є неодмінною умовою розвитку суспільства та держави, в основі якого мають бути ефективні адміністративно-правові заходи.

Останнім часом в Україні відбуваються якісні зміни у процесах державного управління на всіх рівнях, які зумовлені інтенсивним упровадженням новітніх інформаційних технологій. Швидке вдосконалення інформатизації, проникнення її в усі сфери життєво важливих інтересів зумовило, крім безперечних переваг, і появу низки стратегічних проблем. Посилюється небезпека несанкціонованого втручання в роботу комп'ютерних, інформаційних і телекомунікаційних систем. У зв'язку із цим особливого значення набувають адміністративно-правові заходи захисту службової інформації.

Основу даної праці склав аналіз норм сучасного національного інформаційного законодавства, а також науковий доробок вітчизняних та зарубіжних авторів, серед яких виокремимо А.О. Антонюка, В.М. Білоножко, К.В. Габучан, В.І. Даля, А.П. Загнітко, В.Н. Лопатина, А.І. Марущака, С.Ф. Ожегова, Л.М. Полюгу, В. Темченка, В.Ф. Шаньгина.

Нормативно-правові акти надають різні визначення поняття «захист інформації», зокрема його визначають як сукупність

організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованої системи та осіб, які користуються інформацією (п. 2.8 Положення про порядок та умови видачі інформації з Єдиного ліцензійного реєстру, затвердженого наказом Ліцензійної палати при Мінекономіки України від 15.11.1996 р. № ЛП-37 [1]). Крім того, Законом України «Про державну таємницю» від 21.01.1994 р. № 3855-XII [2] вживається термін «охорона державної таємниці» як комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню таємної інформації та втратам її матеріальних носіїв. Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 р. № 80/94-ВР [3] поняття «захист інформації в системі» розглядається як діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі.

Крім того, законодавство не диференціює поняття «охорона» і «захист» інформації. Так, «термін «охорона» у термінологічних словосполученнях Конституції України вживається для позначення достатньо широкого кола повноважень державних органів, що передбачають, зокрема, запобігання правопорушенням, їх недопущення та відновлення прав і свобод у випадку їх порушення, а також притягнення винних до юридичної відповідальності. Головною особливістю вживання цього терміна у Конституції є його вживання зі значенням, аналогічним до терміна «захист», як обов'язку держави та інших зобов'язаних суб'єктів до дій щодо забезпечення прав і свобод людини [4, с. 63].

Отже, виходячи із зазначених визначень, можна констатувати, що терміни «захист» та «охорона» у нормативному контексті, слід вживати як синоніми чи схожі за значенням поняття щодо мети, завдань, методів і суб'єктів забезпечення прав, тому вони можуть використовуватись у практиці як ідентичні поняття. Однак у науці інформаційного права вони не розглядаються як тотожні. Охорона інформації – встановлення її загального правового режиму, захист, заходи, які використовуються у тих випадках, коли суб'єктивні права на інформацію порушені або залишаються спірними. Проте в цій частині дослідження термін «захист

інформації», на нашу думку, доцільно застосовувати в тому широкому значенні, яке йому надає законодавець, воно охоплює і заходи, спрямовані на відвертання можливості неправомірних дій із службовою інформацією, і заходи, спрямовані на захист і відновлення вже порушених прав.

Плутанина навколо понять «захист» та «охорона» прав цілком логічна з огляду на невизначеність цих понять і в тлумачних словниках. Зокрема, відповідно до Тлумачного словника В. Даля, «захист» – це заступництво [5, с. 542]. С. І. Ожегов визначає поняття «захищати» як «охороняючи, захистити від замахів, від ворожих дій, від небезпеки» [6, с. 196]. Водночас «охорона» означає «берегти, оберігати, захищати, тримати в цілісності, спасати» [7, с. 774], а також «слідкувати, щоб не зробили шкідливого кому-небудь або чому-небудь» [8, с. 234]. Отож, захист у соціально-філософському розумінні становить охорону, а охорона, своєю чергою, – захист. Зауважимо, що в Словнику синонімів [9, с. 322] досліджувані поняття також вживаються як синоніми, тобто можуть бути взаємно замінюваними залежно від контексту. Проте, в деяких тлумачних словниках указується, що захист чого-небудь здійснюється в процесі охорони, в той час як «охороняти» визначається як «ставитися з обережністю, берегти». Цікавим є і те, що в словнику української мови «захист» визначається як заступництво, охорона, підтримка [10, с. 99].

У тлумачному словнику сучасної інформаційно-правової лексики захист інформації розглядається з п’яти позицій:

1) як діяльність, спрямована на забезпечення конфіденційності, цілісності й доступності інформації;

2) як сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації в умовах впливу на неї загроз природного й штучного характеру, реалізація яких може призвести до заподіяння шкоди власникам чи користувачам інформації;

3) як комплекс заходів, спрямованих на забезпечення інформаційної безпеки. На практиці під цим розуміється підтримка цілісності, доступності і, якщо потрібно, конфіденційності інформації і ресурсів, що використовуються для введення, збереження, обробки і передачі даних;

4) як діяльність, спрямована на збереження державної, службової (комерційної) або особистої таємниці, а також на збереження носія інформації будь-якого змісту;

5) як використання в системах збору, передачі, збереження і переробки інформації спеціальних методів і засобів з метою забезпечення схоронності інформації, що захищається, і запобігання витоку технічними каналами [11, с. 147].

Отже, нормативно-правове розуміння адміністративно-правових заходів захисту інформації, в тому числі службової, зводиться до системи правових, організаційних, інженерних, технічних заходів, що спрямовані на збереження цілісності службової інформації та запобігання її витоку.

Тому зміст адміністративно-правового захисту службової інформації ототожнюється з процесом забезпечення інформаційної безпеки як необхідності нормального функціонування держави, суспільства, окремої людини.

А.О. Антонюк відносить до сфери безпеки інформації не захист інформації, а захист права власності на неї [12, с. 103]. Справді, захист інформації організовує і здійснює власник, користувач інформації або уповноважена ними особа (фізична чи юридична), а також держава в особі компетентних органів у межах своєї правоохоронної функції. Захистом інформації власник охороняє свої права на володіння і розпорядження інформацією, намагається запобігти незаконному заволодінню нею і використанню її на шкоду власним інтересам. Система захисту може бути різна, на розсуд власника, а може і не мати такого захисту взагалі. Він здійснюється на основі диспозитивних методів, що входять у сферу цивільно-правового розгляду. Захист інформації стає предметом адміністративно-правового регулювання у випадках, коли обмеження доступу до інформації прямо передбачені законами, коли ці обмеження пов'язані із забезпеченням інформаційних прав і свобод людини, інформаційних аспектів національної, державної, громадської безпеки, моральності, громадського здоров'я тощо і, що дуже важливо, суб'єктом застосування цих обмежень є держава в особі її компетентних органів [13, с. 108].

Від поняття «захист інформації» слід відмежувати захист інформаційних прав особи. У визначенні, що надається А.І. Мару-

щаком, «суб'єктивне право на інформацію – гарантована державою можливість фізичних осіб і держави (державних органів) вільно одержувати, використовувати, поширювати та зберігати відомості, необхідні їм для реалізації своїх прав, свобод і законних інтересів, здійснення завдань і функцій, що не порушує права, свободи і законні інтереси інших громадян, права і інтереси юридичних осіб». Отож, у поняття «захист інформаційних прав особи» входить комплекс можливих видів інформаційної діяльності, де захист інформації є лише однією зі складових. З погляду теорії права об'єктами правового захисту є права і законні інтереси, у тому числі право на інформацію [14, с. 42]. Як стверджує В.Н. Лопатін, «сама інформація не може мати прав та інтересів, а її захист (організаційними, технічними іншими засобами) може і повинен залишатися умовами охорони права на інформацію (наприклад, стосовно інформації з обмеженим доступом)» [15, с. 91].

З уваги на вищенаведене, на нашу думку, «охорона» і «захист» інформації можна визначити як комплекс дій власника інформації для забезпечення прав на її володіння і розпорядження, а також сприяння життєдіяльності людини, суспільства і держави на основі створення органами управління безпечних умов, що обмежують розповсюдження і виключають або істотно ускладнюють несанкціонований, незаконний доступ до інформації та її носіїв.

Форми адміністративно-правового захисту службової інформації традиційно можна класифікувати на юрисдикційні і неюрисдикційні. До перших належить захист порушених прав суб'єктів інформаційних правовідносин у судовому та адміністративному порядку. До других – організаційні, технічні, криптографічні адміністративно-правові засоби захисту службової інформації.

Механізм захисту службової інформації є певним поєднанням організаційних, технічних, криптографічних і юрисдикційних засобів захисту інформації. Усі вони є правовими, оскільки встановлюються правовими актами управління, у тому числі нормативно-правовими. Адміністративно-правовий захист службової інформації – це діяльність щодо застосування юрисдикційних і неюрисдикційних форм її захисту.

Різноманітні моделі і рекомендації щодо створення системи організаційних заходів захисту службової інформації ґрунтуються на універсальному комплексі послідовних заходів:

- формування служби інформаційної безпеки або призначення особи (групи осіб), відповідальної за забезпечення інформаційної безпеки в цій структурі органу виконавчої влади;
- призначення відповідальних осіб у виділених приміщеннях, на конкретних інформаційних об'єктах, а також у приміщеннях, де зберігається службова інформація, у тому числі на паперових носіях;
- розробка і затвердження плану заходів щодо забезпечення інформаційної безпеки (річного, квартального, місячного тощо);
- конкретизація плану з певною метою, завданнями, місцем і часом здійснення заходів;
- навчання, підвищення кваліфікацій фахівців щодо забезпечення захисту службової інформації, контроль за рівнем їх підготовки з огляду на можливості бюджетного фінансування.

Вказані вище плани і заходи щодо організаційного забезпечення безпеки інформації, безумовно, мають свою специфіку щодо окремих видів інформаційних ресурсів і регламентуються підзаконними нормативно-правовими актами, які, як правило, мають гриф обмеження доступу.

Проте на рівні законів визначаються загальні напрями комплексу адміністративно-правових заходів щодо забезпечення захисту службової інформації, які повинні створювати основу для використання технічного, криптографічного та інших адміністративно-правових заходів захисту службової інформації, спрямованих проти несанкціонованого доступу до цієї інформації, проти її спотворення, блокування, знищення.

Так, діяльність щодо технічного захисту службової інформації, що підлягає ліцензуванню, повинна відповідати таким вимогам: наявність спеціальної освіти у осіб, що її здійснюють, або наявність у них спеціальної підготовки; відповідність виробничих приміщень, виробничого, випробувального і контрольно-вимірювального устаткування технічними нормами і вимогами,

встановленими державними стандартами і нормативно-методичними документами щодо технічного захисту службової інформації; використання сертифікованих (атестованих за вимогами безпеки інформації) автоматизованих інформаційних систем і засобів їх захисту; використання третіми особами програм для ЕОМ або баз даних на підставі договору з їх правовласниками.

Наступний адміністративно-правовий захід захисту службової інформації – криптографічний, який є захистом інформації за допомогою шифрувальних засобів (криптографічні засоби захисту інформації – КСЗІ) [16, с. 32], повинен здійснюватися на підставі спеціальної Інструкції, що визначає порядок організації і забезпечення безпеки зберігання, обробки, передачі каналами зв'язку з використанням криптографічних засобів захисту інформації обмеженого доступу, державною таємницею. Зазначимо, що ліцензіати відповідно до цієї інструкції зобов'язані забезпечувати комплексність захисту конфіденційної інформації, тобто використовувати інші засоби захисту, окрім криптографічних, в їх оптимальному поєднанні. Так, наприклад, усі співробітники органів криптографічного захисту інформації зобов'язані дотримуватись вимог щодо надійного зберігання експлуатаційної і технічної документації, ключових документів (ключів, шифрів), негайно вживати заходів щодо відвертання та просочування інформації у разі втрати, розкрадання, недостачі КСЗІ, ключів, шифрів посвідчень, пропусків тощо. Порушені права можуть бути відновлені також у результаті розгляду судом заяви громадянина про неправомірність дії посадовця або колегіального органу. До юрисдикційних форм захисту належать також застосування кримінальних, адміністративних, а також дисциплінарних санкцій.

Що стосується юрисдикційних форм реалізації адміністративно-правових заходів захисту службової інформації у сфері діяльності публічної влади, то на нашу думку, вони повинні реалізовуватися з метою відновлення порушених прав суб'єктів інформаційних правовідносин. До таких заходів насамперед слід віднести:

- документування службової інформації, що є основою для реєстрації інформаційних ресурсів;
- обмеження доступу до службової інформації, що забезпечується системою їх захисту;

- правовий захист службової інформації, що виражається існуванням інституту адміністративно-правової відповідальності за порушення законодавства про службову інформацію, який є однією з гарантій належної її реалізації та правового захисту.

Найменш урегульованим є порядок реєстрації баз, банків даних у частині визначення права власності на ці ресурси і порядок обліку їх у складі державного майна. З метою удосконалення цієї проблеми, необхідна систематизація адміністративного законодавства в частині об'єднання норм, які встановлюють адміністративно-правову відповідальність за правопорушення, предметом посягання яких може бути службова інформація.

Висновок. Таким чином, з метою обґрунтування власної позиції слід зазначити, що адміністративно-правові заходи захисту службової інформації можна визначити як сукупність методів, засобів і прийомів, спрямованих на забезпечення інформаційної безпеки людини, суспільства і держави у всіх сферах їх життєво важливих інтересів. Сутність їх полягає у виявленні, вилученні і нейтралізації негативних джерел, причин і умов впливу на інформацію. Ці джерела становлять загрозу безпеці інформації, а цілі і заходи адміністративно-правового захисту службової інформації повинні здійснюватися з огляду на її зміст.

1. Положення про порядок та умови видачі інформації з Єдиного ліцензійного реєстру: наказ Ліцензійної палати при Мінекономіки України [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0693-96
2. Про державну таємницю: Закон України від 21.01.1994 р. № 3855. – [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3855-12.
3. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. – [Електронний ресурс]. – http://zakon1.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
4. Темченко В. Особливості юридичного змісту термінів «захист» та «охорона» у механізмі забезпечення прав людини / В. Темченко // Вісник Академії управління МВС. – 2007. – № 2–3. – С. 58–65.
5. Даль В. Толковый словарь живого великорусского языка: В 4-х томах / В. Даль. – М.: Русский язык, 1999. – Т. 1: А–З. – 1999. – 699 с.
6. Ожегов С.И. Словарь русского языка / С. И. Ожегов; под ред. докт. филол. наук, проф. Н. Ю. Шведовой. – М.: Рус. яз., 1984. – 797 с.

7. Даль В.И. Толковый словарь живого великорусского языка / В.И. Даль. – Т. 2. – М.: Русский язык, 1979. – 780 с.
8. Габучан К.В. Учебный толковый словарь русского языка / К.В. Габучан. – М.: Русский язык, 1988. – 441 с.
9. Полюга Л.М. Словник синонімів української мови / НАН України; Інститут українознавства ім. І. Крип'якевича; Український мовно-інформаційний фонд. – 3-тє вид. / Левко Михайлович Полюга. – К.: Довіра, 2007. – 477 с.
10. Білоножко В.М. Великий тлумачний словник сучасної української мови / В.М. Білоножко, А.А. Бурячок, Г.М. Гнатюк, І.С. Гнатюк, С. І. Головащук, Г.Н. Горюшина // Інститут української мови НАН України; Інститут мовознавства НАН України; Всеукраїнське товариство «Просвіта» ім. Тараса Шевченка. – К.: Дніпро, 2009. – 1332 с.
11. Загнітко А.П. Тлумачний словник сучасної української мови / А.П. Загнітко, І.А. Щукіна. – Донецьк: БАО, 2009. – 960 с.
12. Антонюк А.О. Основи захисту інформації в автоматизованих системах: навч. посіб. / А.О. Антонюк. – К.: КМ Академія, 2003. – 244 с.
13. Марущак А.І. Інформаційне право: доступ до інформації / А.І. Марущак: навчальний посібник. – К.: КНТ, 2007. – 532 с.
14. Марущак А.І. Інформаційне право: регулювання інформаційної діяльності: навч. посібник / А.І. Марущак. – К.: Скіф; КНТ, 2008. – 343 с.
15. Правовая охрана и защита служебной тайны / В.Н. Лопатин // Государство и право. – 2000. – № 6. – С. 88–93.
16. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: уч. пособ. / В.Ф. Шаньгин. – М.: Форум, 2008. – 416 с.

КОМП'ЮТЕРНИЙ ТЕРОРИЗМ: СУЧАСНИЙ СТАН ТА ШЛЯХИ ПРОТИДІЇ

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

Особливості розвитку процесів глобалізації в сучасних умовах обумовлені переходом від суспільства індустріального до інформаційного. На сьогоднішній день практично кожна галузь у господарстві країни, включаючи енергетику, транспорт, зв'язок, банківський сектор тощо, використовує комп'ютерні мережі і, відповідно, залежить від їх працездатності. Порушивши роботу

цих мереж, можна паралізувати інфраструктуру країни. Таким чином, швидкий прогрес у розвитку інформаційних технологій призводить до виникнення нових істотних проблем у сфері міжнародної безпеки й стабільності й може мати несподівані наслідки у вигляді зростаючої уразливості систем.

У цьому контексті, однією з нових і небезпечних загроз людству стає використання терористичними організаціями новітніх інформаційних технологій [1].

На сьогоднішній день єдиного визначення комп'ютерного (кібер-) тероризму, закріпленого на законодавчому рівні, поки не існує.

Але взагалі під «комп'ютерним тероризмом» слід розуміти свідоме, цілеспрямоване застосування комп'ютерної інформації, комп'ютерів, комп'ютерних систем та мереж для захоплення комп'ютерних систем управління потенційно небезпечними об'єктами з метою:

- виведення цих об'єктів з ладу або їх руйнування, що прямо чи опосередковано створює або загрожує виникненням загрози надзвичайної ситуації внаслідок цих дій;
- створення умов для аварій і катастроф техногенного характеру;
- залякування населення та органів влади;
- вчинення провокацій воєнного конфлікту та міжнародного ускладнення;
- здійснення впливу на прийняття рішень вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об'єднаннями громадян, юридичними особами;
- забезпечення організаційного чи іншого сприяння створенню або діяльності терористичної групи чи терористичної організації [2].

Сьогодні так звана «комп'ютерна», або «кіберзлочинність» є однією з найбільш серйозних проблем багатьох держав, щорічні збитки від якої становлять мільярди доларів США.

У Шрі-Ланці в травні 1998 року «тигри звільнення Тамілу» вперше серед терористичних груп провели кібернетичну атаку, яка була спрямована проти посольств у столиці [3].

Японське терористичне угруповання «Аум Сінрікьо», яке здійснило газову атаку в токійському метро в 1995 році, перед цим створило комп'ютерну систему, що була здатна перехоплювати повідомлення поліцейських радіостанцій і відслідковувати маршрути руху поліцейських автомобілів.

Значної економічної шкоди, аж до повного знищення інформаційної інфраструктури, можуть завдавати, на перший погляд, безвинні комп'ютерні віруси. Як приклад, можна привести резонансне зараження 16 листопада 2001 року вірусом «Nimda» комп'ютерної мережі Укртелеком (провідного оператора зв'язку в Україні). Вірусна атака серйозним чином вплинула на працездатність обчислювальної мережі Генеральної дирекції ВАТ «Укртелеком», яка налічує більше 700 комп'ютерів та десятки серверів. Як наслідок, це спричинило тимчасове відключення комп'ютерів від Інтернету, а також вивело з ладу систему корпоративної електронної пошти. За попередніми підрахунками, збитки від атаки складають більше 1млн. грн.

Поштовий комп'ютерний вірус SirCam «викрадав» документи з органів державної влади, в тому числі адміністрації Президента України. Відомі також спроби знищення офіційного web-сайту Президента України [3].

У протистоянні з новою терористичною загрозою можна виділити ряд основних напрямів боротьби:

- уніфікація та гармонізація національного законодавства та міжнародних актів;
- розробка єдиного понятійного апарату;
- проведення наукових розробок в області створення сучасних технологій виявлення та запобігання кримінальним і терористичним впливам на інформаційні ресурси;
- створення спеціалізованих підрозділів у сфері боротьби з комп'ютерними злочинами та комп'ютерним тероризмом;
- удосконалення міжнародної організаційно-правової взаємодії з питань протидії комп'ютерній злочинності та комп'ютерному тероризму;
- удосконалення багаторівневої системи підготовки кадрів у сфері інформаційної безпеки [1].

Отже, протидія проявам комп'ютерного тероризму вимагає комплексного підходу, що поєднує силові, політико-дипломатичні, економічні й гуманітарні форми та методи дій, а також ефективного поєднання антитерористичних заходів, що вживаються як на національному, так і на міжнародному рівнях.

1. Гавриш С.Б. Комп'ютерний тероризм: сучасний стан, прогнози розвитку та шляхи протидії // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2009. – № 20.
2. Габрелян А.Ю., Стороженко С.В. Інформаційна безпека: проблеми боротьби з кібер-тероризмом // Матеріали Всеукраїнської інтернет-конференції «Соціум. Наука. Культура». – Режим доступу: http://intkonf.org/gabrelyan-ayu-storozhenko-sv-informatsiyna-bezpeka-problemi-borotbi-z-kiber-terorizmom/
3. Гуцалюк М.В. Міжнародне співробітництво щодо протидії злочинам у сфері інформаційних технологій // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2008. – № 8.

МОЖЛИВОСТІ ВИКОРИСТАННЯ СИСТЕМИ ВІДДАЛЕНОГО ДОСТУПУ ТА АДМІНІСТРУВАННЯ ДЛЯ ПОДОЛАННЯ КОРУПЦІЇ

Магеровський Дмитро Вікторович,
студент Національного університету «Львівська політехніка»
Респляк Дмитро Михайлович,
викладач кафедри інформатики ЛьвДУВС

Застосування систем віддаленого керування та адміністрування широко використовується у комерційних структурах для діагностики системи та надання віддаленої допомоги офісним працівникам під час неполадок на їх робочих комп'ютерах. Проте, офіційно ніхто не говорив про можливість використання таких систем для подолання окремих соціальних проблем, наприклад, корупції.

У даній роботі описано підхід до створення концептуальної моделі базових принципів та функціональності систем віддаленого доступу та адміністрування для фізичного та психологічного стримування проведення корупційних операцій.

Головним завданням у цьому напрямі є аналіз вимог до програмного забезпечення, яке буде здатне проводити контроль за електронними засобами працівників установ та організацій, а також створення концепту програми віддаленого адміністрування, прийнятної для використання у різних підрозділах. Така програма має виконувати певний спектр дії:

- проводити перевірку файлів та їх оновлення;
- проводити стеження за декількома користувачами одночасно;
- мати можливість записувати ці дані у вигляді, прийнятному для використання, як речовий доказ;
- за необхідністю отримувати контроль над певним пристроєм.

Аналіз систем віддаленого доступу та адміністрування. Для розуміння того, якою повинна бути система віддаленого доступу та визначити основні принципи, необхідні для її специфікації, потрібно переглянути основні системи віддаленого доступу, що доступні на ринку.

Популярними програмами віддаленого доступу/адміністрування на ринку є:

- Remote Office Manager (далі - ROM);
- TeamViewer;
- My Remote Files;
- Radmin (Remote administrator) [1].

ROM [2] включає в себе сервер та клієнт.

Серверна частина встановлюється на той комп'ютер, до якого необхідно отримати віддалений доступ, клієнтська – на комп'ютер, з якого буде вестися віддалене адміністрування.

Окрім стандартної функції спостереження за екраном віддаленого комп'ютера, утиліта містить набір інструментів, за допомогою яких можна, наприклад, працювати віддалено з диспетчером процесів, дистанційно працювати з командним рядком, переглядати список встановлених на віддаленому комп'ютері додатків. У програмі є можливість обміну текстовими повідомленнями між клієнтом і сервером.

Спостереження за робочим столом віддаленого комп'ютера може відбуватися з перехопленням клавіатури і миші.

Програму можна оптимізувати залежно від швидкості з'єднання. Програма перехоплює напівпрозорі вікна. Також для економії трафіку можна встановлювати різні варіанти передачі кольору зображення.

У процесі роботи з віддаленим комп'ютером певні поєднання клавіш, наприклад «Ctrl + Alt + Del» або «PrintScreen», не можуть використовуватися, оскільки будуть перехоплені операційною системою, під якою ведеться віддалене адміністрування. Однак за допомогою ROM можна послати спеціальну команду на віддалений комп'ютер для емуляції натиснення цих та деяких інших комбінацій клавіш. Програма дозволяє перехоплювати відтворений звук.

У **TeamViewer** [3] кожному користувачу присвоюється свій номер-ідентифікатор. Користувач задає сам собі пароль доступу.

Фактично повнофункціональна версія програми є безкоштовною. Так, TeamViewer Free не можна використовувати в комерційних цілях, не можна одночасно запускати більше однієї сесії з іншим комп'ютером, не можна встановлювати на серверні операційні системи. TeamViewer має спеціальний менеджер для управління з'єднаннями, можливість доступу до віддаленого комп'ютера через браузер, версія для запуску програми з USB-накопичувача.

Будь-яка передача даних від сервера до клієнта здійснюється тільки у вигляді зашифрованих даних, що гарантує абсолютно безпечну роботу TeawViewer. В якості алгоритмів шифрування трафіку, використовується передача даних з ключем AES (256 біт), а також безпечні з'єднання HTTPS/SSL. TeawViewer підтримує роботу через проксі-сервер.

Програма використовує чотири різних режими підключення: віддалений контроль, показ власного робочого стола, режим роботи з файлами, а також режим організації мережі VPN з віддаленим комп'ютером.

Програма також дозволяє переносити файли з одного комп'ютера на інший. Всі версії TeawViewer включають в себе спеціальний файловий менеджер, за допомогою якого можна керувати копіюванням і переміщенням даних. Інтерфейс менеджера виконаний у вигляді двох панелей, як у Far або Total Commander.

Для того, щоб швидкість передачі даних була максимальною, в програмі використовується додатковий алгоритм стиснення даних.

TeamViewer підтримує функцію IP-телефонії, чату, відеоконференції. У програмі присутній інструмент Whiteboard – віртуальна дошка для малювання, свого роду мініатюрний графічний редактор.

My remote files [4] дає можливість розгорнути на локальному комп'ютері веб-сервер, за допомогою якого користувач може отримати доступ до файлів, використовуючи підключення до Інтернету.

Знаючи IP-адресу віддаленого комп'ютера, можна зайти на нього як на звичайну веб-сторінку в браузері. Далі робота відбуватиметься через веб-інтерфейс. Користувач зможе переглядати дані на віддаленому комп'ютері, створювати віртуальні архіви, сортувати дані, переглядати вміст архівів, а також розділяти великі файли на частини для більш зручного завантаження.

Перед тим як почати працювати з програмою, необхідно скласти список користувачів, а також вказати, які з директорій будуть доступні тому чи іншому користувачеві.

Щоб адміністратор міг проконтролювати дії певного користувача, він може бути сповіщений про кожне нове підключення до сервера. В налаштуваннях утиліти можна вказати список довірених IP-адрес, а також папки, доступ до яких блокується для будь-якого користувача. Програма може автоматично завершувати сесію через деякий час, при відсутності активності з боку користувача.

My remote files веде статистику підключень і дає можливість переглядати історію з використанням фільтрів часу, імені користувачів тощо.

Radmin [5] – одна з найвідоміших програм такого класу в СНГ.

У програмі реалізовані можливості передачі файлів з функцією докачки у разі втрати зв'язку, є підтримка декількох одночасних підключень до екрану віддаленого комп'ютера. Також можна встановлювати свої права для кожного користувача, використовувати IP-фільтри для обмеження доступу до певних IP-

адрес і підмереж. Використовуючи інтегровані текстовий і голосовий чати, можна обмінюватися особистими повідомленнями, а також проводити конференції між декількома користувачами.

Для передачі даних з екрану віддаленого комп'ютера використовується технологія DirectScreenTransfer (загальна назва Video Hook Driver), основною особливістю якої є висока швидкість передачі даних при мінімальному завантаженні центрального процесора і невеликому мережевому трафіку. В основі роботи цієї технології – отримання даних безпосередньо від відеодрайвера операційної системи ще до їх попадання в пам'ять графічного адаптера.

Безпека даних, переданих з одного комп'ютера на інший за допомогою Radmin, забезпечується завдяки інтеграції таких розробок, як Windows Security, NTLM / Kerberos і підтримці Active Directory. В останній версії програми аутентифікація користувача виконується з допомогою модифікованого алгоритму Diffie-Hellman, а спеціальна таблиця IP-фільтрації дозволяє звузити права доступу до зазначених IP-адрес і мереж. У таблиці зазначено основні характеристики описаних вище систем.

Основні характеристики систем віддаленого доступу та адміністрування

	ROM	TeamViewer	MRF	Radmin
Сервер-клієнт	+	-	-	+
Відображення екрану	+	+	-	+
Отримання доступу до файлів	-	-	+	-
Перехоплення пристроїв введення	+	+	-	+
Підключення з допомогою IP	-	-	+	-
Лог роботи користувачів	-	-	+	-
IP телефонія	+	+	-	+
Графічний редактор	-	+	-	-
Налаштування дозволів	+	+	+	+
Безпека передавання даних	+	+	+	+

Моделювання системи. Для ефективної роботи з виявлення хабарників у силових структурах з допомогою системи віддаленого адміністрування необхідно:

- забезпечити можливість постійного спостереження за особами, що підозрюються у хабарництві;
- забезпечення можливості переглядати зміни у файлах співробітників – тобто можливість записувати дані у сховище даних з певним часовим інтервалом або за запитом адміністратора системи;
- забезпечення можливості переглядання файлів напряму;
- забезпечення можливості блокувати використання певного комп'ютера.

Чинники зменшення рівня корумпованості. *Фізичний рівень*. Полягає у забезпеченні постійного контролю за працівниками під час роботи. Дозволяє проводити зріз документів та виявляти у них невідповідності. Дозволяє блокування комп'ютера працівника.

З фізичного рівня виникає *психологічний рівень***.** Він полягає у тому, що працівник, знаючи, що за ним проводиться слідкування не наважується виконувати протиправні дії.

Опрацювання даних у системі. Опрацювання даних у системі може бути аналогічне програмі My Remote Files. Так, на локальному комп'ютері можна запустити веб-сервер, що дозволить перезаписати файли до бази знань. Підключення може здійснюватися по черзі до кожного комп'ютера в мережі за присвоєним йому кодом. Дані, що отримали зміни, записуються до сховища з необхідною датою. Дані, в свою чергу, прив'язані до кожного конкретного працівника. Дані, що не є свідченням протиправних дій працівника – видаляються. Решта даних записується у інше сховище. Щоб вберегти дані від втрати або дій зловмисника – дані кодуються.

Юридична точка зору. Для використання системи, що безперервно стежить за особою, тим самим забираючи в неї право на особистий простір, необхідно підготувати законодавчі акти. Також, працівник має бути попереджений про факт стеження за ним та погодитись на такі умови в обов'язковому порядку при бажанні працевлаштуватись або продовжити роботу.

Висновок. Система віддаленого доступу/адміністрування загалом може ефективно використовуватись для зниження рівня корупції. Проте, для її впровадження та використання необхідно

вносити зміни до законодавства або контракту працівника. Також потрібен додатковий контроль над адміністратором системи.

1. http://download.chip.eu/ru/Remove-Administration-CHIP-Review_6903958.html
2. http://remotedesktopmanager.com/Home/Features
3. http://www.teamviewer.com/ru/products/remotecontrol.aspx
4. http://my-remote-files.en.softonic.com/
5. http://www.radmin.ru/solutions/telecommuting.php

СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОВС

Подра Ольга Павлівна,
доцент кафедри менеджменту ЛьвДУВС, к.е.н.
Ковалик Олена Володимирівна,
студентка ЛьвДУВС
Омелян Ірина Ігорівна,
студентка ЛьвДУВС

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 тощо.

З огляду на зазначену актуальність виникає необхідність обґрунтування сучасного стану, проблем та перспектив розвитку інформаційного забезпечення діяльності органів внутрішніх справ. Практика боротьби зі злочинністю переконливо свідчить про суттєву, а в багатьох випадках пріоритетну роль системи інформаційного забезпечення органів внутрішніх справ як ланки, що зумовлює ефективність роботи правоохоронних структур.

Система інформаційного забезпечення здійснює інформаційну підтримку органів внутрішніх справ у розкритті та попередженні злочинів, установленні і розшуку злочинців, надає багатоцільову статистичну, аналітичну та довідкову інформацію.

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.

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.

Основними завданнями функціонування системи інформаційного забезпечення ОВС вважаються:

- забезпечення можливості оперативного отримання інформації у повному, систематизованому та зручному для користування вигляді співробітниками та підрозділами ОВС для розкриття, розслідування, попередження злочинів і розшуку злочинців;
- збір, обробка та узагальнення оперативної, оперативно-розшукової, оперативно-довідкової, аналітичної, статистичної, і контрольної інформації для оцінки ситуації та прийняття обґрунтованих оптимальних рішень на всіх рівнях діяльності ОВС;
- забезпечення динамічної та ефективної інформаційної взаємодії усіх галузевих служб ОВС України, інших правоохоронних органів та державних установ;
- забезпечення захисту інформації [1].

Вирішення завдань сучасного інформаційного забезпечення має бути досягнуто на основі впровадження єдиної політики інформаційного забезпечення, створення багатоцільових інформаційних підсистем діяльності ОВС, удосконалення організаційно-кадрового забезпечення інформаційних підрозділів, розбудови інформаційної мережі, створення умов для ефективного функціонування інформаційних обліків, забезпечення їх повноти, вірогідності, актуальності та безпеки, впровадження сучасних інформаційних технологій.

Досвід використання комп'ютерних інформаційних систем і технологій в правоохоронній сфері свідчить, що основними тенденціями їх розвитку та удосконалення є:

- удосконалення форм та методів керування системами інформаційного забезпечення;
- централізація та інтеграція комп'ютерних банків даних;
- впровадження новітніх комп'ютерних інформаційних технологій для ведення кримінологічних обліків;
- розбудова та широке використання ефективних та потужних комп'ютерних мереж;
- застосування спеціалізованих засобів захисту та безпеки інформації;
- налагодження ефективного взаємообміну кримінологічною інформацією на міждержавному рівні.

Концентрація зусиль на визначених напрямах забезпечила суттєве підвищення рівня боротьби зі злочинністю в розвинених державах світу.

Аналіз існуючої системи інформаційного забезпечення органів внутрішніх справ засвідчує необхідність реорганізації та оновлення. 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 [2]. 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.

Основною метою системи інформаційного забезпечення органів внутрішніх справ України визначено всебічну інформаційну підтримку практичної діяльності ОВС у боротьбі із злочинністю на основі комплексу організаційних, нормативно-правових, технічних, програмних та інших заходів.

---

1. Плішкін В.М. Теорія управління органами внутрішніх справ: Підручник / В.М. Плішкін. – К. : Національна академія внутрішніх справ України, 1999. – 694 с.
2. Інформаційні підсистеми ОВС України // [Електрон. ресурс]. – Режим доступу: http://www. naiau.kiev.ua/biblio/books/Kriminal inform/tema 3/htm.

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ АФІННИХ ПЕРЕТВОРЕННЯ У КРИПТОГРАФІЧНІЙ СИСТЕМІ ЛЕСТЕРА ХІЛЛА

Поберейко Богдан Петрович,
професор кафедри інформаційних технологій НЛТУ, д.т.н.
Грицюк Павло Юрійович,
магістр НЛТУ

Протягом багатьох століть криптографія, тобто наука про шифрування або «приховування» інформації від несанкціонованого використання, застосовувалася в основному для захисту повідомлень, якими обмінювалися державні чиновники або військові. Тому коло людей, які застосовували криптографію, було вельми обмежене, а самі методи цієї науки – секретні. Проте в останні десятиліття, коли людство вступило в стадію інформаційного суспільства, криптографічні методи захисту інформації почали використовуватися дуже широко, обслуговуючи, насамперед, потреби бізнесу [1, ст. 12]. Тому традиційно криптографія необхідна тільки для інформації, котра потребує захисту, тобто містить таємницю, чи має бути захищеною від зловмисника, секретною, конфіденційною. Класичними методами захисту інформації є Афінна системи підставлянь Цезаря і, як продовження, криптографічна системи Лестера Хілла, в яких чітко виявлена спільність числових методі афінних перетворень.

Математична модель. У системі шифрування Цезаря[1] [1, ст. 38] використовуються тільки адитивні властивості множини цілих чисел $\overline{Z}_m$ (m = 26 – кількість букв латинського алфавіту). Застосовуючи одночасно операції додавання та множення за модулем m над елементами множини цілих чисел $\overline{Z}_m$, можна отримати систему перетворень, яку називають афінною системою підставлянь Цезаря [1, ст. 45]. Математичні перетворення в цій монограмній системі підстановки мають такий вигляд:

[1] Ю́лій Це́зар (лат. Imperator Gaius Iulius Caesar (*13 липня 100 до н. е. – †15 березня 44 до н. е.) – давньоримський державний і політичний діяч, полководець, письменник. Діяльність Цезаря докорінно змінила культурний і політичний вигляд Західної Європи і залишила визначний слід в житті наступних поколінь європейців.

$$k = f(t) = (a \cdot t + b) \bmod m; \quad (1)$$

$$t = f^{-1}(k) = (a' \cdot k + b') \bmod m; \quad (2)$$

$$a' = a^{-1} \bmod m,\ b' = -a^{-1} \cdot b \bmod m,\ a^{-1} = x, \quad (3)$$

де: a, b – цілі числа, $0 \le a, b \le m$, НСД(a, m) = 1. У перетворенні (1), тобто шифруванні вхідного повідомлення, символ, який відповідає числу t, замінюють на символ k, що відповідає числовому значенню $(a \cdot t + b)$ за модулем m, внаслідок чого отримуємо зашифроване повідомлення. При зворотному перетворенні (2), тобто дешифруванні повідомлення, символ, який відповідає числу k, замінюють на символ t, що відповідає числовому значенню $(a' \cdot k + b')$ за модулем m. Щоб знайти значення x, необхідно розв'язати лінійне рівняння $a \cdot x + m \cdot y = 1$. Для цього застосовуємо алгоритм Евкліда, внаслідок чого знаходимо його корені, а також з формулою (3) виконуємо деякі розрахунки.

Спробуємо зашифрувати вхідне повідомлення «*Все йде, все минає, і краю немає*» при таких значеннях вхідних даних: m = 256 (кількість символів у таблиці ASCII), a = 19, b = 57. Результати його шифрування матимуть такий вигляд:

$\bar{\bar{T}}_{сим} =$

В	_	е	в	_	н	,	_	а	н	а
с	й	,	с	м	а	_	к	ю	е	є
е	д	_	е	и	є	і	р	_	м	.

$\bar{\bar{T}}_{кс} =$

194	95	229	226	95	237	44	95	224	237	224
241	233	44	241	236	224	95	234	254	229	186
229	228	95	229	232	186	179	240	95	236	46

$\bar{\bar{T}} = (a \cdot t + b)$

3743	1862	4408	4351	1862	4560	893	1862	4313	4560	4313
4636	4484	893	4636	4541	4313	1862	4503	4883	4408	3591
4408	4389	1862	4408	4465	3591	3458	4617	1862	4541	931

$\bar{\bar{K}} = \bar{\bar{T}} \bmod 256$

159	70	56	255	70	208	125	70	217	208	217
28	132	125	28	189	217	70	151	19	56	7
56	37	70	56	113	7	130	9	70	189	163

$\bar{\bar{K}}_{сим} =$

ц	F	8	я	F	Р	}	F	Щ	Р	Щ
	„	}		S	Щ	F	—		8	
8	%	F	8	q		,		F	S	J

ц8 F„% 8}F я8 FSq РЩ }F, F— ЩF Р8S Щ J

тобто, отримаємо на виході таке зашифроване повідомлення:
ц8F„%8}Fя8FSqPЩ}F,F— ЩFP8SЩ J

Для його дешифрування спочатку за розв'яжемо лінійне рівняння $19 \cdot x + 256 \cdot y = 1$, внаслідок чого отримаємо такі корені: $x = 27$, $y = -2$. За формулою (3) знаходимо: $a^{-1} = 27$, $a' = 27 \bmod 256 = 27$, $b' = -1539 \bmod 256 = 253$. Після цього, виконавши необхідні розрахунки за формулою (2), знову ж таки повернемося до вхідного повідомлення.

Перевага афінної системи підставлянь Цезаря над іншими методами простої заміни насамперед полягає у простоті числової реалізації. Особливо зручно виконувати усі дії шифрування та дешифрування у середовищі Microsoft Excel з використанням тільки стандартних текстових і математичних функцій. Другою перевагою є зручність управління ключами, тобто ключі шифрування та дешифрування подаються в компактній формі у вигляді пари чисел (a, b). Недоліки афінної системи аналогічні недолікам системи шифрування Цезаря, тому вона хоча і широко використовувалася раніше, проте сьогодні її застосовують переважно як ілюстративні приклади для висвітлення основних криптологічних положень різних систем шифрування.

Практична реалізація. Алгебричний метод, який узагальнює афінну систему підставлянь Цезаря, було сформульовано Лестером С. Хіллом[2] для визначення n-грам [2, ст. 83]. Подальше висвітлення методу шифрування та дешифрування передбачає початкові знання дій над матрицями. Множина цілих чисел $\overline{Z}_m$, для якої визначені операції додавання, віднімання та множення за модулем m, є прикладом кільця R, тобто алгебричної системи пар елементів. Математичні перетворення в цій системі мають такий вигляд:

$$\overline{\overline{K}} = F(\overline{\overline{T}}) = (\overline{\overline{A}} \times \overline{\overline{T}} + \overline{B}) \bmod m; \quad (4)$$

$$\overline{\overline{T}} = F^{-1}(\overline{\overline{K}}) = (\overline{\overline{A}}' \times \overline{\overline{K}} + \overline{B}') \bmod m; \quad (5)$$

$$a = \det(\overline{\overline{A}}) \bmod m,\ a' = \det^{-1}(\overline{\overline{A}}) \bmod m,\ \det^{-1}(\overline{\overline{A}}) = x, \quad (6)$$

$$\overline{\overline{A}}' = \left(\overline{\overline{A}}^{-1} \times \det(\overline{\overline{A}}) \times a'\right) \bmod m, \overline{B}' = -\overline{\overline{A}}' \times \overline{B} \bmod m, \quad (7)$$

[2] Шифр Лестера Хілла (Lester Hill) – поліграмний шифр підстановки, який базується на лінійній алгебрі. Лестер С. Хілл винайшов цей шифр в 1929 р., і це був перший шифр, який давав змогу на практиці оперувати більш ніж з трьома символами разом.

де: $\bar{\bar{A}} = \{\bar{A}_i = \{a_{ij}, j = \overline{1,n}\}, i = \overline{1,n}\}$ – матриця шифрування; $\bar{B} = \{b_i, i = \overline{1,n}\}$ – стовпець коригування; a – ціле число, НСД(a, m) = 1; $\bar{\bar{T}} = \{\bar{T}_j = \{t_{ij}, i = \overline{1,n}\}, j = \overline{1,l}\}$ – матриця, елементами якої є числові коди символів вхідного повідомлення; $\bar{\bar{K}} = \{\bar{K}_j = \{t_{ij}, i = \overline{1,n}\}, j = \overline{1,l}\}$ – матриця, елементами якої є числові коди символів зашифрованого повідомлення. У перетворенні (4), тобто шифруванні вхідного повідомлення, символи n-грами, яким відповідають числа стовпця матриці $\bar{T}_j$, замінюють на символи n-грами, що відповідають числовим значенням $(\bar{A}_i \times \bar{T}_j + b_i)$ за модулем m, внаслідок чого отримуємо зашифроване повідомлення. При зворотному перетворенні (5), тобто дешифруванні зашифрованого повідомлення, символи n-грами, яким відповідають числа стовпця матриці $\bar{K}_j$, замінюють на символи n-грами, що відповідають числовим значенням $(\bar{A}'_i \times \bar{K}_j + b'_i)$ за модулем m. Розв'язавши лінійне рівняння $a \cdot x + m \cdot y = 1$ за допомогою алгоритму Евкліда, знаходимо його корені, а значить і значення a'.

Спробуємо зашифрувати вхідне повідомлення «*Все йде, все минає, і краю немає*» (див. вище) при таких значеннях вхідних даних: $m = 256$,

$$\bar{\bar{A}} = \begin{Vmatrix} 32 & 42 & 23 \\ 27 & 59 & 51 \\ 31 & 34 & 19 \end{Vmatrix} \text{ і } \bar{B} = \begin{vmatrix} 32 \\ 26 \\ 49 \end{vmatrix}.$$

При цьому: det(A) = 4287,0; a = det(A) mod 256 = 191,0; НСД(191; 256) = 1,0. Результати шифрування вхідного повідомлення $\bar{\bar{T}}_{сим}$ матимуть такий вигляд:

$$\bar{\bar{P}} = \bar{\bar{T}}_{кс} \times \bar{\bar{A}}$$

21597	18070	11361	22621	18288	21270	9515	18388	20021	22630	16038
31136	27940	13624	32000	28321	29101	15922	28611	25879	31946	19368
18559	15199	10400	19551	15377	18497	7995	15461	17385	19617	14142

$$\bar{\bar{K}} = (\bar{\bar{P}} + \bar{B}) \bmod 256$$

125	182	129	125	144	54	75	244	85	134	198
186	62	82	26	187	199	76	221	49	228	194
176	144	209	144	66	114	108	150	26	210	111

$\bar{\bar{K}}_{сим} =$

}	¶	Ґ	}	ђ	6	K	ф	U	†	Ж
є	>	R		«	З	L	Э	l	д	В
°	ђ	C	ђ	В	r	l	–		Т	о

}є° ¶>ђ ҐRC }ђ ђ»В 63r KLl фЭ– U1 †дТ ЖВо

тобто, отримаємо на виході таке зашифроване повідомлення:

}є°¶>ђҐRC}ђђ»В63rKLlфЭ–U1†дТЖВо

Для дешифрування спочатку розв'яжемо лінійне рівняння $191 \cdot x + 256 \cdot y = 1$, тобто отримаємо: $x = 63$, $y = -47$. За формулою (6) знаходимо: $\det^{-1}(\bar{\bar{A}}) = 63$, $a' = 63 \bmod 256 = 63$, а за формулою (7) знаходимо:

$$\bar{\bar{A}}' = \begin{Vmatrix} 37 & 16 & 47 \\ 212 & 41 & 51 \\ 207 & 170 & 142 \end{Vmatrix} \text{ і } \bar{B}' = \begin{vmatrix} 193 \\ 147 \\ 174 \end{vmatrix}.$$

Після цього, виконавши необхідні розрахунки за формулами (5), знову ж таки повернемося до вхідного повідомлення.

У розглянутому прикладі матриця шифрування мала розмір 3×3 і шифрувалися 3-грами (парами) букв. Проте у навчальному процесі курсанти і студенти використовують матриці розміром 5×5. Хоча буква *е* може бути зашифрована по-різному в різних парах початкового повідомлення, однак одна і та ж пара, наприклад *Все*, шифруватиметься завжди однаково впродовж всього вхідного повідомлення. Тому система шифрування Лестера Хілла є одноалфавітною в широкому сенсі цього слова.

Висновки. Наведено математичне формулювання деяких класичних методів захисту інформації – афінної системи підстановлянь Цезаря і криптографічної систем Хілла, в яких простежено спільність числових методі афінних перетворень. Розглянуті методи захисту інформації реалізовано у середовищі Microsoft Excel з використанням тільки текстових і математичних функцій, що дає змогу студентам покращити свій рівень освіченості як з даної області знань, так і в удосконаленні майстерності програмування.

1. Кузнецов Г.В. Математичні основи криптографії : навч. посібн. / Г.В. Кузнецов, В.В. Фомичов, С.О. Сушко, Л.Я. Фомичова. – Дніпропетровськ : Вид-во Нац. гірн. ун-ту, 2004. – 391 с.
2. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии : учебн. пособ. / А.В. Черемушкин. – М. : Изд-во МЦНМО, 2002. – 104 с.

РОЗРОБЛЕННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ВІДСЛІДКОВУВАННЯ РЕЙТИНГУ ПОШУКОВИХ СИСТЕМ СЕРВЕРІВ З ВИКОРИСТАННЯМ CASE ЗАСОБІВ

Поберейко Богдан Петрович,
професор кафедри інформаційних технологій НЛТУ, д.т.н.
Олійник Андрій Ігорович,
магістр НЛТУ

Доступ до глобальної мережі Інтернет став невід'ємним атрибутом високотехнологічного суспільства, широкий доступ до інформаційних ресурсів є складовою сучасного культурно-освітнього середовища. Всесвітня мережа надає нові можливості для пошуку інформації та спілкування, але поряд з визнаними перевагами, Інтернет приносить нам нові ризики, ставлячи на порядку денному питання онлайнової безпеки. Одним із основних питань в сучасному інформаційному світі є захист Інтернет ресурсів від несанкціонованого доступу або збою в їх роботі. Пріоритетним засобом захисту являється обмеження доступу до ресурсу шляхом переміщення IP адреси в чорний список (список IP – адрес яким заборонено доступ до конкретного ресурса.).

Метою роботи є створення інформаційної системи відслідковування рейтингу пошукових систем серверів, яка допоможе визначати рівень довіри до IP-адрес користувачів а також перевірити їх на предмет наявності в білому або чорному списку.

Аналіз основної загрози обмеження доступу до Інтернет ресурсу. DDoS атака – це атака на обчислювальну систему з метою вивести її ресурси з ладу, зробити недоступними для користувачів. DDoS актаки організовуються за допомогою (botnet) – мережі інфікованих хостів (ботів). Схематично атака виглядає приблизно так: на вибрану жертвою інформаційну систему надходить величезна кількість помилкових запитів з сотень або тисяч хостів з різних кінців світу. В результаті цього сервер витрачає всі свої ресурси на обслуговування цих запитів і стає практично недоступним для звичайних користувачів.

Коротко суть мережевої атаки можна описати так: через керуючу консоль зловмисник зв'язується з головними серверами

ботнету, з якого безпосередньо відправляються команди інфікованим хостам, що формують сотні запитів різних типів, якими атакується вузол-мішень.

Архітектура кластера DDoS наведена на рис.1

Рис. 1. Архітектура кластера DDoS

Огляд технологій для реалізації проекту. В даному проекті використовуються наступні технології:

Java – об'єктно орієнтовна мова програмування, випущенна компанією Sun Microsystems у 1995 році як основний компонент платформи Java. Вона володіє наступнимим перевагами:

- незалежність від архітектури
- об'єктно орієнтованість мови
- розподіленість

Spring MVC – програмний фреймоворк з відкритим кодом та контейнер з підтримкою інверсії управління. Використовується для побудови сучасних web –додатків на базі платформи Java EE.

Hibernate – засіб відобрадення між об'єктами та реляційними структурами, який надає легкий для використання фреймоворк для відображення між об'єктно-орієнтованою моделлю даних і традиційною реляційною БД.

Висновок. Розроблений сервіс надасть змогу звичайним користувачам моніторити хибні блокування їх доступу до певних ресурсів. А в свою чергу Інтернет ресурси зможуть отримати об'єктивний аналіз рейтингу довіри до Ір-адрес з метою покращення своїх послуг кінцевим користувачам.

1. Bruce Eckel, "Thinking in Java" (4th Edition)
2. Кларенс Хо, Роб Харроп, "Spring 3 для профессионалоа"
3. "Hamessing Hibernate" by James Elliott, Timothy M.
4. "Java Persistence with Hibernate" by Christian Bawer, Gavin King

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ У ПРОТИДІЇ НАРКОТИЗМУ СЕРЕД НЕПОВНОЛІТНІХ

Мельник Ольга Миколаївна,
старший науковий співробітник наукової лабораторії ЛьвДУВС, к.ю.н.
Фещин Г.М.,
магістр ЛьвДУВС

Ст. 2 Закону України «Про оперативно-розшукову діяльність» визначає оперативно-розшукову діяльність як систему гласних і негласних, пошукових, розвідувальних і контррозвідувальних заходів, які здійснюються із застосування оперативних та оперативно-технічних засобів [1]. Як влучно зауважив В.А. Лукашов, оперативні підрозділи, здійснюючи заходи, застосовують оперативно-розшукові сили, засоби і методи, що стає їх класифікаційною ознакою [2, с. 31].

Результативність діяльності оперативних підрозділів залежить не тільки від особистих ділових якостей і оперативно-технічної оснащеності співробітників, але і від ефективності системи інформаційно-аналітичного забезпечення.

Інформаційно-аналітичне забезпечення, на підставі Концепції національної програми інформатизації України [3], передбачає вдосконалення системи статистичного обліку і звітності в країні, інформування про стан, динаміку, структуру правопорушень, критеріїв оцінки ефективності діяльності правоохоронних органів,

збору необхідної і достатньої інформації для ефективної діяльності суб'єктів профілактики і ухвалення відповідних управлінських рішень щодо запобігання цим правопорушенням.

Основною метою системи інформаційно-аналітичного забезпечення діяльності у боротьбі з наркотизмом серед неповнолітніх є всебічна інформаційна підтримка практичної діяльності підрозділів МВС України на основі комплексу організаційних, нормативно-правових, технічних, програмних та інших заходів [4].

Основними завданнями функціонування системи інформаційно-аналітичного забезпечення у протидії наркотизму серед неповнолітніх є:

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

Актуальність проблеми інформаційного забезпечення оперативно-розшукової діяльності МВС, ГУВС, УВС України, спрямованої на боротьбу із правопорушеннями у сфері незаконного обігу наркотичних засобів і психотропних речовин, характеризуються такими чинниками:

- комплексним характером процесу боротьби з такими правопорушеннями, в якому беруть участь різні служби органів внутрішніх справ, інші правоохоронні органи, а також державні і суспільні організації;
- широкими просторовими масштабами діяльності злочинних структур наркодилерів, мобільністю, технічною оснащеністю;
- необхідністю здійснення заходів щодо боротьби із протиправними структурами на території різних районів, регіонів, держав;

- жорсткими тимчасовими межами здійснення слідчих (розшукових) дій та негласних слідчих (розшукових) дій, особливо на первинному етапі;
- особливостями оперативно-розшукової характеристики таких кримінальних правопорушень і протиправних структур, що їх здійснюють;
- сучасним станом кримінальних правопорушень у сфері незаконного обігу наркотичних засобів і психотропних речовин і організації оперативно-розшукової діяльності підрозділами МВС України щодо протидії наркотизму серед неповнолітніх.

Правильна організація інформаційно-аналітичного забезпечення управління діяльністю ОВС, що охоплює систематичне накопичення достовірної інформації, всебічно характеризує оперативну обстановку, її своєчасний і якісний аналіз і прогноз.

Основними інформаційними джерелами, що застосовуються у процесі інформаційно-аналітичної діяльності, є:

1. Банки даних оперативно-розшукових обліків, що формуються інформаційно-аналітичними підрозділами кримінальної міліції.
2. Інформаційні масиви оперативно-довідкових, довідкових і статистичних обліків.
3. Фонди експертно-криміналістичних обліків.
4. Інформаційні банки даних галузевих служб МВС України.

Для досягнення оптимального варіанту інформаційного забезпечення своєї діяльності співробітники підрозділів у боротьбі з незаконним обігом наркотичних засобів і психотропних речовин МВС, ГУВС, УВС України повинні забезпечити накопичення інформації з використанням такої системи обліків:

1. Єдина спеціалізована територіально-розподільна автоматизована система «Наркобізнес», яка діє на всіх рівнях у центральному апараті України.
2. Криміналістичні обліки підроблених медичних рецептів на отримання наркотичних і сильнодіючих лікарських засобів і взірців почерку осіб, що здійснюють їх підробку.
3. Фотоальбоми осіб, що здійснюють підробку рецептів, інших осіб, що скоюють правопорушення, пов’язані з незаконним обігом наркотичних засобів і психотропних речовин, які ведуться в спеціалізованих підрозділах МВС, ГУВС, УВС України.

Для інформаційного забезпечення ОРД підрозділів по боротьбі з незаконним обігом наркотичних засобів і психотропних речовин МВС, ГУВС, УВС України також застосовуються:

1. Оперативно-довідкові обліки:

- щодо осіб, які стосуються протиправних фактів у минулому (поіменний облік засуджених, дактилоскопічний облік засуджених, облік іноземних громадян, що вчинили правопорушення);
- розшукові обліки;
- відомості про осіб, оголошених у державний розшук.

2. Криміналістичний облік осіб із позиції їх фізіологічних, соціально-психологічних і кримінальних портретів [5, с. 212].

На виконання Указу Президента України від 20 жовтня 2005 року № 1497 «Про першочергові завдання щодо впровадження новітніх інформаційних технологій» [6] та з метою подальшого вдосконалення оперативно-службової діяльності ОВС із використанням сучасних інформаційних технологій наказом МВС від 07.06.2006 р. № 571 затверджено Програму створення Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України [7]. Метою створення цієї системи є вдосконалення оперативно-службової діяльності органів внутрішніх справ із застосуванням сучасних інформаційних технологій, комп'ютерного та телекомунікаційного обладнання.

З метою вдосконалення інформаційно-аналітичного забезпечення оперативно-розшукової діяльності підрозділів МВС України у боротьбі з незаконним обігом наркотичних засобів, психотропних речовин необхідно створити і впровадити спеціалізовану інформаційну систему, яка повинна відповідати таким вимогам:

- функціонувати у посиленому режимі користування, об'єднуючи зусилля всіх співробітників оперативних підрозділів МВС, ГУВС, УВС України;
- здійснювати швидку обробку великих масивів даних, миттєво відстежуючи зміни, що вносяться декількома користувачами;
- обробляти будь-яку, навіть неструктуровану інформацію, автоматично її впорядкувавши;

- бути масштабною і легко керованою, надійною і невибагливою, не потребувати регулярних багатогодинних індексацій, складного адміністрування;
- відповідати жорстким вимогам безпеки інформації, органічно підтримуючи різні рівні доступу до даних для різних користувачів.

А також пропонуємо під час входу в таку інформаційно-аналітичну систему мати змогу миттєво виявляти дані, що були змінені і внесені користувачами, які мають доступ до цієї системи.

Отже, інформаційно-аналітичне забезпечення щодо протидії наркотизму серед неповнолітніх слід розуміти як порядок отримання оперативними підрозділами необхідної інформації, що характеризує оперативну обстановку на певній території чи об'єкті, має безпосереднє або потенційне значення для вирішення стратегічних, тактичних і організаційних завдань ОРД і містить відомості, отримані з різноманітних джерел, із застосуванням гласних і негласних оперативно-пошукових та аналітичних заходів.

1. Про оперативно-розшукову діяльність: Закон України від 18.02. 1992 р. // Відомості Верховної Ради України. – 1992. – № 22. – С. 303.
2. Лукашов В. А. Введение в курс. Оперативно-розыскная деятельность органов внутренних дел / В. А. Лукашов. – К., 1976. – 128 с.
3. Про Концепцію Національної програми інформатизації: Закон України від 04.02. 1998 р. // Відомості Верховної Ради України. – 1998. – № 27-28. – С. 182.
4. Орлов Ю. Ю. Застосування оперативної техніки в оперативно-розшуковій діяльності міліції (теорія і практика): монографія / Ю. Ю. Орлов. – К.: Київський національний університет внутрішніх справ, 2007. – 559 с.
5. Рибалко Я. В. Експертні обліки як галузь криміналістичної техніки: етапи розвитку, завдання і зміст / Я. В. Рибалко // Проблеми правознавства та правоохоронної діяльності: збірник наукових статей. – Донецьк: Донецький інститут внутрішніх справ при Луганському державному університеті, 2001. – № 1. – С. 212–218.
6. Про першочергові завдання щодо впровадження новітніх інформаційних технологій: Указ Президента України від 20 жовтня 2005 року № 1497 [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/ documents/3398.html

7. Про затвердження Програми створення Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України: наказ МВС від 17.06.2006 р. № 571. – К.: МВС України, 2006. – 14 с.

ПРОЕКТУВАННЯ ІНТЕРНЕТ ДОДАТКУ З ВИКОРИСТАННЯМ ПЛАТФОРМИ JavaFX

Карашецький Володимир Петрович,
доцент кафедри інформаційних технологій НЛТУ, к.т.н
Мосолов Артем Юрійович,
магістр НЛТУ

Швидкий розвиток мов програмування призвів до складного вибору платформи написання якісних, безпечних, швидких, портативних та інтерактивних програм. Програма повинна забезпечувати швидке реагування і видавання результату на дії користувача, не втручатись в роботу операційної системи без дозволу, забезпечувати портативність роботи на сучасних пристроях (телефон, планшет, комп'ютер), та мати зручний графічний інтерфейс користувача.

З вище описаної актуальності дану проблему вирішує платформа JavaFX та найпопулярніша мова програмування Java.

Метою роботи є створення швидкого, інтерактивного, графічного, насиченого інтернет додатку (RIA) для демонстрації різних можливостей платформи JavaFX рис 1.

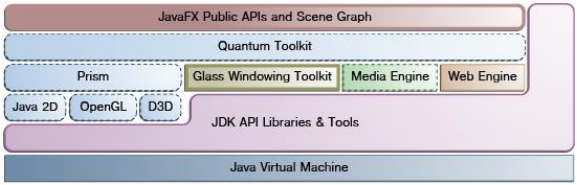


Рис. 1 Архітектура платформи

Спосіб реалізації. При написанні програми буде використано багато різноманітних бібліотек, фреймворків, інструментів, середовищ та методологій. Для написання програми буде використано безкоштовне середовище програмування Eclipse із підтримкою плагіна для платформи JavaFX. Для розділення програми на різні частини, для зручного процесу написання буде використано

паттерн MVC (Модель, Представлення, Контролер), де модель, це дані, котрі будуть прийматись або передаватись, представлення – візуалізація клієнтської частини з графічним інтерфейсом, контроллер – компонент, відповідаючий за бізнес логіку. Доступ до бази даних буде забезпечений з допомогою ORM фреймворка, котрий динамічно оперує об'єктами та зберігає данні в базі даних, використовуючи JDBC та SQL на нижньому рівні. Для місце збереження даних буде використано реляційну базу даних MySQL. Для збірки проекта та завантаження залежностей, плагінів буде використано Maven.

Висновки. При написанні програми було реалізовано інтерфейс для зручної взаємодії користувача, забезпечив безпеку роботи як користувача, так і програми від прямого доступу до операційної системи, швидке реагування на дії для отримання результату, стабільність роботи програми та продемонстрував можливості вибраної платформи.

1. Richard Bair «February Open Source Update». Oracle Corporation. 2013. – 837 p.
2. Richard Bair (2012-12-03). «Porting JavaFX». NotecOld 2011. – 411p.
3. Tomas Brandalik «Survey: JavaFX on tablets and mobile devices». 2012. – 531 p.
4. Pavel Safrata «More of JavaFX open-sourced». Oracle Corporation. 2013. – 321 p.
5. JavaFX FAQ. Oracle Corporation. 2012. tutorial

ІНФОРМАЦІЙНІ СИСТЕМИ В ОВС ТА ЗАХИСТ ІНФОРМАЦІЇ

Бездух Ірина Ярославівна,
магістр ЛьвДУВС
Бовшик Христина Василівна,
магістр ЛьвДУВС
Живко Павло Богданович,
магістр ЛьвДУВС

Досліджуючи сутність поняття «інформація» в соціальній сфері, можемо стверджувати, що за своїм значенням воно

найбільш співзвучне з поняттями «дані», «відомості». Спільними для них є такі характеристики, як вірогідність, точність, повнота, первинність, вторинність, корисність, старіння тощо. З впровадженням інформаційних систем та комп'ютеризацією діловодства в ОВС, поруч з поняттям «інформація» вживається поняття «комп'ютерна інформація». Комп'ютерна інформація – це не самі дані, а форма їх представлення у машинному вигляді, сукупність символів, яка зафіксована у пам'яті комп'ютера, або на машинному носії [1]. Враховуючи специфіку діяльності ОВС, слід пам'ятати, що за певних обставин й фізичні поля можуть виступати носіями інформації, зокрема при розгляді справ.

Для систематизації та обробки інформації використовують класифікацію інформації за різними ознаками. За джерелами отримання інформації її поділяють на первинну і вторинну, за формою фіксації – на документальну і не документальну; за способом передачі – на ручну та механізовану; за способом обробки – на вихідну та оброблену [2, с. 32-38], за повнотою – на повну та часткову; за ступенем доступу – загальну, службову (ДСК), таємну та цілком таємну тощо.

Беззаперечним є місце інформації в процесі управління, адже без неї неможливо сформулювати мету управління, дослідити внутрішнє та зовнішнє середовище, оцінити ситуацію, визначити проблеми, поставити завдання, спрогнозувати розвиток подій, сформувати управлінські рішення, довести їх до колективу і проконтролювати виконання [3, с. 780]. Сфера охорони правопорядку, охоронна діяльність дотичні до формування системи економічної безпеки кожного окремо взятого підприємства. Підприємство, в залежності від обсягів виробництва, фінансового стану та кількості персоналу може мати власну службу безпеки, користуватися послугами охоронних структур ОВС чи приватних фірм, але в кожному випадку буде взаємодіяти з правоохоронними органами, здійснювати обмін інформацією.

Сфера діяльності ОВС щодо забезпечення громадського порядку є надзвичайно динамічною, комплексною і потребує постійного вдосконалення та знаходиться у прямопорційній залежності від інформаційного забезпечення. В правоохоронних структурах, крім інформаційного забезпечення, використовують

такі терміни, як інформаційна робота, інформаційна безпека, захист інформації. Спільною властивістю цих понять є необхідність в організуванні (організації). Так, організація інформаційної роботи – це вплив на дану роботу з метою її оптимізації, тобто одержання найбільш ефективного результату при найменших зусиллях і витратах. Інформаційна робота плюс її організація складають поняття інформаційного забезпечення. Інформаційна робота – складова частина інформаційної системи, який притаманні наступні компоненти: люди (персонал), інформація, технічні засоби, методи, процедури збору та перетворення інформації [4, с. 343].

Інформаційне забезпечення ОВС України слугує всебічній інформаційній підтримці основних напрямів діяльності органів внутрішніх справ, зокрема у боротьбі зі злочинністю, в тому числі й економічною. Основою діяльності підрозділів ОВС є комплекс організаційних, нормативно-правових, фінансових, технічних, програмних та інших заходів, які залежать від повноти та достовірності інформації. Розрізняють загальновідомчі та галузеві інформаційні підсистеми, які складають основу системи інформаційного забезпечення органів внутрішніх справ. Система інформаційного забезпечення ОВС сформована за такими принципами: функціонального призначення; нормативно-правової забезпеченості; фактичності даних; доцільності впровадження та експлуатації; нарощення та розвитку [3, с. 120].

Інформаційні підсистеми як складові частини системи інформаційного забезпечення, призначені для збирання, накопичення, зберігання та обробки інформації певних напрямків обліків й орієнтовані на використання в діяльності багатьох служб, мають загальновідомчий характер і відносяться до загальновідомчих інформаційних підсистем.

Інформаційні підсистеми можуть належати до певного рівня та визначатися принципами територіальності, специфіки використання та обсягом інформації, яка обробляється. Кожен з рівнів має свої особливості, зокрема: (1) перший рівень – центральний, інтегрує інформаційні підсистеми ОВС загальновідомчого значення та галузевих служб МВС України; (2) другий рівень – регіональний, охоплює інформаційні обліки, які є складовими

загальновідомчих інформаційних підсистем, і використовуються службами ГУМВС, УМВС, УМВСТ; (3) третій рівень – територіальний, охоплює інформаційні обліки, що є складовими загальновідомчих інформаційних підсистем і які використовуються в міських, районних та лінійних ОВС, спеціалізованих підрозділах міліції [3].

Як зазначає М.Ковалів, на територіальному рівні управління в міських та районних і лінійних органах формуються банки даних оперативно-розшукового, оперативно-довідкового, адміністративного та статистичного призначення [5, с. 126-134].

Інформаційна система (ІС) – це організований людиною комплекс збирання, зберігання (накопичення), оброблення, оновлення, пошуку, відображення та видання інформації, яка потрібна для ефективного управління.

Система інформації – це сукупність інформаційних систем органу управління.

Компоненти інформаційної системи: інформація (відомості); персонал; організаційні і технічні засоби; методи та процедури роботи з інформацією; зв'язки (джерело, канал, здобувач); носії інформації (паперові, електронні, ін.).

Є дуже багато критеріїв для класифікації інформаційних систем. Розглянемо лише два з них:

1) за особливостями обробки інформації інформаційна система розподіляються на; розрахункові; аналітико-статистичні; інформаційно-пошукові;

2) за класом розв'язуваних завдань: облікові (довідкові, статистичні, слідкуючи); аналітичні (діагностичні, прогнозуючі, дорадчі); вирішуючи (плануючі, керуючі).

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.

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 [6, с. 106-108].

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.

Система інформаційної безпеки має бути спрямована на запобігання втраті інформації, її перекручення, несанкціонованого доступу та незаконного її використання під час проектування, впровадження та експлуатації інформаційних підсистем.

Визначальним в безпеці та захисті системи інформаційного забезпечення є адміністрування інформаційних підсистем, яке запроваджується та контролюється інформаційною службою МВС України.

Безпека інформації забезпечується на технологічних етапах збирання, накопичення, обробки та передачі інформації. Відповідальність за безпеку інформації на відповідних технологічних етапах всіх рівнів інформаційного забезпечення несуть підрозділи, що їх здійснюють.

Організація загальної безпеки інформаційного забезпечення запроваджується та контролюється Центром технічного захисту інформації МВС України, який разом з інформаційною службою визначає та впроваджує відповідні засоби, захисту [7, с. 280].

З метою виконання функцій щодо захисту інформації в інформаційних службах створюються відповідні підрозділи або призначаються відповідальні службовці на всіх рівнях системи інформаційної о забезпечення, які у своїй роботі використовують відповідні накази та інструкції.

Система безпеки та захисту інформації має закладатись ще на етапі розробки технічного завдання на проектування інформаційних підсистем. Всі проекти, що розробляються, в обов'язковому порядку повинні мати розділ «Захист інформації», який, у свою чергу, розробляється відповідно до «Тимчасових рекомендацій щодо розроблення розділу із захисту інформації в технічному завданні на створення автоматизованої системи» [8, с. 554].

Отже, кожна інформаційна технологія орієнтована на обробку інформації певних видів: даних (системи програмування й

алгоритмічні мови, системи управління базами даних – СУБД, електронні таблиці); текстової інформації (текстові процесори і гіпертекстові системи); статичної графіки (графічні редактори); знань (експертні системи); динамічної графіки, анімації, відеозображення, звуку (інструментарій створення мультимедійних додатків, що охоплює засоби анімації й управління відеозображенням та звуком). Інформаційні технології відрізняються за типом інформації, яка обробляється, але можуть і об'єднуватися, утворювати інтегровані системи, що мають різні технології.

Реалізація загроз несанкціонованого використання інформації наносить зараз набагато більший збиток, чим, наприклад, «випадкові» пожежі в приміщеннях або фізичний вплив на співробітників. Однак витрати на побудову системи захисту інформації ще поки незрівнянно малі у порівнянні з витратами на захист від грабіжників або на протипожежний захист.

Оцінка можливого економічного збитку у випадку витоку даних є основою формування переліку даних, що складають конфіденційну інформацію установи.

Модель впровадження комплексної системи захисту інформації складається з

- формування політики інформаційної безпеки;
- вибору основних рішень по забезпеченню захисту інформації;
- впровадження обраних засобів та заходів захисту.

На заключному етапі варто провести аналіз функціонування системи захисту інформації, перевірку виконання заходів захисту інформації, контроль ефективності захисту, підготувати і видати вихідні дані для керування системою захисту інформації.

1. Про інформацію: Закон України від 02 жовтня 1992р. № 48, ст.651, станом на 06 квітня 2000 р. № 27, ст. 213.
2. Бабаскін В.В., Жалгунова С.А. Проблемні питання інформаційного забезпечення діяльності ОВС // Науковий вісник ЮА МВС. – 2005. – № 3. – С.32-38.
3. Бандурка О.М. Управління в органах внутрішніх справ України: Підручник. – Харків, 1998. –780 с.
4. Державне управління: Навч. посіб./Мельник А.Ф., Оболенський О.Ю., Васіна А.Ю., Гордієнко Л.Ю.; За ред. А.Ф. Мельник. – К.: Знання-Прес, 2003. – 343 с.

5. Ковалів М.В. Інформаційно-аналітична робота в ОВС // Проблеми інформаційного забезпечення діяльності практичних підрозділів ОВС та впровадження інформаційних технологій в навчальний процес. – Львів, 2004. – С. 126-134.
6. Леженіна О.І. Аналіз та напрями розвитку інформаційного забезпечення міжнародної правоохоронної діяльності ОВС України: організаційно-правовий аспект // Право і безпека. – К., 2002. – №4. – С. 106-108.
7. Навроцька Н.Г. Правова статистика: Навчальний посібник. – К.: Знання, 2007. – 280 с.
8. Пєтков С.В. Ефективний менеджмент в органах внутрішніх справ. – Сімферополь: Таврія, 2004. – 564 с.

АЛГОРИТМІЗАЦІЯ ДІЙ СЛІДЧОГО – МЕТОДОЛОГІЧНА ОСНОВА УСПІШНОГО РОЗКРИТТЯ ЗЛОЧИНУ

Вишня Володимир Борисович,
професор кафедри інформатики та інформаційних технологій в діяльності ОВС ДДУВС, д.т.н., професор
Вишня Олег Володимирович,
доцент кафедри кримінально-правових дисциплін ДДУВС, к.ю.н., доцент
Прокопов Сергій Олександрович,
старший викладач кафедри інформатики та інформаційних технологій в діяльності ОВС ДДУВС

Для ефективного розкриття кримінальних злочинів доцільно корис-туватися типовими алгоритмами їх розслідування.

Методику створення алгоритму розкриття типового злочину розглянемо на прикладі побутового вбивства. Для цього спочатку визначимо обставини, що визначають особливості такого злочину.

В першу чергу це особлива передісторія злочину:

- про проблеми кримінального характеру у родині правоохоронним органам вже було відомо із попередніх скарг жертви злочину;
- агресор, відчуваючи безкарність, становився ще жорсткішим у поводженні зі своїми жертвами;

- приймаючи до уваги «родинний» характер конфлікту, правоохоронні органи, як і раніше, не реагували на повідомлення, традиційно припускаючи наступ тяжких наслідків;
- конфлікт досяг своєї кульмінації, наслідком чого наступила смерть жертви побутового насилля або самого агресора (необхідна оборона);
- малозначущість приводу останнього (рішучого) конфлікту може ввести в оман, якщо не знати усього попереднього поводження сторін;
- за результатами події може бути дана невірна юридична кваліфікація і до кримінальної відповідальності притягнена невинна людина.

Далі, це простота, яка вводить в оману. На місці пригоди знаходяться усі учасники злочину та речові докази: особа, що скоїла вбивство, і не відхрещуючись від цього; свідки, які, в принципі, підтверджують це; труп; знаряддя злочину; сліди різного виду.

У результаті, слідчий попадає у своєрідну психологічну западню – йому усе виглядає зрозумілим і доведеним свідченнями. Тому він обмежується лише допитами, не звертаючи уваги на особливості місця пригоди. Не приймається до уваги схема (криміналістичний алгоритм) розслідування даного виду злочину. Не враховується, що підозрюємий і свідки (його близькі родичі) з часом можуть по різним причинам кардинально змінювати свої свідчення.

Для прикладу розглянемо фабулу діла, яка виглядає наступним чином. О десятої години 22 лютого поточного року до райвідділу подзвонила громадянка О., яка сповістила, що в її домі сталося вбивство. З її слів, вбитий є її громадянським чоловіком Р., до якого зранку прийшов один з його численних знайомих, громадянин Б. Удвох вони стали розпивати горілку, а її послали до магазину за їжею та пивом. Вона була відсутня хвилин сорок, а коли повернулася, знайшла свого чоловіка, що лежав на кухні у крові. На голові у нього була велика рана.

Для виїзду на місце події збирається оперативна слідча група. Основні завдання виїзду на місце події виглядають наступним чином:

1. Оглянути місце події і труп.
2. Якщо буде можливим, організувати переслідування злочинця по «гарячих» слідах.
3. Встановити можливих свідків злочину (не вважаючи громадянку О.) і опитати їх.

Названі задачі, у свою чергу, визначають оптимальний склад виїзної слідчої групи, зокрема:

1. Слідчий.
2. Технік-криміналіст.
3. Судово-медичний експерт.
4. Дільничний інспектор.
5. Інспектор карного розшуку.
6. Кінолог із собакою.

Прибувши на місце злочину слідча оперативна група побачила будинок (рис. 1) та кімнату (рис. 2) де було скоєно вбивство.

Задача слідчого відразу по прибуттю на місце події полягає у необхідності:

1. Оцінити особливості місця події
- упевнитися, що нікому не потрібна медична допомога;
- визначити границі місця події;
- поставити задачу дільничному, інспектору карного розшуку і кінологу щодо здійснення по гарячих слідах розшук особи, яка сховалася.

Подальша робота слідчого на місці події.

2. Організувати огляд місця події в статиці
- організувати судову фотозйомку місця події (і стежити за тим, чи вірно вона здійснюється);
- визначити порядок (послідовність) огляду;
- разом із судово-медичним експертом приступити до зовнішнього огляду трупа;
- намалювати чорнову схему місця події, у яку пізніше внести результати вимірів.

3. Здійснити динамічний огляд місця події:
- разом з експертом-медиком зробити повний огляд трупа відповідно до рекомендацій судової медицини;
- оглянути кожний об'єкт на місці події (предмет, документ, речовину), застосовуючи при цьому засоби криміналістичної техніки;

- вилучити й упакувати об'єкти, що можуть мати значення в справі.

4. Допитати свідка О. надавши наступні питання:

1) З якого часу вона мешкала з громадянином Р.?
2) Як може його характеризувати?
3) Де працював Р., якими були доходи родини й інші матеріальні обставини сімейного життя?
4) Чи були між ними конфлікти, як часто, по яких приводах, у чому виражалися?
5) Коло друзів Р., усі їхні дані?
6) З якого часу Р. був у контакті з Б., які між ними були відносини?
7) Як може охарактеризувати Б., що відомо про його місце проживання, види діяльності, сімейному і матеріальному становищах?
8) Які конфлікти і з яких причин виникали між Р. і Б. у минулому?
9) При яких обставинах, де і коли зустрілися Р. і Б. 22 лютого?
10) Як проходила їхня зустріч, що могло сприяти конфлікту?
11) Де вона була під час конфлікту, якщо була там же, то що бачила і чула – максимально деталізовано?
12) Якщо не була на місці, то де і хто може підтвердити це?
13) О котрій годині повернулася додому?
14) У якім положенні були вхідні двері?
15) У якому стані вона знайшла Р.?
16) У якім положенні він був (де й у якій позі лежав)?
17) Які були в нього видимі тілесні ушкодження?
18) По яких ознаках вона визначила, що він уже мертвий?
19) Якою була обстановка на місці події (меблі, чужі речі, ушкоджене майно і т.ін.)?
20) Де знаходилася сокира? Кому вона належить? Чи брала вона його в руки після події?
21) Чи робила вона які-небудь зміни на місці до приїзду слідчої групи?
22) Який матеріальний збиток заподіяний їй вчиненим злочином?

Після проведення судово-медичної експертизи слідчий повинен отримати відповіді на наступні питання:

1) Які тілесні ушкодження маються на трупі Р.?
2) Коли і чим вони могли бути заподіяні?
3) Яка ступінь ваги прижиттєвих тілесних ушкоджень?
4) У якій послідовності тілесні ушкодження були нанесені?
5) Чи заподіяні тілесні ушкодження сокирою, знайденою на місці події?
6) Яка причина смерті Р.?
7) Коли наступила смерть?
8) Чи вживав Р. перед смертю алкогольні напої, токсичні чи наркотичні речовини?

Взагалі, типовий криміналістичний алгоритм розслідування побутового вбивства наведено на рис 3. На ньому виділено три напрямки дій слідчої оперативної групи: місце пригоди, підозрюваний, можливий свідок. Для нашого випадку, на місці пригоди знаходять труп, знаряддя вбивства (топор), пляшка, стакани. Останні передаються на дактилоскопічну експертизу, а труп і знаряддя вбивства ще й на судово-медичну експертизу. В якості підозрюваного, а потім затриманого, виступає громадянин Б., можливого свідка – громадянка О. Із алгоритму слідує, що їх треба допитати, здійснити дактилоскопірування, впізнання, та при необхідності, судово-психіатричну експертизу. Послідовність та зміст наступних слідчих дій (наприклад, слідчий експеримент) визначені наведеним алгоритмом.

Рис.1. Будинок, в якому здійснено злочин.

Рис. 2. Схема місця побутового злочину за наведеною фабулою

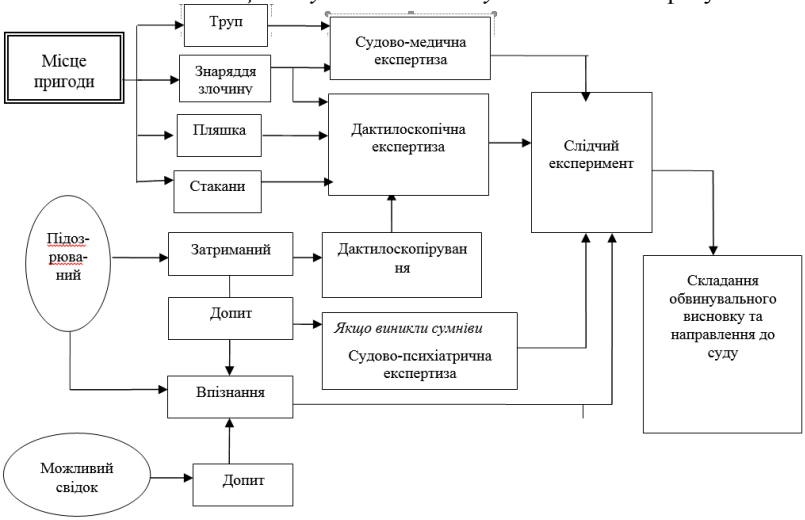


Рис 3. Алгоритм розслідування побутового вбивства

ІНФОРМАЦІЙНА СКЛАДОВА ОСОБИ ЗЛОЧИНЦЯ У РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ЩОДО НЕЗАКОННОГО ЗАВОЛОДІННЯ ТРАНСПОРТНИМИ ЗАСОБАМИ

Захарова Олександра Василівна,
доцент кафедри кримінального процесу та криміналістики, ЛьвДУВС
Ізьо Марта Ігорівна,
студентка ЛьвДУВС

У ефективності розслідування кримінальних правопорушень щодо незаконного заволодіння транспортними засобами, неабияке місце займає глибоке та всебічне вивчення криміналістичної характеристики, а саме особа злочинця. Даний напрямок дозволить правильно висунути слідчі версії, визначитись з тактикою проведення окремих слідчих (розшукових) дій та негласних слідчих (розшукових) дій.

Кримінальні правопорушення, що посягають на незаконне заволодіння транспортними засобами можна назвати «чоловічими правопорушеннями», якщо ж вони вчинялися жінками то лише у співучасті з чоловіком.

Слід зауважити, що незаконним заволодінням транспортних засобів в основному займаються злочинні групи – (75%). Як правило, в таку групу входять: лідер (організатор) – 74,8% випадків; особи, що спеціалізуються тільки на транспортуванні автотранспортних засобів – 65,3%; фахівці з технічного переобладнання й перефарбування автотранспортних засобів – 27,4%; збувальники краденого, особи, що знаходять покупця – 38,5%; перегонщики автомашини до місця її реалізації – 61,3%; особи, що визначають місце зберігання й марку автомобіля, «наміченого» для викрадення – 17,4%.

Групи з трьох осіб становлять – 16,7%, із чотирьох – 11,1%, з п’яти – 14,3%, із шести – 12,8%, із семи – 5,6%, з восьми – 6,9%, з дев’яти – 8,6%, а з десяти й більше осіб – 24% випадків. Зауважимо, що групи мають у своїх складах як дорослих, так і неповнолітніх учасників. На частку груп, що включають у себе

тільки неповнолітніх, припадає 11,8%. Учасники інших злочинних груп обов'язково мають значний життєвий досвід.

Групи, які спеціалізуються на незаконному заволодінні транспортних засобів залежно від території злочинної діяльності, класифікуються на такі три види: районні злочинні групи (що діють у масштабі одного району області) 23,5%; регіональні (що діють у межах області) – 54,3%; міжрегіональні (що діють на території декількох областей) – 11,2%; міждержавні (які діють на теорії кількох держав) – 11% [1, с.61-62].

Із метою класифікації організованих злочинних груп із урахуванням наведеної дефініції варто також виділити кілька криміналістичних типів злочинних груп.

1. Випадкові, що об'єдналися для вчинення групового злочину. У таких випадках співучасники беруть участь у групі з почуття солідарності.

2. Злочинні групи типу компанії. Вони більше організовані, особовий склад у них, як правило, стабілізований, яскраво виражена антигромадська установка. Злочинна діяльність посідає значне місце й починає відігравати провідну роль, однак немає чітких планів цієї діяльності.

3. Організована група, що характеризується стійкістю, ієрархічною структурою, обов'язковою наявністю лідера, здійненням планування злочинної діяльності.

4. Злочинні організації. По суті, це ті ж організовані злочинні групи, але з вищим ступенем організованості. Структура цих груп більше складна й ступінь суспільної небезпеки цієї категорії груп дуже високий [2].

У загальному вигляді структура групи може бути наступною: безпосередні виконавці незаконного заволодіння транспортними засобами («кучери»); особи, що займаються укриттям і переробкою викрадених автотранспортних засобів (автослюсарі, власники приватних майстерень, працівники сфери автообслуговування тощо); особи, що переганяють автомобілі з одного населеного пункту в інший («кур'єри»); особи, що займаються збутом транспорту, а також організатори.

Що стосується неповнолітніх, вони одноособово вчиняють близько 27% незаконних заволодінь транспортними засобами, в групі за їх участю – 73%, групи, що складаються виключно з

неповнолітніх: дві особи – 67% випадків, три – 28% випадків, чотири і більше – 5% випадків; групи за участю дорослих: дві особи – 67% випадків, три особи – 24% випадків, чотири і більше – 9% випадків [3, с.83].

За останні роки, характер протиправної діяльності у сфері автотранспорту змінився радикально, зокрема після введення електронних іммобілайзерів, іммобілайзерів нового покоління (пристрій, який використовуєть для сканування відбитків пальців). Для запуску двигуна потрібно докласти подушечку пальця до оптичного приладу (сканера). Якщо автомобілем користується багато людей, то зразки їх відбитків потрібно внести в загальну систему. Є і методика відбитків різних двох пальців, один з них блокує систему. Треба відмітити, що освітній рівень у особи злочинця виріс у декілька раз, адже для незаконного заволодіння транспортним засобом потрібні не аби які зусилля, які потребують спеціальних знань.

Так у порівнянні з даними 1998 року, із загальної кількості осіб, тільки 12,7% мали середню спеціальну освіту, 43,1% не мали навіть середньої [4, с.95]. На даний час із загальної кількості осіб найвищий показник (48%) становлять особи, які мають середню освіту; найнижчий показник (21%) особи які мають вищу освіту.

Аналіз обставин вчинення незаконних заволодінь транспортних засобів дозволяє зробити висновок, що цим видом злочинної діяльності займаються організовані угруповання, які добре законспіровані, мають необхідні технічні, транспортні засоби та ролі виконавців у таких угрупованнях чітко розподілені.

1. Колпаков В.К, Захаров В.П, Гордєєв В.В та ін. Незаконне заволодіння транспортом: протидія засобами попередження. Монографія. – Х.: Харків юридичний, 2012. – С.61-62.
2. Быков В. М. Преступная группа: криминалистические проблемы / Быков В. М. – Ташкент, 1991. – 143 с.
3. О.В.Лускаатов., Д.А.Петрелюк. Вивчення особи злочинця у справах про незаконні заволодіння транспортними засобами, вчинені неповнолітніми // Бюлетень міністерства юстиції України. – Київ : МЮУ, 2011 – №2. – С.83.
4. Ю.Іванов. Особа злочинця у злочинах про посягання на автотранспортні засоби // Юридичний журнал Право України. – Київ., 1998 – №8, С.95.

КОНТРРОЗВІДКА В СИСТЕМІ БЕЗПЕКИ БІЗНЕСУ

Живко Зінаїда Богданівна,
завідувач кафедри менеджменту ЛьвДУВС, д.е.н., доцент
Вольних Анастасія Іванівна,
студентка відділення інформаційних технологій
Технологічного коледжу НУ «Львівська політехніка»
Муж Павло Олегович,
студент ЛьвДУВС

З давніх часів в розвідці існують чітко визначені принципи, які залишаються непорушними донині. Серед них – зв'язок між збиранням розвідувальних даних і захистом своєї власної інформації. За одним із визначень, «контррозвідка – це захист своєї конфіденційної інформації від шпигунства». Слід зазначити, що тільки з переходом підприємств до ринкових відносин економічна (промислова) контррозвідка одержала легітимність і стала складовим елементом ділового процесу. В умовах конкуренції роль вивчення намірів конкурента і приховування своїх планів стає визначальною. Як і в традиційній контррозвідці, запобігання розкриттю своїх джерел інформації (нехай навіть і відкритих), а також методів збору інформації для конкурентної контррозвідки є пріоритетним завданням. Особливо розвинена ця система в США, за довгі роки практики американські розвідники і контррозвідники розробили методики і технології захисту як збору даних про конкурентів, так і захисту власної компанії від просочування конфіденційної, стратегічно важливої інформації. Багато вітчизняних підприємств ще в 90-і рр. на етапі становлення роботи своїх служб безпеки брали приклад із західних фахівців з конкурентної розвідки, а також охоче залучали до роботи колишніх працівників спецслужб.

Значення і роль контррозвідки в сучасних умовах ведення бізнесу обумовлено принаймні трьома обставинами: по-перше, прагненням деяких підприємців усунути або нейтралізувати своїх конкурентів послуговуючись засобами промислового шпигунства; по-друге, погіршення кримінальної ситуації в країні, що створює поживний ґрунт для певних верств населення вирішувати свої проблеми злочинним шляхом; по-третє, потребою здійснення

захисних дій щодо представників державних органів управління, які використовують своє службове становище у злочинних цілях.

У найзагальніших рисах процес конкурентної розвідки і контррозвідки в системі економічної безпеки підприємства складається з трьох взаємопов'язаних складових: внутрішнього моніторингу, зовнішнього моніторингу та аналітичної роботи (рис. 1).

Рис. 1. Місце конкурентної розвідки та контррозвідки в системі економічної безпеки підприємства [1]

Внутрішній моніторинг припускає, що працівники служби безпеки всіляко захищають підприємство від проникнення «шпигунів» і розвідників, а також відстежують дотримання співробітниками підприємства внутрішніх правил по нерозголошуванню конфіденційних даних. Для цих потреб активно застосовуються спеціальні інформаційні системи. Однією із найбільш поширених є IPC (Information Protection and Control), яка захищає інформацію методом шифровки носіїв, а також повним контролем всіх можливих носіїв і каналів, через які, з технічної точки зору, може відбуватися витік важливої інформація (e-mail, icq, Skype, соціальні мережі, принтери, зовнішні носії, накопичувачі, USB, WiFi, Bluetooth і так далі).

Особливої цінності така система набуває, враховуючи, той факт, що до 75% конфіденційної корпоративної інформації розголошується мимоволі, помилково або з необачності персоналу.

Зовнішній моніторинг, у відповідності до вище викладених положень, – це і є конкурентна розвідка в найбільш загальному розумінні. Він припускає збір повного об'єму інформації про

конкурентів: технології, управління, об'єми збуту, чинники конкурентної переваги, стратегічні плани на майбутнє, стратегії завоювання ринку, можливі загрози для свого підприємства, методи оптимізації роботи, інновації і так далі.

Аналітична робота припускає проведення порівняльної характеристики, виявлення своїх сильних і слабких сторін, розробку конкретних рекомендацій для менеджменту з метою недопущення збитків, втрати частки ринку тощо. Метою контррозвідки є недопущення витоку чи оприлюднення інформації, розгляд способів ворожого збору та використання інформації.

У криміналістичній літературі слушно зазначається, що не існує тотожних злочинів. Водночас кожна окрема подія – це вияв однотипних (однопорядкових) подій, що характеризуються наявністю не тільки індивідуальних, а й типових ознак [2; 3]. Способи конкретного виду злочину мають загальні ознаки, які повторюються, що дає змогу узагальнити їх, тобто типізувати системи операцій і прийомів злочинних діянь. Звідси, стосовно предмету нашого дослідження можна виділити три групи типових способів злочинних посягань на інформацію, що становлять комерційну або банківську таємницю: 1) незаконне збирання інформації, що становить комерційну або банківську таємницю; 2) незаконне використання такої інформації; 3) умисне розголошення такої інформації.

Незаконне збирання інформації може виявлятися у [1]:

1) викраденні відповідної інформації чи об’єктів, що її містять, з приміщень, де вони зберігалися. Така крадіжка може бути як відкритою, так і завуальованою, коли справжні предмети посягання (документи, вироби, що містять комерційну таємницю) викрадаються разом із іншими і в такий спосіб створюється хибне уявлення про дійсні цілі злочинців;

2) таємному проникненні злочинця до приміщення й копіювання інформації паперовим чи електронним способом. Для фіксації інформації та її пересилання можуть застосовуватися мобільні телефони з вбудованими фотокамерами й послуга MMS;

3) підкупі співробітника підприємства, який мав чи має законний доступ до інформації. Працівник за певні матеріальні чи інші блага копіює інформацію та передає її замовникові. Якщо

людина вже звільнилася або на сьогодні не має законного доступу, але інформація, якою вона володіла раніше, ще не втратила комерційної привабливості, то вона її просто повідомляє;

4) підкупі посередників у переговорах, які володіють певною інформацією;

5) незаконному отриманні інформації у співробітників правоохоронних або контролюючих органів, яким вона стала відома внаслідок виконання ними службових обов'язків;

6) погрозах фізичним насильством над особою чи її близькими родичами, якій інформація була довірена в результаті виконання її трудових обов'язків;

7) шантажі працівника, який знаходиться на «гачку» внаслідок певних життєвих обставин;

8) впровадженні свого агента в штат підприємства під виглядом звичайного співробітника;

9) вербуванні діючого працівника або спонуканні до розголошення звільненого із застосуванням мотивів етнічної, расової, релігійної близькості, бажанням помститися керівникові за незаконне звільнення, переведення на іншу роботу, зняття з посади;

10) використанні різних технічних пристроїв, що фіксують і передають інформацію. За допомогою спеціальної техніки здійснюється прослуховування приміщень або зняття інформації з каналів зв'язку. Для цього застосовуються радіозакладки, мікрофони направленої дії, пристрої для зняття інформації з вікон за допомогою лазерних промінів, апаратура для виявлення й розшифровування електромагнітного випромінювання від офісної техніки, мініатюрні фото- та відеокамери. Таку техніку можуть встановлювати або використовувати як спеціально підготовлені особи, так і завербовані співробітники підприємства;

11) проникненні в комп'ютерні мережі. Для цього злочинці застосовують спеціальні комп'ютерні програми, які дозволяють відшуковувати необхідні дані та копіювати їх.

Найпоширенішими програмними засобами, які використовуються для несанкціонованого доступу є [4]: 1) експлоіти (сканери) – програми, які використовують певні недоліки в програмному забезпеченні ЕОМ чи мережі, що призводить до настання бажаних для злочинця результатів; 2) сніфери – дозволяють перехоплювати дані, що передаються мережами електрозв'язку;

3) «троянський кінь» – програми цієї групи приховано встановлюються в будь-який спосіб на комп'ютері, що цікавить злочинців, як правило шляхом вбудовування в іншу легальну програму. При цьому програма-носій, виконуючи свої прямі функції, здійснює й додаткові, закладені в неї розробником; 4) руткіти – набір програм, який дозволяє злочинцю внести певні зміни в програмне середовище комп'ютера-жертви для здійснення контролю та отримання в подальшому легкого доступу до нього.

Незаконним використанням комерційної чи банківської таємниці є впровадження у виробництво або врахування під час планування чи здійснення господарської діяльності без дозволу власника чи уповноваженої на те особи таких відомостей. Зокрема, незаконне використання може мати такі форми: 1) пред'явлення майнових або інших вимог до власника комерційної чи банківської таємниці за повернення або нерозголошення відповідних відомостей. Такі вимоги можуть стосуватися повернення на роботу, призначення на вищу посаду, звільнення іншого працівника тощо; 2) продаж інформації третім особам; 3) обмін інформації, що становить комерційну чи банківську таємницю, на іншу або матеріальні цінності; 4) корегування своїх дій при укладанні договорів з власником такої таємниці.

Протидія охарактеризованим вище способам злочинного посягання на конфіденційну інформацію є головним завданням контррозвідки. Водночас, на нашу думку, запобігання злочину є набагато ефективнішим у порівнянні із ліквідацією наслідків. Зазначене обґрунтовується тим, що проведення внутрішнього моніторингу дозволяє визначити сукупність слабких місць, завчасна ліквідація яких і унеможливить реалізацію значної кількості загроз. Типовий перелік таких слабких місць для вітчизняних підприємств можна визначити наступною сукупністю: неефективна кадрова політика; відсутність потрібного інструктажу та регулярних перевірок щодо дотримання персоналом умов збереження комерційної та конфіденційної інформації; відсутня мотивація робітника, неефективне керівництво, атмосфера в колективі. При розробленні та/або вдосконаленні методичних засад здійсненні контррозвідувальних дій, доцільно взяти до уваги науковий доробок відомого фахівця з організації служб безпеки підприємств В. Мак-мака, який не лише включив в організаційну

схему служби безпеки підприємства – відділ розвідки, але і положення про підрозділ розвідки, що визначає основні напрями її діяльності, функціональні обов'язки її співробітників, права їх у взаєминах з іншими підрозділами компанії. Останнє важливе з тієї точки зору, що до них відносяться і співробітники інших підрозділів підприємства, що займаються збором і дослідженням інформації.

Особливістю організації інформаційних потоків на підприємстві з метою захисту «критичної» інформації, протидії промисловому шпигунству та організації дезінформування є розроблення на підприємстві Порядку поширення інформації з обмеженим доступом, яка належить підприємству.

Керівник підприємства вирішує всі питання щодо розповсюдження власними силами, оприлюднення через ЗМІ та реалізації права на розпорядження комерційною таємницею. Проте необхідно взяти до уваги виняток, зафіксований в ч. 11 ст. 30 Закону України «Про інформацію»: Інформація з обмеженим доступом може бути поширена без згоди її власника, якщо ця інформація є суспільно значимою, тобто якщо вона є предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право її власника на її захист [5]. Звідси питання про оприлюднення через ЗМІ інформації, що становить комерційну таємницю та конфіденційну інформацію, вирішує керівник підприємства за винятком випадків, коли така інформація підпадає під кваліфікацію ч. 11 ст. 30 Закону України «Про інформацію».

З’ясування біографічних та інших характеристик претендентів на робочі місця. Зміст інформації про особу співробітника включає в себе дві групи відомостей: службові (прогули, скарги відвідувачів тощо) і особисті (аморальна поведінка, сімейні проблеми тощо). Вважається, що сукупність вищевказаних відомостей може достатньою мірою характеризувати співробітника підприємства і допомогти його керівництву у зміцненні дисципліни.

Консультування співробітників підприємства з питань забезпечення економічної безпеки відбувається переважно за всіма видами безпеки. Форми консультування можуть бути груповими (лекції, семінари тощо) та індивідуальними. Серед персоналу підприємства слід виділити ті групи, які необхідно

систематично інструктувати. Якщо є необхідність, то можна створити спеціалізовані навчальні курси зі здачею заліків. Цілі, завдання, функції та інші основні питання діяльності контрозвідки, зазвичай, відображаються в положеннях про контрозвідувальний підрозділ.

Серед методів, що найчистіше використовують співробітники контррозвідки, можна відзначити приховане спостереження; відкриті і зашифровані опитування; отримання довідок; дослідження предметів і документів; зовнішній і внутрішній огляд будівель, приміщень та інших об'єктів.

Для об'єктивного оцінювання діяльності контррозвідувального підрозділу служби економічної безпеки підприємства необхідно розробити відповідні критерії та показники. До критеріїв діяльності контррозвідувального підрозділу можна віднести ступінь протидії розвідувальним заходам ділових конкурентів і злочинців, рівень запобігання та припинення правопорушень на підприємстві. Показниками, що доповнюють критерії, можуть бути такі:

- чисельність працівників, притягнутих до відповідальності за розголошення комерційної таємниці підприємства;
- кількість виявлених економічних (промислових) шпигунів;
- кількість виграних судових процесів у цивільних справах на підставі матеріалів контррозвідки;
- кількість службових розслідувань, проведених щодо персоналу підприємства;
- сума втрат, яких вдалося уникнути в наслідок виконання своїх функцій контррозвідкою.

Отже, контррозвідувальна діяльність як функція системи економічної безпеки підприємства дозволяє запобігти втратам в діяльності підприємства, зберегти його комерційну таємницю та конфіденційну інформацію і зрештою зміцнити економічну безпеку підприємства. Але для цього контррозвідувальна діяльність має бути належним чином організована, нею не можна у наш час нехтувати.

1. Живко З.Б. Методологія управління економічною безпекою підприємства. Монографія / З.Б. Живко . – Львів : Вид-во Ліга-Прес, 2013. – 474 с.
2. Настільна книга слідчого : наук.-практ. вид. для слідчих і дізнавачів / [М. І. Панов, В. Ю. Шепітько, В. О. Коновалова та ін.]. – [2-ге вид., перероб. і допов.]. – К. : Ін Юре, 2007. – С. 179.
3. Шепитько В. Ю. Криминалистика : курс лекций / В.Ю. Шепитько. – Х. : Одиссей, 2003. – С. 249.
4. Збірник методичних рекомендацій з викриття та документування злочинів у сфері інтелектуальної власності та комп'ютерних технологій / [Л. П. Скалозуб, В. І. Василинчук, С. А. Лебідь та ін.] ; за ред. О. М. Джужі. – К. : ДДСБЕЗ, 2009. – С. 56–58.
5. Про інформацію: закон України // Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650 в редакції від 02.03.2014, підстава 763-18.

ФОРМУВАННЯ МОДЕЛІ ПІДСИСТЕМИ КОНКУРЕНТНОЇ РОЗВІДКИ

Портнова Анастасія Володимирівна,
магістр ЛьвДУВС
Живко Михайло Олександрович
доцент кафедри адміністративного права Львівського університету бізнесу та права, к.ю.н.
Трипітьон Олена Сергіївна,
студентка ЛьвДУВС

Розглядаючи місце конкурентної розвідки в сучасній економіці, необхідно підкреслити, що зважаючи на суттєвий і негативний вплив світової фінансової кризи 2008-2009 рр. на ефективність господарської діяльності та низький рівень економічної безпеки вітчизняних підприємств, організована та ефективно діюча конкурентна розвідка повинна стати інновацією, інструментом виживання, засобом перемоги, стратегічною альтернативою і ефективним інструментом ведення бізнесу. Звідси, на нашу думку, конкурентна розвідка як завдання для окремого підрозділу чи певної посадової особи повинна мати місце з моменту заснування бізнесу і здійснюватися упродовж усього життєвого циклу.

Якщо розглядати сучасні погляди на природу життєвого циклу підприємства, то серед них доцільно виділити думку колективу авторів під керівництвом Є. М. Короткова, який розглядає шестиетапний цикл розвитку підприємницьких структур [1]. Кожному з етапів відповідають певні особливості стану соціально-економічної системи, які визначають характер діяльності і тип організації підприємства, а в нашому випадку повинні визначати і сукупність завдань для конкурентної розвідки (рис. 1).

Кожен блок на схемі відповідає певному етапу розвитку соціально-економічної системи підприємства. Зв'язки між блоками характеризують розвиток підприємства, що може поліпшувати стан та ефективність діяльності підприємства, а може призвести і до кризи [2].

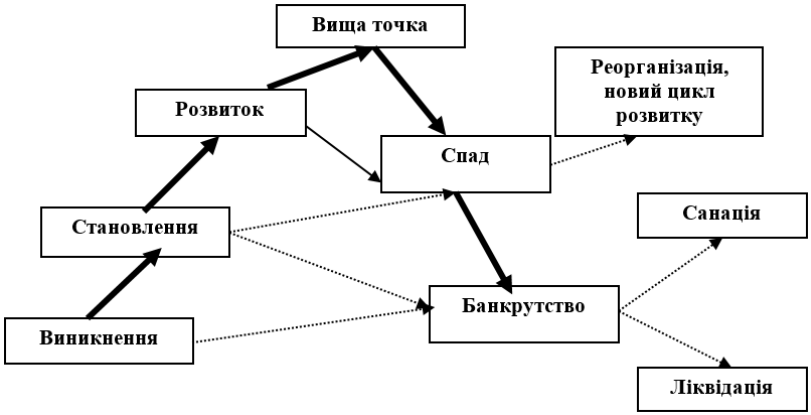


Рис. 1. Життєвий цикл підприємства [3]

Перший етап відповідає виникненню підприємства і характеризує його як таке, що займається ризикованою діяльністю, стратегія якого орієнтована на радикальні нововведення. На цьому етапі відбувається зародження підприємства в ринковому економічному середовищі, формування його початкової структури. Це етап прихованого розвитку майбутньої цілісності. Зовнішня диференціація і внутрішня інтеграція підприємства починають визначатися, з'являються потенційні характеристики підприємства, здійснюються перші крокі виходу на ринок з експериментальними зразками продукції. Цей етап характеризується діяльністю з високим рівнем ризику. Процес кризового

розвитку може мати наслідки зростання підприємства і перехід на другий етап життєвого циклу (позитивний наслідок), а також руйнацію підприємства (негативний наслідок).

Погоджуємося з автором [2], що на етапі «виникнення» – пріоритетними завданнями конкурентної розвідки повинні бути: дослідження зовнішнього бізнес-середовища; формування банку даних щодо основних конкурентів, споживачів, постачальників; визначення основних ризиків та розрахунок ймовірності їх реалізації; інформаційний супровід прийняття управлінських рішень.

На другому етапі відбувається становлення підприємства, тобто для нього є характерним зростання і збільшення масштабів діяльності. У зв'язку з тенденціями росту виникає необхідність перебудови структури, диференціації функцій управління, підвищення ефективності діяльності. Відбувається захоплення певного сегмента ринку, укріплення ринкових позицій, напрацювання конкурентної стратеги, підвищення ролі маркетингу в управлінні підприємством. Цей етап можна розглядати як етап кількісного зростання, оскільки перебудова в управлінні підприємством пов'язана, переважно з кількісними змінами.

Кризовий розвиток другого етапу пов'язаний, першою чергою, з зовнішніми причинами: зовнішніми циклами розвитку економіки, ринковою кон'юнктурою, політикою. Результатом цього етапу може бути як руйнація підприємства, так і перехід на наступний етап життєвого циклу підприємства. Саме подальше зростання в значній мірі залежить від повноти та ефективності виконання своїх функціональний обов’язків відповідальних осіб за конкурентну розвідку, перед якими повинні стояти наступні завдання: забезпечення керівників усіх рівнів управління актуальною інформацією про стан та динаміку ринку; налагодження горизонтальних і вертикальних зв’язків між підрозділами підприємства; визначення об’єктів, процедури та інших параметрів проведення моніторингу бізнес-середовища; визначення та ідентифікація ризиків та додаткових можливостей; відстеження тенденцій розвитку та складання прогнозів стосовно підприємства та бізнес-середовища; визначення інформаційних потреб та їх задоволення.

Третій етап зумовлений підйом підприємства, на якому воно досягає зрілого та стійкого стану на ринку. Таке підприємство характеризується високим рівнем технологічного озброєння,

масовим випуском продукції, високим рівнем конкурентоспроможності.

Якщо зважити на те, що кризовий розвиток третього етапу пов'язаний, здебільшого, з якістю управління, що унеможливлює досягнення вищої точки розвитку, то завданнями конкурентної розвідки повинно стати: збір інформації про поточне конкурентне положення підприємства; аналіз ризиків й можливостей; ідентифікація кризових явищ та кризових ситуацій; систематичне проведення бізнес-середовища; інформаційний супровід прийняття управлінських рішень; оцінка ефективності інформаційно-аналітичної діяльності; інформаційний супровід процесу коректування стратегії розвитку; визначення перспектив розвитку підприємства.

На четвертому етапі – динамізм третього поступово втрачається, а на зміну йому приходить стійка стабільність, що забезпечується великими розмірами, диверсифікацією, наявністю мережі філіалів.

Проблеми четвертого етапу пов'язані з тим, що, зберігаючи гігантський товарообіг, підприємство поступово втрачає здатність отримувати адекватний прибуток, а згодом починає зазнавати збитків. Причинами такого розвитку можуть бути надвисока активність за усіма напрямками діяльності, ускладнення організаційної структури, втрата перспектив виробництва.

Для запобігання подібним явищам необхідно своєчасно закривати збиткові виробництва, знижувати витрати на існуючих виробництвах, виділяти пріоритетні напрямки діяльності, що є можливим в першу чергу через ефективне виконання конкурентною розвідкою наступних завдань: відстеження досягнутих результатів через позиціонування конкурентної позиції підприємства у бізнес-середовищі; відстеження дій зі сторони конкурентів; пошук нових ринків збуту; диверсифікація системи постачання; прогнозування змін і визначення шляхів реагування на них; інформаційний супровід прийняття рішень; задоволення інформаційних потреб структурних підрозділів підприємства; пошук шляхів розвитку, виявлення сприятливих для бізнесу можливостей.

П'ятий етап життєвого циклу є періодом спаду, тобто занепаду, старіння, коли найважливіші параметри життєдіяльності

значно погіршуються, а розвиток як подальше удосконалення не є доцільним. При цьому структура підприємства спрощується, а конкурентні переваги втрачаються. За таких умов перед конкурентною розвідкою доцільно поставити наступні завдання: пошук та аналіз нових можливостей і шляхів утримання ринків; оцінка нових технологічних рішень; інформаційний супровід прийняття рішень; задоволення інформаційних потреб структурних підрозділів підприємства; аналіз нових технологій та інновацій; визначення перспектив функціонування підприємства; пошук шляхів розвитку, виявлення сприятливих для бізнесу можливостей; виявлення загроз, своєчасна ідентифікація відповідних сигналів; визначення проблемних зон, протиріч і труднощів, їх аналіз [2].

Для запобігання подальшого занепаду підприємства необхідно провести його реструктуризацію та реорганізацію, що дасть можливість підприємству вийти на новий цикл своєї життєдіяльності і розвиватися згідно з попередніми характерними тенденціями. В іншому разі підприємство може прийти до шостого етапу свого розвитку – банкрутства.

У разі існування хоча б найменшої можливості відтворення діяльності підприємства проводять спеціальні процедури санації з метою мінімізації збитків при банкрутстві підприємства чи його розподілі.

Здійснення реанімаційних дій, які б мали відновити нормальну діяльність підприємства, також в значній мірі пов’язані із ефективним виконанням своїх завдань конкурентною розвідкою, зокрема щодо пошуку джерел фінансування санації, збору інформації про певного інвестора, оцінки можливості реалізації санаційного плану і т. д.

Поруч із виділенням завдань конкурентної розвідки на усіх етапах життєвого циклу підприємства, зважаючи на важливість їх виконання для підтримання швидких темпів розвитку та збереження бізнесу, на нашу точку зору, доцільно виділити та охарактеризувати стратегічну, тактичну і оперативну різновиди конкурентної розвідки (рис.2).

За результатами проведених теоретико-аналітичних досліджень, методичні засади реалізації конкурентної розвідки сформовані у вигляді моделі підсистеми конкурентної розвідки (рис. 3).

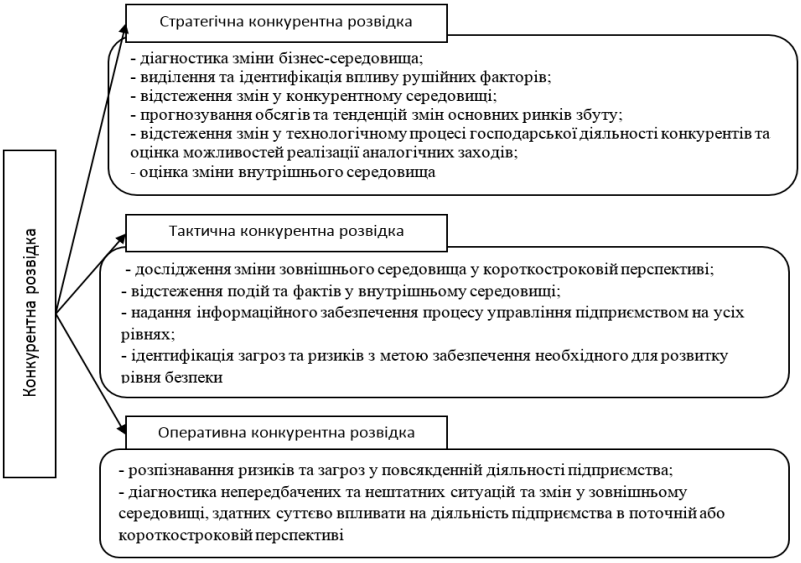


Рис. 2. Пріоритети стратегічної, тактичної та оперативної конкурентної розвідки [3]

За результатами проведених теоретико-аналітичних досліджень, методичні засади реалізації конкурентної розвідки сформовані у вигляді моделі підсистеми конкурентної розвідки (рис. 3).

Мета управління підсистемою конкурентною розвідкою випливає із її трактування, є підпорядкованою меті КСЕБП, а відтак у нашому розумінні полягає у розроблені та застосуванні заходів щодо інформаційного забезпечення керівного складу підприємства усіх рівнів управління щодо фактичного стану та можливих змін зовнішнього і внутрішнього середовища для найбільш ефективного використання наявних ресурсів та ринкових можливостей, завчасної ідентифікації загроз та ризиків.

Суб'єктами конкурентної розвідки, в залежності від масштабів діяльності певного підприємства, можуть виступати як працівники окремого функціонального підрозділу, так і фахівців служби безпеки, тобто окремі її представники, до обов'язків яких буде включено виконання сукупності завдань щодо конкурентної розвідки. *Об'єктом* підсистеми конкурентної розвідки виступає зовнішнє конкурентне середовище та внутрішнє середовище, тобто інформаційні ресурси та економічні інтереси.

Виконання сформованої сукупності завдань конкурентною розвідкою підприємства є можливим лише у випадку дотримання шести правил логістики, а саме: 1) добувати потрібну інформацію, 2) необхідної якості, 3) в необхідній кількості, 4) представляти її у потрібний час, 5) у потрібне місце (керівникові), 6) з мінімальними трудовими, фінансовими і матеріальними витратами.

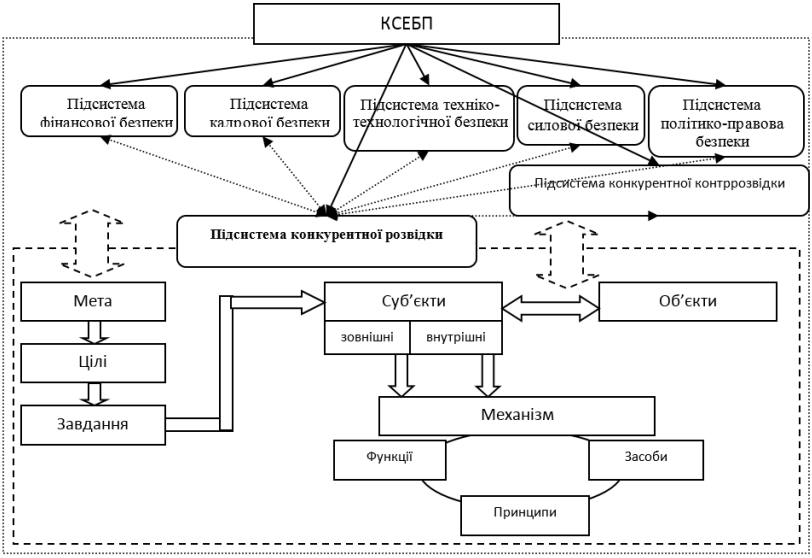


Рис.3. Модель підсистеми конкурентної розвідки [2]

Дотримання перелічених правил уможливить не лише виконання ключових завдань, але, що є особливо важливим, забезпечить ефективність здійснення конкурентної розвідки через раціональне використання ресурсів та співрозмірність витрат із очікуваним ефектом. Зазначене обумовлене тим фактом, що процес отримання потрібної інформації та перетворення її у важливі дані, як зазначалось уже вище, – дуже багатогранний, складний, змістовний та енергомісткий, хоча він набагато дешевший аніж його результат.

Механізм управління підсистемою конкурентної розвідки — це системне застосування методів функцій, засобів та принципів, які повинні сприяти досягненню максимального рівня економічної безпеки підприємства.

Функції – це види діяльності, які здійснюються суб'єктами конкурентної розвідки для забезпечення економічної безпеки підприємства. Основними з них, стосовно підсистеми конкурентної розвідки, на нашу точку зору, можна вважати:

- формування організаційної структури здійснення конкурентної розвідки;
- організація збору та аналізу інформації щодо внутрішнього та зовнішнього середовища підприємства;
- моніторинг конкурентної середовища з метою виявлення загроз та ризиків, їх ідентифікації та розроблення відповідних превентивних заходів з метою нейтралізації або зменшення негативного впливу;
- організація інформаційного забезпечення процесу управління підприємством.

Засоби для забезпечення ЕБП через здійснення конкурентної розвідки – це можливості, які можуть бути використанні суб'єктом безпеки. Основними з них є: правові, економічні, інформаційні, організаційні, техніко-технологічні, політичні, моральні.

У відповідності до сформованої вище суті підсистеми конкурентної розвідки, на нашу точку зору, до переліку основних *принципів* управління нею потрібно віднести наступні:

- системності інформації (забезпечення достовірності інформації, а відповідно й якості та ефективності розвідки);
- неперервності (реалізація заходів щодо здійснення інформаційного забезпечення повинно мати постійний характер);
- економічної доцільності (витрати на отримання і аналіз інформації не можуть перевищувати цінності такої інформації);
- раціональності (вибір періодичності, глибини та масштабності моніторингу адекватно до цінності отримуваної інформації);
- превентивності (пріоритетність завчасного отримання інформації про рівень ризику та ймовірності реалізації певної загрози);
- гнучкості (застосування різних способів та методів отримання інформації).

Мистецтво розвідника визначається його інтелектуальними критеріями: компетентністю, ерудицією, роботоздатністю, вмінням спілкуватися з людьми і навичками пошуку інформації.

Сформовані вище методичні засади реалізації конкурентної розвідки повинні сприяти забезпеченню високого рівня економічної безпеки підприємства через:

- досягнення стратегічних і тактичних цілей функціонування підприємства;
- покращення результатів діяльності підприємства;
- підвищення конкурентоспроможності бізнесу;
- підвищення життєстійкості підприємства як соціально-економічної системи;
- прогнозування можливості виникнення загроз, пошук шляхів їх уникнення та ліквідації можливих наслідків реалізації;
- зниження фінансових ризиків та підвищення фінансової стійкості;
- формування нових конкурентних переваг.

Поруч із переліченими вигодами, доцільно ще раз підкреслити, що головним призначенням конкурентної розвідки стає робота на випередження, недопущення виникнення нестандартних ситуацій, тих чи інших деструктивних подій за допомогою ідентифікації загроз та ризиків і своєчасного корегування стратегії розвитку, тобто розробка та реалізація заходів щодо зміцнення її конкурентного імунітету.

Потрібно враховувати і те, що швидка зміна зовнішнього середовища впливає не лише на діяльність підприємницьких структур, але і спричиняє удосконалення конкурентної розвідки. Основні тенденції у змінах цього виду розвідувальної діяльності можна коротко охарактеризувати наступним чином:

- вона набуває пріоритетного значення у порівнянні з військовою та політичною розвідкою;
- об’єктом розвідувальної діяльності стає перш за все новітня науково-технічна інформація, а також всі інші види відомостей: фінансові та бізнесові плани корпорацій, маркетингові програми, умови переговорів з партнерами та конкурентами тощо;
- понад 90 % економічної та військово-економічної інформації вилучаються з відкритих джерел;

- прибутки від здійснення розвідувальної діяльності зростають більш високими темпами у порівнянні із витратами;
- разом з традиційними засобами збору, аналізу і узагальнення розвідувальної інформації активно використовуються всі досягнення науково-технічної революції для отримання та обробки розвідувальних даних;
- активне і ефективне ведення економічної інформаційно-аналітичної діяльності має особливе значення для тих держав, в яких з тих чи інших причин на певний час загальмувався економічний та науково-технічний прогрес.

1. Антикризисное управление [Текст]: учеб. / Э. М. Коротков, А. А. Беляев, Д. В. Валовой и др.; под ред. Э. М. Короткова. – М. : ИНФРА-М, 2001. – 432 с.
2. Живко З. Б. Економічна безпека підприємства: сутність, механізми забезпечення, управління. Монографія / З. Б. Живко. – Львів : Ліга-Прес, 2012. – 256 с.
3. Економічна безпека держави: міждисциплінарний підхід: колективна монографія / за науковою редакцією д.е.н., проф. Хлобистова Є. В. – Черкаси : видавець Чабаненко Ю.А., 2013 . – 642с.

ЗАСТОСУВАННЯ ЕЛЕКТРОННИХ ЗАСОБІВ КОНТРОЛЮ ЗА КРИМІНАЛЬНИМ ПРОЦЕСУАЛЬНИМ ЗАКОНОДАВСТВОМ: ПИТАННЯ ТЕОРІЇ ТА ПРАКТИКИ

Ханас Василь Андрійович,
курсант 3курсу факультету з підготовки фахівців для підрозділів кримінальної міліції ЛьвДУВС
Дуфенюк Оксана Михайлівна,
доцент кафедри кримінального процесу та криміналістики факультету з підготовки фахівців для підрозділів слідства ЛьвДУВС, к.ю.н., доцент

У зв’язку із розвитком інноваційних технологій значного поширення набула тенденція застосування передових розробок, пов’язаних із використанням комп’ютерних засобів, периферійних пристроїв, програмного забезпечення у різноманітних сферах

життя. Зокрема у правоохоронної діяльності слід звернути увагу на новелу чинного Кримінального процесуального кодексу України, яка передбачає застосування електронних засобів контролю (далі – ЕЗК) до осіб, щодо яких обрано запобіжний захід у вигляді домашнього арешту. Питання теорії та практики використання вказаного заходу забезпечення кримінального провадження потребує більш докладного вивчення, адже досвіду використання таких інноваційних геоінформаційних технологій органи досудового слідства не мають. У зв'язку з цим можуть виникати певні труднощі ефективної реалізації їх можливостей, пов'язані із здійсненням моніторингової діяльності, реагування на спроби несанкціонованого зняття засобу тощо. Відтак не викликає сумніву актуальність дослідження теоретичних та прикладних аспектів апробації ЕЗК у вітчизняній правозастосовній практиці.

Передусім, потрібно зазначити, що ЕЗК – це електронний пристрій, виконаний у вигляді браслета, що закріплюється на тілі підозрюваного або обвинуваченого з метою його дистанційної ідентифікації та відстеження місцезнаходження, який призначений для носіння на тілі і захищений від самостійного знімання, пошкодження або іншого втручання в його роботу з метою ухилення від контролю та має сигналізувати про спробу особи здійснити такі дії [3]. Застосування ЕЗК полягає у закріпленні на тілі підозрюваного, обвинуваченого пристрою, який дає змогу відслідковувати та фіксувати його місцезнаходження [2]. Правовою підставою застосування електронного засобу контролю є ухвала слідчого судді чи суду.

Важливо звернути увагу на принципи використання та функціонування електронного браслету. Відповідно до Положення про порядок застосування електронних засобів контролю затверджене наказом МВС України № 696 від 09.08.2012 р. особа, яка зобов'язана носити ЕЗК, повинна перебувати на відповідному обліку в правоохоронних органах. Ці функції обліку, як зазначає В.В. Бірюков, можна описати поняттям «позиціонування», що трактується як прив'язка певного об'єкта, в нашому випадку підозрюваного, обвинуваченого, до системи координат на карті [4]. Таким чином процес застосування і використання електронних засобів контролю можна віднести до категорії геоінформаційних систем, адже ця

система охоплює процеси, пов'язані з опрацюванням даних, що мають просторову локалізацію [4, с.294].

З урахуванням викладеного вище можна сказати, що використання електронних браслетів має свої переваги, адже, застосовуючи до підозрюваного чи обвинуваченого запобіжні заходи, вказані учасники кримінального провадження мають можливість перебувати на волі та не переривати суспільні зв'язки. Особливо це стосується окремих найбільш вразливих категорій осіб, зокрема: неповнолітніх, перебування яких в слідчому ізоляторі може негативно вплинути на їх психіку; осіб похилого віку; осіб, які піклуються про неповнолітніх дітей; осіб, які страждають на хронічні хвороби.

Розглядаючи міжнародний досвід застосування ЕЗК, слід зазначити, що законодавство багатьох країн передбачає використання електронних браслетів щодо осіб за вчинення ними злочинів невеликої тяжкості. Безумово, цей інститут домашнього арешту для України є новим, але в світі його вже застосовують понад 30 років. Так, Сполучені Штати Америки були одними із перших, хто запровадив систему електронного контролю ще на початку 1980-х. [5]. За американським законодавством електронні браслети носять особи, які засудженні за викрадення автомобілів, за збут наркотичних засобів, а також особи, які порушують правила дорожнього руху чи зловживають спиртними напоями. Також міжнародна спільнота практикує застосування електронних браслетів до осіб, які претендують на умовно-дострокове звільнення або до дрібних злодіїв.

Утім поряд із позитивними аспектами застосування ЕКЗ існують певні проблеми впровадження цього інституту в ході досудового розслідування. Узагальнення даних слідчої практики дозволяють виділити такі проблемні питання застосування ЕКЗ під час кримінального провадження: відсутність спеціалізованого підрозділу ОВС, до функціональних обов'язків яких входить виключно моніторинг об'єктів, щодо яких застосовані запобіжні заходи; недосконаліть правового регулювання реагування на несанкціоноване знімання чи пошкодження ЕЗК; необхідність забезпечення підрозділів ОВС значною кількістю електронних браслетів, ретрансляторів, пультів моніторингу, серверів моніторингу та інших пристроїв без яких неможливо здійснювати

моніторинг об'єктів. За словами В.В. Бірюкова, головним недоліком впровадження геоінформаційних технологій є відсутність спеціалізованих підрозділів у міськрайвідділах МВС, які повинні бути суб'єктами поновлення облікових даних та моніторингу об'єктів.

Комплексне вирішення вищезазначених проблем дасть змогу державі заощаджувати на триманні осіб під вартою і на їх доставлені до суду, а в майбутньому є перспектива використання таких ЕЗК й під час відбування особами покарання, що, як свідчить міжнародна практика, значно зменшить наповненість місць позбавлення волі та затрати на тримання засуджених. Згідно з статистичними даними в Україні впродовж одного року на доставляння осіб з місць попереднього ув'язнення до суду для участі в засіданнях держава витрачає близько 20 млн. грн., а тримання таких осіб у слідчих ізоляторах в тому ж році обходиться платникам податків у більш, ніж 85 млн. грн.[5].

Отже, підсумовуючи зазначене, можна зробити висновок, що правове, організаційне та матеріально-технічне забезпечення застосування ЕЗК великою мірою впливає на реалізацію завдань кримінального провадження у випадках обрання до особи підозрюваного (обвинуваченого) запобіжного заходу у вигляді домашнього арешту. Беручи до уваги міжнародну практику використання ЕЗК, можна ствердно говорити про перспективи апробації цього інституту в умовах реформованого національного кримінального процесу, що, у підсумку, допоможе державі заощаджувати значні кошти, передбачені на утримання та транспортування відповідного контингенту суб'єктів, дасть змогу оптимізувати практику застосування заходів забезпечення кримінального провадження, засвідчить гуманізацію пенальної політики держави і наближення її до європейських стандартів правоохоронної діяльності.

1. Конституція України: офіц. текст: [прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 р] [Електронний ресурс]. – Режим доступу:http://zakon.rada.gov.ua.
2. Кримінальний кодекс України [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.
3. «Про затвердження Положення про порядок застосування електронних засобів контролю»: Наказ Міністерства внутрішніх справ

України [Електронний ресурс].– Режим доступу: http://zakon.rada.gov.ua.
4. Бірюков В.В. Теоретичні основи інформаційно-довідкового забезпечення розслідування злочинів / В.В. Бірюков. – Луганськ: ЛДУВС ім. Дідоренка, 2009. – 644 с.
5. Шевердін М., Бабич С. Держава заощаджує, або тюрма по-домашньому. Новели КПК України / М. Шевердін, С. Бабич [Електронний ресурс]. – Режим доступу http://www.kopartners.com.ua/pr /maksim-sheverdin-svitlana-babich-derzhava-zaoshchadzhuie-abo-tyurma-po-domashnomu-noveli-kpk.

АКТУАЛЬНІ ПРОБЛЕМИ ДОСЛІДЖЕННЯ ДОКУМЕНТІВ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У СФЕРІ СТРАХУВАННЯ

Заєць О.М.,
доцент кафедри конституційного та міжнародного права кандидат юридичних наук ОДУВС

Кожна фінансова, господарська операція у сфері економічної діяльності відображається в облікових документах і на електронних носіях інформації, на підставі яких робляться записи в облікових регістрах, журналах, рахунках. За допомогою документів даються розпорядження про здійснення фінансово-економічних операцій, висновку операцій, договорів; документи відображають виконання цих розпоряджень; вони мають правове значення; встановлюють відповідальність виконавців за проведені ними фінансові, господарські операції. При розслідуванні економічних злочинів документи відносяться до основних джерел інформації про подію злочину, його способи, виконавці, інших обставинах. Тому дослідження документів є одним з основних напрямів роботи слідчого. Участь фахівця в дослідженні документів допоможе знайти ознаки матеріальних та інтелектуальних фальсифікацій, встановити виконавців документів, відібрати документи, необхідні для експертного дослідження.

Кримінальне процесуальне законодавство України до документів, як джерелам доказів, відносити письмові документи (у

тому числі цифри, нотні знаки, ієрогліфи), фото-, відео-, фоно-, кіно- документи, малюнки, карти, схеми, креслення, табуляграми. В криміналістиці більшість дослідників до документів відносить письмовий або спеціально виготовлений предмет, на якому за допомогою листа, інших знакових систем зафіксовані відомості про обставини, що мають доказове значення для кримінального провадження [1]. Заслуговує уваги точка зору М. В. Салтевського, який розглядає документ як матеріально фіксовану інформацію, що відображає криміналістичні значущі відносини і факти [2, С. 337]. В більшості випадків документи по досліджуваній категорії злочинів мають письмову форму.

При розслідуванні кримінальних злочинів у сфері страхування слідчий стикається з величезною кількістю документальних джерел інформації, що відображає спосіб здійснення злочину, способи формування організованої групи і створення фіктивної фірми; зміст фінансово-економічних операцій, що використовуються членами злочинної групи як засіб реалізації наперед запланованого і ретельно підготовленого способу злочину; захована слідів організованої злочинної діяльності; обстановку, яка використовувалася або спеціально створювалася для здійснення злочинних дій [3, С. 134]. Тому всестороннє дослідження документів – важливий напрям розслідування. На наш погляд, дослідження документів включає комплекс процесуальних і не процесуальних дій, що дозволяють слідчому виявити механізм віддзеркалення злочинних дій в облікових документах, визначити виробничі ділянки, фінансово-економічні, господарські операції, які були використані правопорушниками, висунути версії про способи здійснення кримінального злочину, можливих учасників організованих груп, їх зв'язки.

Дослідження документів під час досудового розслідування дозволяє ознайомитися із структурою суб'єктів господарської діяльності. Зокрема, документів, підтверджуючих: а) факт створення суб'єкта підприємницької діяльності; б) здійснення виробничої, фінансової операції суб'єктом господарської діяльності; в) характер виробничо-господарських, фінансово-економічних операцій і їх відповідність Статуту; г) невідповідність документів фактичному положенню справ; д) безпосередніх їх виконавців тощо.

Слідчий має у своєму розпорядженні різноманітні засоби дослідження документів, що дозволяють на основі їх вивчення і перевірки встановити обставини здійснення економічного злочину тим або іншим способом, захована слідів злочинної діяльності. Ці засоби повинні використовуватися в комплексі. Зокрема, до них відносяться:

- особисте ознайомлення з документами самостійне або за допомогою фахівців. Це може бути як не процесуальне ознайомлення, так і слідчий огляд;
- вивчення документів страховика і в різних організаціях, пов'язаних з ним в тому або іншому ступені. Наприклад, з банківськими документами – в банку; із Статутом і рішенням про реєстрацію – в районній адміністрації; а також з документами, що знаходяться в податковій інспекції, у контрагентів тощо;
- призначення документальної ревізії на вимогу слідчого;
- допити та інші слідчі (розшукові) дії з участю обізнаних осіб, причетних до операцій;
- виробництво різних експертиз по документах;
- проведення негласних слідчих (розшукових) дій органами дізнання за дорученням слідчого [4, С. 73].

Документальні джерела інформації про обставини події злочину, що вивчається, утворюють певну систему, що дозволяє їх згрупувати в окремі групи, визначити інформаційний зміст, місця знаходження. По даній категорії кримінальних проваджень можна виділити наступні групи документів:

1. Для систематизації і накопичення інформації, що міститься в прийнятих до обліку первинних облікових документах, для віддзеркалення на рахунках бухгалтерського обліку і в бухгалтерській звітності ведуться регістри бухгалтерського обліку (в електронному вигляді і у вигляді машинограм): головна книга; журнали-ордери: журнал-ордер по рахунку 30 «Каса»; журнал-ордер по рахунку 37 «Розрахунки з різними дебіторами»; журнал-ордер по рахунку 66 «Розрахунки з оплати праці»; журнал-ордер по рахунку 49 «Страхові резерви»; журнал-ордер 76 «Страхові платежі»; журнал-ордер по рахунку 36 «Розрахунки з покупцями та замовниками»; касова книга; книга (реєстр) фінансових вкладень (цінних паперів і ін.); оборотні відомості по синтетичних і аналітичних рахунках.

2. Основну увагу в обліку страхових організацій надається роботі з договорами страхування і перестрахування. Роль регістрів бухгалтерського обліку страхових операцій виконують наступні журнали: журнал обліку укладених договорів страхування і перестрахування; журнал обліку збитків і достроково припинених договорів страхування; журнал обліку договорів, прийнятих на перестрахування; журнал обліку збитків за договорами, прийнятими на перестрахування.

3. Для здійснення бухгалтерських записів по обліку страхових премій використовуються наступні документи: договір страхування; правила страхування; рахунок на оплату страхового внеску; платіжне доручення, касовий чек; виписка банку; прибутковий касовий ордер; агентський договір (договір доручення); звіт страхового агента (страхового брокера); бухгалтерська довідка-розрахунок; повідомлення (лист) страхувальнику про заборгованість (несплаченої частини) страхової премії; наказ керівника про перелік надмірно одержаної страхової премії.

4. Для здійснення бухгалтерських записів по обліку страхових виплат використовуються наступні документи: договір страхування; заява страхувальника про настання страхового випадку; страховий акт; документи, підтверджуючі витрати страхувальника по страховому випадку; наказ керівника про страхову виплату (поверненні страхової премії (внесків)); витратний касовий ордер; виписка банку, платіжне доручення і др.; агентський договір (договір-доручення); бухгалтерська довідка-розрахунок; заява страхувальника про утримання з страхового відшкодування або страхових сум у разі погашення заборгованості страхувальника по оплаті чергового страхового внеску.

5. Для здійснення бухгалтерських записів по обліку витрат на ведення страхової справи є наступні документи: рахунки; платіжне доручення, касовий чек; виписка банку; витратний касовий ордер; агентський договір (договір доручення); звіт страхового агента (страхового брокера); бухгалтерська довідка-розрахунок; акти виконаних робіт; лімітно-обмежувальні карти, вимоги; авансовий звіт; наказ керівника.

Криміналістичною, слідчою практикою вироблені різні прийоми і форми розпізнавання підроблених документів. До числа поширених відносяться огляд і вивчення документів. Процес дослідження документів поділяється на три етапи: огляд

документів; вивчення; виявлення документів, що підлягають експертному дослідженню.

На всіх етапах процесу дослідження документів слідчому доцільно використовувати допомогу фахівця. Консультативна допомога фахівця відноситься до поширених не процесуальних форм. З урахуванням ситуації, що склалася, слідчий вирішує питання, коли і якого фахівця необхідно запросити і що потрібно з його допомогою з'ясувати, оглянути, витребувати. Саме на основі правильно організованих консультацій і створюються умови для вибору вірного напряму слідчої роботи по справі, виникають взаємозв'язки з іншими формами використовування спеціальних пізнань.

Отже, правопорушники скоюють витончені економічні кримінальні злочини з використанням сучасних інформаційних технологій, корупційних, міжрегіональних, транснаціональних зв'язків. Тому консультативна допомога фахівця, як і інші форми його участі в розслідуванні вказаних злочинів, є необхідною умовою для їх ефективного попередження, виявлення та припинення.

1. Журавель В. А. Криміналістичні методики: сучасні наукові концепції: монографія. / В. А. Журавель. – Х.: Вид. агенція «Апостіль», 2012. − 264 с.; Затенацький Д. В. Ідеальні сліди в криміналістиці (техніко-криміналістичні та тактичні прийоми їх актуалізації): монографія / Д. В. Затенацький; за ред. проф. В. Ю. Шепітька. – Х.: Право, 2010. − 160 с. та ін.
2. Салтевський М. В. Криміналістика (у сучасному викладі): Підручник. − К.: Кондор, 2005. − 588 с.
3. Комаха В.О. Тактика попереднього дослідження криміналістичних об’єктів при проведенні слідчого огляду: Монографія/ за ред. Комахи В.О.; Одеська національна юридична академія. – Чернівці,: Золоті литаври, 2003. − 652 с.
4. Криміналістика: ситуаційні моделі та завдання: Навч. посібник / за ред. проф. О. Я. Баєва, проф. В. Ю. Шепітька. – Х.: Апостіль, 2012. − 264 с.

ВИКОРИСТАННЯ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ДЛЯ ФІКСАЦІЇ ПРОЦЕСУАЛЬНОГО ЗАТРИМАННЯ ОСОБИ ЗА ПІДОЗРОЮ ВЧИНЕННЯ КРИМІНАЛЬНОГО ПРАВОПОРУШЕННЯ

Гуменюк Юлія Ігорівна,
здобувач кафедри кримінального права та кримінології факультету з підготовки фахівців для підрозділів слідства ЛьвДУВС

Згідно вимог кримінального процесуального законодавства працівник міліції має право без ухвали слідчого судді, суду затримати особу, підозрювану у вчиненні злочину, за який передбачене покарання у вигляді позбавлення волі, лише у випадках, якщо цю особу застали під час вчинення злочину або замаху на його вчинення;якщо безпосередньо після вчинення злочину очевидець, в тому числі потерпілий, або сукупність очевидних ознак на тілі, одязі чи місці події вказують на те, що саме ця особа щойно вчинила злочин (ст. 208 КПК України).Про затримання особи, підозрюваної у вчиненні злочину, складається протокол, в якому обов'язково вказується дата і точний час (година і хвилини) затримання. Копія протоколу негайно під розпис вручається затриманому, а також надсилається прокурору. Особа є затриманою з моменту, коли вона силою або через підкорення наказу змушена залишатися поряд із уповноваженою службовою особою чи в приміщенні, визначеному уповноваженою службовою особою (ст. 209 КПК України). Відповідно до вимог ст. 210 КПК України працівник міліції зобов'язаний доставити затриману особу до найближчого територіального підрозділу внутрішніх справ, де є орган досудового розслідування, в якому негайно реєструються дата, точний час (година і хвилини) доставлення затриманого та інші відомості, передбачені законодавством. Службова особа, відповідальна за перебування затриманих у територіальному підрозділі органу внутрішніх справ, зокрема черговий чергової частини, зобов'язана негайно зареєструвати затриманого. Згідно вимог наказу № 1050 від 19.11.2012, яким

затверджено Інструкцію про порядок ведення єдиного обліку в органах і підрозділах внутрішніх справ України заяв і повідомлень про вчинені кримінальні правопорушення та інші події, під реєстрацією розуміється присвоєння кожній заяві, повідомленню про вчинення кримінального правопорушення та іншої події порядкового номера і фіксація в електронних базах стислих даних по факту. По суті працівник міліції складає вмотивований рапорт, який реєструється в єдиному обліку, та направляється відповідальному працівникові для передачі в органи досудового розслідування. Призначений керівником органу досудового розслідування слідчий отримує під розпис в журналі єдиного обліку рапорт, ставить дату та час його отримання та складає протокол затримання, після чого вносить в електронному виді відомості про реєстраційний номер єдиного обліку, номер кримінального провадження, дату та час отримання рапорту, дату та час складання протоколу затримання.

Вищеописаний процес необхідно проводити у найкоротший по можливості термін з метою уникнення безпідставних скарг з боку затриманих на неправомірні, на їх думку, дії працівника міліції, який безпосередньо затримав особу.

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ: СТАН ТА ПРОБЛЕМИ

Босак Христина Зіновіївна,
старший слідчий ЛМУ ГУМВСУ у Львівській області
Браташ Ольга Ігорівна,
магістр ЛьвДУВС
Воробець Ірина Богданівна,
магістр ЛьвДУВС

В умовах технічного прогресу, коли обсяг інформації в сучасних інформаційних системах, стрімко зростає, особливо актуальними стають питання захисту інформації в цих системах. До інформації, яка поступає, зберігається, опрацьовується та використовується підприємствами висувається ціла низка вимог, основними з яких вважаємо: цілісність, своєчасність, повнота, достовірність тощо. За даними сайту Вікіпедії [1], цілісність

інформації (англ. *data integrity, information integrity*) – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом. Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації та видалення. Цілісність інформації – задачі забезпечення цілісності і доступності інформаційних об'єктів у обчислювальних мережах, модель системи зв'язку. Методи захисту від помилок: мажоритарний (принцип Вердана) і метод передачі інформаційними блоками з кількісними характеристиками блоку [1]. Отже, цілісність інформації – це захист даних від умисного або неумисного пошкодження, знищення, доступу сторонніх осіб.

Зазвичай, неправомірний доступ до інформації здійснюється з використанням чужого імені, шляхом використання підроблених документів, розкраданням носіїв інформації, зміною програмного і апаратного забезпечення та фізичних адрес технічних пристроїв, установкою спеціальних пристроїв чи апаратури перехоплення інформації з систем її передачі, а також порушенням систем захисту інформації. Неправомірний доступ до файлів чинного користувача може бути здійснений через наявність слабких місць в захисті системи. Виявивши прорахунки в системі захисту, злочинець може дослідити інформацію на комп'ютері, причому робити це можна так, що факт «злому» системи захисту буде встановлений дуже пізно. Одним із таких шляхів може бути використання шкідливих програм для комп’ютера, програм-вірусів, програм-шпигунів, які спрацьовують при певних умовах і повністю або частково паралізують роботу комп'ютерної системи. Всім відомий грецький міф про Троянську війну, по аналогії діють програми типу «троянський кінь». Цей спосіб полягає у внесенні в чужу програму спеціальних функцій, не порушують роботу програми. Наприклад, при введенні «троянського коня» в бухгалтерські програми можна переводити собі на банківський рахунок невелику суму з кожної операції. Виявити «трояна», безумовно, можливо. Проте це дуже клопітка робота. Із сотень і тисяч команд необхідно виявити ті, які внесені ззовні. Однак існують і такі «Трояни», які складені за наступним принципом. У програму вставляються не самі команди, що формують злочинну операцію, а програмний код, після

виконання якого формуються ті самі команди, що виконують «брудну роботу», після виконання якої вони самознищується.

Зокрема, компанія Касперського запустила на сайті інтерактивну карту кібератак (рис.1)

Рис. 1. Карта кібератак [2]

«Шкідливе програмне забезпечення заподіює шкоди вашій системі, але це рідко видно неозброєним оком, особливо в цифрових областях поза вашого власного комп'ютера. Однак у вас є можливість побачити масштаб і величину проблеми власними очима завдяки нашій карті, що зображає шкідливі епідемії в реальному часі», – йдеться на сайті компанії [2].

На сайті проекту досить обертати глобус і змінювати масштаб, щоб отримати уявлення про локальну ситуації в будь-якій частині світу. Різнобарвні точки на глобусі позначають різні види кібератак, виявлені в режимі реального часу. Сервіс дозволяє користувачеві отримати опис кожної загрози, а також відключити відображення тих типів загроз, які його не цікавлять. Натискаючи на країну, можна побачити кількість атак, виявлених там з 0:00 за Гринвічем, є також окремий розділ «статистика». Карта доступна в російській та англомовної версії. На сайті також доступне посилання для перевірки власного комп'ютера на наявність шкідливого програмного забезпечення.

По доповіді Лабораторії Касперського, більше 98% шкідливих програм для мобільних пристроїв з'явилися якраз на платформі Android. Зокрема, 175442 погрози були виявлені в 2014 році, що показує зростання на 18.3% порівняно з усім 2013 роком. Результати 12-місячного дослідження показують, що 59.06%

шкідливих програм, які визначені інструментами Касперського, зможуть вкрасти ваші гроші [3]. За даними інтернету можна побудувати графік зростання кібератак за період 1999-2012 років (рис.2).

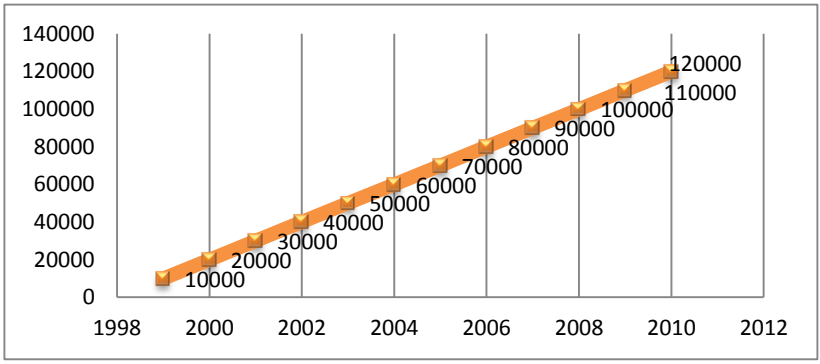


Рис. 2.Статистика атак в Інтернеті

На рис. 3 показана статистика атак через глобальну мережу Інтернет на локальний комп'ютер. Розробка та розповсюдження комп'ютерних вірусів. Небезпека вірусів не слід применшувати. Вірус може виявитися причиною виходу з ладу банківської системи, системи життєзабезпечення в лікувальних установах, систем навігації літаків, кораблів і т.п.

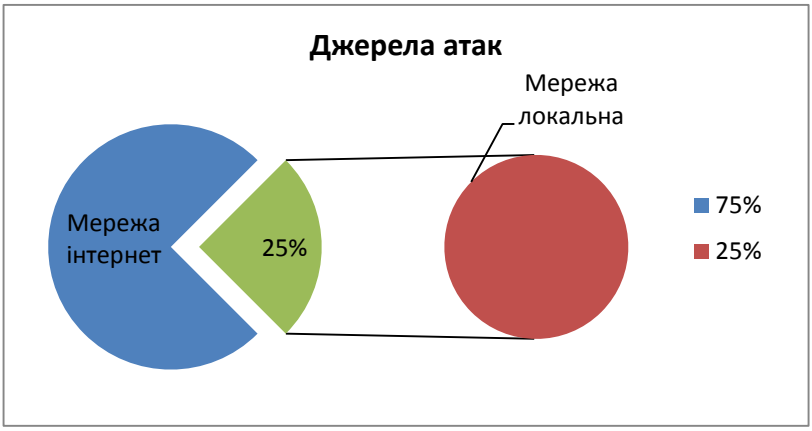


Рис. 3. Джерела атак на локальний комп'ютер

Кримінальний кодекс передбачає покарання за внесення вірусу на комп'ютерні системи, навіть якщо вірус не спрацював

або не встиг спрацювати. Покарання за будь-який вид умисного розповсюдження вірусу, будь то продаж програми з вірусом, дарування, обмін чи таємне внесення в систему. Те, що ваш комп'ютер працює нормально, ще не означає, що він не заражений вірусами. Можливо, комп'ютер тільки починає «хворіти» і симптоми зараження будуть помітні тільки досвідченим користувачам. Можливі як вихід з ладу програм на даному комп'ютері, так і пошкодження апаратних частин комп'ютера (жорсткий диск). Варіантів вірусів може бути безліч. На сьогоднішній день відомі сотні типів вірусів і десятки тисяч видів вірусів. Від найпростіших, які уповільнюють роботу комп'ютерів, до складних, що вносять серйозні пошкодження і повністю паралізують роботу.

На рис.4 подано реалізовані атаки у системі OSI.

Рис. 4. Реалізовані атаки у системі OSI

Вочевидь, що проти вірусів прийняті надзвичайні заходи, що призвели до створення захисних програм. Антивірусні програми можна розділити на три види:

- фільтруючі, що перешкоджають проникненню вірусу на комп'ютер;
- проти інфекційні, що контролюють роботу додатків в системі;
- противірусні, що здійснюють пошук вірусів серед файлів комп'ютера і здійснюють «лікування файлів».

Однак, зауважимо, що віруси спочатку з'являються, а вже потім спеціальні антивірусні лабораторії шукають «вакцину» проти даного конкретного вірусу. Так що, використовуючи останню версію антивірусного пакету, ви можете бути захищені тільки

від тих видів вірусів, які були відомі творцям пакету на момент виходу. А від сотень вірусів, написаних пізніше, не завжди можна вберегти свій комп'ютер. Можна акуратно управляти своїм транспортним засобом, не заважаючи оточуючим, але існує ймовірність по необережності викликати серйозну дорожньо-транспортну пригоду, що спричинить тяжкі травми людей, так і в комп'ютерних системах.

Однак, при використанні комп'ютерної техніки існує одна особливість. Практично неможливо розробити алгоритм вирішення задачі, а вже тим більш програмно реалізувати його, без якихось дрібних помилок і неточностей. Помилки реалізації виявляються на етапі налагодження програми, та й то не завжди вони виключаються повністю. І якщо, наприклад, при будові якихось споруд (мостів, доріг, будинків) розрахунки ведуться з певним запасом надійності, то у сфері програмування така надійність дуже умовна. Сутність даного виду комп'ютерної злочинності полягає в наступному. Розробник програмного продукту замість, наприклад, побудови математичної моделі об'єкта, з метою отримання якихось вихідних параметрів, просто імітує отримання цих параметрів. Це може бути у випадку, коли об'єкт не відповідає вимогам, які накладаються на нього, а запуск виробництва цього об'єкта дуже важливий для третьої особи. Ну і до того ж, розробити математичну модель складніше, ніж просто зімітувати вихідні дані.

Як висновок, що захист інформації в комп'ютерних системах – процес особливо важливий і актуальний як для підприємств, наукових організацій, так і для правоохоронних структур, які працюють з важливою інформацією та розслідують кіберзлочини.

1. Матеріали сайту Вікіпедії [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki
2. Матеріали сайту Лабораторії Касперського [Електронний ресурс]. – Режим доступу: http://portalsafety.at.ua/news/laboratorija_kasperskogo_v_marte_2014_zapustila_globalnuju_kartu_kiberatak_prognoz_kiberatak_2014/2014-03-28-4072
3. Статистика кібератак для Android: угроза реальна [Електронний ресурс]. – Режим доступу: http://galaxy-droid.ru/6063-statistika-kiber-ugroz-dlya-android-ugroza-realna.html

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

АНАЛІЗ РЕФОРМУВАННЯ СИСТЕМИ ОСВІТНІХ ПОСЛУГ ДЕЯКИХ КРАЇН ЄВРОПИ В КОНТЕКСТІ НАСТАНОВ БОЛОНСЬКОГО ПРОЦЕСУ

Кулешник Ярема Федорович,
професор кафедри інформатики ЛьвДУВС, к.т.н., доцент
Рудий Тарас Володимирович,
доцент кафедри інформатики ЛьвДУВС, к.т.н., доцент
Брилич Мар'яна Тарасівна,
студентка магістратури ЛьвДУВС
Харченко Ярослав,
студент ЛьвДУВС

Зовнішні фактори, обумовлені комплексом політичних, економічних і соціальних чинників на світовому, європейському і національному рівнях, а також об'єктивні внутрішні зміни безпосередньо у сфері вищої освіти кожної країни, є основою становлення єдиного європейського освітнього простору в цілому, та виникнення Болонського процесу зокрема.

Європейська інтеграція у вищій освіті на наднаціональному рівні обумовлена характерними для кінця XX століття тенденціями цивілізаційного розвитку – посиленням процесів глобалізації та становленням суспільства, заснованого на знаннях. Намагання вирішити освітні проблеми у межах окремих держав, не приводить до їх повного усунення. У зв'язку з цим виникає потреба в об'єднанні зусиль для подолання становища, що склалося у вищій школі, на наднаціональному рівні.

Розвиток Болонського процесу базується на двох основних принципах. Перший полягає в досягненні високої якості європейської вищої освіти, що є необхідною умовою підвищення її

конкурентоспроможності та привабливості [10]. Другий принцип полягає в розвитку академічної мобільності, що дозволяє ефективно використовувати досягнення кожної з країн-учасниць процесу й повною мірою реалізовувати ідею об'єднаної Європи. Інші положення Болонського процесу – введення багаторівневої вищої освіти, застосування системи взаємозаліку кредитних одиниць, використання європейського додатку до диплома – є, по суті, інструментами досягнення перших двох принципів Болонського процесу.

Зміна системи надання освітніх послуг у будь-якій країні вимагає внесення змін у внутрішні законодавства та освітні стандарти цих країн.

Стандарти освіти є істотним елементом будь-якої національної системи освіти, тип якої визначається політичними, соціально-економічними умовами, традиціями певної країни тощо. У свою чергу тип системи освіти впливає на функції, вид та структуру освітніх стандартів. Але незалежно від цього на підставі загальних підходів до стандартизації національні стандарти за ознаками компетенції розроблюються та затверджуються на рівні держави, галузі або організації [9, С.69].

На початок Болонського процесу структура вищої школи ФРН була представлена однорівневою до дипломною освітою і дворівневою підготовкою наукових кадрів; функціонування вузів традиційно знаходиться у сильній залежності від державної влади, що виявляється у фінансуванні і різних формах контролю – і ця обставина виступає гарною аналогією для порівняння з українською. Болонський процес обумовлює початок нової хвилі реформування німецької системи вищої освіти. Вона цілком і повністю визначається принципами та положеннями процесу створення загальноєвропейського освітнього простору, проте, впровадження настанов Болонського процесу у вищій школі ФРН виступає не запереченням, а відновленням традицій класичної вищої освіти згідно концепції Гумбольдта, яка визначає ідеал університету як такий, що заснований на самоврядуванні, свободі навчання й на поєднанні навчання та наукової діяльності. Саме завдяки таким фундаментальним ознакам, цей ідеал визначає основи також і сучасної, конкурентоспроможної, універсальної та фундаментальної вищої освіти. Втілення болонських принципів у

ФРН починається зі зміни відповідного законодавства і призводить до глибоких перетворень у вищій школі, до трансформації основ її функціонування. Відбувається перегляд базисних установок щодо забезпечення єдності освітнього простору Німеччини: здійснюється впровадження стандартизованого порядку проведення іспитів, що гарантує спільність учбових програм і присуджуваних ступенів у різних землях. Створюється відсутня до того в ФРН система оцінки якості вищої освіти. Вона ґрунтується на взаємодії двох складових – експертизи й акредитації. Сформована інфраструктура органів і установ, що здійснюють оцінку, регламентований порядок проведення кожної з процедур, затверджені стандарти освітніх програм. Встановлено, що специфіка Німеччини полягає в домінуванні оцінки якості окремих навчальних програм над загальною діяльністю вузів – остання має місце переважно в недержавних вищих навчальних закладах. Здійснюється перехід до трирівневої системи вищої освіти: «бакалавр» – «магістр» – «доктор». Основу багаторівневої освіти складає модульна організація освітнього процесу та використання залікових одиниць за системою ECTS, що дозволяє розв'язати головну проблему вищої школи ФРН – забезпечити скорочення термінів навчання. Специфіка Німеччини в цьому аспекті полягає в тому, що введення бакалаврату і магістратури не розповсюджується на спеціальності загальнодержавного значення (такі як медицина, педагогіка, технологія харчової промисловості, фармація, юриспруденція).

Аналіз наслідків окремих аспектів впливу Болонського процесу в країнах Балтії також має велике значення для послідовного вивчення системних змін, що відбуваються в цих державах, і одночасно – особливостей проявів тенденцій глобалізації, інтеграції та локалізації в освітній сфері, взаємного впливу державного управління та вищої освіти в даному контексті.

Співробітник «Центру оцінки якості вищої освіти» Латвійської Республіки Ю. Дзелме у своїх наукових працях підкреслює, що зміни в політичній системі Латвії в середині 90-х років зробили популярною ідею академічної свободи та автономії навчальних закладів. Вчений вказує на те, що у подальшому стало зрозумілим: університети не можуть нести повну відповідальність за свою діяльність, а захист споживачів (студентів) у процесі

надання освітніх послуг виявився не менш важливим, аніж захист академічної свободи університетів [3, с. 20].

В рамках Болонського процесу в Латвії (як і в Литві та Естонії) реалізовано трирівневу систему освіти (бакалавр – магістр – доктор), терміни якої визначено у Законі «Про вищу школу», де передбачено узгодження бакалаврських та магістерських програм з Державним стандартом академічної освіти. В умовах розвитку багаторівневого навчання постає питання про створення та реалізацію національних програм підготовки на рівні бакалавра та магістра відповідно з європейськими вимогами до нових перспективних напрямів і спеціальностей.

Вчені виділяють певні недоліки, що притаманні литовській освіті, а саме: вища освіта заснована на ідеях прагматизму, а не гуманізму (її розвиток спрямовано на потреби роботодавця, а не на суспільні інтереси); цілі професійної освіти формулюються на основі соціального замовлення, тому своєрідність індивідуальності студентів часто обмежена; нестабільний і динамічний розвиток ринку праці обмежують забезпечення потреб більшої частини студентів; не створюються умови самостійного пошуку професії та кар'єри самим студентом; педагогічна діяльність викладачів вузів обмежена сформульованими на основі епістемології цілями навчання (головна увага приділяється не студенту, якого повинні готувати до життя, а предмету, що викладають); недостатньої уваги приділяється стимулюванню пізнання студентами самих себе, пошуку єдності цінностей особистості і світу [4, с. 133-135].

О. Барчкуте, Б. Галінене, А. Марчінскас, А.-В. Матуліоніс досліджували питання розвитку університетської освіти Литви, яка характеризується достатньо високими показниками класичної освіти серед інших країн Балтії, в той же час маючи найнижчий рівень освіченості. Поступово ситуація змінюється, й університетська освіта трансформується, що пов'язано з демократизацією вищої освіти та її доступністю широким верстам населення. Сучасні університети за підтримки уряду стають науковими центрами, але мають інші нові проблеми: не вистачає матеріальної підтримки у вигляді державного фінансування університетів, держава обмежує їх автономність, губиться соціальний статус викладачів, вартість навчання підвищується тощо.

Незважаючи на зазначені проблеми, литовським університетам вдалося зберегти достатньо високий рівень наукового потенціалу й одержати більшу аніж за радянських часів автономію. З 1991 р. п'ятирічна модель навчання у вищій школі перетворилась на чотирьохрічну підготовку бакалавра та дворічну підготовку магістра. Однак за такої моделі Литва не змогла досягти рівня британської, німецької або американської освіти. Проголошення гарантії безкоштовної вищої освіти для добре встигаючих студентів у Литовській Конституції (з 1992 року) на практиці фактично не реалізується. Коли Литва стала суб'єктом європейського університетського простору, відбулось порушення балансу між правами та відповідальністю за якість освіти освітніх закладів через вплив держави на управління університетами. На сьогодні заробітна плата педагогів Литви найнижча не тільки у Балтійському регіоні, але й у інших країнах ЄС [8, с. 75-78].

Відомі науковці Х. Бауман [2] та І. Калакаускас [1], досліджуючи систему вищої освіти Естонії, розглядають діючу систему держзамовлення на підготовку спеціалістів. За їхньою оцінкою Міністерство освіти Естонії щорічно заключає договори з університетами про підготовку визначеної кількості фахівців на певний термін, а також фінансує їхнє навчання. Але кількість «бюджетних місць» у державних ВНЗ щороку дедалі скорочується. Із кожним роком вступ до університету дедалі менше розцінюється в суспільстві як успіх абітурієнта, оскільки зберігається дисбаланс між потребами суспільства в тих або інших професіях і здатністю ВНЗ навчити цим професіям швидко і якісно. Як і в інших країнах Балтії, першою стадією вищої освіти є підготовка бакалаврів, другою – магістрів, а третьою – докторів. По закінченні кожної стадії присвоюються такі кваліфікації: перша стадія – диплом про прикладну вищу освіту, диплом ступеня бакалавра; друга стадія – ступінь магістра або диплом з певної спеціальності (медицина, ветеринарія, стоматологія, фармація, архітектура), де існують свої правила, а ступінь магістра не видається; третя стадія включає ступінь доктора.

Результати впровадження Болонських рішень в прибалтійські системи вищої освіти характеризуються: успішною реалізацією всіма вузами Латвії, Литви та Естонії переходу до

системи трьох освітніх рівнів, запровадженням європейських додатків до дипломів; створення системи забезпечення і контролю якості вищої освіти; реалізацією механізмів обов'язкової участі студентів у діяльності ВНЗ, в частині організації та навчання і оцінці його якості; зростанням рівня мобільності студентів, академічного та адміністративного персоналу вузів, яка майже досягла середньоєвропейських показників; введенням в дію національних систем оцінки обсягів навчальної роботи в кредитах і поступовим переходом від національних систем кредитів до системи кредитів ECTS.

На сучасному етапі основні стимули зміни державної політики країн Балтії у сфері вищої освіти багато в чому виходять від міжнародних інституцій та організацій (ЮНЕСКО, Рада Європи). Вузівське та наукове співтовариство Латвії, Литви та Естонії, будучи толерантним до освітніх реформ, тим не менш, не являється групою, що форсовано їх лобіює, незважаючи на те, що в державних структурах країн Балтії відсоток представників освіти і науки досить значний. Причиною цього є розуміння складності реформ і тих небезпек, які стоять за різкими трансформаціями освітньої сфери [5, с. 13].

Процеси реформування вищої освіти країн Балтії показали складні проблеми пострадянського періоду розвитку, якими стали:

- скорочення бюджетного фінансування;
- нерівність доступу до вищої освіти в силу поширення його «комерціалізації»;
- зниження питомої ваги і якості фундаментальних навчальних дисциплін у програмах підготовки;
- зниження частки громадян, які навчаються за магістерськими і докторськими програмами;
- зростання безповоротної академічної мобільності за межі національних кордонів;
- різке зростання кількості ВНЗ, у тому числі, недержавних (у регіоні діють дев'яносто вищих навчальних закладів, з яких п'ятнадцять є багатопрофільними університетам);
- зниження рівня вимог до підготовки у вищій школі, з боку студентів і суспільства, у зв'язку з екстенсивним етапом розвитку освітньої системи та неефективністю самого процесу

реформування, в ході якого через масштабність перетворення упускаються окремі аспекти, що і веде до зниження якості (подолання цих викликів передбачає визначення збалансованої державної політики у сфері освіти, яка передбачає, в тому числі, якісне вдосконалення законодавчих та інших загальнодержавних регуляторів);

- послаблення ролі держави в освітній політиці;
- захоплення орієнтованими на ринкові умови освітніми проектами;

Погодьтеся, що більша частина цих недоліків та проблем притаманна і українській системі освіти.

Франція була однією з перших країн, яка разом з Англією, Італією і Німеччиною започаткували Болонський процес. Цей процес перебудови вищої освіти триває у Франції вже понад 37 років. Тому важливим є завдання виявити ті зміни у змісті університетської освіти Франції, які відбуваються в контексті сучасних європейських реформ. Якщо проаналізувати закони та міністерські циркуляри, які регламентували університетську освіту у Франції в другій половині XX – на початку XXI ст., то стає очевидним, що в реформуванні можна виділити чотири етапи, а саме: децентралізація; створення європейських університетських полюсів, що посилювали роль регіонів у формуванні освіти; уведення професійних ліцензій; створення трьох рівнів у системі вищої освіти та зарахування здобутих знань та навичок на основі кредитів [11, С.28].

Важливу роль у розвитку вищої освіти відіграли закони про децентралізацію 1983 та 1985 рр. Під їхнім впливом університети поновили своє функціонування, нову роль отримали регіони щодо підтримки досліджень університетських утворень. Завдяки цим законам регіони набули право фінансувати університети, що значно доповнило державне фінансування. Воно здійснюється в тих галузях, у яких зацікавлені регіони. Внаслідок дії згаданих законів держава зберегла відповідальність за вищу освіту, проте відбулася передача регіонам компетенції та відповідальності за професійну освіту, що у свою чергу спричинило введення професійних ліцензій, яке характерне для третього етапу реформування університетської системи вищої освіти Франції.

Децентралізації вищої освіти стосувався також закон від 10 липня 1989 р. Головна інновація його полягає в утворенні університетських інститутів з підготовки вчителів. Це були також автономні заклади, пов'язані через угоди з університетами та зобов'язані готувати вчителів першого і другого рівнів.

Створення в 1991 р. університетських європейських полюсів означає другий етап реформування університетської освіти Франції, що гармонійно пов'язаний із попереднім і є його наслідком. Вони ставлять за мету розробити регіональну політику.

Третій етап реформування університетської освіти розпочався уведенням професійних ліцензій у 1999 р. Він був спричинений звітом Атталі і впроваджений міністром освіти Клодом Аллегром. Професійні ліцензії представлені як еквівалент до традиційного ліценціата. Для отримання цього диплома студент повинен пройти стажування на підприємстві. Парадокс в тому, що він займає місце оплачуваного робітника, але при цьому не одержує зарплати.

У 2002 році реформою LMD/ECTS (Ліценціат, магістратура, докторат/Європейська система трансформаційних кредитів) розпочався четвертий етап реформування університетської освіти Франції. Жак Ланг оголосив у квітні 2001 р. про видання дипломів на основі накопичувальних кредитів. 23 квітня 2001 р. він подав до CNESER (Національна рада з питань вищої освіти та дослідження) проект нових реформ вищої освіти.

Таким чином, створення єдиного європейського освітнього простору, гармонізація національних СВО не можливі без розроблення процедури визнання, що прийнятна для усіх європейських країн, – «офіційного підтвердження уповноваженим органом значущості іноземної освітньої кваліфікації з метою доступу її власника до освітньої та/або фахової діяльності» [12]. У свою чергу прийняття рішення про визнання має ґрунтуватися на результатах процедури встановлення еквівалентності освітніх стандартів, тобто академічних кваліфікацій, навчальних курсів, дипломів, свідоцтв тощо.

Висновки. Розроблення прийнятної для всіх країн-учасниць Болонського процесу, процедури встановлення еквівалент-

ності освітніх стандартів, тобто академічних кваліфікацій, навчальних курсів, дипломів, свідоцтв тощо, неможливе без гармонізації вимог системи стандартів ВО України зі стандартами фахових асоціацій та вимогами професійних спілок європейських країн і освітніх стандартів провідних університетів за прийнятими в Європі критеріями, механізмами та методами оцінювання якості фахової підготовки та освіти.

Дослідження результатів вступу країн Балтії, Німеччини та Франції в Болонський процес, на основі аналізу реформ освіти, є актуальними не тільки для більш повного розуміння соціально-політичних механізмів перетворень в цих країнах, але й для прогнозування напрямків подальшого розвитку аналогічних процесів у сучасній Україні.

1. Калакаускас, І. Освіта в Естонії / І. Калакаускас // Упр. освітою. – 2010 – Лют. (чис. 4). – С. 24–25.
2. Бауман, Х. Система высшего образования в Эстонии / Х. Бауман // Альма матер. Вестн. высш. шк.– 2004. – № 1. – С. 33–36.
3. Дзелме, Ю. Структура системы гарантии качества высшего образования в Латвии / Ю. Дзелме // Альма матер. Вестн. высш. шк. – 2004. – № 1 – С. 17–22.
4. Думчене, А. О сочетании прагматических и гуманистических цінностей студентов / А. Думчене. С. Даукилас // Социол. исслед. Социс. – 2007. – № 5. – С. 132–136. – Библиогр.: 11 назв.
5. Никифоровс, Н. В. Политические аспекты Болонского процесса на примере Латвии, Литвы и Эстонии [Электронный ресурс] : автореф. дисс. ... канд. полит. наук : 23.00.04 / Никифоровс Никита Валерьевич ; Моск. гос. ин-т междунар. отношений. – Электрон. дан. – М., 2010. – 30 с.
6. Розвиток міжнародного співробітництва в галузі освіти у контексті Болонського процесу : [матеріали міжнар. наук.- практ. конф., 15–16 берез. 2007 р., Ялта] / МОН України, АПН України, Ун-т Ніцца-Софія антиполіс, Вища катол. шк. Намюра [та ін.]. – Ялта, 2007. – С. 184–191. – Библиогр.: 3 назв.
7. Симаева, И. Н. Модернизация образования и науки в России, Польше и Литве : сравнительный анализ / И. Н. Симаева, Т. Ю. Кузнецова, М. И. Короткевич // Балтийский регион. – 2011. – № 2. – С. 95–101. – Библиогр.: 20 назв.
8. Университетское образование в Литве в контексте трансформации / О. А. Барчкуте, Б. А. Галинене, А. Ю. Марчинскас, А.-В. А.

Матулионис // Социол. исслед. Социс. – 2007. – № 10. – С. 75–80. – Библиогр.: 5 назв.
9. Проблеми освіти: Наук.-метод.зб. / НМЦ ВО МОН України. – К., 2005. – Вип.45: Болонський процес в Україні. – Ч.1. – 192 с.
10. Конференція міністрів, відповідальних за вищу освіту, 19 травня 2005 р. м. Берген.
11. Шлях освіти. – 2007. – № 4. – 56 с.
12. Конвенція щодо визнання кваліфікацій з вищої освіти в європейському регіоні / Рада Європи та ЮНЕСКО. – Лісабон, 1997.

МОДЕЛЮВАННЯ ДІЙ ПІДРОЗДІЛІВ МІЛІЦІЇ В НАДЗВИЧАЙНИХ СИТУАЦІЯХ З ВИКОРИСТАННЯМ КОМП'ЮТЕРНОГО СИМУЛЯТОРА

Сеник Володимир Васильович,
начальник кафедри інформаційних технологій у діяльності ОВС та економічної безпеки ЛьвДУВС, к.т.н., доцент

За період незалежності України правоохоронні органи, у тому числі органи внутрішніх справ, залишили за собою, успадковану з часів Радянського Союзу, мілітаризовану модель діяльності, що у свою чергу активно впливало на усі сфери її роботи. Особливо помітним таке успадкування проявлялося під час охорони громадського порядку, яке було зорієнтоване на жорстке реагування в умовах масових заворушень. Поведінка спеціальних підрозділів міліції під час таких заворушень носила характер притаманний скоріш військовим аніж поліцейським підрозділам. Наочно це проявилося під час подій Євромайдану, коли силові акції спецпідрозділів міліції та внутрішніх військ спричинили тілесні ушкодження значній кількості учасникам мирного зібрання та журналістам. При цьому МВС продовжувало вважати себе активним борцем зі злочинністю, успішність якого не залежала від підтримки населення, а ефективність роботи оцінювалась морально застарілою системою кількісних показників боротьби зі злочинністю. В результаті лише 2013 році МВС отримало близько 195 тисяч звернень громадян стосовно неправомірних дій правоохоронців (1). Певні спроби змінити порядок обчислення кількісних показників у роботі міліції успіху не мали.

В результаті рівень довіри громадян до міліції після подій Євромайдану, за даними Інституту соціології Національної академії наук України, впав до 0,8% опитаних. При цьому довіра самих працівників міліції до влади традиційно не перевищувала 3% (1). Причинами такої тотальної недовіри владних структур одна до одної, як і вкрай низького кредиту довіри населення до правоохоронців, стали системні недоліки в діяльності МВС України.

В той же час, визначений курс до Євросоюзу, висунув перед Україною завдання реформування органів внутрішніх справ у професійний деполітизований і ефективний інститут, заснований на принципах верховенства права, ринкової економіки і толерантності стосовно культурних, релігійних та етнічних груп. Як результат, перелік завдань для органів внутрішніх справ необхідно розширити наступними положеннями:

- встановлення ефективного громадського контролю;
- демократична та ефективна система підзвітності суспільству;
- партнерські відносини із населенням;
- професіоналізм персоналу,
- вироблення професійної етики;
- підвищення рівня диверсифікованості персоналу для кращого відображення етнічної та гендерної структури населення;
- постійний зв'язок з поліцейськими підрозділами інших держав.

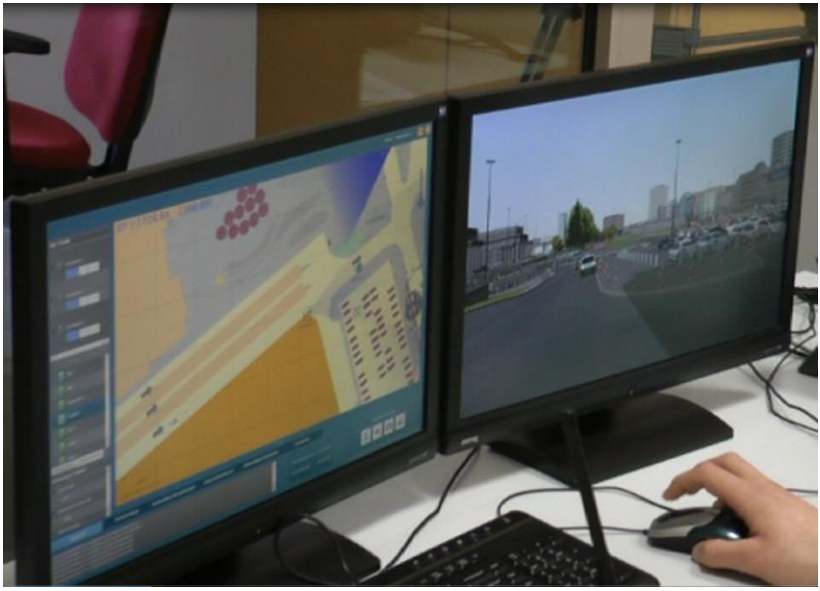
Для більшості європейських поліцейських систем досягнення означених вимог стало можливим за умови реформування, яке відбувалось за декількома провідними принципами, одним із яких є професійна підготовка персоналу.

Зрозумілим є те, що система освіти МВС, побудована сьогодні за ступеневим принципом, також потребуватиме реформування у відповідності до вимог сьогодення. Не останнім у цьому плані є обмін досвідом з іншими європейськими поліцейськими навчальними закладами щодо створення нових програм підготовки фахівців.

З цією метою у кінці листопада 2014 року група фахівців Львівського державного університету внутрішніх справ відвідала Вищу школу поліції в м. Щитно (Республіка Польща), де, окрім

ознайомлення з матеріально-технічною базою, бібліотечним фондом, навчальними програмами, особливу увагу приділила вивченню сучасного комп'ютерного симулятора поліцейських операцій в надзвичайних ситуаціях, а також можливості адаптації його до умов українського законодавства, навчання працівників ОВС (зокрема, створення відповідних курсів для керівників міліції громадської безпеки).

Даний симулятор дозволяє моделювати такі надзвичайні ситуації, як масові заворушення, захоплення заручників, закладення вибухівки у приміщення тощо. Також події можуть ускладнюватися іншими факторами, наприклад, пожежею. При цьому керівники штабу міліції громадської безпеки можуть для ліквідації надзвичайної події задіювати служби дорожньої поліції, надзвичайних ситуацій, давати вказівки щодо застосування спецзасобів та ін. На рис. 1-5 представлені зображення, які дозволяють отримати уявлення про даний симулятор.



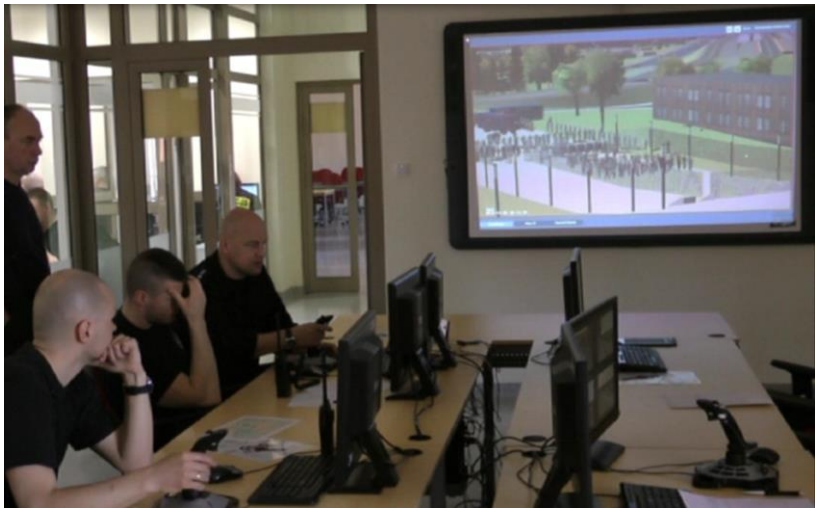


Рис. 1-6. Симулятор дій поліцейських в надзвичайних ситуаціях

Враховуючи можливості даної програми, її оцінку польськими поліцейськими-практиками та науковцями, недостатність практичних навичок дій у надзвичайних ситуація наших керівників міліції громадської безпеки, зрештою, вимоги сьогодення

щодо реформування органів внутрішніх справ, група науково-педагогічних працівників Львівського державного університету внутрішніх справ під керівництвом ректора вважає за доцільне вийти з ініціативою перед МВС України, щодо впровадження подібного симулятора поліцейських операцій в надзвичайних ситуаціях у навчальний процес Львівського державного університету внутрішніх справ та створення відповідних курсів підвищення кваліфікації для керівників усіх ланок міліції громадської безпеки.

РОЛЬ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ В ОРГАНІЗАЦІЇ НАВЧАЛЬНО-ВИХОВНОГО ПРОЦЕСУ ВИЩОЇ ШКОЛИ

Чорномаз Оксана Богданівна,
доцент кафедри адміністративного права та адміністративного процесу ЛьвДУВС, к.ю.н., доцент

Досягнення у сфері комп'ютерних технологій та телекомунікацій, масова комп'ютеризація та розвиток ефективних інформаційних технологій привели на порозі третього тисячоліття до якісної зміни інформаційної складової розвитку сфер виробництва, науки, соціального життя. Інформація, тісно пов'язана з управлінням та організацією, перетворилася в глобальний ресурс людства, багаторазово збільшуючи його потенційні можливості в усіх сферах життєдіяльності.

Одним із пріоритетних напрямків інформатизації суспільства стає процес інформатизації освіти, який передбачає використання можливостей нових інформаційних технологій, методів та засобів інформатики для реалізації ідей розвиваючого навчання, інтенсифікації усіх рівнів навчально-виховного процесу, підвищенню його ефективності і якості, підготовку студентів до комфортного (як в психологічному, так і в практичному відношенні) життя в умовах інформатизації суспільства [8, с.32].

Швидке і невпинне зростання обсягу знань, яким володіє людське суспільство, вдосконалення технологічних та соціальних процесів зумовлює потребу звернути увагу на проблеми освіти.

Нове інформаційне суспільство вимагає від фахівців нових умінь та знань. Україна задекларувала свій намір увійти в Європейський освітній простір у травні 2005 року, приєднавшись до Болонського процесу. Зміст та суть принципів Болонського процесу, а також проблеми їх впровадження у вищих навчальних закладах викладені в праці. Наразі наша держава зобов'язана докласти всіх зусиль для приведення національної системи освіти до світових стандартів. Це зумовлює активне використання новітніх інформаційних систем у навчальному процесі для підготовки конкурентоздатних спеціалістів.

Застосування сучасних інформаційних технологій (ІТ) у навчальному процесі вищого навчального закладу потребує змін у методиці викладання дисциплін та оцінювання знань студента. Робиться акцент на розвиток умінь аналізування, зіставлення, оцінювання виявлення зв'язків, планування, групової взаємодії з використанням ІТ. Використання нових технологій під час проведення занять дає можливість забезпечити студентів електронними навчальними посібниками для самостійного опрацювання, завданнями для самостійного виконання та перевірки знань тощо. Збільшення часу самостійної роботи студента відповідає вимогам Болонського процесу.

В інформаційному суспільстві активно створюється та розвивається інформаційно-комунікаційне середовище, створюються умови для ефективного використання знань у розв'язанні найважливіших завдань розвитку суспільства та демократизації громадського життя. Виникають нові види комунікативних здібностей до вибору оптимального режиму роботи з комп`ютером, засвоєнню етикету електронного спілкування, спілкуванню з партнером у віртуальній групі. Відповідно розвивається вміння спілкуватися електронною поштою, вільно орієнтуватися у світі інформаційно-комунікаційних технологій, відбувається перехід від одного програмованого засобу до іншого, оволодіння методами збору та переробки інформації.

В епоху інформаційного суспільства освіта має бути безперервною. Це означає, що людина вчиться постійно, у спеціальних освітніх установах, або самостійно. Забезпечення безперервної освіти є складною проблемою, вирішення якої залежить від

багатьох факторів, зокрема від стану інформаційно-комунікаційного середовища.

Інформаційно-комунікаційне середовище – системно організована сукупність інформаційного, організаційного, методичного, технічного та програмного забезпечення, що сприяє виникненню й розвитку інформаційно-навчальної взаємодії між студентом, викладачем і засобами нових інформаційних технологій, а також формуванню пізнавальної активності студентів за умови наповнення окремих компонентів середовища предметним змістом певного навчального курсу.

В.Ізвозчиков розглядає інформаційно-комунікаційне середовище не як теоретичну абстракцію, а як відповідаючу практичним потребам людини конструкцію, що виступає у трьох основних формах:

- фізичний простір (це простір сумісної навчальної педагогічної та освітньої діяльності з використанням сучасних електронно-комунікативних систем, засобів та технологій освіти населення та навчання;
- віртуальний простір гіпертекстів, семантичних взаємозв`язків понять та тезаурусів;
- ієрархічні педагогічні та освітні системи та простори в категоріях загального (глобальне ІКС), особливого (регіональне ІКС) та одиничного (локальне ІКС) [2, с. 45].

У свою чергу Л.Петухова в своїй монографії подає власне трактування поняття «інформаційно-комунікаційне педагогічне середовище», під яким розуміє сукупність знанієвих, технологічних і ментальних сутностей, які в синхронній інтеграції забезпечують якісне оволодіння системою відповідних знань.

На думку Л.Петухової інформаційно-комунікаційне педагогічне середовище як компонент навчального процесу:

- сприяє формуванню мотивації підростаючого покоління до споживання контенту, що циркулює у ньому;
- надає доступ до ресурсів у будь-який зручний для людини час;
- володіє зручним, гнучким, дружнім, інтелектуальним сервісом, що допомагає людині знайти необхідні інформаційні ресурси, дані або знання;

- функціонує відповідно до запитів людини стільки, скільки їй необхідно;
- забезпечує наявність значного об’єму інформації, що збільшується зі зростаючою швидкістю;
- дозволяє організувати практично безкоштовні, зручні в часі контакти між будь-якою кількістю людей, забезпечити зручний і гнучкий обмін інформацією (причому в будь-якому вигляді) між ними;
- бере на себе все більше рутинних операцій, пов’язаних з операційною діяльністю людини;
- стандартизує й інтегрує функціональність усіх попередніх, нині, так званих, традиційних засобів отримання, збереження, обробки і представлення необхідної людству інформації, даних та знань;
- одержує все більше контролю над даними та операційною діяльністю людства [5].

Впровадження інформаційно-комунікаційних технологій (ІКТ) в освітню систему України та формування єдиного інформаційно-освітнього простору – одні з пріоритетних напрямів сучасної державної політики. Зокрема, в «Національній доповіді про розвиток освіти в Україні» відмічається, що головною метою в контексті створення інформаційного суспільства й освітньо-інформаційного простору є забезпечення доступу до інформації широкого спектру споживання; розвиток та впровадження сучасних комп'ютерних технологій у системи освіти, державного управління, науці та інших сферах; створення в найкоротші строки необхідних умов для забезпечення широкого доступу навчальних закладів, наукових та інших установ до мережі Інтернет; розвиток освітніх і навчальних програм на базі комп'ютерних інформаційних технологій [3].

Під ІКТ розуміють сукупність методів та технічних засобів, які використовуються для збирання, створення, організації, зберігання, опрацювання, передавання, подання й використання інформації.

Про масштаб та комплексність проблеми використання ІКТ у навчальному процесі йдеться в дисертації М.Жалдака [1]. На його думку, широке впровадження нових інформаційних технологій в навчальний процес породжує ряд проблем, які стосуються

змісту, методів, організаційних форм і засобів навчання, гуманітаризації освіти та гуманізації навчального процесу, інтеграції навчальних предметів і фундаменталізації знань, підготовки і удосконалення кваліфікації педагогічних кадрів, створення системи неперервної освіти, зокрема, системи самоосвіти і самовдосконалення вчителів, яка забезпечувала б оволодіння ними основами сучасної інформаційної культури.

Ми поділяємо думку О. Співаковського [6], що використання нових інформаційних технологій навчання у педагогічному вищому навчальному закладі, крім сприяння досягненню основних, запланованих цілей навчання у конкретній предметній галузі, сприяє досягненню і додаткових цілей навчання – формуванню у майбутнього вчителя позитивного відношення до нових інформаційних технологій навчання, переконаності у ефективності цих технологій навчання, практичного засвоєння методів навчання в умовах нових інформаційних технологій навчання. Студенти долають психологічний бар'єр між традиційними формами, методами і засобами навчання і навчанням із застосуванням комп'ютерних засобів набагато швидше, ніж вчителі, що вже мають досвід роботи традиційними методами.

Застосування інформаційних технологій в освіті вносить у розвиток людини різні зміни, які відносяться як до пізнавальних, так і до емоційно-мотиваційних процесів, вони впливають на характер людини, під час цього відзначається підсилення пізнавальної мотивації студентів у процесі роботи з комп’ютером. Використання засобів ІКТ у навчанні сприяє збільшенню частки самостійної навчальної діяльності й активізації студента «формуванню особистості того, кого навчають, через розвиток його здатності до освіти, самонавчання, самовиховання, самоактуалізації, самореалізації» [4, с. 154].

Таким чином, зростання ролі ІКТ у багатьох видах людської діяльності цілком природно спричинює зміни в системі освіти, спрямовані на переорієнтацію навчально-виховного процесу з суто репродуктивних механізмів мислення на заохочення творчої активності студентів, що розвиватиметься на базі належного інформаційного забезпечення.

Глобальне розширення інформаційного потенціалу призвело до реорганізації освіти й забезпечення нового рівня якості

підготовки спеціалістів та формування гнучкої системи підготовки робочих кадрів із швидкою орієнтацією до змінних умов професійної діяльності. Сучасна наука зосереджує увагу на теоретичній розробці концепції й структурно-організаційних моделей комп'ютеризації освіти, тому що на даний момент, через відсутність стабільних позицій у цьому питанні, реальна комп'ютеризація навчального процесу на місцях фактично відсутня.

Використання ІКТ у навчальному процесі може забезпечити передачу знань і доступ до різноманітної навчальної інформації нарівні, а іноді й інтенсивніше й ефективніше, ніж за традиційного навчання.

1. Жалдак М.И. Система подготовки учителей к использованию информационной технологии в учебном процессе: Дис. в форме науч. доклада докт. пед. наук: 13.00.02 / АПН СССР. НИИ содержания и методов обучения. – Москва, 1989. – 48 с.
2. Извозчиков В.А., Соколова Г.Ю., Тумачева Е.А. Интернет как компонент информационной картины мира и глобального информационно-образовательного пространства // Наука и школа. – 2000. – № 4. – С. 42-49.
3. Матеріали виїзного спільного засідання Комітету Верховної Ради України з питань науки і освіти та Консультативної ради з питань інформатизації при Верховній Раді України « Про хід виконання Державної програми «Інформаційні та комунікаційні технології / Ком. Верх. Ради України з питань науки і освіти упоряд.: І. Б. Жиляєв, М. К. Родіонов, А. І. Семенченко, редкол.: К. С. Самойлик (голова) та ін. – К.: СофтПрес, 2007. – С. 53-54.
4. Панюкова С.В. Концепция реализации личностно-ориентированного обучения при использовании информационных и коммуникационных технологий. – М.: Изд-во РАО, 1998. – 120 с.
5. Пєтухова Л.Є. Теоретичні основи підготовки вчителів початкових класів в умовах інформаційно-комунікаційного педагогічного середовища: Монографія. – Херсон: Айлант, 2007. – 200 с.
6. Співаковський О.В. Підготовка вчителя математики до використання комп'ютера у навчальному процесі //Комп'ютер у школі та сім'ї. – 1999. – № 2. – С. 9-11.
7. Науково-дослідна робота студентів як чинник удосконалення професійної підготовки майбутнього вчителя: зб. наук. пр./редкол.: Л.І.Білоусова та ін. – Х.: Віровець А.П. «Апостроф», 2012. – Вип.7. –192 с.

8. Торубара О. М. Застосування новітніх інформаційних технологій в навчальному процесі вищих навчальних закладів / О.М. Торубара. // Вісник Чернігівського національного педагогічного університету. Педагогічні науки . – 2013. – Вип. 108.2. – Режим доступу: http://nbuv.gov.ua/j-pdf/VchdpuP_2013_2_108_20.pdf.

ПЕРСПЕКТИВИ ІНФОРМАТИЗАЦІЇ КРИМІНАЛІСТИЧНОЇ ОСВІТИ У ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ СИСТЕМИ МВС УКРАЇНИ

Дуфенюк Оксана Михайлівна,
доцент кафедри кримінального процесу та криміналістики факультету з підготовки фахівців для підрозділів слідства ЛьвДУВС, к.ю.н., доцент
Кунтій Андрій Ігорович,
викладач кафедри кримінального процесу та криміналістики факультету з підготовки фахівців для підрозділів слідства ЛьвДУВС

Підготовка компетентних фахівців, здатних якісно та ефективно працювати в умовах глобальної інформатизації усіх сфер діяльності суспільства, детермінує необхідність перегляду підходів до організації навчального процесу, методології педагогічної роботи. Втім формування та реалізація інноваційної державної освітньої політики засвідчує проблемний характер впровадження світових цінностей та стандартів у систему національної освіти, що підтверджують і міжнародні рейтинги ARWU і TIMES, за підсумками яких жоден український вищий навчальний заклад досі ніколи не потрапляв до числа кращих 200 чи 500 університетів світу [1, с. 122]. Безумовно, процес удосконалення та модернізації національної освітньої системи не лише забезпечить підготовку кадрів з розвиненим інноваційним мисленням, спроможним генерувати нові нестандартні ідеї, а й стане рушійним засобом забезпечення інтересів держави в глобальному інформаційному світі [2, с. 70]. Актуальність обговорення питань модернізації вищої освіти зростає, коли йдеться про підготовку праців-

ників правоохоронних органів, зокрема фахівців слідчих та оперативних підрозділів, адже в умовах реформування системи МВС закономірними є очікування суспільства бачити компетентного правоохоронця-професіонала нового покоління, що обумовлює посилення уваги до питань його підготовки та професіоналізації.

Основними проблемами криміналістичної підготовки вчені сьогодні відзначають відставання рівня викладання криміналістики від потреб практики, існування суперечностей між вимогами сучасного суспільства до рівня підготовки майбутніх правоохоронців та її реальним станом, низький рівень засвоєння випускниками навчальних закладів необхідних знань, умінь та навичок [3, с.8; 4, с.232; 5, с.59; 6, с.13; 7, с.14]. Доволі часто оснащення злочинності випереджає можливості протидії їй, якими володіють правоохоронні органи. Однак доречно зауважити, що існує об'єктивна тенденція значного збільшення об'єму знань, швидких темпів його старіння, тому справедливими є зауваги вчених про те, що ні у школі, ні в найкращому університеті неможливо навчити людину на все життя [8, с.22; 9, с.233].

Інформатизація криміналістичної освіти (далі − ІКО) здатна сформувати методологічний фундамент підвищення якості освітнього середовища та формування належних умов підготовки працівників органів досудового розслідування, працівників оперативних підрозділів, яким доведеться працювати в умовах інформатизованого кримінального провадження. Реалізація ІКО передбачає імплікацію дидактично-методичного, матеріально-технічного, кадрового та методологічного компонентів.

Дидактично-методичний компонент передбачає наявність бінарного дидактичного комплексу курсанта (студента, слухача) та методичного комплексу викладача криміналістичних навчальних дисциплін, розрахованого на впровадження та застосування інформаційно-технологічних засобів навчання та управління. До таких засобів відносимо вербальні, графічні, електронні матеріали, презентації для сенсорної дошки, мультимедійного обладнання, педагогічні програмні засоби навчального призначення, засоби моніторингу навчання, оцінювання якості навчально-виховного процесу, засоби забезпечення дистанційного навчання, організації самостійної роботи тощо.

Матеріально-технічний компонент передбачає наявність технічних засобів, пристроїв, апаратів, які забезпечують здобуття курсантами (студентами, слухачами) криміналістичних знань, умінь та навиків діяльності в умовах, наближених до реальної обстановки. Йдеться про створення інтерактивних тренажерів, тренувальних полігонів, прототипів автоматизованих пошукових систем, автоматизованих робочих місць, програмно-апаратних комплексів. Майбутні фахівці органів досудового розслідування та оперативних підрозділів повинні апробувати у навчальному процесі прототипи цих технологічних систем, ознайомитись із механізмом їх функціонування. Типовими напрямами використання інноваційних технологій у ході кримінального провадження є робота з криміналістичним обліками, інформаційно-пошуковими системами, одержання формалізованих знань з усіх видів баз даних; здійснення статистичного, порівняльного, математичного аналізу подій та фактів; побудови суб'єктивних портретів осіб; фіксації криміналістичної інформації (складання планів, схем, карт, діаграм, графіків, таблиць); графічного моделювання події кримінального правопорушення з допомогою спеціальних програмних продуктів; демонстрації стимульного матеріалу для актуалізації ідеальних слідів у пам'яті учасників кримінального процесу; застосування геоінформаційних технологій (використання баз даних, які дають змогу визначати де і в якому місці перебувають об'єкти криміналістичного обліку) [10, с.196; 11, с.131; 12, с.299].

Кадровий компонент передбачає наявність професорсько-викладацького персоналу вищого навчального закладу, здатного ефективно, системно впроваджувати інформаційні технології у навчальний процес. Професіограма сучасного педагога передбачає існування таких якостей як впевненість у корисності впровадження інформаційних технологій на різних етапах навчально-виховного процесу, уміння працювати на персональному комп'ютері, знання можливостей периферійних пристроїв, уміння орієнтуватися в різноманітних програмних середовищах, уміння опановувати засоби розробки педагогічних програм, використання електронних засобів навчального призначення, уміння розробляти та підтримувати веб-ресурси, уміння працювати в мережі

Інтернет [13, с.84]. Педагог-криміналіст крім того повинен володіти навиками роботи з програмними продуктами, які використовуються у досудовому розслідуванні.

Методологічний компонент передбачає наявність концептуального підходу до інформатизації криміналістичної освіти, метою якої є формування методологічних засад перетворення навчального середовища криміналістичної підготовки фахівців правоохоронних органів в інформаційно-технологічну систему, яка забезпечить здобуття необхідних знань, умінь та навичок збирання, систематизації, обробки, використання криміналістично значимої інформації, з метою оптимізації процесу виявлення та розслідування кримінальних правопорушень.

Підсумовуючи сказане, можна висновувати, що реалізація ІКО має важливе значення, оскільки передбачає формування спеціальної стратегії впровадження новітніх технологій у навчальний процес, створює передумови формування ІТ–компетентного працівника правоохоронного органу, здатного ефективно застосовувати здобуті знання у практичній діяльності досудового розслідування.

1. Приходько В.В. Інноваційна реформа вищої освіти в сучасній Україні / В.В. Приходько. – Дніпропетровськ : Пороги, 2010. – 454 с.
2. Бірюк О.О. Глобалізація, реформи національних систем вищої освіти та професіоналізація педагогічних працівників / О.О. Бірюк // Правничий університет «Крок». – 2011. – Вип. 7. – С. 67−71.
3. Алексєєв О.О. Оптимізація криміналістичної підготовки слідчих в системі МВС України : автореф. дис. … канд. юрид. наук / О.О. Алекєєв. − Київ : [б.в.], 2004.− 19 с.
4. Кубарєв І.В. Проблеми криміналістичної підготовки курсантів / І.В. Кубарєв // Підготовка працівників міліції (поліції) : державні та міжнародні стандарти : матеріали міжнародної науково-практичної конференції (м. Донецьк, 28 квітня 2011 р.). − Донецьк : ДЮІ ЛДУВС ім. Е.О. Дідоренка, 2011. – С. 231−232.
5. Строков І.В.Правові та моральні засади застосування криміналістичних засобів / І.В. Строков. – К.: РВЦ НАВС України. – 2003. – 325 с.
6. Удовенко Ж.В. Криміналістичне забезпечення процесу доказування на досудовому слідстві : автореф. дис. … канд. юрид. наук / Ж.В. Удовенко. − К. : [б.в.], 2004. – 16 с.

7. Шерман М.І. Теоретичні та методичні основи професійної комп'ютерно-інформаційної підготовки майбутніх слідчих у вищих навчальних закладів МВС України автореф. дис. … д-ра пед. наук / М.І. Шерман. − Київ : [б.в.], 2010.− 44с.
8. Козяр М.М. Формування графічної діяльності студентів вищих технічних закладів освіти засобами комп'ютерних технологій / М.М. Козяр. – Рівне: НУВГП, 2009. – 280 с.
9. Мусієнко І.І. Деякі питання криміналістичної підготовки співробітників правоохоронних органів в умовах інноваційного суспільства / І.І. Мусієнко // Питання боротьби зі злочинністю. – 2011. – Вип. 21. – С. 232−236.
10. Шепітько В.Ю. Авдєєва Г.К. Інформаційні технології в криміналістиці та слідчій діяльності / В.Ю. Шепітько, Г.К. Авдєєва // Питання боротьби зі злочинністю. – 2010. – Вип. 19. – С. 194−202.
11. Затенацький Д.В. Ідеальні сліди в криміналістиці (техніко-криміналістичні та тактичні прийоми їх актуалізації) / Д.В. Затенацький ; за ред. В.Ю. Шепітька. – Х.: Право, 2010. – 160 с.
12. Бірюков В.В. Теоретичні основи інформаційно-довідкового забезпечення розслідування злочинів / В.В. Бірюков. – Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка, 2009. – 664 с.
13. Карташова Л.А. Система навчання інформаційних технологій майбутніх вчителів суспільно-гуманітарних дисциплін / Л.А. Карташова. − Київ : Київський національний лінгвістичний університет, 2011. – 264 с.

ПИТАННЯ СТВОРЕННЯ ЕЛЕКТРОННИХ ПІДРУЧНИКІВ

Чередниченко Віталій Борисович,
старший викладач кафедри соціально-економічних дисциплін Сумської філії ХНУВС

Багато сторіч паперові підручники були єдиним засобом фіксації знань для передачі їх студентам. Зараз університетські бібліотеки пропонують підручники, які були випущені у попередні роки та містять інформацію, частково застарілу ще на час друку книг. Для постійної закупівлі нових підручників з усіх предметів у кількості, достатній для забезпечення кожного студента, потрібні кошти, які вряд чи має будь-який навчальний заклад. Сучасні інформаційні технології можуть вирішити цю

проблему шляхом впровадження «електронних» підручників, які можна постійно оновлювати без суттєвих витрат. Ними може користуватись кожен студент у будь-який час та на необмеженій відстані від навчального закладу. Розглянемо можливу структуру та властивості електронного підручника (Е-підручника).

Найпростішим Е-підручником може бути звичайна книга, відсканована у комп'ютерний файл. У ньому не використані величезні можливості електронних технологій, а обсяг інформації не відрізняється від друкованого підручника.

У «Положенні про електронні освітні ресурси» Міністерства освіти і науки України визначено, що «електронний підручник – електронне навчальне видання з систематизованим викладом дисципліни (її розділу, частини), що відповідає навчальній програмі» [1]. Складові частини Е-підручника та його мультимедійні властивості у цьому документі не визначені.

Позиції різних авторів про складові частини Е-підручника відрізняються мало. Перш за все він повинен містити весь необхідний навчальний матеріал з певної дисципліни. Головні властивості Е-підручників такі: можливість побудови зручного механізму навігації, розвинений пошуковий механізм, наявність практичних завдань, віртуальних лабораторних (практичних) робіт, засобів поточного контролю засвоєння матеріалу, механізмів тестування та підсумкового контролю.

До суттєвих особливостей електронного підручника в порівнянні з друкованим слід віднести: можливість включення мультимедійних блоків, анімаційних фрагментів, різноманітного додаткових матеріалів, які наочно ілюструють положення навчальної дисципліни, моделюють фізичні і технологічні процеси; тощо. Доцільно приєднати як додатки до підручника аудіо або відео-файли із записом лекцій викладачів. Корисним є включення у структуру посібника механізмів для «електронного» спілкування з викладачем, організації відео конференцій, вебінарів, консультації через «Скайп» та ін.

Матеріал Е-підручника має бути поданий дещо інакше в порівнянні з традиційним друкованим виданням. Так, «електронні» глави повинні бути коротшими та лаконічними, а кожен розділ потрібно розбивати на логічно завершені фрагменти, які містить

необхідний і достатній матеріал щодо конкретного вузького питання. Як правило, такий фрагмент повинен містити від кількох текстових абзаців до 2-3 екранів дисплея. Менший обсяг тексту треба компенсувати включенням малюнків, графіків, таблиць, мультимедійних фрагментів і т.п. Таким чином, студент переглядає не безперервний текст, а окремі логічно закінчені та добре ілюстровані екранні фрагменти. На основі таких інформаційних блоків створюється багатоступінчаста структура навчального матеріалу. Вона містить: перший шар, мінімально обов'язковий для вивчення; другий шар для поглибленого засвоєння матеріалу (для одержання доброї або відмінної оцінки); та верхній шар для можливості наукових досліджень у даній галузі. Для зручності студентів створюється окремий розділ – глосарій (список визначень), у якому організований перехід від термінів до їх визначень, що викладені в основному тексті. Бажано мати окремий розділ з практичними завданнями та рекомендаціями щодо застосування отриманих знань [2].

На відміну від звичайного (паперового) підручника електронний підручник може і повинен володіти дещо «більшим інтелектом», оскільки комп'ютер може імітувати деякі аспекти діяльності викладача (наприклад, не відкривати подальший текст без відповіді на контрольні питання, і т.п.). Наявність «інтелектуальних» можливостей в електронному підручнику дає йому значні переваги перед паперовим варіантом у швидкості пошуку необхідної інформації, компактності, дешевизні і т.д. Наочні властивості електронного підручника значно вищі, ніж друкованого. Так у одному з підручників географії на паперовому носії було представлено близько 50 ілюстрацій. У новий мультимедійний підручник з цим же курсом включено близько 800 слайдів. Електронний підручник забезпечує багатоваріантність, багаторівневість і різноманітність перевірочних завдань та тестів. Е-підручник дозволяє всі завдання і тести давати як у заліковому, так і в тренувальному режимах. При невірній відповіді під час тренування можна показати вірну відповідь з роз'ясненнями та коментарями [3].

Електронні підручники по своїй суті є гнучкими та відкритими системами. Їх можна доповнювати, коректувати, модифікувати у будь-який час, без суттєвих витрат на друк та розповсюдження.

Технологія створення електронних підручників включає наступні етапи:

- визначення цілей і завдань розробки;
- розробка структури електронного підручника, тематики розділів та інформаційних блоків;
- напрацювання змісту підручника, ілюстративного та мультимедійного матеріалу, тестів, тощо;
- підготовка сценаріїв окремих структур електронного підручника;
- компоновка змісту усіх складових частин у єдиний підручник;
- програмування навігації, гіпертекстових посилань, логічних зв'язків, тощо;
- апробація підручника у навчальному процесі;
- підготовка методичних рекомендацій для користувача;
- корегування змісту Е-підручника за результатами апробації.

В Е-підручнику для побудови зручного механізму навігації використовуються гіпертекстові посилання та значки, що дозволяють швидко перейти до потрібного розділу або фрагменту і так само швидко повернутися назад. Така навігація організується всередині тіла підручника, а також між ним і відокремленими файлами, розміщеними на локальному ресурсі або на сайтах Інтернету. Слід зауважити, що у друкованому виданні можливостей переміщення по тексту дві: зміст і глосарій. Для практичної реалізації цих механізмів необхідно гортати сторінки підручника, а для перегляду інших видань треба йти до бібліотеки (якщо у ній взагалі є потрібна книга).

Одна з переваг електронного підручника – це можливість інтерактивної взаємодії між студентом і елементами підручника. Рівні такого «спілкування» змінюються від простого при переміщенні по посиланнях, до високого при тестуванні або при особистій участі студента в моделюванні процесів. Якщо «електронне» тестування подібно до співбесіди з викладачем, то комп'ютерне моделювання процесів можна порівняти з придбанням практичних навичок у ході виконання лабораторних робіт на обладнанні або виробничої практики.

З впровадженням електронних підручників змінюються і функції бібліотеки. Тепер її роль виконує читальний зал, обладнаний комп'ютерами, об'єднаними в локальну мережу, яка зв'язана з сервером-сховищем електронних ресурсів та має вихід в Інтернет. Користувачі такої бібліотеки без черги і очікування видачі книги можуть самостійно вибирати і через індивідуальні паролі читати будь-які електронні підручники, доступні для них у потрібний час та у зручному місці.

На жаль, створення Е-підручників ще не стало пріоритетом навіть для викладачів молодої генерації, і для того є певні причини. По-перше, вкрай мало конкретних і детальних інструктивних та методичних матеріалів щодо програмно-технічного інструментарію для створення Е-підручників. По-друге, далеко не усі науковці, особливо гуманітарного профілю, мають достатній обсяг технічної підготовки та навичок у комп'ютерних технологіях. По-третє, створення такого складного засобу навчання вимагає витрат великого часу, значно більшого, ніж для звичайного підручника. Є інші об'єктивні та суб'єктивні фактори, які ускладнюють досягнення позитивного результату.

Автор бачить кілька напрямків подолання цих проблем. Так, можна у навчальному закладі створити невелику групу фахівців, яка б оформляла у вигляді Е-підручника матеріали, що надаватимуть викладачі. Групу можна навчити на базі МОН або аналогічного підрозділу іншого ВНЗ, а після набуття практичного досвіду вона стане базою навчання для власних викладачів. Досить перспективним виглядає створення програмного засобу, де знаходились би макети інформаційних, тестуючих, словарних та інших блоків, включено можливість організації зв'язків між даними, тощо (на зразок пакетів для дистанційного навчання). Такі програмні засоби можуть мати галузеві різновиди – для технічних, гуманітарних, інших тематичних напрямків. Найшвидший результат може принести звернення до фірм, які пропонують послуги по створенню Е-підручника «під ключ» (відповідні пропозиціє є в Інтернеті). Звичайно, така робота вимагає певних витрат, але тут доцільно зіставити вартість цих послуг та типографського друку.

Вважаємо, що для викладацької спільноти пріоритетом повинно стати створення сучасних Е-підручників, а для керівництва навчальних закладів – стимулювання цієї роботи.

1. Положення про електронні освітні ресурси : Наказ МОН молодьспотру від 01.10.2012. № 1060 // Зареєстровано в Міністерстві юстиції України 5 жовтня 2012 р. за № 1695/22007.
2. Пілінський В. В. Технології та засоби формування електронного підручника «Електроживлення спеціальних установок». // Электроника и свіязь № 5 2008 с. 79-85.
3. Риженко С. С. Про досвід використання мультимедійних технологій у навчальному процесі ВНЗ. // Інформаційні технології і засоби навчання: електронне наукове фахове видання – 2009. – № 3(11). [Електронний ресурс]. Режим доступу http:// www.ime.edu-ua.net/em.html. ISSN 2076-8184.

ПЕРЕВАГИ І НЕДОЛІКИ ВИКОРИСТАННЯ КОМП'ЮТЕРНОЇ ТЕХНІКИ ПРИ ВИВЧЕННІ АНГЛІЙСЬКОЇ МОВИ

Бондаренко Вікторія Анатоліївна,
доцент кафедри іноземних мов ЛьвДУВС, к.ю.н.

Успішність процесу навчання, ефективність використання в ньому різноманітних методів навчання значною мірою залежать від матеріальних передумов. У зв'язку з високим рівнем розвитку техніки на сучасному етапі і загальною тенденцією до раціоналізації будь-якої діяльності, в тому числі мовленнєвої, все частіше застосовують технічні засоби навчання, зокрема комп'ютерну техніку.

Використання комп'ютера на заняттях з англійської мови сприяє глибокому сприйняттю матеріалу, що вивчається, і дає можливість розвивати логічне, конкретизоване мислення. А активізація розумової діяльності тісно пов'язана з формуванням позитивних мотивів на практичному занятті. При виконанні різних форм і видів роботи у студентів з'являються певні емоційно-особистісні відношення, потреби, які підсилюють мотивацію, сприяють формуванню позитивних мотивів, і тим самим сприяють оптимізації оволодіння іноземною мовою [2, с. 34].

Навчальний комп'ютер є тим інструментом, за допомогою якого можна здійснити контроль за самостійною роботою студентів у процесі опрацювання мовного матеріалу.

Серед рекомендацій щодо використання комп'ютерів у викладанні англійської мови слід пам'ятати, що комп'ютер – це знаряддя, яке повинно працювати на вас, а не проти вас. Першочергову роль відіграє відбір програмного матеріалу, який студенти могли б опрацювати за допомогою комп'ютера, а який – на звичайних заняттях під вашим керівництвом. [1, с.245]

Матеріал, що входить до комп'ютерних програм, повинен:

- сприяти розвитку техніки читання, формувати і створювати додаткові стимули для мовлення;
- підвищувати оперативність контролю і корекції;
- активізувати самостійну роботу слухачів, привчаючи їх до самоконтролю і самокорекції;
- диференціювати і індивідуалізувати процес навчання на основі різних навчальних програм;
- дати можливість працювати за зразками мовлення, використовувати матеріал згідно з вимогами поетапного формування розумових дій;
- спонукати студентів до творчого пошуку.

Деякі автори вважають найбільш доцільним застосовувати на заняттях програми-енциклопедії і програми-тести [3, с. 72].

Програми-енциклопедії в основному розширюють інформаційну базу студентів. Програми-тести використовуються не тільки для контролю і самоконтролю знань, але і для актуалізації знань і формування вмінь. Переваги тестів, які виконуються на комп'ютері, полягають насамперед у високому рівні інтерактивності процесу. До переваг використання програм-тестів можна також віднести:

- уніфікованість лексичного матеріалу;
- комунікативність засобу навчання мові;
- розширення знань з фаху;
- збагачення словникового запасу студента;
- розвиток навичок прийняття правильних рішень;
- розвиток мислення;
- залучення студентів до самостійної роботи.

На жаль, недосконалість комп'ютерного забезпечення не допускає широкого вибору тестових завдань (як правило, це тести багатоваріантного вибору і відповіді на запитання). Але численні

переваги використання комп'ютерних засобів для перевірки отриманих знань свідчать на їхню користь.

Крім того, комп'ютер можна використовувати на різних етапах навчання. На початковому і середньому етапах навчання комп'ютер дає можливість, за рахунок збільшення обсягу мовного тренування, прискорити процес засвоєння і активізації лексико-граматичного матеріалу. На старших етапах навчання за допомогою комп'ютерних засобів можливо здійснювати міжпредметні зв'язки, що є дуже важливим для забезпечення професійної освіти.

У сучасних умовах комунікативний метод викладання англійської мови у внз націлений на зв'язок усіх видів мовленнєвої діяльності (аудіювання, говоріння, читання і письма). Забезпечити таку взаємодію викладач може теж за допомогою комп'ютера. Текстові редактори дають змогу працювати з текстом (писати статті, анотувати прочитане, складати власний словник). Студенти також мають можливість читати іншомовні тексти і діалоги з подальшим опрацюванням. Працюючи з комп'ютером, студент має можливість отримувати і аудіо-, і відеоінформацію, що є корисною для відтворення мовленнєвої ситуації. Мультимедійні засоби відкрили широкі можливості вивчення за допомогою інформаційних технологій не тільки граматики, орфографії і лексики, але й фонетики – одного із більш складних аспектів іншомовного мовлення. За їх допомогою студенти мають можливість слухати іншомовні тексти і потім перевіряти себе на їх розуміння. Комп'ютерні засоби можуть замінити і фоно- і відеозали, і навіть бібліотеку. Це значно оптимізує навчальний процес, роблячи його більш ефективним та інформаційно ємним.

На сьогодні все більшої популярності набуває Інтернет – міжнародна комп'ютерна інформаційна мережа. За останні роки Інтернет перетворився у могутній засіб спілкування, реклами, бізнесу, і що найголовніше, – отримання корисної інформації. Важко перелічити всі можливості й послуги, що надаються за допомогою інтернет-технологій. Зокрема, сучасні інформаційні технології відкривають унікальні можливості як для студентів, так і для викладачів. Студенти мають можливість працювати з оригінальними текстами з фаху, набувати ґрунтовних знань з

конкретної галузі науки, користуватися електронними словниками тощо.

Водночас педагоги повинні враховувати й негативні моменти. Передусім робота з комп'ютером стомлює студентів, може погано впливати на зір або навіть призводити до розладу нервової системи. Комп'ютеризоване навчання не розвиває здатності студентів чітко й образно висловлювати свої думки, істотно обмежує можливості усного мовлення, формуючи логіку мислення на шкоду збагаченню емоційної сфери. Здебільшого інтерес до програми з обмеженою інформативністю швидко згасає, оскільки діалог з машиною синтаксично збіднений. Використання комп'ютерної техніки є доцільним лише в деяких навчальних ситуаціях, пов'язаних з формуванням навичок, але зовсім недостатнє в ситуаціях, пов'язаних з розвитком основних сфер формування особистості. Іншими словами, застосування комп'ютера в процесі навчання має сенс на етапі актуалізації знань.

Отже, використання комп'ютерної техніки значно розширює та урізноманітнює програму вивчення англійської мови у внз. При вдалому виборі матеріалу та його цілеспрямованому плануванню застосування цих технічних засобів вносить елементи новизни в навчальний процес, зацікавлює студентів до вивчення іноземної мови, надаючи їм доступ до різноманітних автентичних матеріалів, розширює їх мотивацію, а також сприяє поглибленню мовних знань, стимулює творче ставлення до навчання.

1. Жовнірук З.Л. Застосування комп'ютерних технологій на заняттях з іноземних мов у вузі / З.Л. Жовнірук, Г.Т. Ісаєва // Лінгвометодичні концепції викладання іноземних мов у немовних вищих навчальних закладах України. – К., 2003. – С. 244-251.
2. Зеленська О.П., Бондаренко В.А. Тестовий контроль за фаховою лексикою з використанням комп'ютерних технологій / О.П. Зеленська, В.А. Бондаренко // Актуальні проблеми викладання іноземних мов у вищій школі. – Донецьк : ДонНУ, 2004. – С. 32-37.
3. Маслова О.О. Комп'ютеризація навчання. ЇЇ переваги і недоліки / О.О. Маслова, Н.О. Карпова // Актуальні проблеми викладання іноземних мов у вищій школі. – Донецьк : ДонНУ, 2005. – С. 71-73.
4. Маслыко Е.А. Настольная книга преподавателя иностранного языка / Е.А. Маслыко, П.К. Бабинская, А.Ф. Будько, С.И. Петрова, А.И. Попов. – Минск, 1992. – 445 с.

АКТУАЛЬНІСТЬ ВИКОРИСТАННЯ МЕДІАОСВІТНІХ ТЕХНОЛОГІЙ У ПРОФЕСІЙНІЙ ПІДГОТОВЦІ ФАХІВЦІВ ВНЗ

Кулешник Оксана Ігорівна,
асистент кафедри менеджменту ЛНАМ
Унятович Богдан,
магістрант ЛьвДУВС

Комп'ютери, як відомо, використовують сьогодні практично в усіх галузях роботи працівників ОВС, тому вміння працювати із сучасними інформаційними технологіями розглядаються у нашій державі як обов'язкові та необхідні для кожної особистості. Можливості використання цих технологій у навчальному процесі є невичерпними.

Сучасна освітня парадигма вимагає переходу від пасивних до активних технологій навчання. Використання інформаційно-комунікаційних технологій в освіті є черговим етапом запровадження новітніх поглядів на викладання дисциплін у ВНЗ який потребує розроблення сучасних педагогічних підходів із застосуванням медіаосвітніх технологій. [5].

Саме комп’ютерні технології забезпечили можливість комбінації різних видів медіа, їх одночасного застосування в одному продукті мультимедіа. Широке поширення і швидке вдосконалення електронних медіа на початку 2000-х років докорінно вплинуло на способи отримання, обробки та зберігання інформації. Це привело до активного впровадження інформаційних технологій в освіті.

В цілому, слід зауважити, що розуміння медіаосвіти (англ. *media education* від лат. *media* – засоби навчання) зарубіжними та вітчизняними педагогами суттєво відрізняється. Якщо на Заході наголос робиться на формування автономної від медіа особистості, то в Україні – на опанування медіа обладнанням та використання можливостей медіа в навчальному процесі.

Медіаосвіта є типовим породженням техногенного суспільства доби інформатизації. Із застосуванням медіа-освітніх технологій пов’язана успішність навчального процесу та подальшої професійної діяльності студентів ВНЗ.

Засобами медіа-освітніх технологій є апаратні і програмні. До програмних засобів, застосування яких є актуальним і доступним у викладанні дисциплін, віднесемо мультимедійні додатки і засоби створення мультимедійних медіа-продуктів. Мультимедійні програми включають: мультимедіа презентації, мультимедіа доповіді, електронні мультимедіа видання та мультимедійні Інтернет ресурси. До засобів створення мультимедійних продуктів віднесемо: програми створення і редагування презентацій, відео редактори, редактори зображень, звукові редактори, програми для реалізації гіпертекстів, розміщені локально на комп'ютері та онлайнові аудіо і відео редактори, Інтернет платформи для створення блогів та електронних сторінок.

На думку фахівців ЮНЕСКО, медіаосвіта є частиною основних прав кожного громадянина будь-якої країни світу на свободу самовираження і права на інформацію та є інструментом підтримки демократії. При цьому, медіаосвіта рекомендується для запровадження в національні навчальні плани всіх держав, у систему додаткової, неформальної та «по життєвої» освіти [1].

Особливо важливою є думка про те, що медіаосвіта відноситься до основних прав людини і що вона повинна мати пожиттєвий характер [1].

Основні завдання медіаосвіти – підготувати нове покоління працівників ОВС до життя в сучасних інформаційних умовах, до сприйняття різної інформації, навчити людину розуміти її, усвідомлювати наслідки її впливу на психіку, опановувати способи спілкування на основі невербальних форм комунікації за допомогою технічних засобів.

З усіх проблем та завдань використання медіаосвіти слід виокремити завдання про те, як найбільш ефективно використовувати професійно-орієнтовані медіатексти в підготовці майбутніх спеціалістів ОВС, щоб у подальшому вони успішно застосовували навички роботи з мас-медіа для підвищення професійного рівня, самоосвіти впродовж усього життя.

Досвід впровадження медіаосвіти у навчальний процес ВНЗ України переконує в тому, що на часі не просто вести мову про *професійно-орієнтовану медіаосвіту,* її переваги, а й всіляко сприяти її впровадженню у навчальний процес. Завдяки медіа-

освіті особистість зможе ефективно послуговуватися медіасферою впродовж усього життя, «усвідомлено вибудовувати своє життя, успішно навчатися протягом усього життя, працювати, ефективно вирішувати проблеми особистого та суспільного характеру». Інформаційно грамотна особистість зможе успішно використовувати *медіазасоби* для професійного й культурного зростання, а особистість медіаграмотна для цього залучатиме *матеріали мас-медіа.* Оскільки сучасні Інтернет-технології потребують одночасного володіння інформаційною та медійною грамотністю, зрозуміло, чому нове поняття «медіа-інформаційна грамотність» – набуває швидкого поширення не тільки в сучасному середовищі.

Оскільки мас-медіа активно втручаються в освіту, змінюючи зміст і технології навчально-виховного процесу, викладачі зобов'язані мати розвинуті методичні навички роботи з мультимедіа. У зв'язку з безперервним оновленням і зміною технологій, особливо в галузі програмних засобів, він має опановувати ці мультимедійні технології.

Медіатехнології як основний елемент електронних освітніх ресурсів сьогодні ефективно інтегруються практично в усі навчальні дисципліни.

Нові медіа сприяють використанню наочності (анімація, комп'ютерна графіка, моделювання), розширюють можливості зворотного зв'язку та індивідуальної роботи (технології віртуальної реальності), дають доступ до різноманітної інформації (телекомунікації). Викладач при цьому повинен досліджувати і використовувати можливості конкретних медіа для свого предмету. Позаяк молодь так чи інакше проводить багато часу в контакті з медіа, метою медіаосвіти є використання цього феномену для розвитку процесу пізнання та особистості загалом. Оскільки сучасна медіаосвіта тісно пов'язана з інформатизацією навчального процесу, безумовно, методологічні та методичні проблеми їх упровадження мають вирішуватися комплексно.

Для інтернет-технологій в сфері дистанційної освіти та навчання існують значні перспективи, а їх використання в сучасному педагогічному процесі є актуальним і доцільним завданням. Можна вважати аргументованим таке сприйняття мережі

Інтернет, за яким вона почне виступати як найбільш ефективний засіб отримання систематизованих знань, умінь і навичок як з погляду зручності, витрат часу і грошей, так і з погляду обсягу необхідної інформації.

Використання інформаційних технологій у сфері дослідницької діяльності студентів дає можливість навчальній спільноті обмінюватися наявним та набутим досвідом у процесі пізнання, долати обмеження індивідуального мислення та користуватися «колективним розумом», розширюючи способи пізнання.

Сьогодні тривають активні пошуки нових педагогічних технологій для підготовки майбутніх фахівців ОВС, зорієнтованих на формування особистості, розвиток творчості й самостійності. Мова йде про розробку нових концепцій навчання, спрямованих на особистісно орієнтований розвиток майбутнього працівника ОВС, формування його як творця, здатного не лише самостійно здобувати знання, а й реалізувати їх відповідно до вимог сьогодення.

Висновок. Таким чином, у процесі дослідження теоретичних положень стосовно формування медіакультури студентів вищої школи ОВС можна зробити висновок, що вища освіта потребує певного переосмислення характеру підготовки сучасних фахівців і може стати середовищем інтегрування медіаосвіти в навчальний процес вищих навчальних закладів як необхідної умови його професіоналізму та конкурентоспроможності. Крім того, залучення студентів вищої школи ОВС до створення творчих проектів для формування їхньої медіакультури стане більш ефективним за умови використання аудіовізуальних технологій. На жаль, Україна тут робить лише перші кроки, хоча необхідність запровадження медіаосвіти ні в кого не викликає сумнівів. Однак залишається невирішеним питання, хто саме має займатися і відповідати за формування програм медіаосвіти.

Таким чином, проведений аналіз свідчить про те що, медіаосвітні технології надають широкі перспективи у підготовці нового покоління до активної життєдіяльності в умовах стрімкого розвитку інформаційно-технологічного суспільства. Саме тому подальша розробка та удосконалення методик використання медіаосвітніх технологій в навчанні студентів ОВС належить до перспективних напрямків досліджень.

Застосування досягнень новітніх медіатехнологій відкриває перед викладачами та студентами нові можливості, значно розширює та урізноманітнює зміст навчання, методи та організаційні форми навчально-виховного процесу, забезпечує високий науковий і методичний рівень викладання. Медіаосвітні технології якнайкраще відповідають принципам особистісного підходу. Їх застосування підвищує ефективність подання нового матеріалу, розвиває їх розумові та творчі здібності. Медіатехнології – це потужна мотивація студентів до навчання.

Застосування медіаосвітніх технологій у навчальному процесі навчальних закладів є не лише доцільним, а й необхідним. Вони виконують такі основні функції:

- інформатизація навчального процесу (доступ до різних джерел інформації);
- активізація навчально-пізнавальної діяльності студентів навчальних закладів;
- підвищення мотивації студентів навчальних закладів до навчання;
- інтерактивність навчання;
- моніторинг навчального процесу;
- підвищення ефективності засвоєння студентами навчальних закладів навчального матеріалу;
- спонукання до творчої діяльності (підготовка презентацій з використанням комп'ютерних програм; і т.д.) [5].

Вони дають можливість моделювати ситуації, які максимально наближені до умов професійної діяльності; активізувати навчальну діяльність студентів, посилювати їх самостійну роботу (можливість обирати інформацію, що безпосередньо стосується їхньої професійної діяльності, працювати у темпі, відповідно до рівня знань студента); розвивати критичне мислення студентів навчальних закладів.

Важливим аспектом окресленої проблеми є удосконалення *інформаційно-комунікативних технологій*, які сьогодні є невід'ємною складовою навчально-виховного процесу.

Використання сучасних інформаційних технологій і в тому числі застосування відповідних форм медіаосвіти в навчальному процесі студентів ОВС є вимогою часу.

1. Recommendations Addressed to the United Nations Educational Scientific and Cultural Organization UNESCO // Education for the Media and the Digital Age. – Vienna : UNESCO, 1999. – P. 273–274.
2. Гуріненко І. Ю. Медіа-освіта як засіб професійної підготовки фахівця цивільного захисту / І. Ю. Гуріненко // Інформаційні та телекомунікаційні технології в сучасній освіті: досвід, проблеми, перспективи : зб. наук. праць. – частина 1. / за ред. М. М. Козяра та Н. Г. Ничкало. – Львів : ЛДУ БЖД. – 2009. – С. 181–184.
3. Зязюн І. А. Антропологічний вимір комп'ютерних технологій // Інформаційно-телекомунікаційні технології в сучасній освіті: досвід, проблеми. перспективи : збірник наукових праць. – частина 1 / за ред. *М. М. Козяра* та *Н.Г. Ничкало*. –Львів : ЛДУ БЖД, 2009. – С. 6–13.
4. Сахневич І.А. Педагогічні умови використання медіаосвітніх технологій у професійній підготовці майбутніх фахівців нафтогазового профілю: Автореф. дис. …. канд. пед. наук. – К.: ІВО АПН України, 2012. – 22 с.
5. Концепція впровадження медіаосвіти в Україні [Електронний ресурс]. – Режим доступу : http://www.ispp.org.ua/news_44.htm

III. ДЕЯКІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ІНШИМИ МІНІСТЕРСТВАМИ ТА ВІДОМСТВАМИ, КОМЕРЦІЙНИМИ УСТАНОВАМИ

АНАЛІЗ І ОЦІНКА МОЖЛИВОСТЕЙ ЗНЕШКОДЖЕННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ, ЯКІ ЗАСТОСОВУЮТЬСЯ ДЛЯ РОЗВІДУВАЛЬНИХ ЦІЛЕЙ У ВІЙСЬКОВИХ КОНФЛІКТАХ

Шабатура Юрій Васильович,
завідувач кафедри електромеханіки та електроніки Академії сухопутних військ ім. гетьмана Петра Сагайдачного, д.т.н., професор
Борисов Віктор Михайлович,
інженер кафедри інформаційних технологій НЛТУУ
Атаманюк Віталій Володимирович,
доцент кафедри електромеханіки та електроніки Академії сухопутних військ ім. гетьмана Петра Сагайдачного, к.т.н.
Королько Сергій Володимирович,
доцент кафедри спеціальних технологій Академії сухопутних військ ім. гетьмана Петра Сагайдачного, к.т.н.

Стрімкий розвиток науки і техніки дає людству нові і більш широкі можливості поступального розвитку. Прямі наслідки цього сьогодні спостерігаються насамперед у тому, що у важких і небезпечних для життя і здоров‘я умовах працюють уже не люди, а дистанційно керовані, чи повністю автономні, наділені відповідним комп‘ютерним інтелектом роботизовані системи. Яскравим

прикладом, що ілюструє дану тенденцію є розвиток такої високотехнологічної галузі як авіація. Усі без винятку авіалайнери сьогодні основну частину польоту здійснюють під управлінням не льотчиків а автопілота, причому, на думку провідних експертів з даної галузі [1], з 2020 року не менше 85% літаючих у повітряному просторі об‘єктів будуть пілотовані не людьми а кібернетичними системами. Однак, якщо у «великій» авіації місце для людини, принаймні у якості пасажира усе-таки буде залишатися, то з авіаційних систем спеціального призначення людина буде повністю виключена, принаймні уже через те, що саме її перебування на борту таких систем стає фактором, який обмежує можливості нарощування їх тактико-технічних характеристик.

Сьогодні вище означені літальні апарати більш відомі як безпілотні літальні апарати (БПЛА), в англомовній літературі зустрічаються наступні скорочення: UAV – Unmanned Aerial Vehicles, UCAV – Uninhabited Combat Aerial Vehicles. Поряд з вирішенням задач цивільного призначення БПЛА все ширше використовують для військових цілей: спостереження та розвідка, наведення вогню артилерійських і ракетних систем, виконання різного роду бойових завдань.

Швидке поширення військового використання БПЛА пов‘язано не лише з зменшенням ризику для військовослужбовців, але і з зменшенням вартості літальних апаратів, хоча аварійність БПЛА поки що у 100 разів перевищує аварійність пілотованих літаків [1]. Перевагами тактичних БПЛА також є відсутність «людського чинника» – втоми, нездатності людського організму переносити значні перевантаження. Також зникає необхідність у бортових системах життєзабезпечення, що дозволяє збільшити вагу приладів спеціального призначення та озброєнь. Все це робить БПЛА більш маневровими та збільшує їх радіус дії і тривалість польоту [2]. Крім того, БПЛА притаманна значно менша помітність (радіо- та візуальна) порівняно із звичайними літаками. Усі ці аспекти зумовлюють актуальність задачі як виявлення, так і знешкодження БПЛА, які використовуються в неправомірних цілях.

Метою даної статті є проведення аналізу і оцінка можливостей виявлення і знешкодження безпілотних літальних апаратів, які застосовуються для розвідувальних цілей у військових конфліктах.

Аналіз доступних інформаційних джерел [3] переконливо свідчить, що технологіями виготовлення і експлуатації БПЛА сьогодні володіють переважна більшість країн світу. За принципами своєї будови і тактико-технічними характеристи-ками БПЛА можна класифікувати як літаки, вертольоти та мультикоптери, які відповідно поділяються на: розвідувально-спостережні; ударні; спеціальні; мішені. Така класифікація є досить умовною, адже часто сучасні БПЛА здатні поєднувати кілька функцій.

Перші задокументовані спроби бойового застосування БПЛА були здійснені під час громадянської війни у США, коли армії Півдня та Півночі використовували повітряні кулі для доставки та підриву вибухових пристроїв на території противника [5]. Під час Другої світової війни США намагалися використати пілотований літак у безпілотному режимі. Цей прототип БПЛА називався «Афродіта», проте на той час ще не було технологій, які б дозволяли достатньою мірою керувати польотом апарата. У 1960-х роках США активно почали розробляти так звані «дрони» – БПЛА призначені для шпигування та розвідки. Вони широко застосовувалися під час в'єтнамської війни. Спочатку дрони «Firebee» були оснащені простими фотокамерами, а згодом були доукомплектовані пристроями нічного бачення, засобами зв'язку та електронної розвідки. Починаючи із 1980-х років подальші розробки активно проводяться в Ізраїлі. Такі відомі американські БПЛА як Hunter та Pioneer безпосередньо походять від ізраїльських розробок.

За розмірами і вагою БПЛА можуть відрізнятися в сотні разів, від кількох сантиметрів і сотень грам до кількох метрів і кількох тон. Поряд з такими безпілотними гігантами стратегічного призначення як американський «Global Hawk» (рис. 1), що стоїть на озброєнні ВПС флоту США, та російським «Скат» (рис. 2), сьогодні активно ведуться роботи по створенню мініатюрних БПЛА (micro air vehicle (MAV)) (рис. 3). На відміну від великих БПЛА вони можуть здійснювати посадку у певних місцях та приховано продовжувати спостереження.

Для порівняння розглянемо характеристики найбільш потужних стратегічних БПЛА.

Рис. 1. RQ-4 Global Hawk – американський стратегічний розвідувальний БПЛА

Рис. 2. «Скат» – російський стратегічний ударний БПЛА

Рис. 3. Мініатюрні БПЛА

RQ-4 Global Hawk. Довжина його сягає 13 метрів, вага – понад 12 т. Цей БПЛА містить у собі апаратуру розвідувального призначення вагою 900 кг. Дальність польоту Global Hawk становить 10000 км, а висота – до 20 км; тривалість польоту – 24 год. На відміну від інших БПЛА Global Hawk здатний самостійно здійснювати зліт-посадку за будь-яких погодних умов.

«Скат» – стратегічний ударний БПЛА. Розмах крила – 11,5 м, довжина – 10,25 м, швидкість – 800 км/год, висота польоту – 12 км, дальність – 4000 км, вага бойового навантаження – 2000 кг.

Усі інші представники безпілотної авіації, інформація по яким доступна на даний момент часу у відкритих джерелах, мають менш вражаючі параметри, однак разом з тим вони мають і не менш суттєву перевагу – це їхня вартість. Вона є невисокою, що дозволяє прогнозувати вже в недалекому майбутньому появу в небі великої кількості таких БПЛА.

Враховуючи сучасну ситуацію на сході України для нас найбільш актуальним є аналіз і вивчення парку БПЛА, який перебуває на озброєнні в Російській Федерації. Дослідження проведені у цьому напрямку дозволили згрупувати основні типи і модифікації БПЛА Росії у класифікацію, яка представлена у таблиці 1.

За повідомленнями ЗМІ та силових відомств України БПЛА типу «Орлан-10» (рис. 4) неодноразово застосовувалися з розвідувальними цілями на північному сході нашої країни.

Таблиця 1.

Схема БПЛА	Призначення	Типи БПЛА і їх модифікації
Літаки	Розвідка, спостереження	«Аіст»; ГрАНТ: «Данем»; «Дозор-85»; «Дозор-100»; «Інспектор 101»; «Інспектор 201»; «Інспектор 301»; «Іркут-2М»; «Іркут-10»; «Іркут-200»; «Іркут-850»; К-2; Ла-17Р; мБЛА-С «Авіс»; мБЛА-С «Стерх»; «Орлан-3М»; «Орлан-10»; ПС-01 «Комар»; «Пчела-1Т»; Т-3; Т23 «Елерон»; «Типчак»; Ту-123 «Ястреб»; Ту-141 «Стриж»; Ту-143 «Рейс»; Ту-243 «Рейс-Д»; Ту-300 «Філин-1»; «Форпост»; «Шмель-1»; «Штиль»; »Ельф-Д»; ZALA 421-04M; ZALA 421-08; ZALA 421-16; ZALA 421-16EM; «Дань-Барук»
	Ударні	«Дозор-600»; «Скат»; Ту-130; Ту-300 «Коршун-У»; «Дань-Барук»
	Спеціальні	А-03 «Нарт»; Ту-300 «Філин-2»
	Мішені	«Дань» М; Е-85; Е08; Е95; Ла-17; М-19; М-21; МиГ-15М
Гелікоптери	Розвідка, спостереження	Ка-37; Ка-135; Ка-137; «Коршун»; мБПА-6-Б; мБПА-8-Б; мБПА-12-Б; мБПА-20-Б; мБПА-50-Б; мБПА-130-; БПА-450-Б; БПА-500-Б; ZALA 421-02; ZALA 421-06; ZALA 421-21
	Морські патрульні	ДПВ-6-Б; ДПВ-8-Б; ДПВ-12-Б; ДПВ-20-Б; ДПВ-50-Б; ДПВ-130-Б; БПВ-500

Рис. 4. Запуск розвідувального фюзеляжного БПЛА «Орлан-10» з катапульти

Основні тактико-технічні характеристики БПЛА «Орлан-10»: вага – 14 кг; вага корисного вантажу – 5 кг; двигун – бензиновий (А95); швидкість – 90-150 км/год; максимальна дальність польоту – 600 км; зліт – з катапульти; посадка – на парашуті. Комплекс управління такого БПЛА забезпечує одночасне управління 4 БПЛА. Програмування маршруту здійснюється по електронній карті, або по растровому зображенню місцевості і може включати в себе до 60 наперед визначених точок для яких задається висота польоту, його режим і т.п., передбачено кілька алгоритмів поведінки БПЛА для нештатних ситуацій. Корегування маршруту здійснюється по радіоканалу, живлення апаратури під час польоту забезпечує бортовий генератор. «Орлан-10» може використовуватися у складних погодних умовах (допустима швидкість вітру на старті 10 м/с).

Таким чином у повітряному просторі Україні вже діють ворожі БПЛА а тому підрозділи ЗСУ та МВС повинні бути готовими до протидії їх використанню.

Аналіз демаскуючих ознак та методів виявлення і знешкодження. Завдяки застосуванню композитних матеріалів і малим розмірам більшість БПЛА малопомітні не тільки на екранах РЛС, адже вони мають ефективну площу розсіювання, яка не перевищує 0,1 м^2. Їх малопотужні двигуни виділяють так мало тепла, що застосування тепловізорів також не дає бажаних результатів у виявлені «дронів». Спеціальне забарвлення корпусів БПЛА добре маскує їх на фоні неба в оптичному діапазоні випромінювання. Можливість запису інформації отриманої розвідником на вмонтовану пам'ять робить необов’язковим радіовипромінювання, тому вони можуть і не з’являтися на екранах засобів радіотехнічної розвідки. Тому для збільшення імовірності захоплення і супроводу такої повітряної цілі доцільно використовувати комбіновані засоби, які дозволяють вести спостереження паралельно за різними ознаками, як у радіочастотному, так і у видимому та інфрачервоному спектрах електромагнітних хвиль. Однак поряд з такими традиційними методами і засобами виявлення і спостереження, які були розглянуті вище, для БПЛА доцільно проаналізувати і більш нетрадиційні властиві їм демаскуючі ознаки. Зокрема при польоті БПЛА створюють певну

турбулентність в повітрі атмосфери, викликають незначні збурення магнітного і гравітаційного полів, наявність бортової оптики спричиняє появу певних відблисків при попаданні сфокусованих променів, для БПЛА з двигунами внутрішнього згоряння очевидною буде присутність диму вихлопу і відповідної зміни складу ближньої атмосфери і незалежно від типу двигуна будь-який БПЛА при польоті створює досить потужний і специфічний акустичний сигнал.

Успішне вирішення задачі знешкодження БПЛА повинно передбачати послідовне виконання двох етапів. На першому етапі необхідно виявити БПЛА, причому це виявлення повинно передувати в часі виконанню бойового завдання самого БПЛА, в противному випадку усі подальші і навіть успішні дії втрачають свою цінність. На другому етапі є більше можливих варіантів: фізичне нищення; дезорієнтація; зіпсування бортової електроніки; засліплення бортових оптичних скануючих систем.

Зупинимося більш детально на першому етапі. Усі без винятку технології виявлення базуються на фіксації демаскуючих ознак. Основною проблемою раннього виявлення залишається досягнення достатнього співвідношення корисний сигнал/шум. Сучасні засоби активного виявлення, якими є в першу чергу радіолокаційні станції (РЛС) цілком спроможні виявляти невеликі БПЛА на значних відстанях. Наприклад, радари типу «Harrier» виробництва компанії DeTect (www.detect-inc.com) розроблені спеціально для виявлення невеликих літальних апаратів, наземних та надводних цілей із нелінійним характером руху. Ці радари здатні виявляти типові БПЛА на віддалі 9 км, а мікро-БПЛА – на віддалі 5 км. Основними недоліками такого вирішення задачі виявлення БПЛА є висока вартість РЛС, значні енергетичні витрати під час її роботи, а також можливість виявлення місця розташування РЛС за їх випромінюваннями технічними засобами противника.

Найбільш перспективним вирішенням задачі раннього виявлення на нашу думку є пеленгування БПЛА за акустичним сигналом. Переваги такого підходу визначаються перш за все тим, що використовується пасивна система спостереження, яка конструкційно і схемотехнічно є достатньо простою, а тому має

відносно невисоку вартість і крім того споживає дуже мало електричної енергії. Важливим також є те, що поширення звукових хвиль не обмежується лінією зору, тобто акустична система охоплює одразу широкий тілесний кут не здійснюючи сканування. Для визначення напрямку на БПЛА, як джерело характерного звуку, використовується система лінійної або іншої геометричної конфігурації розміщення сенсорів. Особливо цінним є те, що здатність акустичної системи до виявлення БПЛА залежить не від розміру останніх, а лише від сили звуку який створюється їх двигунами і повітряними гвинтами [4].

У ході експериментальних досліджень був виконаний аналіз звукової сигнатури БПЛА побудованого за схемою квадрокоптера з електричними двигунами. Фрагмент підсиленого акустичного сигналу в часовій області показаний на рис. 5. На ньому добре простежується регулярна структура інформативного сигналу на фоні випадкових шумів. Результати його спектрального аналізу показані на рис. 6. Виявлено, що звуковий сигнал від БПЛА складається із вузької смуги гармонічних тонів, що накладаються на широку смугу із випадковим розподілом інтенсивності. Найбільше енергії вузькосмугової компоненти припадає на частоти від 200 Гц до 2 кГц у той час як частоти звукових коливань у широкій смузі спостерігаються до частот 6 кГц.

Застосування крос-кореляційного методу для системи із трьох акустичних сенсорів, розташованих у вершинах рівностороннього трикутника дозволяє визначити кутові параметри траєкторії БПЛА. За даними [5] межа виявлення акустичною пеленгацією тактичних БПЛА перевищує 4.4 км для детектування за вузькосмуговим сигналом, та 8.8 км для широкосмугового сигналу. Причому, дальність виявлення БПЛА із бензиновим двигуном приблизно уп'ятеро перевищує таку для БПЛА з електричним двигуном.

Ефект Допплера разом із врахуванням часу затримки надходження до сенсора різних гармонік дозволяє зробити оцінку параметрів траєкторії БПЛА використовуючи лише один акустичний сенсор. Причому особливо ефективну систему акустичного виявлення БПЛА можна на основі застосування так званого акустичного векторного сенсора (АВС) (acoustic vector sensor,

AVS). АВС – це невеликий пристрій, здатний вимірювати як скалярний тиск звукової хвилі, так і три взаємно перпендикулярні компоненти швидкості частинок середовища у одній точці повітряного простору. Акустичний векторний сенсор є потужним засобом, що дозволяє дуже точно визначити напрямок на джерело звуку за допомогою простих алгоритмів. У роботі [5] здійснено оцінку параметрів руху БПЛА, що летить на низькій висоті, шляхом реєстрації звуку акустичним векторним сенсором. Для аналізу сигналів використовувався нелінійний метод найменших квадратів та автокореляційний метод.

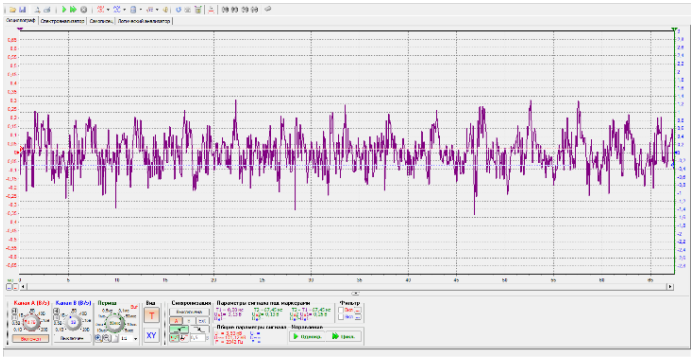


Рис. 5. Фрагмент акустичного сигналу

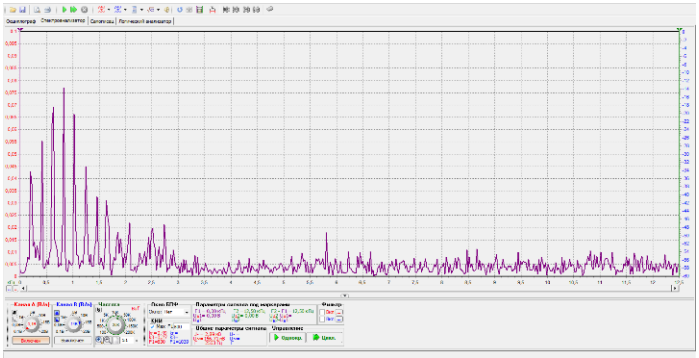


Рис. 6. Частотний спектр сигналу

Якщо етап виявлення БПЛА противника буде успішно виконаний, то його логічним продовженням стає етап знешкодження. У тривіальному варіанті знешкодження передбачає фізичне знищення. Зрозуміло, що знищення маломіцної і незахищеної

конструкції можливе шляхом взаємодії: з матеріальною субстанцією; нематеріальним утворенням. За технологіями доставки взаємодіючої компоненти можливі варіанти: з наземного базування; з повітряного базування. За принципом наведення: за рахунок прицілювання без автокорекції; з попереднім прицілюванням і авто наведенням; з попереднім підсиленням демаскуючої ознаки і без цього. У якості матеріальної субстанції можуть бути використані: матеріальні об`єкти з значною кінетичною енергією; сіточні перепони значного розміру; хімічні реагенти клеючої взаємодії; хімічні реагенти об`ємного згоряння. Нематеріальні утворення можуть досилатися до БПЛА з джерел наземного базування шляхом формування високоенергетичного лазерного променя, високоенергетичного і добре сфокусованого НВЧ-променя, або пучка елементарних частинок високої інтенсивності. У випадку використання матеріального носія доставки джерела нематеріального утворення поблизу БПЛА можна використати детонація пристрою, який генерує потужний електромагнітний імпульс.

Ретельний аналіз усіх вище означених методів і необхідних для їх реалізації технічних засобів знешкодження БПЛА у просторі координат вартість-ефективність-мобільність показав, що на даний момент часу найбільш ефективним є фізичне знищення БПЛА шляхом використання спеціального боєприпасу для стрілецької зброї підвищеного калібру, який на підльоті до БПЛА підривається і утворює велику кількість дрібних уламків з високою кінетичною енергією, площа розсіювання яких різко підвищує ймовірність ураження такої маломірної цілі як БПЛА.

Висновки. На підставі проведено огляду і аналізу відомих з відкритих джерел інформації методів і засобів виявлення та знешкодження БПЛА на теперішній час можна зробити наступні висновки:

1. Серед методів оперативного виявлення і ідентифікації БПЛА найбільш перспективним є акустичний метод, який базується на постійному моніторингу акустичної обстановки, причому значне збільшення його ефективності і зручності використання в оперативних умовах досягається при використанні акустичного векторного сенсору.

2. Для знешкодження малорозмірних розвідувальних БПЛА на теперішній час найбільш ефективним методом залишається їх фізичне знищення, причому для практичного застосування цього методу достатньо використання стрілецької зброї підвищеного калібру з спеціальним, модернізованим боєприпасом.

1. E. Bone, C. Bolkcom. Unmanned Aerial Vehicles: Background and Issues for Congress. Report for Congress. 2008. P. 1 – 48. Congressional Research Service – The Library of Congress, 2008
2. Unmanned Aerial Vehicles: Implications for Military Operations. D. Glade. Occasional Paper No. 16, Center for Strategy and Technology Air War College Air University Maxwell Air Force Base, 2000, p. 1 – 39.
3. UCAVs-Technological, Policy, and Operational Challenges. C.L. Barry, E. Zimet. Defense Horizons. № 3, 2001, p. 1 – 8.
4. Low-Cost Acoustic Array for Small UAV Detection and Tracking. E.E. Case, A.M. Zelnio, B.D. Rigling. Aerospace and Electronics Conference, 2008. NAECON 2008. IEEE National Date 16-18 July 2008.
5. Exploitation of Acoustic Signature of Low Flying Aircraft using Acoustic Vector Sensor. A. Saravanakumar, K. Senthilkumar. Defence Science Journal, Vol. 64, No. 2, March 2014, pp. 95-98.

ЧИСЛОВИЙ АЛГОРИТМ РОЗВ'ЯЗУВАННЯ НЕСТАЦІОНАРНОЇ ЗАДАЧІ ТЕРМОПЛАСТИЧНОСТІ ПРОСТОРОВИХ ТІЛ

Неспляк Дмитро Михайлович,
викладач кафедри інформатики ЛьвДУВС
Магеровська Тетяна Валеріївна,
доцент кафедри інформатики ЛьвДУВС, к.ф.-м.н, доцент

В останнє десятиріччя вийшли у світ багато публікацій, присвячених числовому розв’язуванню задачі термопружнопластичності у просторових тілах за теорією пластичної текучості [4-7]. Проте, у більшості із них лінеаризація здійснюється методами послідовних наближень або послідовних навантажень. Це пов’язано з тим, що лінеаризація методом Ньютона-Рафсона вимагає значно більше обчислювальних ресурсів. Використання методу

проміжної точки для обчислення скінченного приросту пластичних деформацій дозволяє покращити збіжність ітераційного процесу Ньютона-Рафсона.

Числове обчислення нелінійної задачі термопластичності [1-3] здійснюється за допомогою розробленого програмного забезпечення для розв'язування просторових нестаціонарних задач неізотермічної пружнопластичності у складових тілах, які задаються у криволінійній системі координат $\{\alpha_1, \alpha_2, \alpha_3\}$, яка пов'язана із базовою поверхнею співвідношенням $\vec{\mathbf{R}}(\alpha_1, \alpha_2, \alpha_3) = \vec{\mathbf{r}}(\alpha_1, \alpha_2) + \alpha_3 \cdot \vec{\mathbf{n}}(\alpha_1, \alpha_2)$, де $\vec{\mathbf{r}}(\alpha_1, \alpha_2)$ – рівняння базової поверхні, $\vec{\mathbf{n}}(\alpha_1, \alpha_2)$ – вектора нормалі до базової поверхні.

Опишемо ітераційний процес обчислення термопластичного напружено-деформівного тіла (НДС) у просторових тілах. Величини

$$\begin{matrix} \alpha_1 & \alpha_3 & \Phi_{k_1k_2k_3} & \dfrac{\partial \Phi_{k_1k_2k_3}}{\partial \alpha_1} & \dfrac{\partial \Phi_{k_1k_2k_3}}{\partial \alpha_3} \\ A_1 & A_2 & \dfrac{dA_1}{d\alpha_1} & \dfrac{dA_2}{d\alpha_2} & K_1 \quad K_2 \quad \dfrac{dK_1}{d\alpha_1} \quad \dfrac{dK_2}{d\alpha_2} \end{matrix}, \qquad (0.1)$$

потрібно один раз обчислювати у точках інтегрування і зберігати на зовнішніх носіяк інформації, оскільки їх необхідно буде використовувати на кожній ітерації як для визначення розподілу температурного поля, так і для визначення НДС у тілі. Тут $\Phi_{k_1k_2k_3}$ – функції форми, $A_1 = \sqrt{a_{11}}$, $A_2 = \sqrt{a_{22}}$, $K_1 = b_{11}$, $K_2 = b_{22}$, a_{ii} і b_{ii} – коефіцієнти першої і другої квадратичних форм.

НДС і необхідний для його обчислення розподіл температурного поля будемо шукати у моменти часу

$$0 = \tau_0 < \tau_1 < \ldots < \tau_m < \tau_{m+1} < \ldots < \tau_M = t.$$

Припустимо, що у момент часу τ_m нам відомі розподіл температурного поля, переміщення, деформації і напруження у тілі. Опишемо ітераційний процес, який здійснюється для обчислення приросту переміщень, деформацій і напружень, що виникли за час $\Delta\tau_m$. Співвідношення длячислового обчислення скінченно малих

приростів пластичних деформаційна q-тій ітерації $\Delta\varepsilon_{ij}^{p(mq)}$ у ітераційному процесі Ньютона-Рафсона

$$\vec{\mathbf{u}}^{(m,q+1)} = \vec{\mathbf{u}}^{(mq)} + \Delta\vec{\mathbf{u}}^{(mq)},$$
$$\hat{\boldsymbol{\varepsilon}}^{(m,q+1)} = \hat{\boldsymbol{\varepsilon}}^{(mq)} + \Delta\hat{\boldsymbol{\varepsilon}}^{(mq)},$$
$$\hat{\boldsymbol{\sigma}}^{(m,q+1)} = \hat{\boldsymbol{\sigma}}^{(mq)} + \Delta\hat{\boldsymbol{\sigma}}^{(mq)},$$
$$\lambda^{(m,q+1)} = \lambda^{(mq)} + \Delta\lambda^{(mq)}$$

зручно записати у вигляді

$$\Delta\varepsilon_{ij}^{p(mq)} = r_{ij}^{p0} + r_{ij}^{p\lambda}\Delta\lambda^{(q)} + r_{ijks}^{p\sigma}\Delta\sigma_{ks}^{(mq)}, \qquad (1)$$

де

$$r_{ij}^{p\lambda} = \frac{\partial F\left(\overset{\circ}{\hat{\boldsymbol{\sigma}}}{}^{(m)} + \theta\hat{\boldsymbol{\sigma}}^{(mq)}, \overset{\circ}{T}{}^{(m)} + T^{(m)}\right)}{\partial\sigma_{ij}},$$

$$r_{ij}^{p0} = \lambda^{(q)} r_{ij}^{p\lambda} - \varepsilon_{ij}^{p(mq)},$$

$$r_{ijks}^{p\sigma} = \theta\lambda^{(q)} \frac{\partial^2 F\left(\overset{\circ}{\hat{\boldsymbol{\sigma}}}{}^{(m)} + \theta\hat{\boldsymbol{\sigma}}^{(mq)}, \overset{\circ}{T}{}^{(m)} + T^{(m)}\right)}{\partial\sigma_{ij}\partial\sigma_{ks}}.$$

Тут $\Delta\vec{\mathbf{u}}^{(mq)}$, $\Delta\hat{\boldsymbol{\varepsilon}}^{(mq)}$, $\Delta\hat{\boldsymbol{\sigma}}^{(mq)}, \Delta\lambda^{(mq)}$ є величинами вищого порядку мализни у порівнянні з $\vec{\mathbf{u}}^{(mq)}$, $\hat{\boldsymbol{\varepsilon}}^{(mq)}$, $\hat{\boldsymbol{\sigma}}^{(mq)}$ і $\lambda^{(mq)}$ відповідно.

Враховуючи фізичні співвідношення $\overset{\circ}{\sigma}{}_{ij}^{(m+1)} = \overset{\circ}{\sigma}{}_{ij}^{+(m)} + \sigma_{ij}^{(m)}$, де

$$\overset{\circ}{\sigma}{}_{ij}^{+(m)} = a_{ijks}(\overset{\circ}{T}{}^{(m)} + T^{(m)})\left(\left[\mathbf{A}^{-1}(\overset{\circ}{T}{}^{(m)})\right]_{kspt} \overset{\circ}{\sigma}{}_{pt}^{(m)} - \varepsilon_{ks}^{th}(T^{(m)})\right),$$

$$\sigma_{ij}^{(m)} = a_{ijks}(\overset{\circ}{T}{}^{(m)} + T^{(m)})\left(\varepsilon_{ks}^{(m)}(\vec{\mathbf{u}}^{(m)}) - \varepsilon_{ks}^{p(m)}\right)$$

та значення скінченно малих приростів пластичних деформацій (1) $\Delta\varepsilon_{ij}^{p(mq)}$ співвідношення для визначення скінченного приросту напружень $\Delta\sigma_{ij}^{(mq)}$, отриманих при розв'язуванні термопружно-пластичної задачі, може бути записане у вигляді

$$\Delta\sigma_{ij}^{(mq)} = a_{ijks}\left(\overset{\circ}{T}{}^{(m)} + T^{(m)}\right)\left(\Delta\varepsilon_{ks}^{(mq)} - r_{ij}^{p0} - r_{ij}^{p\lambda} - r_{ijks}^{p\sigma}\Delta\sigma_{ks}^{(mq)}\right).$$

Звідси отримаємо

$$\Delta\sigma_{ij}^{(mq)} = r_{ij}^{\sigma 0} + r_{ij}^{\sigma\lambda}\Delta\lambda^{(q)} + r_{ijks}^{\sigma\varepsilon}\Delta\varepsilon_{ks}^{(mq)}, \qquad (2)$$

де

$$r_{ij}^{\sigma 0} = -a_{ijks}^{*}\left(\overset{\circ}{T}{}^{(m)} + T^{(m)}\right)r_{ks}^{p0}, \quad r_{ij}^{\sigma\lambda} = -a_{ijks}^{*}\left(\overset{\circ}{T}{}^{(m)} + T^{(m)}\right)r_{ks}^{p\lambda},$$

$$r_{ijks}^{\sigma\varepsilon} = a_{ijks}^{*}\left(\overset{\circ}{T}{}^{(m)} + T^{(m)}\right),$$

$$\mathbf{A}^{*}\left(\overset{\circ}{T}{}^{(m)} + T^{(m)}\right) = \mathbf{I}^{*-1} : \mathbf{A}\left(\overset{\circ}{T}{}^{(m)} + T^{(m)}\right),$$

$$\mathbf{I}^{*} = \delta_{it}\delta_{jq} + a_{ijks}\left(\overset{\circ}{T}{}^{(m)} + T^{(m)}\right)r_{ijks}^{p\sigma}.$$

Проте для визначення скінченно малих приростів пластичних деформацій $\Delta\varepsilon_{ij}^{p(mq)}$ за допомогою співвідношення (1) і скінченно малих приростів напружень $\Delta\sigma_{ij}^{(mq)}$ відповідно до (2) необхідно визначати значення скалярного множника $\Delta\lambda^{(q)}$, який визначає величину приросту пластичних деформацій у точках тіла. Для цього запишемо рівняння поверхні пластичного течіння $F\left(\overset{\circ}{\hat{\boldsymbol{\sigma}}}{}^{(m)} + \hat{\boldsymbol{\sigma}}^{(mq)} + \Delta\hat{\boldsymbol{\sigma}}^{(mq)}, \overset{\circ}{T}{}^{(m)} + T^{(m)}\right) = 0$ у вигляді

$$F\left(\overset{\circ}{\hat{\boldsymbol{\sigma}}}{}^{(m)} + \hat{\boldsymbol{\sigma}}^{(mq)} + r_{ij}^{\sigma 0} + r_{ij}^{\sigma\lambda}\Delta\lambda^{(q)} + r_{ijks}^{\sigma\varepsilon}\Delta\varepsilon_{ks}^{(mq)}, \overset{\circ}{T}{}^{(m)} + T^{(m)}\right) = 0. \quad (3)$$

Для лініаризації даного співвідношення відносно $\Delta\lambda^{(q)}$ використаємо метод Ньютона. Нехай $\Delta\lambda^{(q)(p)}$ – деяке наближення шуканої скалярної величини $\Delta\lambda^{(q)}$ на p-тій ітерації. Тоді значення $\Delta\lambda^{(q)}$ на $(p+1)$-й ітерації може бути записане у вигляді

$$\Delta\lambda^{(q)(p+1)} = \Delta\lambda^{(q)(p)} + \delta\lambda^{(q)(p)}, \qquad ()$$

де $\delta\lambda^{(q)(p)}$ є величиною вищого порядку мализни у порівнянні з $\Delta\lambda^{(q)(p)}$.

Рівняння поверхні пластичного течіння (3) з урахуванням значення $\Delta\lambda^{(q)(p+1)}$ (4) буде мати вигляд

$$F\left(\boldsymbol{\sigma}^{F(mqp)}, \overset{\circ}{T}{}^{(m)} + T^{(m)}\right) = 0\,, \qquad (5)$$

де $\sigma_{ij}^{F(mq)(p)} = \overset{\circ}{\sigma}{}_{ij}^{(m)} + \sigma_{ij}^{(mq)} + r_{ij}^{\sigma 0} + r_{ij}^{\sigma\lambda}\Delta\lambda^{(q)(p)} + r_{ijks}^{\sigma\varepsilon}\Delta\varepsilon_{ks}^{(mq)} + + r_{ij}^{\sigma\lambda}\delta\lambda^{(q)(p)}$.

Розкладемо фуннкцію F, яка визначає поверхню течіння (5), у ряд Тейлора в околі точки

$$\hat{\boldsymbol{\sigma}}^{\circ(m)} + \hat{\boldsymbol{\sigma}}^{(mq)} + \mathbf{r}^{\sigma 0} + \mathbf{r}^{\sigma\lambda}\Delta\lambda^{(q)(p)} + \mathbf{r}^{\sigma\varepsilon} : \Delta\boldsymbol{\varepsilon}^{(mq)}.$$

Отримаємо

$$F\left(\overset{\circ}{\boldsymbol{\sigma}} + \boldsymbol{\sigma}^{(q)} + \mathbf{r}^{\sigma 0} + \mathbf{r}^{\sigma\lambda}\Delta\lambda^{(q)(p)} + \mathbf{r}^{\sigma\varepsilon} : \Delta\boldsymbol{\varepsilon}^{(q)}, \overset{\circ}{T} + T\right) +$$

$$\frac{\partial F\left(\overset{\circ}{\boldsymbol{\sigma}} + \boldsymbol{\sigma}^{(q)} + \mathbf{r}^{\sigma 0} + \mathbf{r}^{\sigma\lambda}\Delta\lambda^{(q)(p)} + \mathbf{r}^{\sigma\varepsilon} : \Delta\boldsymbol{\varepsilon}^{(q)}, \overset{\circ}{T} + T\right)}{\partial\boldsymbol{\sigma}} : r^{\sigma\lambda}\delta\lambda^{(p)(q)} = 0\,.$$

Отже,

$$\delta\lambda^{(p)(q)} = -\left[\frac{\partial F\left(\overset{\circ}{\boldsymbol{\sigma}} + \sigma^{(q)} + \mathbf{r}^{\sigma 0} + \mathbf{r}^{\sigma\lambda}\Delta\lambda^{(q)(p)} + \mathbf{r}^{\sigma\varepsilon} : \Delta\boldsymbol{\varepsilon}^{(q)}, \overset{\circ}{T} + T\right)}{\partial\boldsymbol{\sigma}} : \mathbf{r}^{\sigma\lambda}\right]^{-1} \times$$

$$\times F\left(\overset{\circ}{\boldsymbol{\sigma}} + \boldsymbol{\sigma}^{(q)} + \mathbf{r}^{\sigma 0} + \mathbf{r}^{\sigma\lambda}\Delta\lambda^{(q)(p)} + \mathbf{r}^{\sigma\varepsilon} : \Delta\boldsymbol{\varepsilon}^{(q)}, \overset{\circ}{T} + T\right). \qquad (6)$$

Числовий алгоритм для обчислення термопластичного НДС на m-му часовому інтервалі можна записати у вигляді

1. Обчислюємо приріст температурного поля T_m.

$$\overset{\circ}{T}{}^{(m+1)} = \overset{\circ}{T}{}^{(m)} + T^{(m)};$$

2. Лічильник ітерацій $q = -1$;

3. $\vec{u}_i^{(m,q+1)} = 0$, $\varepsilon_{ij}^{(m,q+1)} = 0$, $\sigma_{ij}^{(m,q+1)} = 0$, $\lambda^{(q+1)} = 0$; $q = q + 1$;

4. Обчислюємо $\Delta\vec{u}_i^{(mq)}$ із співвідношення рівноваги

$$\int_V (\overset{\circ}{\sigma}{}_{ij}^{(m)} + \sigma_{ij}^{(mq)} + \Delta\sigma_{ij}^{(mq)})\delta\varepsilon_{ij}^{(m)} dV =$$

$$= \int_V (\overset{\circ}{Q}{}_i^{(m)} + Q_i^{(m)})\delta u_i^{(m)} dV + \int_{S_\sigma} (\overset{\circ}{\sigma}{}_{vi}^{(m)} + \sigma_{vi}^{(m)})\delta u_i^{(m)} dS\,;$$

5. Лічильник ітерацій для обчислення $\Delta\lambda^{(q)}$ $p=-1$;
6. $p=p+1$;
7. $\Delta\lambda^{(q)(p+1)}=0$;
8. Обчислюємо $\delta\lambda^{(p)(q)}$ згідно (6);
9. $\Delta\lambda^{(q)(p+1)}=\Delta\lambda^{(q)(p)}+\delta\lambda^{(q)(p)}$;
10. Якщо виконується умова

$$\left\|\delta\lambda^{(p)(q)}\right\|_2 \le \beta_\lambda \left\|\lambda^{(q)}+\Delta\lambda^{(q)(p+1)}\right\|_2,$$

де β_λ – точність знаходження $\lambda^{(q)}$, то переходимо на наступний крок. У протилежному випадку переходимо на крок 9;

11. $\Delta\lambda^{(q)}=\Delta\lambda^{(q)(p+1)}$;
12. Визначаємо $\Delta\varepsilon_{ij}^{p(mq)}$ і $\Delta\sigma_{ij}^{(mq)}$ згідно (1) і (2);
13. $\vec{\mathbf{u}}^{(m,q+1)}=\vec{\mathbf{u}}^{(mq)}+\Delta\vec{\mathbf{u}}^{(mq)}$, $\hat{\boldsymbol{\varepsilon}}^{(m,q+1)}=\hat{\boldsymbol{\varepsilon}}^{(mq)}+\Delta\hat{\boldsymbol{\varepsilon}}^{(mq)}$, $\hat{\boldsymbol{\sigma}}^{(m,q+1)}=\hat{\boldsymbol{\sigma}}^{(mq)}+\Delta\hat{\boldsymbol{\sigma}}^{(mq)}$, $\lambda^{(q+1)}=\lambda^{(q)}+\Delta\lambda^{(q)}$;
14. Якщо виконується умова

$$\left\|\Delta\vec{\mathbf{u}}^{(mq)}\right\|_2 \le \beta\left\|\overset{\circ}{\vec{\mathbf{u}}}{}^{(m)}+\vec{\mathbf{u}}^{(mq)}\right\|_2,$$

де β – точність розв'язку задачі, то переходимо на наступний крок. У протилежному випадку переходимо на крок 4;

15. $\vec{\mathbf{u}}^{(m)}=\vec{\mathbf{u}}^{(m,q+1)}$, $\hat{\boldsymbol{\varepsilon}}^{(m)}=\hat{\boldsymbol{\varepsilon}}^{(m,q+1)}$, $\hat{\boldsymbol{\sigma}}^{(m)}=\hat{\boldsymbol{\sigma}}^{(m,q+1)}$, $\lambda=\lambda^{(q+1)}$;
16. Обчислюємо $\overset{\circ}{\hat{\boldsymbol{\sigma}}}{}^{(m+1)}=\overset{\circ}{\hat{\boldsymbol{\sigma}}}{}^{+(m)}+\hat{\boldsymbol{\sigma}}^{(m)}$ згідно $\overset{\circ}{\sigma}{}_{ij}^{(m+1)}=\overset{\circ}{\sigma}{}_{ij}^{+(m)}+\sigma_{ij}^{(m)}$;
17. $m=m+1$;
18. Якщо $\tau_{m+1}<\tau_M=t$, то переходимо на крок 1;
19. Зупинка.

Побудована числова схема розв'язування задачі про термопружнопластичне деформування просторових тіл за теорією пластичного течіння дозволяє ефективніше використовувати обчислювальні ресурси завдяки застосуванню методу проміжної точки для визначення скінченного приросту пластичних деформацій.

1. Муха І.С. Числове дослідження термопластичного деформування товстостінної циліндричної панелі під рухомим тепловим навантаженням / І.С. Муха, Д.М. Неспляк // Сучасні проблеми механіки

та математики: В 3-х т. / Під заг. ред. Р.М. Кушніра, Б.Й. Пташника. – Львів: Інститут прикладних проблем механіки і математики ім. Я.С. Підстригача, 2013. – Т. 1. – С. 155-157.
2. Муха І.С. Комп'ютерне моделювання нелінійних процесів теплопровідності у тонкостінних тілах складної форми / І.С. Муха, Д.М. Неспляк // Вісник Львівського університету. Серія прикл. мат. та інформ. – 2007. – Вип. 11. – С. 134-140.
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. Савченко В.Г. Методы исследования термовязкопластического деформирования трехмерных элементов конструкций (обзор) / В.Г. Савченко, Ю. Н. Шевченко // Прикл. механика. – 1993. – 29, № 9. – С. 3-19.
5. Савченко В.Г. Метод исследования неосесимметричного неупругого деформирования тел вращения с учетом вида напряженного состояния / В.Г. Савченко // Прикл. механика. – 2008. – 44, № 9. — С. 26-35.
6. Савченко В.Г. Пространственные задачи термовязкопластичности / В.Г. Савченко, Ю.Н. Шевченко // Прикл. механика. – 2000. – 36, № 11. – С. 3-38.
7. Шевченко Ю.Н. К решению краевых задач термовязкопластичности при сложных неизотермических процессах нагружения / Ю.Н. Шевченко // Прикл. механика. – 1985. – 21, № 4. – С. 119-127.

РОЗРОБЛЕННЯ ІНФОРМАЦІЙНО-ПОШУКОВОЇ СИСТЕМИ «БОТАНІЧНИЙ САД НЛТУУ»

Коширець Світлана Іванівна,
доцент кафедри інформаційних технологій НЛТУУ, к.т.н.
Бичинюк Ігор Васильович,
викладач кафедри інформатики ЛьвДУВС
Бичинюк Оксана Василівна,
магістр НЛТУУ

Розроблено інформаційно-пошукову, web-орієнтовану систему для ведення колекційного фонду ботанічного саду. Модель бази даних розроблена та фізично реалізована на платформі

MySQL, яка містить 9 таблиць, пов'язаних реляційним зв'язком, та заповнена достовірною інформацією, згідно вимог спеціалістів даного профілю. Web-орієнтований додаток дозволяє доповнювати, коригувати та видаляти дані таблиць, візуалізує дані за різними критеріями пошуку як однієї, так і багатьох таблиць, пов'язаних між собою реляційним зв'язком. Доступ до даних інформаційно-пошукової системи здійснюється згідно привілеїв. Розроблена програма реалізована на віддаленому сервері «хмарі». Запропоновані технології створення інформаційно-пошукової системи можуть бути використані як працівниками ботанічного саду, так і в навчальному процесі студентами вищих навчальних закладів.

Вступ. Для ведення колекційного фонду ботанічного саду, зокрема Національного лісотехнічного університету України, існують програмні продукти, які дозволяють виконувати деякі операції з даними, крім того, вони не розраховані на віддалений доступ, тому актуальною є розробка інформаційно-пошукової системи, що б дозволяла, використовуючи можливість клієнт-серверних баз даних, здійснювати доступ до віддаленого серверу, що містить потрібну інформацію, опрацьовувати її та здійснювати візуалізацію за певними критеріями, уникнувши не комп'ютеризованого опрацювання інформації.

Використані технології:

MySQL Workbench – інструмент для візуального проектування баз даних, що інтегрує проектування, моделювання, створення й експлуатацію БД в єдине безшовне оточення для системи баз даних MySQL.

PHP – скриптова мова програмування, яка була створена для генерації HTML-сторінок на стороні web-сервера. Це широко використовувана мова сценаріїв загального призначення з відкритим вихідним кодом.

Каскадні таблиці стилів (англ. Cascading Style Sheets або скорочено CSS) – спеціальна мова, що використовується для відображення сторінок, написаних мовами розмітки даних.

NetBeans IDE – вільне інтегроване середовище розробки (IDE) для мов програмування Java, JavaFX, C/C++, PHP, JavaScript, HTML5, Python, Groovy. Середовище може бути встановлене і для

підтримки окремих мов, і у повній конфігурації. Середовище розробки NetBeans за умовчанням підтримує розробку для платформ J2SE і J2EE.

Хмарні сервіси дозволяють перенести обчислювальні ресурси й дані на віддалені інтернет-сервери, дозволяють отримати послуги з високим рівнем доступності (англ. high availability) і низькими ризиками непрацездатності, забезпечити швидке масштабування обчислювальної системи завдяки еластичності без необхідності створення, обслуговування і модернізації власної апаратної інфраструктури, [1].

Створення БД. На основі каталогу рослин Ботанічного саду Національного лісотехнічного університету України [2], було створено базу даних для інформаційно-пошукової системи.

Реалізовано 9 таблиць (рис. 1), які зв'язані між собою реляційним зв'язком, [3].

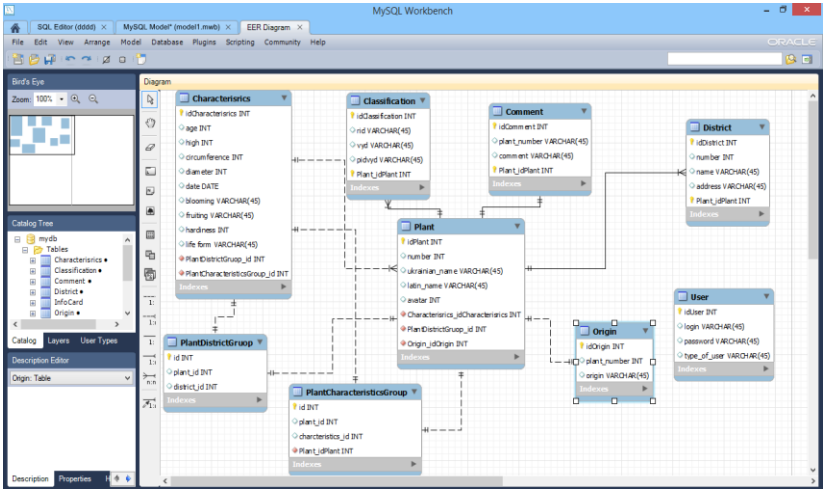


Рис. 1. – ER діаграма бази даних

Призначення таблиць бази даних:

- Characteristics містить в собі дані про характеристики рослин, а саме: вік, висота, окружність, діаметр, цвітіння, плодоношення, зимостійкість.
- Classification призначена для ведення класифікації рослин за такими критеріями: рід, вид, родина, порядок, клас, підклас, надклас, відділ, царство, домен.

- Comment містить поля коментарів стосовно рослин та номер рослини.
- Plant відображає наступні дані про рослину: українська назва, латинська назва, фото.
- District слугує для збереження даних про ділянки Ботанічного саду НЛТУУ, а саме: назва ділянки, номер ділянки, адреса.
- User є системною таблицею і містить інформацію про тип користувачів, їх логіни і паролі.
- InfoCard містить дані про користувачів системи, їхні імена, прізвища, по-батькові, стать та фото.
- PlantCharacteristicsGroup та PlantDistrictGroup слугують для реалізації зєднання між таблицями із зв'язком n:n.

Для реалізації бази даних вибрано СУБД MySQL, дана база є клієнт-серверною і дозволяє підтримувати розподілені технології, володіє всіма необхідними функціями для адміністрування, основною перевагою є її некомерційність, що значно розширює можливість використання розробленої інформаційно-пошукової системи, [4].

Для моделювання даних, розроблення бази, її адміністрування для MySQL розроблено зручний додаток в Workbench, [5].

Можливості інформаційно-пошукової системи. Використовуючи мову PHP та засоби NetBeans розроблено основну сторінку сайту (рис. 2). Дана сторінка дає змогу логування згідно наданих привілеїв: адміністратор, працівник, звичайний користувач, [6].

Адміністратор має право редагувати базу даних: доповнювати, коригувати та вилучати інформацію, використовувати всі розроблені засоби для пошуку інформації. Крім того, здійснювати адміністрування бази: створювати нових користувачів та надавати їм привілеї, вилучати користувачів та коригувати існуючі привілеї. Також адміністратор має право створювати нові таблиці бази даних, вилучати чи змінювати їх структуру, [7]. Працівник має право доступу та ведення каталогу рослинного фонду, що знаходиться в базі даних. Звичайний користувач має право перегляду даних бази.

Основна сторінка дозволяє активувати основні функції сайту, об'єднані в розділи, які активуються відповідно до типу користувача. Розглянемо основні функції сайту. Вони поділені на три блоки: «Ботанічний сад» – дає змогу візуалізації інформації про складові частини ботанічного саду (дендропарк, дендрарій, арборетум, декоративний розсадник), засоби пошуку (рис. 3) та перехід на головну сторінку.

Рис. 2. – Основна сторінка сайту

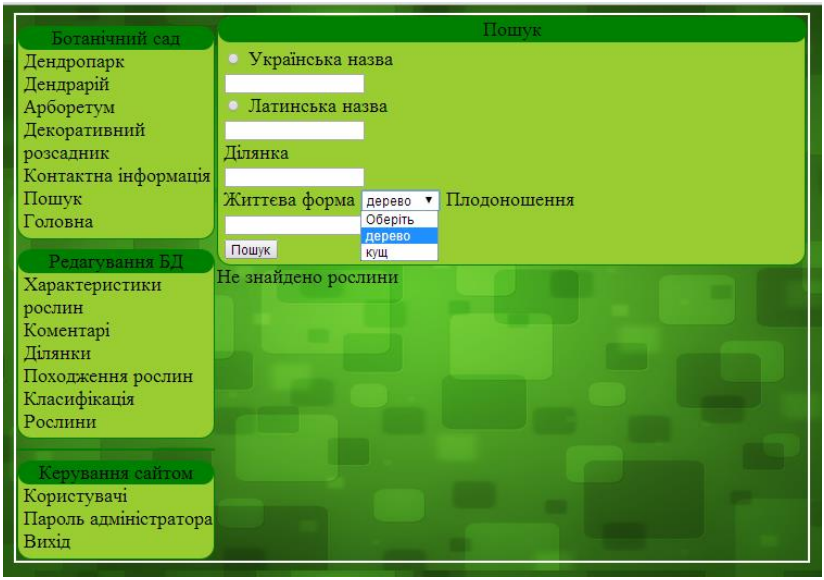


Рис. 3. – Форма для здійснення пошуку даних

Наступним болоком є «Редагування бази даних», який дає змогу працювати з кронкретною інформацією бази: доповнювати, вилучати чи редагувати дані таблиць бази даних працівником або адміністратором (рис. 4).

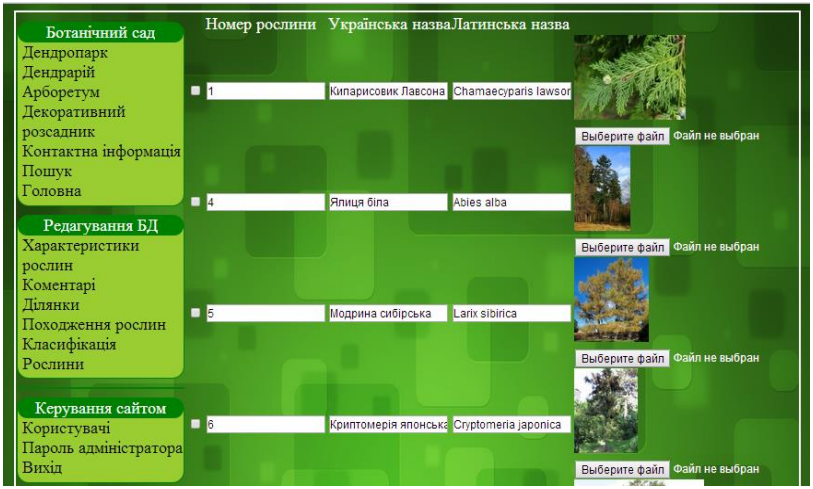


Рис. 4. – Форма для підтримання даних таблиць в актуальному стані

Блок «Керування сайтом» (рис. 5) є доступним лише адміністратору сайту і дозволяє керувати паролями і даними користувачів, надавати привілеї доступу та переглядати інформацію [8].

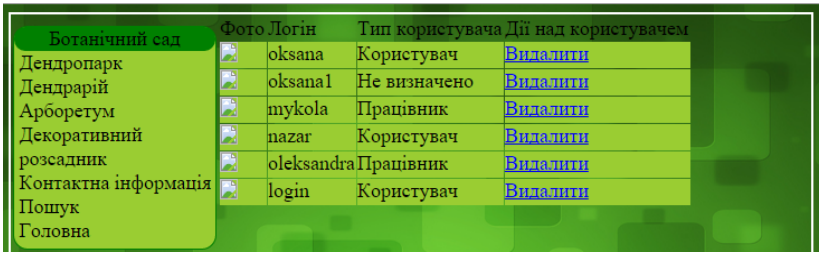


Рис. 5. – Форма для керування адміністратором даними користувачів

Висновки. Для ведення колекційного фонду ботанічного саду було розроблено інформаційно-пошукову, web-орієнтовану систему. Розроблена модель бази даних та фізично реалізована на платформі MySQL, яка містить 9 таблиць, пов’язаних реляційним зв’язком, та заповнена достовірною інформацією, згідно вимог

спеціалістів даного профілю. Розроблено сайт, що дозволяє доповнювати, коригувати та видаляти дані таблиць, візуалізовано дані за різними критеріями пошуку як однієї, так і багатьох таблиць, пов'язаних між собою реляційним зв'язком. Для надання привілеїв доступу до даних, розроблено три типи користувачів: адміністратор, працівник, користувач.

Запропоновані технології створення інформаційно-пошукової системи можуть бути використані як працівниками ботанічного саду, так і в навчальному процесі студентами вищих навчальних закладів.

1. http://uk.wikipedia.org/
2. Третяк П.Р. Каталог рослин Ботанічного саду Національного лісотехнічного університету України / П.Р. Третяк / Довідн. Посібник. – Львів : НЛТУ України, 2006. – 40с.
3. Хомоненко А. Работа с базами даннях / А. Хомоненко, С. Ададуров/. – С.Петербург : БХВ-Петербург, 2006. – 478с.
4. Пасічник В.В. Організація баз даних та знань / В.В. Пасічник, В.А. Резніченко /. – Київ: ВНV, 2006. – 383с.
5. Илюшечкин В.М. Основы использования и проектирования баз даннях / В.М. Илюшечкин / Учебное пособие для ВТУЗОв. – Юрайт, 2009. – 213с.
6. Кузин А.В. Базы данных / А.В. Кузин / – М: Academia, 2008. – 320с.
7. Кузин А.В. Базы данных : учебное пособие для вузов / А.В. Кузин.– М : Академія, 2005. – 320с.
8. http://www.botsad.nltu.edu.ua/

РОЗВИТОК ЛЮДСЬКОГО КАПІТАЛУ В УМОВАХ СТАНОВЛЕННЯ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Подра Ольга Павлівна,
доцент кафедри менеджменту ЛьвДУВС, к.е.н.
Кунцик Роман Володимирович,
студент ЛьвДУВС

Сучасна економіка характеризується динамічним розвитком, ускладненням господарських відносин, виникненням нових форм організації та методів управління, підвищеною роллю

людського чинника у економічному зростанні. Глобалізація господарських процесів, сприяє поширенню знань та інформації у світовому масштабі і, як наслідок, зменшенню розриву в технологічному розвитку між країнами.

Розвиток інноваційних технологій та перебудова соціальних структур під впливом інформаційного суспільства створює передумови для зміни відносин власності, вартості, товарно-грошових відносин; зростання ролі людського капіталу з високими якісними характеристиками. Основними рисами інформаційного суспільства є створення глобального інформаційного простору, що здатен забезпечити нову якість життя, збільшення ваги інформаційно-комунікаційних технологій та на їх основі продуктів і послуг у виробництві ВВП; поява якісно нових інформаційно-комунікаційних технологій, що здатні забезпечити доступ до національних та світових інформаційних ресурсів, сприятимуть подоланню інформаційної нерівності шляхом задоволення потреб населення в інформаційних продуктах та послугах.

В інформаційному суспільстві значення трудових ресурсів актуалізується і вони розглядаються виключно з позиції людського капіталу, що в процесі реалізації створює додаткову вартість. Аналізуючи сучасний стан розвитку України, можна зробити висновок, що в країні переважає індустріальний спосіб виробництва, однак, необхідно відмітити, що паралельно з розвитком індустріальної економіки відбувається інтенсивна інформатизація всіх сфер життя, внаслідок чого новітні інформаційні технології перетворюються у чинник соціально-економічного та духовно-інтелектуального розвитку суспільства, що висуває нові вимоги до якості людського капіталу.

У умовах глобалізації людський капітал, а особливого його інтелектуальний потенціал виступає базисом для інноваційної економіки та впливає на рівень конкурентоспроможності країни. Перехід на наукомісткі та високотехнологічні види виробництва сприяє прискореному накопиченню інтелектуального капіталу, перетворюючи його у головну виробничу силу. Про невизначеність стратегії інформаційно-інноваційного розвитку України свідчать оцінки світового рейтингу національних економік, який щорічно публікується Всесвітнім економічним форумом (ВЕФ).

Результати цього дослідження представленні у «The Global Competitiveness Report. World Economic Forum 2012-2013». Згідно із даними Звіту 2012 р. Україна піднялася на 7 позицій і зайняла 82 місце за індексом глобальної конкурентоспроможності (ІГК), країни лідери – Швейцарія, Сінгапур, Швеція, Фінляндія, США та ін. [1].

Характерною особливістю країн-лідерів за ІГК є домінування в структурі економіки значної частки інтелектуальної та високотехнологічної праці, що є ознакою високого конкурентоспроможного людського капіталу.

У цьому контексті необхідно виділити групу Скандинавських країн, що характеризуються високими показниками розвитку інформаційного суспільства та поступовим переходом до економіки знань на основі людського капіталу. Досвід Фінляндії у побудові інформаційної економіки заслуговує уваги, оскільки країна здійснила ряд реформ щодо прискореного розвитку комп'ютерної інфраструктури, засвоєння інформаційних технологій дітьми та молоддю, модернізації системи вищої та професійної освіти тощо. Рейтинг України за основними складовими є досить низьким, що свідчить про неефективність управління економікою і сконцентрованість на вирішенні поточних проблем, зростання відмежування фундаментальної науки від освіти, а освіти від економічної практики, втрату у суспільства інтересу до нових знань, інновацій та інформації.

Така ситуація вимагає впровадження дієвих механізмів нарощення людського капіталу, на основі інтелектуалізації праці та стимулювання технологічного та інноваційного розвитку, що забезпечать перехід до інформаційного суспільства.

З метою переходу України до інформаційного суспільства, недопущення інформаційної ізоляції та ще більшого відставання від економічно розвинутих країн було прийнято низку законодавчих актів: ЗУ «Про Концепцію Національної програми інформатизації»; «Про Національну програму інформатизації»; «Про основні засади розвитку інформаційного суспільства України на 2007–2015 роки»; «Про електронні документи та електронний документообіг»; «Про електронний цифровий підпис»; «Про захист персональних даних», які спрямовані на прискорення

розробки та впровадження новітніх конкурентоспроможних інформаційно-комунікаційних технологій в економіку та сфери суспільного життя, підвищення рівня комп'ютерної та інформаційної грамотності населення, розвиток інформаційної інфраструктури, її узгодженість з світовою, створення загальнодержавних інформаційних систем, в першу чергу в сферах охорони здоров'я, освіти, науки, культури з метою покращання їх роботи та забезпечення доступу населення, до необхідних інформаційних ресурсів.

Водночас, необхідно зазначити, що в Україні відбувається зростання обсягів інформатизації та готовності населення до використання інформаційних технологій, а отже переходу до інформаційного суспільства. Так, за чисельністю Інтернет-користувачів станом на 2011 р. Україна займає 9 місце в Європі, лідерами є Німеччина – 65100 тис. осіб, Росія – 60000 тис. осіб, Великобританія – 51400 тис. осіб, Франція – 45200 тис. осіб [2, с. 27].

Однак, позитивні зміни в комп'ютеризації та інформатизації в Україні ще не свідчать про істотні зрушення в матеріально-технічному забезпеченні інформаційної сфери. Зокрема за даними дослідження КМІС 34,6 % опитаних відчувають технічні бар'єри у доступі до Інтернет, з яких у 26,9 % опитаних відсутній доступ до комп'ютера, а у 7,7% – технічна можливість підключення до Інтернет. Чисельність користувачів Інтернет знаходиться у лінійній залежності від рівня освіти, так, 41 % складають особи з вищою освітою, 37,4 % – з неповною вищою та середньою спеціальною освітою, 20,7 % – особи з повною загальною середньою освітою, 0,8 % – особи з неповною середньою освітою [2, с. 28]. Тобто, можемо констатувати невідповідність системи освіти та рівня технічного забезпечення вимогам розвитку інформаційного суспільства, що спричиняє зниження конкурентоспроможності людського капіталу.

З метою подолання зазначеної невідповідності необхідно вжити ряд заходів, зокрема: забезпечити підключення до Інтернет навчальних закладів, лікувально-оздоровчих, наукових, культурних закладів; внести зміни до програм навчальних закладів відповідно до вимог інформаційного суспільства; забезпечити доступ населення до інформаційно-комунікаційних технологій та усунути технічні бар'єри.

Зазначені зміни сприятимуть становленню та розвитку інформаційного суспільства, підвищенню рівня конкурентоспроможності людського капіталу на основі покращання його якісних характеристик, що відповідають потребам ринку праці та вимогам роботодавців, а отже забезпечать високу віддачу здійснених інвестицій та досягнення економічних, фінансових чи статусних ефектів.

1. The Global Competitiveness Report / World Economic Forum 2012-2013 // [Електрон. ресурс]. – Режим доступу: http://www3.we-forum.org/docs/WEF_GCR_Report_2011-12.pdf
2. Доповідь про стан інформатизації та розвиток інформаційного суспільства в Україні за 2011 рік. – К., 2011. – 94 с.

ІНФОРМАЦІЙНА СИСТЕМА МОДЕЛЮВАННЯ ЗАБРУДНЕННЯ ПОВІТРЯ АВТОТРАНСПОРТОМ

Дендюк Михайло Володимирович,
доцент кафедри інформаційних технологій НЛТУУ, к.т.н
Онукевич Володимир Вікторович,
магістр НЛТУУ

Інтенсивний розвиток автомобілебудування призвів до негативних змін у навколишньому середовищі, а саме: забруднення атмосфери, гідросфери і літосфери, що особливо помітно насамперед у великих містах, де автотранспорт є, мабуть, основним джерелом забруднення повітря.

Збільшення кількості автомобілів на дорозі прямо пропорційно впливає на підвищення рівня забруднення повітря різними токсичними речовинами, але основним критерієм, який потрібно мінімізувати для покращення середовища проживання людей є концентрація оксиду вуглецю.

З огляду на сказане вище проблеми моделювання розподілу CO вздовж доріг є актуальним.

Метою роботи є створення інформаційної системи моделювання забруднення повітря автотранспортом, яка допоможе визначати рівень оксиду вуглецю на певній ділянці і рекомендацій що до оптимальних планування забудови і озеленення з врахуванням параметрів руху.

Математична модель. Теоретичною моделлю поширення домішок від одиничного джерела є *рівняння дифузії в циліндричних координатах [2]:*

$$div(k\,grad U) - \alpha U = -f(r,\varphi,z), \qquad (1)$$

де k – складові коефіцієнта обміну; α – коефіцієнт, що визначає зміну концентрації за рахунок перетворень домішок; U – концентрація домішок; r – відстань від джерела; z – відстань за вертикаллю; φ – кут повороту відносно осі.

У разі одиничного точкового джерела з урахуванням $f(r,\varphi,z)$ в найзагальнішому вигляді рівняння (1) має вигляд [1]:

$$\frac{\partial}{\partial z}k_z\frac{\partial U}{\partial z}+\frac{1}{r}\frac{\partial}{\partial r}k_r\frac{\partial U}{\partial r}+\frac{1}{r^2}\frac{\partial^2 U}{\partial \varphi^2}-\alpha U+\frac{M}{2\pi r}\delta(r)\delta(z-H)=0, \qquad (2)$$

де M – маса викиду за одиницю часу, δ – функції:

$$\delta(r)=\begin{cases}0, r\neq 0;\\ 1, r=0;\end{cases}\quad \delta(z-H)=\begin{cases}0, z\neq H;\\ 1, z=H.\end{cases} \qquad (3)$$

Як видно з рівняння (3), джерело забруднення розташоване в точці $r = 0$ на висоті H. У точці, відмінній від $r = 0$, рівняння набуває вигляду [2]:

$$\frac{\partial}{\partial z}k_z\frac{\partial U}{\partial z}+\frac{1}{r}\frac{\partial}{\partial r}rk_r\frac{\partial U}{\partial r}+\frac{1}{r^2}\frac{\partial^2 U}{\partial \varphi^2}-\alpha U=0 \qquad (4)$$

Проведемо переріз φ = const по лінії максимального забруднення вздовж факела на висоті z = const :

$$\left.\frac{\partial}{\partial z}k_z\frac{\partial U}{\partial z}\right|_{\substack{\varphi=const\\ z=const}}=g_1(r,U);$$

$$\left.\frac{1}{r^2}\frac{\partial^2 U}{\partial \varphi^2}\right|_{\substack{\varphi=const\\ z=const}}=g_2(r,U) \qquad (5)$$

і рівняння дифузії (3) перетворюється на одновимірне:

$$\frac{1}{r}\frac{\partial}{\partial r}rk_r\frac{\partial U}{\partial r}+g_1(r,U)+g_2(r,U)-\alpha U=0, \qquad (6)$$

де

$$g_1(r,H,U)=a_0\frac{H(U_{i-1}-U_i)}{r_i}+f_1\left(\frac{U_{i-1}-U_i}{r_i},U_i,U_{i-1},\frac{1}{r_i}\right); \qquad (7)$$

$$g_2(r,H,U) = b_0 \frac{H(U_{i-1} - U_i)}{r_i} + f_2\left(\frac{U_{i-1} - U_i}{r_i}, U_i, U_{i-1}, \frac{1}{r_i}\right); \quad (8)$$

$$\alpha = \alpha_1 H U_1,$$

де f_1, f_2 – лінійні функції.

Для розв'язування рівняння (7) запишемо похідні у вигляді різниць [1] та проаналізуємо вхідні фактори (табл. 1).

Задачу оптимізації стану навколишнього середовища можна розглядати як оптимізацію критерію планування забудови і озеленення з врахуванням параметрів руху. Тому спочатку оптимізуємо за параметрами x_3, x_4, x_5 та x_8, а потім – за рештою параметрів.

Алгоритм розрахунку. Уся ділянка, на якій моделюється розповсюдження забруднення СО, від проїжджої частини і на відстань 100 метрів розбивається на ряд дискретних значень з кроком k = 2,5 м. Кожній елементарній ділянці надаються значення густоти верхнього і нижнього рівнів забудови чи озеленення η_1 і η_2. Початкові значення концентрацій U_0 визначаються експериментально. Значення U_{i+1} розраховується за формулами, отриманими з різницевої схеми (7).

Таблиця 1

Вхідні фактори та їх умовні позначення [2]

Фактор	Умовні позначення
Загальна інтенсивність руху автотранспортних потоків, автомобілів/год.	x_1
Частка вантажних автомобілів і автобусів у загальному потоці, %	x_2
Поздовжній схил проїжджої частини, %	x_3
Висота вуличної забудови чи озеленення	x_4
Ширина вулиці до забудови чи озеленення, м	x_5
Ширина проїжджої частини, м	x_6
Середньозважена швидкість руху автомобілів у потоці, км/год.	x_7
Лінійна густота вуличної забудови чи озеленення	x_8
Температурний показник T, °С	$x_9 = T + 16$
Коефіцієнт неоднорідності складу автотранспортних потоків	x_{10}

Результати моделювання розповсюдження забруднення СО від автотранспорту вздовж проїжджої частини без озеленення та з озелененням наведено на рис. 1-2.

Висновки. Розроблена інформаційна система моделювання забруднення повітря автотранспортом дає змогу, виходячи з ширини вулиці, інтенсивності руху, типу і висоти озеленення та ряду інших факторів, забезпечити комфортне проживання людей, недопущення негативного впливу на їхнє здоров'я.

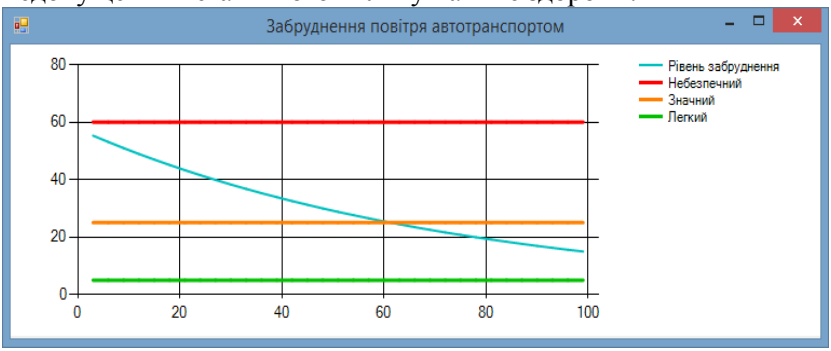


Рис.1. Поширення СО без озеленення

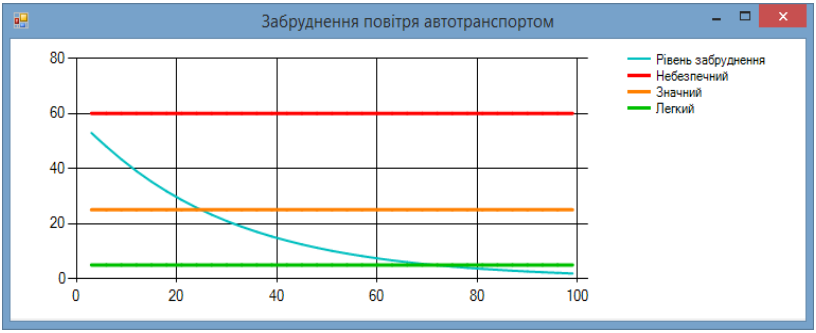


Рис.2. Поширення СО за наявністю озеленення

$$(\eta_1 = 0,5 \;_i\; \eta_2 = 0,7)$$

1. Формалев В.Ф. Численные методы / В.Ф. Формалев, Д.Л. Ревизников. – Изд. 2-е, испр., доп. – М.: ФИЗМАТЛИТ. – 2006. – 400 с.
2. Ковальчук П.І. Моделювання і прогнозування стану навколишнього середовища. Навч. посібник / П.І. Ковальчук. – К.: Либідь. – 2003. – 208 с.

3. Аксенов И.Я., Аксенов В.И. Транспорт и охрана окружающей среды. – М.: Транспорт,1986. – 176 с.
4. Безуглая Э.Ю. Мониторинг состояния загрязнения атмосферы в городах. – Л.: Гидрометеоиздат, 1986.

ПРОЕКТУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПРОГНОЗУВАННЯ СТАНУ ВОДНИХ РЕСУРСІВ ЗАХІДНОГО РЕГІОНУ УКРАЇНИ

Шабатура Юрій Васильович,
професор кафедри інформаційних технологій НЛТУУ, д.т.н., професор
Гузій Сергій Іванович,
магістр НЛТУУ

За допомогою MySql Workbench та Microsoft Visual Studio розроблено програмне забезпечення для відслідковування та прогнозування стану річок Західного регіону України.

Природні води являють собою складні розчини, що містять у своєму складі всі відомі хімічні елементи у вигляді простих та складних іонів, комплексних сполук, розчинених за газоподібних молекул, стабільних та радіоактивних ізотопів.

Різні види водокористування мають свої вимоги до якості, тому можуть існувати різні критерії розрахунку якості води для кожного з них.

Сучасна діяльність людини напряму пов’язана з раціональним використанням водних ресурсів тому відслідковування, розрахунок та прогнозування ступеню забруднення річок є однією з важливих ланок у нашому суспільстві.

Оцінка стану водних ресурсів на даному прикладі у річках за допомогою обрахунків умов поширення забруднюючих речовин є найважливішим етапом розробки системи та являється ключовим елементом в даній роботі.

Математична модель. За умови поширення забруднюючих речовин у річках рівняння в частинних похідних має такий вигляд:

$$\frac{\partial U}{\partial t} = \alpha^2 \frac{\partial^2 U}{\partial x^2} + \lambda(t,x)U - V\frac{\partial U}{\partial x} + f(t,x),$$

з граничними умовами:

$$U(t, x_0) = \xi\, x_0(t);$$
$$U(t, x_N) = \xi\, x_N(t).$$

Тут $U = U(t, x)$ – концентрація забруднюючої речовини; α – коефіцієнт турбулентної дифузії, м^2/сек; $V(t, x)$ – швидкість течії, м/с; $\lambda(t, x)$ – величина, що характеризує швидкість розпаду речовини (самоочищення потоку), 1/с; $f(t, x)$ – функція потужності джерела викидів, що лежить у початку координат

$$f(x,t) = \begin{cases} g(t) \ \textit{при} \ \ x = 0; \\ 0 \quad \textit{при} \ \ x > 0; \end{cases}$$

Розв'язування диференційного рівняння пов'язане зі значними труднощами, адже аналітично отримати чисельні розв'язки можна лише для деяких часткових випадків. Тому використаємо наближений числовий метод – метод скінчених різниць. Його ідея полягає в тому, що досліджувана область дискретизується (розбивається на сітку в просторі та часі), а похідні замінюємо на їх різницеві аналоги.

Структурна схема. Структурна схема комп'ютерної системи аналізу прогнозування стану водних ресурсів Західного регіону України подана на рис. 1.

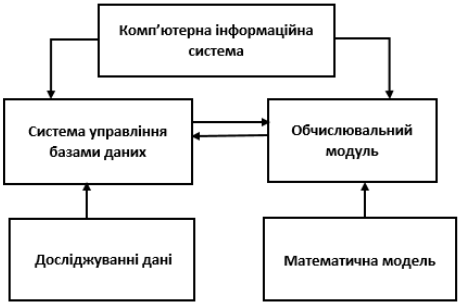


Рис. 1 Структурна схема комп'ютерної системи

Виходячи з даної структури, рішення для обчислення стану водної системи за допомогою ЕОМ можна зобразити в такій послідовності:

а) постановка задачі та її формалізований опис;

б) накопичення інформації;
в) обробка інформації;
г) аналіз;
д) використання результатів досліджень для прийняття рішень щодо покращення якості середовища водних об'єктів.

Розроблена структура класів в Microsoft Visual Studio на рис. 2 показує, що створено абстрактний класс River який наслідують декілька інших класів які відповідають західним областям та показані класи форм.

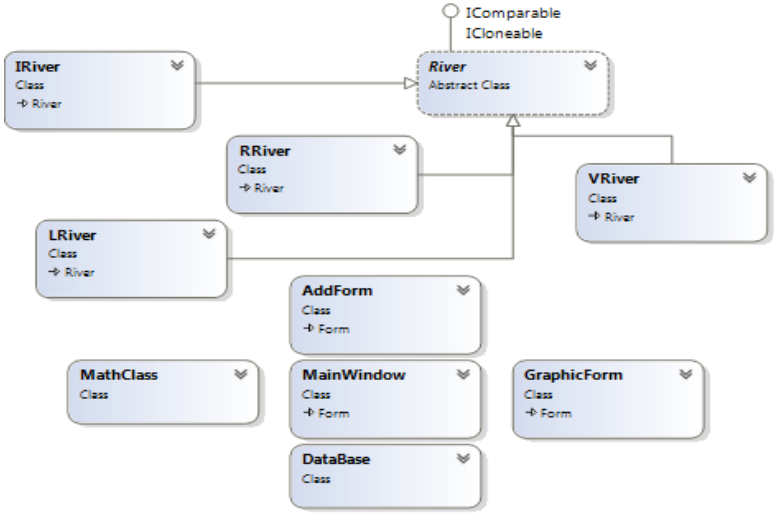


Рис 2. Структурна схема класів

Висновки. Розроблено структурну схему проектування та математичну модель інформаційної системи прогнозування стану водних ресурсів, показано структурну діаграму класів та математичну модель рівняння в частинних похідних за умов поширення забруднюючих речовин. Створено програмний продукт для зручного занесення даних та прогнозування стану річок Західного регіону України.

1. Ковальчук П.І. Моделювання і прогнозування стану навколишнього середовища. Навч. посібник / П.І. Ковальчук. – К.: Либідь. – 2003. – 208 с.

2. Методика встановлення і використання екологічних нормативів якості поверхневих вод суші та естуаріїв України / [В.Д. Романенко, В.М. Жукінський, О.П. Оксіюк та ін.]. – К.: Мінекоресурсів, 2001. – 48 с.
3. Сніжко С.І. Оцінка та прогнозування якості природних вод: Підручник. – К.: Ніка-Центр, 2001. – 264с.: іл.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ОЦІНЮВАННЯ ВЕЛИЧИНИ ПРИРОДНО-РЕСУРСНОГО ПОТЕНЦІАЛУ ЛЬВІВЩИНИ

Грицюк Мар'яна Юріївна,
викладач ЛДУ БЖД

Теорія ігор, як економіко-математична модель задачі прийняття рішень, спрямована на аналітичний аналіз конфліктних ситуацій. У грі проти природи [4] свідомо діє тільки один із гравців, який претендує на максимальний виграш $v_i(z_j)$ залежно від стану природи z_j. Інший гравець (природа) може приймати один зі своїх станів і не претендує на отримання виграшу. Гра проти природи здебільшого подається у вигляді платіжної матриці, елементами якої є виграші

$$\tilde{\tilde{Y}} = \left\{ \tilde{Y}_i = \{ y_{ij} = v_i(z_j),\ j = \overline{1,n} \},\ i = \overline{1,m} \right\} \qquad (1)$$

насамперед гравця $\tilde{X} = \{ x_i,\ i = \overline{1,m} \}$, проте, водночас, вони не є програшами природи $\bar{Z} = \{ z_j,\ j = \overline{1,n} \}$.

Отже, спробуємо дослідити гру з потенційними природно-ресурсними конфліктами на території Львівської області. При цьому гравцем $\tilde{X}$ є територіальна еколого-економічна система в умовних межах Стрийського району, стратегії вибору якого пов'язані з концепцією сталого розвитку [2]. Функція гри – використання природно-ресурсного потенціалу території.

Вибір стратегії поведінки гравця $\tilde{X}$ в такій грі проти природи здійснюється за такими критеріями [1]:

1) Критерій граничного оптимізму (max і max):

$$O = \max \left\{ \max \{ y_{ij},\ j = \overline{1,n} \},\ i = \overline{1,m} \right\} \Rightarrow i^*; x^* = x_{i^*}. \qquad (2)$$

2) Критерій крайнього песимізму Вальда:

$$W = \max\left\{\min\{y_{ij},\ j=\overline{1,n}\},\ i=\overline{1,m}\right\} \Rightarrow i^*; x^* = x_{i^*}. \quad (3)$$

3) Критерій оптимального песимізму Гурвіца:

$$H = \max\left\{\alpha \max\{y_{ij},\ j=\overline{1,n}\} + (1-\alpha)\min\{y_{ij},\ j=\overline{1,n}\},\ i=\overline{1,m}\right\}. \quad (4)$$

Критерій Гурвіца встановлює баланс між випадками граничного оптимізму і крайнього песимізму. Для обчислення значення цього критерію використовуються вагові коефіцієнти, відповідні значення яких можна обчислити за такими формулами:

$$\alpha^P = \frac{\Sigma V_1}{\Sigma V_1 + \Sigma V_2};\ \alpha^O = \frac{\Sigma V_2}{\Sigma V_1 + \Sigma V_2};\ \alpha^R = 0{,}5 \quad (5)$$

де: α^P, α^O, α^R – вагові коефіцієнти відповідно песимізму, оптимізму та реального стану природи [1].

Результати експертного оцінювання величини природно-ресурсного потенціалу Стрийського району [3] подано в табл. 1:

- z_1 – стан природи, який відображає поточну еколого-економічну ситуацією в межах встановленої території;
- z_2 – стан природи, який відображає ситуацією досягнення екологічного порогу – неспроможності природи самостійно відновлюватися;
- z_3 – стан природи, який відображає ситуацією досягнення соціального порогу – наявності факту активних антагоністичних протистоянь;
- z_4 – стан природи, який відображає ситуацією досягнення порогу незворотності – наявності стану трансформації конфлікту в катастрофу;
- x_1 – стратегія перманентного екстенсивного економічного зростання;
- x_2 – стратегія перманентного інтенсивного економічного зростання;
- x_3 – стратегія сталої динаміки поточної ситуації;
- x_4 – стратегія сталої динаміки поточної ситуації та посилення охорони довкілля;
- x_5 – стратегія сталої динаміки поточної ситуації, посилення охорони довкілля та відтворення природних ресурсів;
- x_6 – стратегія зниження рівня забруднення;

- x_7 – стратегія зниження рівня забруднення, пасивної охорони довкілля;
- x_8 – стратегія зниження рівня забруднення, пасивної охорони довкілля та відтворення природних ресурсів;
- x_9 – стратегія зниження рівня забруднення, активної охорони довкілля.
- x_{10} – стратегія зниження рівня забруднення, активної охорони довкілля та відтворення природних ресурсів.

Прогноз, наведений у табл. 1, розраховано на 5 років, починаючи з 2014 року, тобто стан природи (z_1), який відображає поточну еколого-економічну ситуацією в межах встановленої території, є дійсним на поточний рік [1]. Відповідні розрахунки проведено в середовищі MS Excel.

Табл. 1. Результати експертного оцінювання величини природно-ресурсного потенціалу Стрийського району, тис. грн.

Стратегії вибору, $\tilde{X}$	Стан природи, $\overline{Z}$			
	z_1	z_2	z_3	z_4
x_1	3433,75	2493,06	1448,46	592,56
x_2	3817,56	3059,95	2089,06	1045,07
x_3	2564,14	2281,22	1779,56	810,74
x_4	2887,47	2257,79	1819,99	941,28
x_5	3589,17	3081,65	2038,43	1088,21
x_6	1315,60	1312,70	1213,09	511,02
x_7	1623,02	1567,89	1436,93	636,30
x_8	2261,54	1780,69	1573,33	758,04
x_9	1763,21	1815,32	1884,88	892,40
x_{10}	2619,15	2643,83	2159,19	918,61
$\max\{y_{ij}, i=\overline{1,m}\}$	3817,56	3081,65	2159,19	1088,21

Результати розрахунку величини природно-ресурсного потенціалу Стрийського району відносно прийнятих стратегій вибору за критеріями граничного оптимізму (maximax, *O*), крайнього песимізму Вальда (pessimistic, *W*), оптимального песимізму Гурвіца (*H*) з урахуванням відповідних вагових коефіцієнтів подано в табл. 2.

Вагові коефіцієнти оптимізму, песимізму та реалістичності, обчислені за формулою (5), мають такі значення:

$$\alpha^O = \frac{26020,96}{8194,23+26020,96} = 0,761;\ \alpha^P = \frac{8194,23}{8194,23+26020,96} = 0,239.$$

де: $\Sigma V_1 = \sum_{i=1}^{m} O_i = 26020,96$; $\Sigma V_2 = \sum_{i=1}^{m} W_i = 8194,23$.

Табл. 2. Результати розрахунку величини природно-ресурсного потенціалу Стрийського району, тис. грн.

Стратегії вибору, $\tilde{X}$	Критерії оцінювання				
	O_i	W_i	H_i^P	H_i^O	H_i^R
x_1	3433,75	592,56	1273,00	2753,31	2013,15
x_2	3817,56	1045,07	1709,06	3153,58	2431,32
x_3	2564,14	810,74	1230,67	2144,22	1687,44
x_4	2887,47	941,28	1407,37	2421,38	1914,38
x_5	3589,17	1088,21	1687,17	2990,21	2338,69
x_6	1315,60	511,02	703,71	1122,91	913,31
x_7	1623,02	636,30	872,61	1386,71	1129,66
x_8	2261,54	758,04	1118,12	1901,47	1509,79
x_9	1884,88	892,40	1130,09	1647,19	1388,64
x_{10}	2643,83	918,61	1331,78	2230,65	1781,22
$\max\{*_{ij}, i=\overline{1,m}\}$	3817,56	1088,21	1709,06	3153,58	2431,32

З табл. 2 видно, що практично за критерієм граничного оптимізму та критерієм оптимального песимізму Гурвіца з урахуванням відповідних вагових коефіцієнті потрібно реалізувати 2-гу стратегію (i*=2), тобто $x^* = x_2$ – стратегію перманентного інтенсивного економічного зростання, що відповідає певним прибуткам. Тільки за критерієм крайнього песимізму Вальда потрібно реалізувати 5-гу стратегію (i*=5), тобто $x^* = x_5$ – стратегію сталої динаміки поточної ситуації, посилення охорони довкілля та відтворення природних ресурсів, що відповідає прибутку у розмірі 1088,21 тис. грн.

Висновки. На конкретному прикладі показано доцільність використання математичного апарату теорії ігор, зокрема – гри проти природи для прогнозування появи та оцінювання наслідків екологічних конфліктів. Врахування результатів проведеного дослідження при прийнятті управлінських рішень дає змогу більш збалансовано підходити до забезпечення сталого розвитку на територіальному рівні.

1. Евланов Л.Г. Теория и практика принятия решений / Л.Г. Евланов. – М. : Изд-во «Экономика», 1984. – 176 с.
2. Екологічна програма Стрийського району на 2013-2017 роки. [Електронний ресурс]. – Доступний з http://stryirairada.gov.ua/rishennja /XVIIsesija/Programa%20ekologia.pdf
3. Охорона навколишнього природного середовища // Стрийська районна державна адміністрація : офіційний сайт. [Еле-ктронний ресурс]. – Доступний з http://stryi-rda.gov.ua/index.php?option= com_content& view=article&id=69&Itemid=53
4. Петрушенко М.М. Економічні «ігри проти природи»: модель прийняття рішень у сфері управління екологічними конфліктами / М.М. Петрушенко // Бізнес-інформ. – 2012. – № 4. – С. 130-132.

ВИКОРИСТАННЯ СУЧАСНИХ УПРАВЛІНСЬКИХ ТА ІТ ТЕХНОЛОГІЙ ФОРМУВАННЯ ІНТЕЛЕКТУАЛЬНОГО КАПІТАЛУ

Мойсеєнко Ірина Павлівна,
професор кафедри фінансів Львівського державного університету внутрішніх справ, д.е.н.

Сучасне управління інтелектуальним капіталом дозволяє припустити, що комплексне поєднання елементів його інтелектуального потенціалу даватиме нові синергетичні ефекти управління. Поєднання інструментів управління знаннями: комунікації та рефлексії, оргкультури підприємства, інформаційних технологій (технологічний підхід), ключових управлінських компетенцій забезпечує високий рівень адаптації внутрішніх можливостей до вимог зовнішнього середовища. Побудова бази знань, що відображає інтелектуальний капітал, проблеми функціонування та принципи прийняття рішень на основі використання структури інтелектуального потенціалу забезпечує конкурентоздатність. Використання законів організованості та стабілізації структур нового типу формує інноваційні характеристики підприємства.

Елементи сучасних теорій управління, такі як: організаційний процес (формування інфраструктурного капіталу), комунікація (формувння ключових компетенцій), рефлексія (формування

ринкового капіталу), об'єднуються в механізм управління інтелектуальним потенціалом на основі відповідних управлінських компетенцій.

Розвиток методів формування ключових компетенцій передбачає розробку принципів управління навчальними програмами на основі особливостей управлінської діяльності як інтегративного явища. Навчальні програми формування нових знань повинні відображати рівень знань про: базові елементи системи управління; компоненти управлінського процесу; рівні реалізації управлінської діяльності; методи формування компетенцій[1,2].

Моделі та методи, розроблені на основі концепції підприємства, що самонавчається, яка розвивається з 80-х р., мають високу евристичну цінність та допомагають підприємствам реалізовувати успішні навчальні програми. У 90-х роках дослідники в галузі менеджменту знань, відзначаючи специфічну обмеженість даного підходу, запропонували нову концепцію організаційного навчання на основі методики побудови систем управління знаннями. Нова концепція побудови системи управління знаннями відображає зв'язок між основними процесами підприємства: праця, навчання, організація [2].

Важливе значення для «парадигми знання» в умовах багатофакторності управлінських рішень мають нові підходи до визначення поняття «виробництва знань». Найефективнішим вважається підхід, для якого «характерні приклади використання знань, міждисциплінарність, різнорідність та організаційна розмаїтість, зв'язок з культурою та соціальною сферами підприємства та використання знань, розуміння важливості забезпечення якості з врахуванням соціальних критеріїв» [2].

Чинниками формування інтелектуального капіталу підприємства на основі використання підсистем управління знаннями та сучасних ІТ технологій є:

1. Зростання ролі та значення інтелектуального капіталу як нематеріальної форми капіталу в діяльності сучасних соціально-економічних систем.
2. Акцентування на системі знань як ключовому ресурсі в системі менеджменту.

3. Наявність причинно-наслідкового зв'язку між рівнем інтелекту, компетентністю, якістю інформації та результатами діяльності і ефективністю управління.
4. Закономірність наявності цілісної інформаційної системи, яка відповідає стратегії інтелектуалізації систем менеджменту підприємства.
5. Зростання динамічності економічних процесів та невизначеності змін зовнішнього і внутрішнього середовищ підприємства, що зумовлює постійні зміни в структурі систем менеджменту та інформаційної складової.
6. Зростання індивідуальної відповідальності за ухвалені управлінські рішення і, як наслідок, збільшення обсягів інформації для потреб менеджменту вимагає розробки та використання нових підходів до формування ключових компетенцій.
7. Використання системи моніторингу внутріщнього та зовнішнього середовища функціонування, яка дасть змогу діагностувати поточний стан інтелектуального капіталу підприємства і прогнозувати майбутній потенціал його використання для забезпечення відповідного рівня фінансово-економічної безпеки [3].

Організація підприємницького процесу при його започаткуванні сфокусована на час виходу на ринок, а організація діяльності – це процес, який відбувається і в часі, і в просторі[3]. Підприємницька діяльність, узгоджена у просторі та часі, повинна базуватись на таких організаційних системних принципах побудови ключових компетенцій:

- принцип безперервності є невід'ємною ознакою підприємництва і передбачає можливість постійного отримання прибутків і розвитку бізнесу;
- принцип гнучкості підприємницької діяльності відображає здатність суб'єкта підприємництва швидко адаптуватися до мінливого ринкового середовища і знаходити своє місце в ньому;
- оптимальність як принцип підприємства підприємництва спрямована на раціональне поєднання в просторі й часі всіх факторів діяльності для отримання прибутку та зростання добробуту власників. Принцип оптимальності зумовлений законом економії часу, значно мінімізує ризик підприємницької діяльності та є визначальним при прийнятті підприємницьких рішень;

- принцип паралельності дає змогу одночасно виконувати важливі етапи підприємницького процесу, що значно прискорює його;
- принцип синхронізації забезпечить підприємцю певну стабільність, гармонізований рух; рівновагу руху і спокою. Процеси, не синхронізовані в часі, призводять до ризику платоспроможності. Це процеси, пов'язані із строками надходження грошових коштів, виплат тощо;
- принцип системності та науковості також домінує у механізмі ринкових відносин підприємця. Цей принцип багатий за змістом і передбачає певну систему дій підприємця у використанні нововведень, строгу послідовність і відповідну періодичність, наповнення інноваціями бізнес-процесів для забезпечення їх конкурентоспроможності;
- принцип прозорості пов’язаний з формуванням сучасної ринкової інфраструктури, необхідної для просування продукції на ринку та існування ринку капіталів. Новітні системи такої інфраструктури повинні бути побудовані так, щоб заздалегідь передбачити прозорість будь-яких фінансових чи господарських операцій, тобто виконувати їх з урахуванням вимог чинного законодавства всіма суб'єктами, зайнятими підприємницькою діяльністю.

У підприємницькій діяльності одночасно, тобто паралельно, вибирається підприємницька ідея, перевіряється реальність виконання, вибираються види діяльності та й організаційно-правові форми.Підприємницька ідея – це результат творчості. Тому реалізація і втілення ідеї в життя зумовлюються часом виходу на ринок та періодом діяльності. Інакше час буде втрачено, ринкову нішу заповнять інші, а ідея буде нереалізованою. Це означатиме, що процес підприємництва не відбувся у бажаному напрямку. Отже, швидкість реалізації підприємницької ідеї – це фактор часу в понятті підприємства конструктивної поведінки підприємця на ринку. Категорія часу присутня в усіх діях підприємця і на всіх стадіях його підприємницької діяльності. У зв'язку з цим час треба розглядати в контексті загального й конкретного.

Загалом більшість принципів підприємства підприємницького процесу пов'язані із часом (гнучкість, оперативність, паралельність, безперервність, оптимальність тощо). Головні ознаки підприємництва також прив'язані до часу (систематичність, ризик,

уже згадуваний творчий пошук тощо). Але найбільше в підприємницькій діяльності фактор часу проявляється через ризик. Час є невід'ємною складовою частиною ризику, оскільки із віддаленою перспективою зростає ступінь невизначеності і значно зменшується ймовірність бажаного результату [2]. Саме описані фактор визначають необхідність використання нових методів дослідження та діагностики господарських систем.

Суть та роль управління підприємницькою діяльністю визначається через розуміння управління як:

- **науки,** змістом якої є закони та закономірності, принципи, функції, форми та методи цілеспрямованої діяльності людей під час управління;
- **процесу** пов'язання всіх видів управлінської діяльності, а також їх взаємозв'язок під час управління;
- **виду професійної діяльності,** що зосереджує увагу на структурі апарату управління та зв'язках між ланками та рівнями на ступені централізації, повноваженнях та відповідальності робітників, що займають різні посади в апараті управління;
- **мистецтва,** що базується на інтелектуальному капіталі та ключових компетенціях тобто знаннях, вмінні, інтуїції та досвіді людей, що управляють підприємством.

Таким чином, основними положеннями сучасної управлінської парадигми формування управлінських та ключових компетенцій підприємницьких структур є такі: підприємство – це відкрита соціально-економічна система, що діє, змінюється, розвивається та перебудовується у динамічному середовищі; системний та ситуаційний підходи до управління дають можливість використати універсальні теорії та досягнути синергетичного ефекту; теорія систем забезпечує взаємозалежність підсистем управління та вплив на них зовнішнього середовища; орієнтація на якість продукції та послуг, на задоволення потреб споживачів; спрямованість на підвищення ролі організаційної культури та різних типів інновацій, на використання соціально-психологічних методів мотивації робітників; соціальна відповідальність бізнесу та перетворення персоналу у ключовий ресурс підприємства; використання інтелектуального капіталу та систем управління знаннями дозволяє сформувати та розвивати конкурентоспроможний та інноваційний інтелектуальний потенціал структури.

Під час діяльності підприємства можуть виникати проблемні ситуації, для дослідження яких доцільно використовувати ситуаційний підхід до управління ризиками в системі економічної безпеки на основі використання когнітивного моделювання та можливостей data mining, з допомогою якого можна здійснити найбільш точний опис проблемної ситуації, розбити її на задачі, визначити причини виникнення та фактори впливу [4].

Когнітивне рішення ситуації передбачає виявлення у кризовій ситуації негативних ланок і структури факторів («розриви» ситуації), які підлягають заміни новими об'єктами, процесами й досконалішими стосунками, що зменшують негативний вплив і створюють позитивний ефект. У цьому полягає суть управління фінансово-економічною безпекою з інноваціями. Паралельно зі виявленням «розривів» ситуації, часто які кваліфікуються як «виклики» або «загрози», можуть бути виявлені «позитивні відповіді» як цілісні образи стану майбутньої (гармонізованої) ситуації.

Когнітивний аналіз стану і моделювання є принципово новими елементами у структурі систем підтримки прийняття рішень на основі експертної оцінки ситуації та розробки когнітивної карти ситуації. Технологія когнітивного моделювання дозволяє досліджувати проблеми з нечіткими чинниками і взаємозв'язками, враховувати зміни зовнішнього середовища та використовувати об'єктивно тенденції розвитку у своїх інтересах [4].

В загальному випадку когнітивна карта – це суб'єктивна картина ситуації та активних дій в просторо-часових координатах з врахуванням особливостей внутрішнього та зовнішнього середовища функціонування підприємства. Види когнітивних карт: карта-шлях, как послідовне визначення зв'язків між об'єктами за певним маршрутом; карта-огляд, как одночасне представлення просторового разміщення об'єктів. Когнітивні карти можуть бути корисні для формування та уточнення гіпотез про функціонування досліджуваної ситуації з погляду фінансово-економічної безпеки чи об'єкта, досліджуваного як складна система.

Наростання складності управління при зростанні масштабів ієрархії економічних структур настільки уповільнює рух інформації управлінськими каналами, що система просто не встигає реагувати на зміни зовнішнього середовища, яке якраз навпаки – через досягнення інформаційних технологій стає все більш

динамічним. Інтелектуалізація систем менеджменту підприємства у поєднанні із інформаційними технологіями спроможні у якісний спосіб децентралізувати управління, зменшити кількість рівнів ієрархії, перейти до мережевої моделі управління[6].

1. Мойсеєнко І.П. Управління інтелектуальним потенціалом / І.П. Мойсеєнко: монографія. – Львів, Аверс, 2007. – 304 с.
2. Пожуєв В.І. Інтелектуальний капітал як стратегічний потенціал організації Електронний ресурс. режим доступу: http://www.zgia.zp.ua/gazeta/VISNIK_37_1.pdf
3. Мойсеєнко І.П. Управління фінансово-економічною безпекою підприємства / І.П. Мойсеєнко, О.М. Марченко: навч. посібник. – Львів: Видавництво ЛьвДУВС, 2011. – 320с.
4. Вартанова О.В. Сутність стратегічної компеенції як джерела конкуретних переваг підприємства
5. Електронний ресурс. режим доступу: http://pk.napks.edu.ua/library/compilations_vak/eiu/2010/3_4/p_44_47.pdf
6. Мойсеєнко І.П. Когнітивний аналіз умов функціонування суб'єктів підприємництва / І.П. Мойсеєнко // Інформаційні технології, економіка та право: стан та перспективи розвитку: матеріали міжнародної науково-практичної конференції 3-5 квітня 2013. – Чернівці: Книги-ХХШ, 2013. – 288-290.
7. Й.С. Ситник Формування інтегрованої інформаційної системи для потреб інтелектуалізації систем менеджменту промисдових підприємств Електронний ресурс. режим доступу: irbis-nbuv.gov.ua/cgi-bin/.../cgiirbis_64.exe?...

ПОБУДОВА МОДЕЛІ ТА ОПРАЦЮВАННЯ ІНФОРМАЦІЙНИХ ПОТОКІВ НА ПРИКЛАДІ ДЕРЕВООБРОБНОГО ПІДПРИЄМСТВА

Дендюк Михайло Володимирович,
доцент кафедри інформаційних технологій НЛТУУ, к.т.н
Кушпіт Михайло Андрійович,
магістр НЛТУУ

За допомогою MySql Workbench та Borland C++ Builder розроблено програмне забезпечення для обчислення доходів та ризиків деревообробних підприємств

В наш час починають розвиватися багато малих підприємств пов'язаних з деревообробною промисловістю. Більшість з них використовують загальнодоступні програми для ведення документації, розрахунку бізнес планів, обчислення ризиків. Для прикладу, Microsoft Excel є достатньо функціональним, однак коли потрібно наглядно показати клієнту або замовнику конкретні дані то подання та обрахунок даних в цих програмах є досить складним та незрозумілим на перший погляд, що може скласти не найкраще перше враження для клієнта.

Саме з метою більш наглядної подачі даних та пришвидшення роботи з потенційно великими обсягами інформації було вирішено створити модель та опрацювання потоків на прикладі деревообробного підприємства.

Постановка задачі. Оцінка рівня ризику є найбільш складним і відповідальним моментом, оскільки саме від її результатів залежать подальші дії підприємства.

Ризик має математично виражену ймовірність настання втрати, яка базується на статистичних даних і може бути розрахована з достатньо великим ступенем точності.

Математична модель. Величина ризику (ступінь ризику) вимірюється за допомогою двох категорій: середньоочікуваного значення та коливання (змінюваність) можливого результату.

Середньоочікуване значення – це значення величини події, яке пов'язане з невизначеною ситуацією. Середньоочікуване значення показує результат, на який ми сподіваємось в середньому.

Так, наприклад, якщо відомо, що при вкладенні капіталу в проект «А» з 100 випадків прибуток у розмірі 3000 грн. було отримано в 26 випадках (ймовірність 0,26), прибуток в розмірі 2580 грн. було отримано в 48 випадках (ймовірність 0,48), прибуток у розмірі 1790 грн. було отримано в 26 випадках (ймовірність 0,26), то середній очікуваний прибуток становить 2483,8 грн. (3000 ⊙ 0,26 + 2580 ⊙ 0,48 + 1790 ⊙ 0,26). Аналогічно встановлено, що при вкладенні капіталу в проект «В» середній прибуток склав теж 2483,8 грн. (3200 ⊙ 0,2 + 2573 ⊙ 0,6 + 1500 ⊙ 0,2).

Порівнюючи дані за окремими інвестиційними проектами, можна побачити, що розраховані величини доходів по проекту «А» коливаються в межах від 1790 до 3000 грн. при сумі очіку-

ваних доходів в цілому 2483,8 грн., по проекту «В» сума очікуваних доходів в цілому також складає 2483,8 грн., однак їх коливання здійснюється в діапазоні від 1500 до 3200 грн. Навіть таке просте співпадання дозволяє зробити висновок про те, що ризик реалізації інвестиційного проекту «А» значно менший.

Чисельне значення цього коливання характеризує показник середньоквадратичного відхилення (σ), що розраховується за формулою:

$$\sigma = \sqrt{\sum_{i=1}^{n} \left[\varepsilon - \varepsilon_R\right]^2 \times P_i}, \quad (1)$$

де: t – число періодів; n – число спостережень; ε – розрахунковий дохід по проекту при різних значеннях кон'юнктури; εR – середній очікуваний дохід за проектом; Pi – значення ймовірності, що відповідає розрахунковому доходу.

Алгоритм розрахунку. В зв'язку з тим що ми будемо працювати з базою даних, в якій зможуть зберігатися великі обсяги інформації, а також багато обчислень доцільним буде використання паралельних потоків для обчислення.

Потік (thread) – це основний елемент системи, якому ОС виділяє машинний час. Потік може виконувати якусь частину загального коду процесу, у тому числі і ту частину, яка в цей час вже виконується іншим потоком.

Всі потоки одного процесу користуються ресурсами їх процесу. Потоки подібні до процесів, але вимагають менших витрат при своєму створенні. Вони у меншій мірі, чим процеси, захищені один від одного, але дозволяють поєднати виконання операцій і виграти в загальній продуктивності процесу.

Якщо один потік виконує повільні операції введення-виводу, а інший виконує обчислення і використовує лише процесор, то ефективність процесу, що поєднує два потоки, буде значно вища, ніж ефективність двох процесів, виконаних послідовно. Замість очікування, яке пов'язане з дисковими операціями, система може перейти до виконання іншого потоку, що буде ефективно оскільки в наші програмі буде багато роботи з базами даних та багато різноманітних обчислень які можна організувати у паралельних потоках.

Оскільки ми використали базу даних та потоки для максимальної зручності та швидкості обчислень бізнес плану підприємства що включає прибутки, ризики та інші фактори, це дає змогу наглядно показати клієнту, замовнику, чи інвестору на що саме ідуть кошти, які витрати, прибуток та як на це впливають різні фактори.

Розраховані показники середньоквадратичного відхилення по інвестиційних проектах, що розглядаються, можуть бути інтерпретовані графічно (рис. 1).

Висновки. Розроблена математична модель та алгоритм дозволяє створити програму для деревообробних підприємств для ведення документації, обрахунку бізнес плану, та інших функцій з метою наглядної роботи з клієнтами, замовниками або інвесторами. Дана модель передбачає інтерактивну зміну параметрів, що дозволяє наглядно показати залежність прибутку, витрат, ризиків залежно від різних факторів які можна буде змінювати і виконувати швидке пере обчислення даних відповідно до цих параметрів завдяки використанню паралельних потоків.

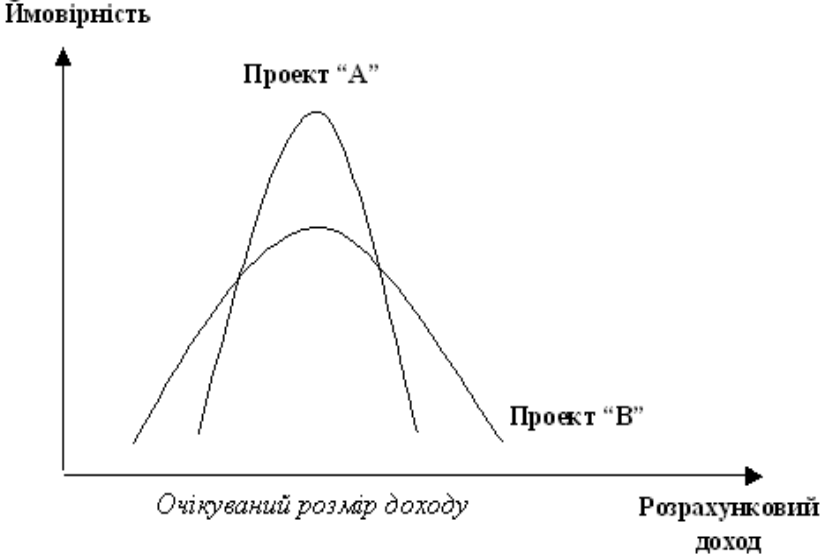


Рис. 1. Розраховані показники середньоквадратичного відхилення по інвестиційних проектах

1. Тєлєтов О.С. Бізнес-план. Навчальний посібник – Су-ми: Вид-во СумДУ, 2005. – 104 с.
2. Горемыкин В.А. Бизнес-план: Методика разработки. 45 реальных образцов бизнес-планов / В.А. Горемыкин, А.Ю. Богомолов – 3-е изд., доп. и перераб. – М. : Ось-89, 2002. – 864 с.
3. Ирэ Пол. Объектно-ориентированное программирование с использованием C++: Пер. с англ. – Киев: НИИПФ ДиаСофт Лтд, 1995. 480с.
4. Вальковский В.А. Распараллеливание алгоритмов и программ. Структурньій подход.-М.: Радио и связь, 1989. – 176 с.
5. Хьюз К., Хьюз Т., Параллельное и распределенное программирование на языке C++.: Пер. с англ. – М.: Издательсктй дом «Вильямс», 2004. – 627 с.
6. Формалев В.Ф. Численные методы / В.Ф. Формалев, Д.Л. Ревизников. – Изд. 2-е, испр., доп. – М.: ФИЗМАТЛИТ. – 2006. – 400 с.

ФОРМУВАННЯ СТРУКТУРИ ЕКОНОМІЧНОЇ БЕЗПЕКИ СОЦІАЛЬНОЇ СФЕРИ ПОСЛУГ В УКРАЇНІ

Руда Ірина Ігорівна,
викладач кафедри економіки та економічної безпеки ЛьвДУВС

Підвищення уваги до проблем соціально-економічного розвитку та економічної безпеки України вимагає неухильного дотримання державними органами влади та органами місцевого самоврядування законодавчо закріплених соціальних прав, гарантій і стандартів життя населення.

Забезпечення цих прав лежить в основі функціонування ринку ритуальних послуг. Відповідно до статті 6 Закону України № 1102-IV від 10.07.2003 р. «Про поховання та похоронну справу» (зі змінами № 1194-VII від 23.02.2014 р.) закріплено право громадян на поховання їхнього тіла та волевиявлення про належне ставлення до тіла після смерті, що може бути виражене в:

- побажанні бути похованим у певному місці, за певними звичаями, поруч з певними раніше померлими чи бути підданим кремації;
- дорученні виконати своє волевиявлення певній особі;

- іншому дорученні, що не суперечить чинному законодавству.

Ринок ритуальних послуг, за своєю суттю відноситься до «абсолютних» ринків, оскільки стосується практично всіх жителів. Він заснований на досить жорсткій залежності покупців від запропонованого асортименту послуг, тому характеризується значною стабільністю та консервативністю. Ці особливості ринку ритуальних послуг роблять його менш схильним до кризових проявів економіки, що підвищує рівень економічної безпеки окремих осіб, суспільства і держави загалом [1]. За таких умов, держава активно втручається в процеси ціноутворення на відповідні послуги, а також, у ряді випадків, надає допомогу споживачам, беручи на себе витрати на похорон. При цьому найважливішою функцією держави в даній сфері у напрямку підвищення рівня економічної безпеки, яка, на нашу думку, не повною мірою реалізується в Україні, є проведення цілеспрямованої діяльності з розвитку конкуренції на ринку ритуально-похоронних послуг.

В цілому, виключною компетенцією держави в розглянутій сфері є виконання таких основних функцій [2]:

1) забезпечення всіх гарантій по похованню громадян, визначених законодавством України;

2) повний контроль відносин в частині створення та експлуатації місць поховань;

3) чітке визначення меж між галузями, в частині визначення та розмежування видів економічної діяльності та взаємовідносин на цих межах;

4) встановлення базових кваліфікаційних та технологічних галузевих вимог;

5) відродження і розвиток ритуальних і обрядових традицій.

На господарську діяльність організацій сфери ритуальних послуг крім зовнішнього впливає і внутрішнє середовище. Воно пов'язане з його економічною безпекою та організацією господарської діяльності, а саме – з питаннями розвитку галузі, розподілу прав, обов'язків та відповідальності між учасниками ринку.

Так, відповідно до інформації Державної служби статистики України, протягом 2013 року ритуальні послуги населенню надавали 509 ритуальних служб та 2590 суб'єктів господарюван-

ня, які здійснюють діяльність на договірних засадах із ритуальними службами. Протягом цього періоду ритуальними службами було поховано понад 582 тис. померлих осіб, що становить 96% від загальної кількості померлих [3].

Ритуальними службами, що створені органами місцевого самоврядування та їх виконавчими органами відповідно до статей № 8-9 Закону України № 1102-IV від 10.07.2003 р. «Про поховання та похоронну справу», протягом минулого року надано населенню ритуальних послуг та реалізовано предметів ритуальної належності на загальну суму понад 712 млн. грн., що на 6% більше порівняно з 2012 роком.

Загальний обсяг наданих ритуальних послуг та предметів ритуальної належності населенню суб'єктами господарювання різних форм власності у 2013 році склав 1,33 млрд. грн., з яких майже 54% було надано ритуальними службами.

Проте, складна економічна ситуація спонукала до зменшення на 10 % загальної чисельності приватних підприємств порівняно з 2012 роком. Найбільша кількість суб'єктів господарювання в сфері ритуальних послуг відмічена в Дніпропетровській (254) та Запорізькій (198) областях.

Відповідно до розглянутих статистичних даних, середня вартість одного поховання в Україні за 2013 рік становила 2326 грн., що на 6 % більше порівняно з 2012 роком (2175 грн.). Найвищий показник середньої вартості поховання відмічено в містах Києві (4239 грн.), Львівській (3500 грн.) та Житомирській (3039 грн.) областях, тоді як найнижчий – в Миколаївській (1066 грн.) області [4].

Проводячи аналіз внутрішнього стану середовища сфери ритуальних послуг в Україні, слід зауважити, що її організаційна діяльність ґрунтується на принципах «правильної» організації. За допомогою цих принципів можна зробити висновок про здатність організації задовольняти потреби громадян в ритуально-похоронних послугах.

Як свідчить стан справ у галузі поховання, нині ще мають місце проблемні питання, що виникають внаслідок недостатньої уваги з боку органів місцевого самоврядування до дотримання положень Закону України № 1102-IV від 10.07.2003 р. «Про поховання та похоронну справу», зокрема, щодо вирішення пи-

тань, спрямованих на удосконалення організації проведення поховання померлих.

Серед таких питань, що потребують нагального вирішення можна виділити наступні:

- підвищення якості надання похоронних послуг та виготовлення предметів похоронної належності;
- створення конкурентного середовища та залучення на конкурсних засадах суб'єктів господарювання різних форм власності;
- розвитку такого напрямку у галузі поховання, як кремація, що дозволило б вирішувати питання дефіциту земельних ресурсів для створення нових кладовищ у населених пунктах України;
- забезпечення належного виділення коштів, необхідних для благоустрою місць поховань, що дало б змогу здійснювати відповідні заходи по збереженню та охороні місць поховань, попередженню навмисного руйнування чи викрадення колумбарних ніш, намогильних споруд та склепів і осквернення могил.

Але вирішення цих питань мають ґрунтуватися на базі організації та проведенні ефективної фінансової політики самих суб'єктів господарювання з метою формування комплексу еко-номічної безпеки, яка залежить як від внутрішніх так і зовнішніх факторів діяльності сфери ритуально-похоронних послуг в Україні.

1. Головешко Д. В. Основные направления модернизации рынка похоронных услуг на муниципальном уровне / Д. В. Головешко // Общество. Среда. Развитие. – 2013. – № 2 (27). – С. 39-42.
2. Максимов И. С. Трансформация локального рынка ритуальных услуг в муниципальных образованиях : дис. … канд. экон. наук : 08.00.05 / Максимов Игорь Сергеевич ; ФГБОУ ВПО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых». – Владимир, 2012. – 173 с.
3. Демографічна ситуація [Електронний ресурс]. – Режим доступу : http://www.ukrstat.gov.ua/operativ/operativ2009/ds/dso. html – Назва з екрану. – (Державна служба статистики України).
4. Стан галузі поховання в Україні за 2013 рік [Електронний ресурс]. – Режим доступу : http://www.minregion.gov.ua/zhkh/Blahoustriterytoriy /stan-galuzi-pohovannya-v-ukrayini--za-2013-rik--642314/ – Назва з екрану. – (Міністерство регіонального розвитку, будівництва та житлово-комунального господарства України).

ПРОЕКТУВАННЯ WEB-ОРІЄНТОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ІДЕНТИФІКАЦІЇ ПОРІД ДЕРЕВ ЗА ЗОБРАЖЕННЯМ ЛИСТКІВ

Шабатура Юрій Васильович,
професор кафедри інформаційних технологій НЛТУУ, д.т.н., професор
Повшук Олександр Володимирович,
магістр НЛТУУ

Було досліджено різні методи розпізнання зображень. Для виконання роботи було обрано алгоритм K внутрішньо-групових середніх. За допомогою MySql Workbench було розроблено базу даних зображень листків різних порід дерев та розпочато роботу над реалізацією алгоритму.

Актуальність проблеми. Web-технології є одним із сучасних напрямків розвитку інформаційних систем. На сьогодні розроблено широкий спектр програмних та технічних засобів для побудови Web-систем. Проте подальший розвиток Web-технологій стає неможливим без побудови ґрунтовної формально-математичної основи, в першу чергу – без створення формальної моделі Web-системи. Як наслідок, на сьогодні відсутні розширення для Web-технологій усталених методів і засобів аналізу та проектування інформаційних систем (зокрема, структурних методологій). Відсутність математичної моделі Web-системи унеможливлює розробку інтелектуальних засобів адміністрування Web-систем, базованих на алгоритмах оптимізації Web-систем та прогнозуванні поведінки Web-системи в часі.

Потреба у математичній основі, яка б дозволяла описувати та моделювати багаторівневі Web-системи глобального характеру, приводить до необхідності побудови формальної моделі Web-системи та алгоритмів оптимізації Web-системи, як основи для якісної розробки ефективних Web-систем, незалежно від їх складності та характеру.

Більшість з нас може оцінити дерева з точки зору їх естетичності, використання деревини, фруктів чи просто екологічної цінності. Справжня цінність дерев, зокрема, приходить з

більш глибокими знаннями, починаючи з ідентифікації листків, кори дерев, тощо, настільки ж миттєво, як розпізнавання марки автомобіля, що проїхав поряд.

Повірте, є досить вагома причина розпізнати отруйний плющ! Розмір, форма, колір і щільність дерева є звісно надзвичайно важливими, але перш за все потрібно розуміти на що ми дивимось, тобто розпізнавати дерево за його листком.

Розглянемо один з алгоритмів, який було обрано для виконання даного завдання.

Математична модель. Алгоритм, представлений нижче, мінімізує показник якості, визначений як сума квадратів відстаней усіх точок, що входять в кластерну область, до центру кластера. Ця процедура, яку часто називають алгоритмом, заснованим на обчисленні К внутрішньо-групових середніх, складається з наступних кроків:

Крок 1. Вибираються К початкових центрів кластерів $z_1(1)$, $z_2(1)$, … $z_k(1)$. Цей вибір робиться довільно, і зазвичай в якості початкових центрів використовуються перші К результатів вибірки із заданої множини образів.

Крок 2. На k-му кроці ітерації задано безліч образів $\{x\}$ розподіляється по К кластерам за наступним правилом:

$$x \in S_i(k), \text{ якщо } \left\|x - z_j(k)\right\| < \left\|x - z_i(k)\right\|$$

для всіх $i = 1, 2, \ldots, K$, $i \neq j$, де $S_j(k)$ – безліч образів, що входять в кластер з центром $z_j(k)$. У разі рівності рішення приймається довільним чином.

Крок 3. На основі результатів кроку 2 визначаються нові центри кластерів $z_j(k + 1)$, $j = 1, 2, ..., K$, виходячи з умови, що сума квадратів відстаней між усіма образами, що належать множинні $S_j(k)$, і новим центром кластера повинна бути мінімальною. Іншими словами, нові центри кластерів $z_j(k + 1)$ вибираються таким чином, щоб мінімізувати показник якості :

$$J_j = \sum_{x \in S_j(k)} \left\|x - z_j(k+1)\right\|^2, j = 1,2, \ldots, K.$$

Центр $z_j(k + 1)$, що забезпечує мінімізацію показника якості, є, по суті, вибірковим середнім, визначеним за множинні $S_j(k)$. Отже, нові центри кластерів визначаються як

$$z_j(k+1) = \frac{1}{N_j} \sum_{x \in S_j(k)} x\,, \quad j = 1,2,\ldots,K.$$

де N_1 – число вибіркових образів, що входять в множину $S_j(k)$. Очевидно, що назва алгоритму «К внутрішньо-групових середніх» визначається способом, прийнятим для послідовної корекції призначення центрів кластерів.

Крок 4. Рівність $z_j(k + 1) = z_j(k)$ при $j = 1, 2, ..., K$ є умовою збіжності алгоритму, і при його досягненні виконання алгоритму закінчується. В іншому випадку алгоритм повторюється від кроку 2.

Якість роботи алгоритмів, заснованих на обчисленні К внутрішньо-групових середніх, залежить від числа обраних центрів кластерів, від вибору вихідних центрів кластерів, від послідовності огляду образів і, природно, від геометричних особливостей даних. Хоча для цього алгоритму загальне доведення збіжності не відомо, отримання прийнятних результатів можна очікувати в тих випадках, коли дані утворюють характерні грона, віддалені один від одного досить далеко. У більшості випадків практичне застосування цього алгоритму зажадає проведення експериментів, пов'язаних з вибором різних значень параметра К і вихідного розташування центрів кластерів.

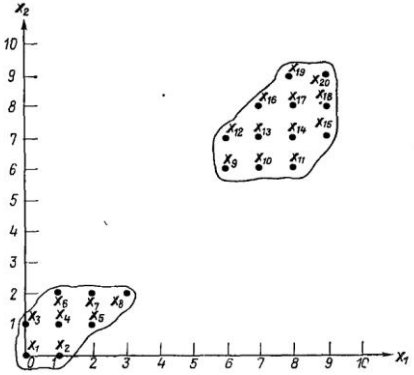


Рис.1 Вибірка образів, використана для ілюстрації роботи алгоритму вибіркових середніх по К центрам кластеризації.

Реалізація бази даних. Звісно для того, щоб створити інформаційну систему, необхідно розробити базу даних. Для цього завдання було використано SQL сервер MS SQL Server 2014

Developer Edition. За допомогою цього додатку було створено базу даний та таблиці в яких зберігатимуться зображення листків з дерев. Реалізований такий тип рядка за допомогою типу даних IMAGE. Завдяки цьому значно полегшується взаємодія даних в коді і зменшується кількість операцій, потрібної для конвертації зображень в потрібний формат.

Висновки. Для створення Web-орієнтованого додатку для ідентифікації породи дерев було розроблено базу даних, в якій будуть зберігатись зображення листків, а також були досліджені алгоритми для розпізнання зображень. У результаті дослідження було вибрано алгоритм К внутрішньогрупових мередніх. Цей алгоритм належить до алгоритмів кластеризації. На основі цього алгоритму, бази даних і однієї з провідних технологій проектування Web додатків і буде розроблено програмний додаток.

1. Циганов О.В. Основи проектування систем штучного інтелектую. Навч. посібник. – К.: Наука і техніка – 2006. – 195 с.
2. Рідкокаша А.А. Основи систем штучного інтелекту. – Черкаси, 2002. – 240 с.
3. Глибовець М.М., Отецький О.В. Штучний інтелект. – К.: Знання. – 2002. – 366 с.

ІНФОРМАЦІЯ ТА УПРАВЛІННЯ ОРГАНІЗАЦІЄЮ

Сватюк Оксана Робертівна,
доцент кафедри менеджменту ЛьвДУВС, к.е.н.
Келба Андрій Ігорович,
студент ЛьвДУВС

Вибір найбільш ефективних методів аналітичної обробки інформації дозволяє ухвалити оптимальні управлінські рішення.

Існують внутрішні і зовнішні чинники які впливають на діяльність організації. Для виконання різноманітних завдань менеджерові необхідно мати доступ до інформації, знати методи її обробки, ефективно розподіляти інформацію, добиваючись здійснення ухвалених рішень. Організація доступу до оперативної інформації припускає отримання відомостей як про внутрішні чинники, що характеризують виробничі процеси, так і про зовнішні

чинники, що визначають стан ринку, поведінку партнерів, інтереси клієнтів і тому подібне. До критичних слід віднести ті чинники, дія яких може істотно вплинути на форму і методи виконання господарських процесів, на весь бізнес. Таким чином, інформаційна діяльність (інформаційна складова бізнесу) входить в менеджмент як його складова частина, а сукупність методів організації і управління інформаційним ресурсом організації визначає відповідно зміст діяльності в області інформаційного менеджменту.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання теоретичних положень інформаційного простору знайшли відображення в роботах вчених: Баранова В., Березовского С.В., Зубенка А.В., Кривицкого А.В. Жданова, Меняева М.Ф., Склара А., Черенка М.

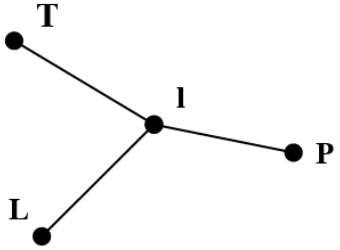
Інформаційний менеджмент реалізує свої функції в інформаційному просторі організації, який характеризує сукупність методів і засобів, що дозволяють найефективніше організовувати процеси отримання, перетворення, зберігання і розподілу інформації з метою реалізації оптимальних режимів управління організацією. Змістовною характеристикою інформаційного простору організації є його інформаційний ресурс. Інформаційний менеджмент направлений на формування і розвиток інформаційного ресурсу підприємства, його використання як інструменту ведення бізнесу.

Інформаційним ресурсом організації є поняття, що відображає рівень використання як внутрішньої, так і зовнішньої інформації, а також сукупність методів і засобів, вживаних організацією для пошуку, обробки і розподілу інформації [4, с.38].

Будь-яка організація (організація) може бути представлена як деяка цілеспрямована система, яку можна досліджувати на основі положень системного аналізу. У такому розгляді слід вивчити системну модель організації, визначувану набором основних елементів (станів) і відносин між ними.

У структурі організації можна виділити наступні основні елементи: цінності організації, бізнес-платформу, бізнес-архітектуру і інформаційний ресурс організації. Відношення між елементами системної моделі характеризують інформаційні відносини усередині організації. Сукупність основних елементів і інформаційних відносин утворює бізнес-структуру організації,

яку можна представити у вигляді системної моделі, показаної на рис. 1. Модель показує значення інформаційного ресурсу організації як основного елементу в системі, визначального відношення між іншими елементами моделі, сприяючого розвитку нових відносин на базі використання ефективніших методів доступу до інформації, формування знань про стан бізнесу.



T-цінності; L-бізнес-платформа; P-бізнес-архітектура;
l-інформаційний ресурс системи

Рис. 1. Системна модель бізнес структури організації [4, с.36].

Графічне відображення системної моделі бізнес-структури має наступні стани:

T – цінності, те, що породжує потік доходів,

L – бізнес-платформа, те, що складає виробництво, його стратегію і ринок (система взаємодії з ринком — маркетинг і т.п.),

P – бізнес-архітектура: організація персоналу організації,

l – інформаційний ресурс системи.

Завдання менеджера полягає в забезпеченні оптимальної взаємодії компонентів бізнес-структури для забезпечення розширеного відтворення капіталу. Основою для вирішення поставленого завдання і є забезпечення доступу до необхідної інформації в режимі реального часу, залучення до управління організацією максимального числа зацікавлених учасників.

Неоднорідність компонентів структури, наявність зовнішніх і внутрішніх обурюючих (що дестабілізують) дій на структуру організації примушують менеджера активізувати дії з пошуку і аналізу інформації про стан бізнесу, про економічний стан суспільства, а також вивчати відомості в тих напрямах, які безпосередньо пов'язані з попередженням збитків на шляху досягнення поставлених цілей. Менеджер також повинен шукати способи і методи передачі інформації, сприяючі оптимізації бізнесу.

Активний розвиток і застосування інформаційного ресурсу організації направлений на облік зовнішніх і внутрішніх чинників діяльності організації, які утворюють внутрішнє і зовнішнє бізнес-середовища, відображають зміст внутрішніх і зовнішніх критичних чинників діяльності організації (рис.2).

Зовнішня бізнес-середовище – сукупність економічних, соціальних, політичних і тому подібне об'єктів, що діють за межами підприємства, і відносини, що складаються між ними і підприємством (фірмою, концерном і т. п.). Вона виявляється у формі зовнішніх критичних чинників діяльності організації: фінансово-сировинні ринки, клієнти, постачальники, конкуренти.

Рис. 2 Зовнішні і внутрішні фактори діяльності організації

Внутрішня бізнес-середовище – це господарські відносини в колективі, визначені інформаційними потоками і знаннями, що формуються в процесі їх функціонування [3, с.7]. Внутрішніми показниками цієї частини бізнес-середовища організації можуть стати: фінанси організації, організація виробничих процесів, якість продукції, що випускається, прийнята виробнича стратегія організації і ін.

Інформаційний ресурс підприємства направлений на забезпечення активного взаємозв'язку з зовнішнім і внутрішнім бізнес-середовищем.

Активне використання інформаційного ресурсу дозволяє підприємству отримати додаткові переваги в наступних напрямах діяльності [2, с.172]:

- **організація бізнесу:** відбираючи і переробляючи необхідну інформацію, менеджер формує знання про бізнес, перетворює їх в інформаційні повідомлення (посилки), які, у свою чергу, впливають на виробничі і адміністративно-господарські процеси;
- збільшення **власності:** знання про бізнес формують інтелектуальну власність, яку можна перетворити в корпоративну інформацію. Ця інформація дозволяє знайти шляхи як збереження самої власності, так і придбання додаткової власності в покладений термін. Основна відмінність цієї форми власності полягає в тому, що вона, як і саме знання, – невичерпна;
- **пошук** і **розвиток нового бізнесу:** досліджуючи інформацію, можна не тільки знайти шляхи до розробки нового виробу, надання нової послуги, але і забезпечити виправданий ризик вибору нового напряму у виробництві, формування нового ринку;
- **віртуалізація бізнесу:** досягнення оптимальних значень риски для менеджера багато в чому визначається не тільки його особистими якостями і умілою роботою у віртуальному інформаційному просторі, але і його уміннями самостійно формувати і використовувати віртуальні відносини в інформаційному просторі. Підприємець виділяється за допомогою засобів віртуалізації бізнесу.

Інформаційна діяльність на підприємстві направлена на:

- підтримку і розвиток систем управління бізнесом на базі інформаційної системи підприємства;
- виявлення основних напрямів інформаційних потреб, відбір джерел інформації;
- збір і обробку інформації, оцінку її повноти, достовірності і значущості;
- аналіз інформації і виявлення тенденцій;
- розробку прогнозів і альтернатив поведінки підприємства;
- ухвалення рішень, що управляють, для реалізації стратегічних планів;
- формування і постійне оновлення бази знань підприємницьких ідей і пов'язаних з ними ризиків і ін.

Інформаційна діяльність менеджера полягає не тільки у формуванні інформаційного ресурсу підприємства, але і в забезпеченні розвитку «підприємницької інтуїції», яка обумовлює виникнення «підприємницької ідеї». Взаємозв'язок станів і процесів пошуку і обробки інформації менеджером показаний на рис.3.

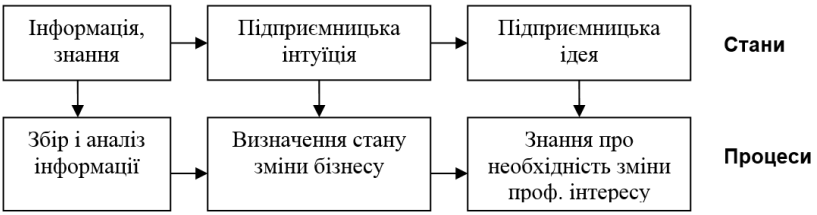


Рис. 3. Взаємозв'язок станів і процесів пошуку і обробки інформації менеджером.

Підприємницька ідея – це розуміння, знання підприємця про те, що він відчуває зміни в області свого професійного інтересу, що намітилися, які дозволяють отримати переваги і реальні економічні результати [1, с.17].

І хоча інформації може бути недостатньо для точної вказівки на зміни, підприємницька інтуїція, що базується на ній, приводить до підприємницької ідеї.

Інформаційний ресурс організації дозволяє відобразити реальний стан бізнесу, виробити адекватну реакцію на зміни в бізнесі і навколишньому середовищі, а також забезпечити пошук найбільш ефективної взаємодії всіх ресурсів підприємства: фінансового, матеріального, інтелектуального і ін. Для цього організовується діяльність щодо:

- підтримці моніторингу виробничого і адміністративно-господарського процесів;
- забезпеченню оперативного доступу до архівів документів управління і технології;
- отриманню інформації про завантаження робочих місць, рух матеріалів, витратах робочого часу і ін.;
- реєстрації і підготовці аналітичних матеріалів про запаси матеріалів, що комплектують і готовій продукції;
- підтримці системи обліку і класифікації витрат;
- пошуку і установці партнерських зв'язків і співпраці;

- аналізу даних про стан бізнесу і розробку проектів розвитку підприємства;
- модернізації інформаційної системи підприємства тощо.

Розвиток інформаційного ресурсу підприємства припускає використання методів і засобів взаємодії на рівні глобальних комп'ютерних (інформаційних) мереж. В цьому випадку створюється основа для організації електронних каталогів і магазинів, застосування електронних платежів, ефективнішого вивчення ринку, реалізації нових методів роботи з клієнтами, виконання комплексу заходів електронного маркетингу і ін. Таким чином, створюється основа для реалізації бізнес-процесів в нетрадиційному (віртуальному, електронному) середовищі. Перехід від звичайного бізнесу до віртуального істотно змінює відносини між постачальниками, виробниками, клієнтами і власниками підприємств, знижує ризики бізнесу до такого рівня, який практично недосяжний в традиційних рамках бізнесу. Розширення інформаційного ресурсу змінює можливості управління підприємством, здійснюючи мінімальну реакцію на зміну умов бізнесу, і додатково грає роль генератора доданої вартості. Останнє реалізується за допомогою інтерактивного діалогу, який збагачує інформаційну сировину, – просуває споживача до виробника.

1. Жданов Б. Новая логика и факторы развития КИС./Б.Жданов. № 3/2006. с.12-17. [Електронний ресурс] – режим доступу: http://www.management.com.ua/ims/ims125.html
2. Меняев М.Ф. Системы управления организацией./ М.Ф.Меняев. – М.: Омега – Л, 2003. – 464с.
3. Меняев М.Ф. Информационные системы управления малым бизнесом: Учебное пособие. / М.Ф.Меняев, Н.А. Тимошенко – М.: МГТУ, 2003. – 48с. [Електронний ресурс] – режим доступу: http://www.creativeconomy.ru/keywords/kontirovka/
4. Склара А. Организационные риски внедрения ERP-систем./ А.Склара. № 5/2006. с. 35-38.
5. Фонд регіональних соціально-політичних та економічних досліджень (Львів) [Електронний ресурс] – режим доступу: http://zluka.isr.lviv.ua

ІНФОРМАЦІЙНА ПОЛІТИКА ДЕРЖАВИ ЩОДО ПІДПРИЄМСТВ ВИСОКОТЕХНОЛОГІЧНОГО СЕКТОРУ ЕКОНОМІКИ

Сліпа Ольга Зіновіївна,
викладач кафедри менеджменту ЛьвДУВС

Важливим аспектом розвитку економіки є належне функціонування всіх сфер виробництва, особливо галузей високотехнологічного сектора. Який визначає рівень соціально-економічного зростання країни та виступає чинником підвищення конкурентоспроможності держави у світі. Одним із важливих напрямків розвитку високих технологій є належна комплексна інформаційна політика, яка є важливою рушійною силою, яка впливає на роботу цього сектора. Тому з'ясування впливу інформаційної політики на високотехнологічний сектор економіки є головною метою дослідження й зумовлюють його актуальність.

Важливість ролі інформаційної політики у забезпеченні належного прогресу сектора високих технологій та обґрунтуванні необхідності його вдосконалення розглянуті та постійно досліджуються у працях, таких науковців В.Геєць, В.Іванова, О.Литвиненка, А.Москаленка, Г.Почепцова, В.Солошенка, С.Чукут та ін. Але незважаючи на ґрунтовні розробки поглибленого вивчення потребує сфера державної підтримки цього сектора зокрема державні програми розвитку науково-технічної й інноваційної сфери України. Згідно з Законом України «Про державне регулювання діяльності в сфері трансферу технологій» високі технології – це «технології, які розроблені на основі новітніх наукових знань, за своїм технічним рівнем перевищують кращі вітчизняні та іноземні аналоги і спроможні забезпечити передові позиції на світовому ринку наукомісткої продукції» [2, с.34].

Щоб відбувалось вдосконалення розробок необхідна державна підтримка, яка забезпечується шляхом належного фінансування та здійснення інформаційної політики під якою розуміють діяльність держави в інформаційній сфері, спрямованої на задоволення інформаційних потреб людини і громадянина через формування відкритого інформаційного суспільства на основі розвитку єдиного інформаційного простору цілісної держави та його

інтеграції у світовий інформаційний простір з урахуванням національних особливостей і інтересів при забезпеченні інформаційної безпеки на внутрішньодержавному та міжнародному рівнях.

Основною метою політики інформаційної безпеки держави у сфері високотехнологічного сектору економіки є управління реальними та потенційними загрозами та небезпеками з метою створення необхідних умов для задоволення інформаційних потреб людини та громадянина який працює в цій сфері, а також реалізації національних інтересів. [3, с.86]

На важливості проведення саме цієї політики у своїх дослідженнях зазначала І. Арістова. Яка стверджувала, що для реалізації національних інтересів в інформаційній сфері слід переглянути пріоритети державної політики, розробити нові концептуальні підходи щодо регулювання ринку інформаційно-комунікаційних технологій, інформаційної та інвестиційної політики, розвитку інформаційного законодавства і забезпечення інформаційної безпеки загалом [1, с.112].

Основне призначення інформаційної політики підприємства – надання співробітникам компанії дієвого інструменту та збірки правил з оцінки важливості даної інформації щодо ефективного використання його у інтересах підприємства з мінімальним ризиком шкоди.

Головною метою інформаційної політики стосовно підприємств є забезпечення ефективного досягнення цілей підприємства шляхом:

- інформаційної підтримки у прийнятті управлінських рішень;
- забезпечення працівників підприємства актуальною, своєчасною, достовірною, об'єктивною інформацією на вирішення конкретних посадових завдань;
- запобігання втрати, витоку, спотворення інформації на підприємстві;
- забезпечення швидкого підвищення рівня компетенції співробітників, що дозволить ефективно вирішувати поставлені завдання;
- реалізації постановки завдань співробітникам з урахуванням рівня їхньої компетенції;

- інформаційної підтримки інтересів підприємства у органах та структурі державної влади;
- підвищення інформаційної протидії щодо конкурентів.

Для здійснення цих заходів безперечно необхідний висококваліфікований кадровий потенціал. Наявність інтелектуальної складової у цьому секторі є запорукою здійснення важливих кроків щодо його вдосконалення. Інформаційна політика також має враховувати реалії сьогодення та зарубіжний досвід щодо її реалізації.

Отже, результати роботи дають підстави говорити про те, що формування умов максимального сприяння у підвищенні пріоритетів науково-технічного розвитку повинна забезпечувати ефективна державна інформаційна політика. Завдяки якій сектор високих технологій має всі можливості для того щоб стати цілісним, концептуально вивіреним, ключовим та перспективним напрямком вітчизняної економічної системи.

1. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти / За загальною редакцією д-ра юрид. наук, проф. Бандурки О.М..: Монографія. – Харків: вид-во Ун-ту внутр.справ, 2000. – 368 с.
2. Жукова, Е. А. Проблема классификации високих технологий / Е. А. Жукова // Вестник ТГПУ. – 2008. – № 1 (75). – С. 34-46.
3. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. Інформаційна безпека України в умовах євроінтеграції – Навчальний посібник. – К.: КНТ, 2006. – 280 с.

ВИКОРИСТАННЯ СТИЛІВ У СЕРЕДОВИЩІ MS WORD

Кульчицький Ігор Маркіянович,
доцент кафедри прикладної лінгвістики Національного університету «Львівська політехніка», к.т.н.

Одна з переваг текстових редакторів у тому, що вони надають користувачеві зручні засоби автоматизації створення та форматування текстів. Один з основних таких засобів – стилі.

Загальний огляд стилів. У термінах редактора MS Word стиль – це сукупність параметрів форматування, якій присвоєно ім'я. Іменування певним стилем деякого фрагмента документа означає, що для нього встановлюються відразу всі значення параметрів форматування, які містить цей стиль. Основна перевага використання стилів полягає в тому, що зміна значення якогось параметра у стилі тягне за собою автоматичну заміну значення цього параметра у всіх фрагментах документу, які оформлені цим стилем. Слід зазначити, що редактор Word автоматично використовує стилі для оформлення особливих елементів документа, таких як номери сторінок (колонцифри), верхні та нижні колонтитули, зміст документа, різноманітні покажчики (індекси) тощо. Це означає, що користувач не може уникнути застосування стилів навіть тоді, коли нічого про них не знає.

Таким чином використання стилів у порівнянні з ручним форматуванням тексту дозволяє:

- *Економити час.* Зміна зовнішнього вигляду документа здійснюється легко і швидко заміною значень параметрів форматування у відповідних стилях.
- *Узгоджувати вигляд документа.* Однотипні елементи тексту завжди будуть виглядати однаково у всьому документі і навіть у різних документах. Принагідно слід зазначити, що стилі значно зменшують кількість помилок при форматуванні документа.
- *Структурувати документ.* За допомогою стилів легко створювати документи, що мають ієрархічну структуру (заголовки, підзаголовки) та утворювати такі додаткові елементи документів, зміст яких залежить від основного тексту – покажчики, індекси, зміст тощо.

Редактор MS Word надає користувачу для використання стилі таких типів:

- стилі абзаців;
- стилі символів;
- зв'язані стилі;
- стилі списку;
- стилі таблиці.

Стиль абзацу визначає вигляд та розміщення рядків та вмісту цілого абзацу. У стилях цього типу можна встановлювати

значення тих параметрів форматування, які наявні у діалогових вікнах **Font**, **Paragraph, Tabs, Borders and Shading, Language**, **Frame, Bullets and Numbering**.

Стиль символів визначає вигляд будь-якої послідовності символів документа. У ньому можна встановлювати значення лише тих параметрів форматування, які наявні у діалогових вікнах **Font**, **Borders and Shading, Language**.

Окрім того у обох випадках можна налаштовувати «швидкі» клавіші клавіатури та анімаційні ефекти. Останнє абсолютно не можна рекомендувати при професійній роботі з текстом.

Зв'язані стилі – це комбінований вид стилю, який веде себе у залежності від того, до якого об'єкту його застосовують, або як стиль абзацу, або як стиль символу. При виділенні всього абзацу чи клацанні всередині абзацу та застосувати зв'язаний стиль, то вказані у ньому параметри форматування будуть застосовані до всього абзацу. Якщо ж зв'язаний стиль застосувати до виділеного слова чи фрази, то він поведе себе як стиль символів.

Стилі списку визначають оформлення списків, зокрема такі параметри, як стиль маркера або схему нумерації, відступи та будь-які надписи.

Стилі таблиці визначають оформлення таблиць, зокрема такі параметри, як форматування тексту в рядку заголовка, лінії сітки та контрастні кольори для рядків і стовпців.

Редактор MS Word має два обов'язкових стилі, які присутні у будь-якому документі, і, якщо користувач не використовує силів взалі, то саме ці два стилі присвоюються тексту документу за замовчуванням. Це абзацний стиль Normal, і символьний стиль Default paragraph font. Окрім цього вказані стилі є базовими всіх інших стилів редактора.

Взаємодія стилів абзаців та символів. Коли стиль символів накладається на стиль абзацу, то перевагу має шрифт стилю символів. Якщо ж значення параметрів форматування визначає стиль абзацу, то перевагу мають параметри стилю абзацу.

Приклад. Маємо стиль абзацу з назвою *Реферат*, у якому описано шрифт *Times New Roman*, кегль 12, курсив, та стиль абзацу *Термін,* у якому описано шрифт *Impact*, кегль 14.

При накладанні цих стилів текст, до якого застосували стиль *Термін* буде відформатовано шрифтом *Impact* 14 пунктів (як і

визначено стилем символів), але все одно він залишиться в курсивному начерку, позаяк стиль символів не має чітко вираженої переваги перед стилем. Коли ж і стиль абзацу, і стиль символів має курсивний начерк Word відформатує текст, до якого застосовано стиль символів, як нормальний (не курсив), вважаючи, що ви хочете вказати відмінності між двома стилями.

Взаємодія ручного форматування та стилів. Значення параметрів ручного форматування має перевагу як перед стилями абзацу, так і перед стилями символів, проте, як і в попередньому прикладі, Word постарається вказувати відмінності. Отже якщо відмітити курсивом абзац, стиль якого уже містить курсив, Word відобразить текст без курсиву.

Для того щоб побачити які елементи оформлення тексту були створені стилем, а які – ручним форматуванням, необхідно натиснути комбінацію клавіш <Shift+F1>, а потім клацнути лівою клавішею миші на тексті, що вас цікавить.

Щоб зняти всі елементи ручного форматування і стилі символу, залишивши лише стилі абзацу, необхідно відмітити потрібний фрагмент тексту і натиснути комбінацію клавіш <Ctrl+пробіл>.

Групи стилів. Для зручності форматування текстів стилі об'єднують у групи. Таку групу називають «експрес-стилями». Параметри форматування у такій групі узгоджено за видимими характеристиками, тому текст, який відформатовано лише стилями однієї групи має елегантний професійний вигляд. Особливістю експрес-стилів є те, що при зміні однієї групи експрес-стилів на іншу, видимі характеристики оформлення міняються узгоджено, позаяк інша група має стилі з тими самими назвами, лише з іншими параметрами форматування.

1. Загальні відомості про стилі у програмі Word // support.office.com/uk-ua/article/Загальні-відомості-про-стилі-у-програмі-Word-d38d6e47-f6fc-48eb-a607-1eb120dec563
2. Herb Tyson. Microsoft Word 2010. Bibel. – Indianapolis: Wileg Publishing, Inc., 2010. – 941 p.
3. Камарда, Билл. Использование Microsoft Word 97: Пер. с англ. – К., М., СПб: Издательский дом «Вильнюс», 1998 – 800 с.

4. Беленький Ю.М., Власенко С.Ю. Microsoft Word 2000. – СПб.: БХВ – Санкт-Петербург, 1999. – 992 с., ил.
5. Нортон Питер и др. Microsoft Office 2000. Избранное от Питера Нортона: Пер. с англ./Питер Нортон и др. – К.: Издательство «ДиаСофт», 1999. – 560 с.

МУЛЬТИПЛІКАТИВНЕ ЗГОРТАННЯ КРИТЕРІЇВ ВИБОРУ ДОПУСТИМИХ АЛЬТЕРНАТИВ

Грицюк Юрій Іванович,
професор кафедри програмного забезпечення
НУ «Львівська політехніка», д.т.н., професор
Грицюк Павло Юрійович,
магістрант НЛТУУ

Врахування декількох критеріїв оцінювання інформації, наприклад, варіантів впровадження системи захисту інформації (СЗІ) у будь-яку організацію, доводиться розв'язувати багатокритеріальну задачу пошуку оптимального варіанту з множини допустимих. Як правило, різні цілі впровадження таких СЗІ здебільшого суперечливі між собою. Наприклад, збільшення доступності інформації часто призводить до зменшення її цілісності. Великі витрати на підвищення конфіденційності інформації значно ускладнюють програмно-апаратні засоби досягнення її доступності і т.д. Надмірна спостережність за роботою СЗІ викликає значні нарікання працівників, що її обслуговують. Тому задача вибору оптимального варіанту впровадження СЗІ з урахуванням критеріїв цілісності, доступності, конфіденційності та спостережності інформації належить до задач багатокритеріальної оптимізації.

Для визначення оптимального варіанту СЗІ широко використовуються методи порівняльного аналізу, які ґрунтуються на співставленні допустимих альтернатив, тому розвиток і удосконалення таких методів є актуальним науковим завданням. Серед цих методів широке розповсюдження отримав підхід, згідно з яким багатокритеріальну задачу вибору допустимих альтернатив зводять до однокритеріальної шляхом згортання декількох часткових критеріїв у один узагальнений показник [1-3]. При цьому

для згортання часткових критеріїв може використовуватися така мультиплікативна згортка [7]:

$$F(\tilde{X}) = \left\{ f_i(x_i) = \prod_{k=1}^{K} f_{ik}^{\alpha_k}(x_i),\ i = \overline{1,M} \right\} \to \max \Rightarrow i^*;\ x^* = x_{i^*}, \qquad (1)$$

де: $\tilde{\tilde{F}}(\tilde{X}) = \{\tilde{F}_i(x_i) = \{f_{ik}(x_i),\ k = \overline{1,K}\}, i = \overline{1,M}\}$ – значення k-го часткового критерію для i-ого допустимого варіанта системи; $\tilde{\mathrm{A}} = \{\alpha_k, k = \overline{1,K}\}$ – значення важливості (ваговий коефіцієнт) k-го часткового критерію; K – кількість часткових критеріїв; $\tilde{X} = \{x_i, i = \overline{1,M}\}$ – множина допустимих варіантів СЗІ; M – кількість допустимих варіантів СЗІ.

У роботі [4] мультиплікативну згортку пропонують здійснювати, виходячи з таких міркувань. Більшість сучасних СЗІ характеризується суперечливими вимогами до часткових критеріїв їхнього функціонування: частину з них потрібно максимізувати, а інші – мінімізувати, тобто критерії поділяються на стимулятори та дестимулятори. Нехай досліджувана система характеризується K критеріями, причому перші K' критеріїв потрібно максимізувати (стимулятори), а інші – мінімізувати (дестимулятори). Тоді у [5] мультиплікативну згортку для вибору найкращої альтернативи пропонується реалізувати в такому вигляді:

$$F(\tilde{X}) = \left\{ f_i(x_i) = \sqrt[K]{\prod_{k=1}^{K'} \frac{f_{ik}(x_i)}{f_k^{\text{н}}} \cdot \prod_{k=K'+1}^{K} \frac{f_k^{\text{н}}}{f_{ik}(x_i)}},\ i = \overline{1,M} \right\} \to$$

$$\to \max \Rightarrow i^*;\ x^* = x_{i^*}, \qquad (2)$$

де $\tilde{F}^{\text{н}} = \{f_k^{\text{н}}, k = \overline{1,K}\}$ – нормативне (еталонне) значення k-го показника. Ця згортка є більш обґрунтованою порівняно з виразом (1), позаяк оперує безрозмірними відхиленнями часткових критеріїв відносно їхніх бажаних значень.

У роботі [6] розглянуто таке поняття, як гіпотетична найгірша альтернатива, яка характеризується найгіршими значеннями часткових критеріїв. При цьому передбачається порівняння кожної альтернативи як з еталонною альтернативою, так і з її найгіршим значенням. Тоді найкращою вважається та альтернатива, яка є найближчою до еталонної та найвіддаленішою від

найгіршої. Практичне застосування цього підходу засвідчило перспективність його використання, тому спробуємо поширити його і на мультиплікативну згортку.

Задача багатокритеріального вибору допустимого варіанта СЗІ полягає в тому, що вона характеризуються K частковими показниками ефективності

$$\tilde{\tilde{P}} = \left\{ \tilde{P}_i = \{ p_{ik},\ k = \overline{1,K} \},\ i = \overline{1,M} \right\},$$

причому K' з цих показників є стимуляторами, а решта – дестимуляторами. Для прийняття управлінського рішення особі, яка його приймає (ОПР), потрібно виявити допустимі варіанти СЗІ. Вважатимемо, що допустимим вважається той варіант, який максимально наближений до найкращого та максимально віддалений від найгіршого з варіантів складу СЗІ.

З огляду на зазначене вище, потрібно вирішити ряд часткових завдань:

1) надати визначення поняттям «найкращий» та «найгірший» варіанти СЗІ, а також визначити числові значення часткових показників ефективності, які характеризують ці варіанти;

2) на основі мультиплікативного згортання сформувати узагальнений показник, який буде характеризувати ступінь віддаленості розглядуваного варіанту від найкращого та найгіршого з варіантів;

3) визначити механізм оцінювання переваги кожного допустимого варіанту;

4) визначити механізм відбору допустимих варіантів, які аналізуватиме ОПР.

Поняття «найкращий варіант» визначимо як варіант, що характеризується найкращими значеннями стимуляторів чи дестимуляторів, визначеними на множині наявних варіантів, тобто

$$\tilde{P}' = \left\{ p'_k = \begin{cases} \max\{p_{ik},\ i = \overline{1,M}\}, \text{ якщо } k \in S; \\ \min\{p_{ik},\ i = \overline{1,M}\}, \text{ якщо } k \in D, \end{cases} k = \overline{1,K} \right\},$$

де S, D – множини стимуляторів і дестимуляторів відповідно.

Поняття «найгірший варіант» визначимо як варіант, що характеризується найгіршими значеннями стимуляторів та дестимуляторів, визначеними на множині наявних варіантів, тобто

$$\tilde{P}'' = \left\{ p''_k = \begin{cases} \min\{p_{ik},\, i = \overline{1,M}\}, \text{ якщо } k \in S; \\ \max\{p_{ik},\, i = \overline{1,M}\}, \text{ якщо } k \in D, \end{cases} \; k = \overline{1,K} \right\}.$$

Узагальнений показник, який характеризуватиvt ступінь віддаленості розглядуваного варіанту від найкращого та найгіршого з допустимих варіантів, сформуємо за мультиплікативною згорткою, виходячи з таких міркувань.

Як зазначалось вище, згортка (2) оперує безрозмірними відхиленнями часткових показників ефективності відносно їхніх бажаних значень. Стосовно стимуляторів «бажаними» є найбільші значення часткових показників ефективності, а для дестимуляторів – найменші значення. Тоді для сукупності стимуляторів і дестимуляторів стосовно найкращого варіанта СЗІ показник переваги для *i*-ої альтернативи набуде такого вигляду:

$$R(\tilde{X}) = \left\{ r_i(x_i) = \sqrt[K]{\prod_{k=1}^{K'} \frac{p_{ik}(x_i)}{p'_k} \cdot \prod_{k=K'+1}^{K} \frac{p'_k}{p_{ik}(x_i)}},\; i = \overline{1,M} \right\} \to \max . \quad (3)$$

Тоді величина, обернена до $r_i(x_i)$, матиме такий вигляд:

$$R'(\tilde{X}) = \left\{ r'_i(x_i) = \frac{1}{r_i(x_i)},\; i = \overline{1,M} \right\} \to \min \quad (4)$$

і показуватиме у скільки разів *i*-ий альтернативний варіант гірший за найкращий варіанта СЗІ. Зрозуміло, що під час визначення оптимального варіанта СЗІ показник (3) доцільно максимізувати, а (4) – мінімізувати.

Виходячи з аналогічних міркувань, отримаємо показник, який характеризує якість *k*-го варіанта складу СЗІ стосовно найгіршого варіанта, а саме

$$H(\tilde{X}) = \left\{ h_i(x_i) = \sqrt[K]{\prod_{k=1}^{K'} \frac{p_{ik}(x_i)}{p''_k} \cdot \prod_{k=K'+1}^{K} \frac{p''_k}{p_{ik}(x_i)}},\; i = \overline{1,M} \right\} \to \max . \quad (5)$$

Показник, розрахований за формулою (5), показує у скільки разів *i*-ий альтернативний варіант кращий за найгірший варіант. Тоді величина, обернена до $h_i(x_i)$, матиме такий вигляд:

$$H'(\tilde{X}) = \left\{ h'_i(x_i) = \frac{1}{h_i(x_i)},\; i = \overline{1,M} \right\} \to \min \quad (6)$$

і показуватиме у скільки разів *i*-ий альтернативний варіант кращий за найгірший варіанта СЗІ. Зрозуміло, що під час визначення оптимального варіанта показник (5) доцільно максимізувати, а (6) – мінімізувати.

Отримані показники (3) та (5) характеризують якість *k*-го допустимого варіанта складу СЗІ стосовно її найкращого та найгіршого варіантів окремо, а їхній добуток $r_i(x_i) \cdot h_i(x_i)$ показуватиме у скільки разів *i*-ий варіант є кращим за найгірший варіант, ніж гірший порівняно з найкращим варіантом СЗІ.

Виходячи з того, що при виборі оптимального варіанта потрібно максимально наблизитись до найкращого варіанта та максимально віддалитись від найгіршого (тобто максимізувати добуток $r_i(x_i) \cdot h_i(x_i)$), то за узагальнений показник переваги одного варіанта від іншим потрібно використати такий вираз:

$$\mathrm{H}(\tilde{X}) = \left\{ \eta_i(x_i) = \sqrt[K]{\prod_{k=1}^{K'} \frac{p_{ik}(x_i)}{p'_k} \prod_{k=K'+1}^{K} \frac{p'_k}{p_{ik}(x_i)}} \cdot \right.$$

$$\left. \cdot \sqrt[K]{\prod_{k=1}^{K'} \frac{p_{ik}(x_i)}{p''_k} \prod_{k=K'+1}^{K} \frac{p''_k}{p_{ik}(x_i)}} \right\}, \; i = \overline{1, M} \to \max, \qquad (7)$$

або

$$\mathrm{H}(\tilde{X}) = \left\{ \eta_i(x_i) = \sqrt[K]{\prod_{k=1}^{K'} \frac{p_{ik}^2(x_i)}{p'_k \cdot p''_k} \cdot \prod_{k=K'+1}^{K} \frac{p'_k \cdot p''_k}{p_{ik}^2(x_i)}}, \; i = \overline{1, M} \right\} \to \max, \qquad (8)$$

який є математичним спрощенням виразу (7) і, водночас, буде мультиплікативною згорткою часткових критеріїв ефективності варіанта СЗІ.

Узагальнений показник, розрахований за формулою (8), показує у скільки разів *i*-ий допустимий варіант СЗІ максимально наближений до найкращого варіанта та максимально віддалений від найгіршого. Тоді величина, обернена до $\eta_i(x_i)$, матиме такий вигляд:

$$\eta'(\tilde{X}) = \left\{ \eta'_i(x_i) = \frac{1}{\eta_i(x_i)}, \; i = \overline{1, M} \right\} \to \min \qquad (9)$$

і показуватиме у скільки разів *i*-ий допустимий варіант мінімально віддалений від найкращого варіанта та мінімально наближений да найгіршого.

Стосовно механізму оцінювання переваги кожного допустимого варіанта складу СЗІ, то потрібно виходити з таких міркувань: кращому варіанту (виходячи з виразу (8)) відповідатиме більше значення узагальненого показника $\eta_i(x_i)$, тому відносне ранжування альтернатив потрібно здійснити за зменшенням їх числових значень. При цьому найбільшому значенню $\eta_i(x_i)$ відповідатиме оптимальний варіант СЗІ, який і доцільно першочергово аналізувати ОПР для прийняття управлінського рішення.

У разі потреби аналізу ОПР декількох варіантів СЗІ, то, відповідно до фізичного змісту узагальненого показника $\eta_i(x_i)$, середній якості варіанта СЗІ буде відповідати така умова: $\eta_i(x_i)=1$. Це означає, що всі варіанти СЗІ, для яких $\eta_i(x_i)<1$, будуть гіршими за середню якість, а варіанти, кращі за середню якість, будуть характеризуватися виконанням такої умови: $\eta_i(x_i)>1$. Тому ОПР для прийняття оптимального рішення потрібно аналізувати тільки ті варіанти СЗІ, які є кращими за середню якість.

Таким чином, розглянута вище методика дає змогу визначити найкращу альтернативу на основі використання мультиплікативного згортання часткових критеріїв ефективності СЗІ, що досліджується, в узагальнений показник.

1. Балыбин В.М. Принятие проектных решений / В.М. Балыбин, В.С. Лунев, Д.Ю. Муромцев, Л.П. Орлова. – Тамбов : Изд-во ТГТУ, 2003. – 80 с.
2. Ногин В.Д. Принятие решений при многих критериях / В.Д. Ногин. – СПб. : Изд-во «Ютас», 2007. – 104 с.
3. Подиновский В.В. Введение в теорию важности критериев в многокритериальных задачах принятия решений / В.В. Подиновский. – М. : Изд-во "Физматлит", 2007. – 64 с.
4. Черноморов Г.А. Теория принятия решений / Г.А. Черноморов // Известия вузов. – Сер.: «Электромеханика». – Новочеркасск : Изд-во Юж.-Рос. гос. техн. ун-та, 2002. – 276 с.

5. Тупкало В.Н. Совершенствование системы управления предприятием на основе реализации принципа «Структура следует за стратегией» / В.Н. Тупкало, С.В. Тупкало // Das Management. – 2009. – № 1 (11-12). – С. 66-71.
6. Потьомкін М.М. Комплексне застосування методів багатовимірного порівняльного аналізу в СППР // Системи підтримки прийняття рішень: теорія і практика : зб. доп. наук.-практ. конф. з міжнар. участю, (8 червня 2009 р.). – К. : Вид-во ІПММіС НАНУ, 2009. – С. 43-46.
7. Потьомкін М.М. Застосування модифікованої мультиплікативної згортки показників для вибору альтернатив / М.М. Потьомкін. [Електронний ресурс]. – Доступний з http://intkonf.org/ kandidat-tehnichnih-nauk-potomkin-mm-zastosuvannya-modifikovanoyi-multiplikativnoyi-zgortki-pokaznikiv-dlya-viboru-alternativ/

ЗМІСТ

І. Науково-методичні, нормативно-правові та програмно-технічні аспекти застосування інформаційних технологій в оперативній діяльності органів внутрішніх справ

НАУКОВЕ ВИДАННЯ

ПРОБЛЕМИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ, СПЕЦІАЛЬНИХ ТЕХНІЧНИХ ЗАСОБІВ У ДІЯЛЬНОСТІ ОВС ТА НАВЧАЛЬНОМУ ПРОЦЕСІ

Збірник наукових статей
за матеріалами доповідей
науково-практичної конференції
26 грудня 2014 р.

Відповідальний за випуск Я.Ф. Кулешник
Упорядник Т.В. Магеровська
Комп'ютерна верстка Т.В. Магеровська

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