ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СПЕЦІАЛЬНА БЕЗПЕКА
НАУКОВИЙ ЖУРНАЛ

№ 1(002) 2016

ЗМІСТ

ВИБІР РЕДАКЦІЇ

М.М. Єрмошенко, **В.Р. Сафонов**
ЕФЕКТИВНИЙ ВЕКТОР ПРИСКОРЕНОГО РОЗВИТКУ – МОБІЛІЗАЦІЯ НОВАТОРСЬКОГО АРСЕНАЛУ УКРАЇНИ НА БАЗІ ІТ……..……...2

Рыбальский О.В., **Тимошенко Л.Н**
ПОДГОТОВКА СПЕЦИАЛИСТОВ ДЛЯ БОРЬБЫ С КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТЬЮ……....12

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, ІТ БЕЗПЕКА

Додонов А.Г., Ландэ Д.В.
МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННЫХ РЕЗЕРВАЦИЙ…..……...16

А. І. Кузьмичов, В. В.Бочаров
ОПЕРАТИВНА РЕКОНФІГУРАЦІЯ КОМУНІКАЦІЙ У МЕРЕЖІ ІЗ ЗАСТОСУВАННЯМ ОПТИМІЗАЦІЙНИХ ЕТ-МОДЕЛЕЙ……27

О.Я. Матов, **В.С. Василенко**

МЕТОДИКА ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ…….....38

Сенченко В.Р
МЕТОДИ ТА ТЕХНОЛОГІЇ ОБРОБКИ ДАНИХ У СИСТЕМІ МОНІТОРИНГУ ТА АНАЛІЗУ ДЕРЖБЮДЖЕТУ…….50

СПЕЦІАЛЬНА БЕЗПЕКА

І.М.Демчак, О. П. Кучеров, О.П.Савицька

ЕКОНОМІКО-МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ СІЛЬСЬКИХ НАСЕЛЕНИХ ПУНКТІВ ЯК ОСНОВА ДЛЯ ФОРМУВАННЯ АГРАРНОЇ ПОЛІТИКИ ……...65

О. П. Кучеров, С.Є. Лавровський
ПІКОСКОП, ЯК ІНСТРУМЕНТ ДЛЯ ВИВЧЕННЯ АТОМАРНОЇ СТРУКТУРИ МОЛЕКУЛ……73

М.П. Руденко

ЛЮДСЬКИЙ ФАКТОР У КОМП'ЮТЕРНИХ МОДЕЛЯХ ДИНАМІЧНИХ ПРОЦЕСІВ СКЛАДНИХ ТЕХНІЧНИХ СИСТЕМ ……..80

РЕЦЕНЗІЇ ТА ІНФОРМАЦІЙНІ ПОВІДОМЛЕННЯ

ПРАВИЛА ДЛЯ АВТОРІВ …….....87

ВИБІР РЕДАКЦІЇ

М.М. Єрмошенко д.е.н., професор

В.Р. Сафонов незалежний експерт у сфері зв'язку та інформатизації України,

Національна академія управління

ЕФЕКТИВНИЙ ВЕКТОР ПРИСКОРЕНОГО РОЗВИТКУ – МОБІЛІЗАЦІЯ НОВАТОРСЬКОГО АРСЕНАЛУ УКРАЇНИ НА БАЗІ ІТ

На виконання програми «Партнерство в навчанні» компанія «Майкрософт Україна» за сприяння Інституту інноваційних технологій і змісту освіти Міністерства освіти і науки України проводить щорічний конкурс «Вчитель-новатор», мета якого – опанування освітянами сучасних педагогічних та інформаційно-комунікаційних технологій (ІКТ), підтримка роботи педагогів у розробці та впровадженні мультимедійних програмних засобів навчання [18].
На базі Рівненського обласного інституту післядипломної педагогічної освіти відбулося чергове засідання Всеукраїнської школи новаторства керівних, педагогічних і науково-педагогічних працівників післядипломної педагогічної освіти, в рамках якого було проведено Всеукраїнський науково-практичний семінар «Педагогічний досвід як фактор оновлення змісту науково-методичної діяльності в установах і закладах освіти: вектори випереджувального розвитку» [4].

Регуляторними органами, що приймали участь в Глобальному симпозіумі для регуляторних органів 2011 р., було визнано, що не існує якої-небудь всеохоплюючої схеми для передової практики, але вони згодні з тим, що можна навчатися на досвіді різних країн, зауваживши, що країни з високим рівнем цифрової грамотності є новаторськими і продуктивними і на них припадає більша частка в світових торгівлі, інвестиціях і робочих місцях [24].

У загальновідомій книзі Б. Гейтса «Дорога в майбутнє», в главі «Освіта – краще вкладення грошей», поміж іншим, зауважено: «Педагоги, як і багато фахівців, крім усього іншого, в сучасній економіці виступають посередниками – посередниками між знаннями і учнями. Відповідно, їм теж доведеться пристосовуватися до мінливих умов. Однак, на відміну від людей інших професій, вони можуть дивитися в майбутнє з безумовним оптимізмом. Коли чергове нововведення підвищує рівень життя суспільства, обов'язково зростає попит на вчителів. І педагоги, здатні привнести в шкільні класи творчий дух та енергію, завжди будуть процвітати» [6].

З урахуванням європейського вибору України варто зауважити, що офіційні документи ЄС завжди містять у собі цілу низку так званих «попередніх» положень, на основі яких стають зрозумілими наступні, основні положення документу. Наприклад, у Директиві 2002/22/ЄС від 7.03.2002 про універсальні послуги та права користувачів електронних мереж зв'язку і послуг таких «попередніх» положень, передуючих основному тексту, міститься 52 [1].

Керуючись саме таким підходом, перш ніж сформулювати пропозиції щодо прискореної побудови в Україні новаторської і продуктивної економіки, з використанням для цього як позитивного досвіду провідних країн світу, так і суто вітчизняних успіхів в освітній, високотехнологічній та інноваційній сферах, викладемо деякі, необхідні для обґрунтування цих пропозицій, позитивні факти.

Нещодавно Університетський Коледж Лондону і Трініті-коледж Дублінського університету, а також британський Відкритий університет, що спеціалізується на дистанційному навчанні, розмістили аудіо- та відеозаписи лекцій своїх провідних викладачів на безкоштовному освітньому розділі порталу "iTunes U". Провідні американські університети (Гарвард, Йель, Стенфорд, Берклі, Массачусетський технологічний інститут тощо) теж застосовують аналогічні підходи. Так, запущена в 2012 р. освітня платформа EdX надає доступ до курсів Гарвардського університету і Массачусетского технологічного інституту (MTI) в режимі "online" всім бажаючим, що мають Інтернет.

За словами професора MTI і президента компанії EdX А. Агарвала, платформою EdX вже скористалися понад 600 тис. з 192 країн світу. «Поки що це експеримент, але експеримент, який зобов'язаний спрацювати», – зазначив він. На його думку, дистанційне навчання значно відрізняється від оцифровки звичайних університетських курсів, порівнюючи цю систему з трансляцією по телевізору відеозапису театральної постановки, яка відмінна від художнього фільму. «Навантаження курсу повинне відповідати звичайному університетському, проте інформація подається по-іншому. Один з моїх улюблених підходів полягає в заміні лекцій серією навчальних інтерактивних відеороликів з вправами». У той же час, відзначає А. Агарвал, дистанційне навчання – це не благодійність, а можливість знайти талановитих студентів по всьому світу і залучити їх до Гарварда та MTI. «Проект переслідує дві мети. Одна – розширити доступ до курсів провідних університетів Гарварду, MTI, Берклі. Однак ми також хочемо, щоб на кампус приходили нові студенти і технології, приносячи з собою інновації» [26].

Аналізуючи стан світової економіки, не можна не звернути увагу на те, що за останні півстоліття Індія досягла вражаючих успіхів у соціально-економічній сфері. У 1998 р. урядом цієї країни була поставлена задача перетворення на світового лідера в галузі IT. Уряд Індії приділяє особливу увагу створенню економічних зон, як багатопрофільних, так і спеціалізованих (понад 150), у т.ч. для інформаційних технологій. У сфері інформаційних технологій величезну роль відіграють парки програмних технологій, які на 100% є експортно-орієнтованими (на них припадає 80% усього експорту програмного забезпечення (ПЗ). У 2008/09 фінансовому році експорт ПЗ склав 47 млрд дол. США (друге місце у світі після США) [8].

На 8-му Глобального симпозіумі регуляторних органів (м. Паттайя, Таїланд, березень 2008 р.) було зазначено, що в країнах, де розвивається колективне користування на рівні кінцевих споживачів, забезпечується розширення можливостей економічного розвитку в цілому. Спільне використання телекомунікаційних ресурсів на рівні кінцевих споживачів дозволяє суттєво зменшити витрати на надання та використання послуг і забезпечує доступність послуг, що надаються. Національним регуляторним органам при цьому відводиться важлива роль у забезпеченні сприятливих умов для організації цих процесів. Ефективне використання спільних ресурсів забезпечує створення відповідних можливостей для формування потенціалу інфраструктури та людського потенціалу. Так, у 1990-х рр. Бюро розвитку електрозв'язку (БРЕ) Міжнародного союзу електрозв'язку (МСЕ) наддало підтримку в проведенні реформи у галузі електрозв'язку Домініканської Республіки та допомогло створити національний регуляторний орган "INDOTEL", а також прийняти першу чергу законодавчих актів щодо галузі електрозв'язку. Далі цей процес був підтриманий Всесвітнім банком. Першим кроком "INDOTEL" була розробка програм із забезпечення базового рівня письменності для різних цільових груп. Окрім того, було створено віртуальну бібліотеку, що нараховує понад 100 тис. томів, доступних у режимі "online". Для підтримки місцевої економіки шляхом ефективного використання ІКТ, практично в усіх центрах "INDOTEL" організовано курси англійської мови, включаючи модулі, орієнтовані на туризм, оскільки він є найбільш стимульованою галуззю місцевої економіки. Як результат, понад 90% населення, зайнятого у секторі обслуговування,

володіє 2–3 мовами завдяки підготовці в таких центрах. Окрім того населення, що займається фермерством, може спільно користуватися інформацією про розвиток фермерства, сільського господарства тощо за допомогою послуг мобільного зв'язку у формі платних SMS та доступу до Інтернет [13].

З метою поширення і подальшого розвитку методології і технології теорії вирішення винахідницьких задач (ТВВЗ) у Німеччині у серпні 1996 р. під керівництвом професора М. Орлова було організовано «Академію Модерн ТВВЗ» з напрямками діяльності: ТВВЗ-консалтинг, ТВВЗ-тренінг, поширення і розвиток ТВВЗ-софтвера, за підтримки Сенату Берліна, як одна з перших науково-дослідних фірм у щойно створеному, першому в Німеччині, центрі співпраці «Захід-Схід» при «Інноваційному центрі "Berlin-Adlershof"».

У результаті декількох успішних інноваційних проектів на початку 2000-х рр. за фінансової підтримки Міністерства економіки Німеччини були розвинені і протестовані основи технології «Модерн ТВВЗ», піонерне навчально-прикладне програмне забезпечення "Idea Navigator", а на замовлення видавництва "Springer" було підготовлено і видано перший підручник «Основи класичної ТВВЗ» німецькою та англійською мовами. На початку 2012 р. це ж видавництво випустило книгу М. Орлова «Неважка ТВВЗ» англійською мовою під назвою "Modern TRIZ. A Practical Course with EASyTRIZ Technology". У 2006 р. підручник «Основи класичної ТВВЗ» вийшов і в Росії. З 2010 р. пілотний проект у вигляді сертифікаційного дистанційного тренінгу використовується Європейськими програмами "TEMPUS" та "ERASMUS" для імплементації технології «Модерн ТВВЗ» в навчальному процесі в 17 університетах Казахстану, Киргизстану, Росії, Узбекистану і України. Наприкінці 2010 р. книга М.Орлова «Основи класичної ТВВЗ» була видана одним з найбільших видавництв Китаю – "Science Press". З урахуванням досвіду роботи за методологією і технологією Модерн ТВВЗ у П. Кореї та Китаї, а також у Росії та Німеччині, протягом двох з половиною років з 2009 р. і до кінця 2011 р. випущено нові підручники – «Азбука ТВВЗ», «Первинні інструменти ТВВЗ», «Неважка ТВВЗ». Створена в Росії «Академія Модерн ТВВЗ» не тільки зберегла і примножила ентузіазм, але й знайшла ресурси для виведення на ринок в 2006 р. і продовження та розповсюдження під час кризи 2008–2010 рр. та після неї дистанційної технології навчання «Модерн ТВВЗ» на основі програми EASyTRIZ™, яка одночасно є навчальним і професійним інструментом [7].

Світовий досвід показує, що електронне навчання ("e-learning") є одним з основних інструментів модернізації освіти. У П.Кореї, Фінляндії та Ірландії реалізуються спеціальні національні програми з електронного навчання. У Франції ІКТ впроваджується в усі сфери освітнього процесу, від дитячого садка до навчання дорослих. У США, Великій Британії, Австралії, Новій Зеландії, Канаді електронне навчання є практикою повсякденного життя. У Казахстані стартував новий етап інформатизації – визнання «e-learning» ключовим напрямком інноваційного розвитку системи освіти. У 2011 р. цей вид навчання впроваджено в 44 казахстанських школах. «До 2015 р. 50% організацій освіти будуть використовувати електронне навчання, а до 2020 р. їх чисельність зросте до 90%», – зазначив Н. Назарбаєв у Посланні до народу Казахстану. Поставлені ним завдання реалізуються в рамках Державної програми розвитку освіти на 2011–2020 роки. «В середньому в освіті ведеться робота по 90% використанню системи електронного навчання, переходу на 12-річну модель навчання, збільшення кількості інтелектуальних шкіл у всіх регіонах Казахстану», – заявив прем'єр-міністр К. Масімов, виступаючи на розширеному засіданні Парламентської фракції НДП «Нур Отан» [27].

В Україні теж ведеться аналогічна робота.

З метою реалізації Основних засад розвитку інформаційного суспільства в Україні на 2007–2015 рр. для забезпечення навчання, виховання, професійної підготовки людини для роботи в інформаційному суспільстві визначено за необхідне:

- розробити методичне забезпечення використання комп'ютерних мультимедійних технологій при викладанні шкільних предметів та дисциплін;

- врахувати особливості роботи з ІКТ в системах навчання студентів педагогічних вищих навчальних закладів і перепідготовки вчителів;

- створити системи дистанційного навчання та забезпечити на їх основі ефективне впровадження і використання ІКТ на всіх освітніх рівнях усіх форм навчання.

Наказом Міністерства освіти і науки України від 24.11.2004 р. № 880, у складі НТУУ «Київський політехнічний інститут», було створено Український інститут інформаційних технологій в освіті. Відповідно до Плану дій щодо забезпечення якості вищої освіти України та її інтеграції в європейське і світове освітнє співтовариство було розроблено:

- механізми запровадження дистанційного навчання (змішаного навчання) в систему вищої професійної освіти та навчання впродовж життя (кейс-технологій, ТВ-технологій, чат-технологій тощо);

- науково-методичні рекомендації щодо використання інформаційних технологій в навчальному процесі вищих навчальних закладів;

- науково-методичні рекомендації щодо створення сучасних підручників, інтерактивних курсів, електронних дидактичних комплексів тощо.

За останні роки дистанційна освіта отримала найбільший розвиток в таких університетах як Національний технічний університет України «Київський політехнічний інститут», Харківський університет радіоелектроніки, Харківський національний технічний університет «Харківський політехнічний інститут», Хмельницький національний університет, Сумський державний університет, Полтавський університет економіки і торгівлі, Тернопільський національний технічний університет ім. І. Пулюя, Національний університет біоресурсів і природокористування України, Університет банківської справи Національного банку України, Київський національний університет технологій та дизайну. Першочергового вирішення потребують наступні питання: формування ієрархії системи, розподілу повноважень і обов'язків, встановлення параметрів оптимального поєднання державного регулювання з автономією (незалежністю) її суб'єктів; розробка науково обґрунтованих вимог (психологічних, педагогічних, соціальних, технологічних) до змісту, методів і форм дистанційної освіти та механізмів контролю їхньої якості, визначення на основі результатів маркетингових досліджень сфери впровадження дистанційного навчання, запитів і потреб потенційних користувачів, розробки системи кадрового забезпечення дистанційного навчання; розроблення та впровадження високоякісного дидактичного та науково-методичного забезпечення дистанційної освіти на рівні міжнародних вимог [17].

24.05.2013 МОН України затвердило «Положення про дистанційне навчання» [2]. Також створюється єдиний електронний портал навчальних ресурсів, школярі отримують індивідуальні навчальні плани. Завершено 1-й етап, на якому 54 навчальні заклади в усіх регіонах України отримали мультимедійні комплекси та комп'ютери для вчителів. При цьому охоплено 4 тис. учнів і викладачів. На 2-му етапі ще 2 тис. шкіл отримали до кінця 2013 р. сучасну матеріально-технічну базу. Усі загальноосвітні школи до 2015 р. заплановано забезпечити комп'ютерами і підключити до високошвидкісного Інтернету.

У червні 2014 р. у м. Рівному відбулася робота 7-ої Всеукраїнської школи новаторства. Цьогорічна тема школи новаторства – «Упровадження системи мережевої взаємодії науково-методичних служб різних рівнів як основа реалізації державних освітніх стандартів». Школа працювала на базі Рівненського обласного інституту післядипломної педагогічної освіти спільно з Університетом менеджменту освіти. Крім цього, до обговорень долучились автори інноваційних розробок із питань науково-методичної роботи з педагогічними кадрами, а також педагогічні і науково-педагогічні працівники Рівненського обласного інституту післядипломної педагогічної освіти, працівники районних, міських методичних служб Рівненщини. Усього майже 300

учасників, зокрема 46 представників із 20 регіонів України. Під час роботи школи відбулась й Інтернет-конференція, де регіональні та зональні школи новаторства презентували інтерактивні форми навчання та всебічне впровадження їх у педагогічну практику, власний новаторський досвід для підвищення фахового рівня керівних і педагогічних працівників дошкільних, загальноосвітніх та позашкільних навчальних закладів [5].

1 вересня 2014 р. стартував пілотний проект «Розумна дитина» з апробації Національного продукту для освіти, розробленого спільними зусиллями представників Міністерства освіти і науки України, компаній «Intel Україна», «Майкрософт Україна», «Навігатор», «Prestigio Україна», мультимедійного видавництва «Розумники», Інституту інформаційних технологій і засобів навчання НАПН України, управління освіти Оболонського району та директорів СШ № 14 та ЗНЗ № 225. Метою дослідження пілотного проекту «Розумна дитина» є створення умов для використання новітніх інформаційно-комунікаційних технологій і електронних освітніх ресурсів під час навчання учнів початкової школи [21].

1 липня 2014 р. Верховна Рада України прийняла новий Закон України «Про вищу освіту». Цей нормативно-правовий акт формує законодавчі підвалини сталого соціально-економічного, високотехнологічного та інноваційного розвитку країни за рахунок якісної підготовки конкурентоспроможного людського капіталу та посилення зв'язків між суспільством, вищою освітою і наукою. Він встановлює основні правові, організаційні, фінансові засади функціонування системи вищої освіти, створює умови для посилення співпраці державних органів і бізнесу з ВНЗ на принципах університетської автономії, поєднання освіти з наукою та виробництвом задля забезпечення потреб суспільства, ринку праці та держави у кваліфікованих фахівцях. Важливим принципом при розробці законопроекту було гармонійне поєднання нововведень з вже працюючими нормами, специфічними для нашої країни [15].

У 2014 р. в НТУУ «КПІ» відбулося завершення комплексної науково-технічної розробки за участю фахівців ТЕФ, ФЕЛ, РТФ, ІТС, ФЕА, які створили перший український університетський наносупутник "PolyITAN-1". Створення подібних мініатюрних супутників серії CubeSat, за версією американського журналу "Science", входить до десяти найбільш визначних світових наукових відкриттів і науково-технічних досягнень 2014 року. Підсумки третього конкурсу інноваційних проектів "Sikorsky Challenge" засвідчили фінансову підтримку 14 проектів-переможців на суму 23,4 млн грн для створення відповідних стартапів, що є ілюстрацією формування в Київській політехніці інноваційного середовища нового для України типу, в якому організація виконання і впровадження інноваційних проектів здійснюється на засадах світового досвіду поєднання інтересів і гармонійної взаємодії освіти, науки, виробництва, бізнесу. Професор Андрій Фокін і доцент Катерина Бутова – у співпраці з колегами з Німеччини, США та Бельгії вперше у світі створили мономолекулярні вуглеводневі діоди з геометричними розмірами близько 1 нм, що має дати можливість на порядок зменшити розміри пристроїв з використанням нових діодів. Результати цієї роботи опубліковані в провідному міжнародному науковому журналі Nature Communications. Молоді науковці НТУУ «КПІ» об'єдналися в Раду молодих учених НТУУ "КПІ", що почала функціонувати з метою всебічного сприяння науковій, інноваційній, винахідницькій та іншій творчій діяльності [14].

31 жовтня 2014 р. в Інституті прикладного системного аналізу НТУУ «КПІ» пройшла конференція «EU IT Outsourcing Experience in Ukrainian Universities: Way to Success» («Європейський досвід аутсорсінгу в сфері інформаційних технологій в українських університетах: шлях до успіху»). Конференція стала значною подією в житті університету не лише тому, що була присвячена важливим для розвитку підготовки спеціалістів для ІТ-галузі питанням та налагодженню тісніших зв’язків між університетською наукою і

бізнесом, але й тому, що розпочалася вона з відкриття на базі ІПСА НТУУ «КПІ» регіонального Міжуніверситетського навчально-виробничого центру аутсорсингу «ITSEA» (IT Service Education Application). Сама церемонія відкриття була доволі незвичайною, бо проводилася майже одночасно з церемонією відкриття такого ж Центру в Одеському національному політехнічному університеті. Учасники урочистостей в обох містах бачили одне одного на великих екранах, які є невід'ємними частинами обладнання новостворених навчально-наукових структур, і спілкувалися в режимі реального часу. Це обладнання дозволяє організовувати читання масових відкритих онлайн-курсів (МВОК) для аудиторій різних міст і навіть різних країн. Можливості апаратури для відеоконференцзв'язку були продемонстровані під час зв'язку з колегами, які перебували у Великій Фізичній аудиторії КПІ, в Одесі та у Сполучених Штатах Америки, Великій Британії, Швейцарії та інших країнах. Центр створено у рамках європейського проекту TEMPUS «Innovation hybrid Strategy of IT-outsourcing partnership with enterprises» (IHSITOP) за підтримки постійної комісії Київради з питань освіти, науки та інноваційної політики [28].

6 лютого 2015 р. відбулося урочисте підписання Протоколу про наміри щодо співпраці НТУУ «КПІ», корпорації «Науковий парк «Київська політехніка», ТОВ «АЙЛАНД МЕНЕДЖМЕНТ» і ТОВ «Технології природи». Цей документ створює підґрунтя співпраці університету з компаніями-партнерами щодо впровадження у життя масштабних проектів «POLYTECO SCIENCE CITY» та «ВЛАСНЕ ТЕПЛО». Обидва проекти є проривними не лише для КПІ, але й для всієї України. На території університету планується побудувати цілий науково-виробничий комплекс загальною площею 251 тис. кв. м – Інноваційне місто КПІ (проект «POLYTECO SCIENCE CITY»). У його будівлях міститимуться бізнес-інкубатор, венчурні фонди, лабораторії прототипів, спеціальні приміщення для високотехнологічних виробництв, лекторії, офісні приміщення, коворкінг-центр, готель, заклади харчування. Інноваційне місто КПІ стане середовищем для розвитку наукоємних технологій за допомогою наукових і виробничих площ КПІ, а також міжнародних і вітчизняних високотехнологічних компаній та інвесторів. Зрозуміло, що його база використовуватиметься не лише для дослідницьких і конструкторських цілей, але й для навчання студентів університету [29].

У рейтингу 50 найбільш інноваційних країн світу, складеному "Bloomberg", Україна розмістилася на 42-ій позиції. На 41-ій позиції опинилася Греція, на 43-їй – Болгарія. Рейтинг складали виходячи з декількох чинників: концентрація високих технологій, продуктивність промисловості та праці, рівень освіти і патентна активність. За рівнем інтенсивності досліджень Україна посіла 37-ме місце, продуктивності праці – 69-те, концентрації високих технологій – 47-ме, числу вчених – 39-те, продуктивності промисловості – 34-те, рівнем освіти – 6-те, а патентної активності – 17-те [22].

А за рейтингом "The Global Innovation Index", який включає 84 індикатори, Україна займає 71-ше місце рейтингу з 142: між Тунісом і Монголією. Між іншим, у 2012 р. Україна займала 63-тє місце, у 2011 р. – 60-те. У 2012 р. наша країна витратила на R&D 0,89% від ВВП при середньому у світі – 1,77% [19].

У 2014 р. Україна зайняла 99-е місце у рейтингу "The Good Country Index". Втім, по одному з показників наша країна потрапила в лідируючу групу – вона стала 13-ю по розвитку «науки та технологій». Перше місце в цій категорії посіла Велика Британія. США, як не дивно, на 26-му, а Росія, яка в загальному рейтингу займає 95-ту позицію, за технологіями опинилася лише на 41-му місці з 125 країн [23].

Але, віддаючи належне принциповій необхідності забезпечення в Україні високого рівня науки та освіти, водночас варто взяти до уваги, що ціла низка провідних високотехнологічних інновацій сучасності, наприклад, запровадження конвеєрного виробництва автомобілів, створення персонального комп'ютера та розробка операційної програмної системи для нього, були реалізовані такими молодими американським

новаторами, як Стів Возняк, Стів Джобс і Білл Гейтс, які не мали вищої освіти [11], а Генрі Форд не мав навіть середньої [25].

24–28 червня 2013 р. в Державній службі інтелектуальної власності України з робочим візитом перебував європейський експерт Всесвітньої організації інтелектуальної власності (ВОІВ) Р. Марчант. Під час візиту були обговорені питання розробки та імплементації Національної стратегії інтелектуальної власності України. Було намічено необхідні кроки на шляху до успішної реалізації цієї стратегії. Говорячи про переваги нашої країни щодо ефективного розвитку сфери інтелектуальної власності (ІВ), Р. Марчант відзначив наступні фактори успіху України: висока якість освіти і великі масштаби ринку. Як зазначив експерт, сьогодні держава має головну увагу направити на підтримку новаторів, а не на роль регулятора сфери ІВ [3].

Відомо, що майже у кожній країні існує три «нескінченних» ресурси:

1. Те, що вирощується на землі.
2. Те, що вирощується у воді.
3. Те, що «вирощується» у головах людей.

І якщо відносно напрямків збільшення перших двох ресурсів сьогодні в Україні майже все відомо та необхідні заходи у відповідних напрямках вже відбуваються, то задля радикального зростання *третього ресурсу України* – тобто для кардинальної мобілізації *творчого потенціалу країни*, зроблено не просто недостатньо, а все ще не сформовано навіть більш-менш повного переліку засобів дієвого стимулювання цього зростання. Один із можливих інноваційних варіантів вирішення цієї проблеми презентовано у статті «Концепція національної інноваційної стратегії «Трансформування України у країну новаторів» [19]. У цій публікації для успішної реалізації в Україні пріоритетних напрямів інноваційної діяльності шляхом масштабного використання телекомунікаційних, інформаційних та дистанційно-навчальних послуг, серед переліку інноваційних заходів запропоновано наступне: «Для розвитку креативного потенціалу України – розробка та викладання у середній і вищій школі, а також у закладах з перекваліфікації дорослого населення країни відповідно адаптованих дистанційних теоретично-практичних курсів «Теорія та методи вирішення винахідницьких задач». У разі виконання в масштабі усієї країни тільки одного цього соціально-освітнього комплексу заходів, виходячи з припущення, що після проходження цього навчання хоча би 0,1% населення України (тобто більше 40 тис. осіб) стане спроможною успішно працювати над новаторськими проектами, а також з урахуванням того факту, що згідно із світовою статистикою у середньому з тисячі інноваційних старт-апів лише один стає проектом світового рівня, можна зробити висновок, що Україна може розраховувати на появу на її теренах не менше ніж 40 інноваційних проектів світового рівня, якщо вони будуть підтримані фінансово. Той факт, що загальновідома програма "Skype", розроблена в Естонії, була нещодавно продана за 2,5 млрд дол. США, дає підстави розраховувати на те, що загальний прибуток від 40 аналогічних інноваційних проектів світового рівня забезпечать збільшення ВВП України не менше ніж на 100 млрд дол. США [20].

На жаль, в Україні не існує інноваційної інфраструктури, яка б зв'язувала в єдине індустріальний запит, інвестиції та інноваційний потенціал. На початку XXI ст. в країні діяв пільговий режим роботи технопарків, який саме і включав ці елементи. Завдяки ним був реалізований ряд важливих інноваційних проектів. Але ідея технопарків дискредитувала себе у вітчизняному виконанні, хоча в інших країнах світу вона суттєво сприяє переходу на інноваційний шлях розвитку.

У той же час 1 березня 2013 р., під час зустрічі з представниками провідних вітчизняних компаній у галузі інформаційно-телекомунікаційних технологій, було зазначено, що в Україні сфера інформаційних технологій є прикладом успішного створення силами приватного капіталу нової і конкурентоспроможної на міжнародних

ринках галузі економіки. В Україні зареєстровано 3292 ІТ-компанії, з них близько 2000 працюють у сфері розробки програмної продукції [10].

Але для того, щоб ІТ-індустрія України була спроможна отримати можливість виконувати масштабні міжнародні проекти «під ключ», а не працювати на підряді у світових грандів програмного забезпечення, слід враховувати, що підґрунтям будь-якого міжнародного ІТ-проекту, передуючи його втіленню, завжди є оригінальна новаторська ідея. І саме про новаторські ініціативи корпорації "Intel Corporation" щодо електронної освіти, які дозволять докорінно змінити парадигму освітянського процесу в Україні в цілому, йшлося 9 квітня 2013 р. у Києві під час проведення Національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації (НКРЗІ), спільно з міжнародною корпорацією "Intel Corporation" круглого столу «Широкосмуговий доступ до Інтернету в Україні: поточний стан та перспективи». У скороченому викладі однойменного аналітичного дослідження, поміж іншим, зазначено: «Ми визнаємо, що… країни з високим рівнем цифрової грамотності є більш новаторськими и продуктивними і на них припадає більша частка у світових торгівлі, інвестиціях і робочих місцях. Ми усвідомлюємо, що в усіх країнах регуляторним й директивним органам належить певна роль у сприянні створенню першокласної системи професійної підготовки для розвитку творчих людських ресурсів» [24].

Слід зазначити, що згідно з «Проектом регіональної системи дистанційного навчання для країн СНД», що здійснюється під егідою МСЕ, в лютому-березні 2000 р. було проведено серію пробних сеансів дистанційного навчання з містами: Київ, Харків, Єреван, Тбілісі, Баку, Кишинів. Виконавці Проекту – група викладачів та вчених вищих навчальних закладів Казахстану (Алматинський інститут енергетики і зв'язку), Росії (Московський технічний університет зв'язку та інформатики, Санкт-Петербурзький державний університет телекомунікацій ім. проф. М.О. Бонч-Бруєвича, Поволзький державний університет телекомунікацій та інформатики, Сибірський державний університет телекомунікацій і інформатики), Узбекистану (Ташкентський електротехнічний інститут зв'язку), України (Одеська національна академія зв'язку ім. О.С. Попова). В 2008–2009 рр. в межах проекту МСЕ щодо Центрів майстерності (Centers of Exellence) для країн СНД, спільно з російським Сибірським державним університетом телекомунікацій і інформатики (м. Новосибірськ), білоруським Вищим державним коледжем зв'язку (м. Мінськ) та Одеською національною академією зв'язку ім. О.С. Попова, було проведено декілька курсів дистанційного навчання з економічних та технічних питань сфери телекомунікацій. Завдяки цим курсам підвищила свою кваліфікацію група співробітників апарату Національної комісії з питань регулювання зв'язку України [16].

Можливості розширення абонентської бази (а відповідно і зростання доходів телекомунікаційних компаній) в Україні є практично вичерпаними. Відносне падіння, у зв'язку із світовою кризою, доходів населення спонукає споживачів телекомунікаційних послуг заощаджувати насамперед на споживанні послуг, пов'язаних із розвагами. У цих умовах найбільш перспективними є послуги, орієнтовані на прискорення розвитку потенціалу соціальної сфери – дистанційне навчання, телеробота, телемедицина, пункти колективного доступу до мережі Інтернет, електронні бібліотеки тощо. Провідні оператори телекомунікацій активно розширюють географію своїх IP/MPLS-мереж – універсального транспорту для всіляких видів трафіку та послуг, що надає їм можливість надавати послуги різного класу у великому об'ємі. Новим джерелом надходжень для операторів фіксованого зв'язку стає надання населенню послуг доступу до Інтернет. Прокладені раніш для потреб голосової телефонії мідні проводові лінії зв'язку зараз одночасно (без перешкод для надання традиційних телефонних послуг) використовуються для доставки абонентам IP-трафіку. При цьому частина послуг голосової телефонії у прибутках таких операторів зменшується і оператори змінюють свою бізнес-модель,

починаючи додатково надавати послуги доступу до мережі Інтернет. Все більше суб'єктів ринку телекомунікацій, використовуючи новітні технології, що дозволяють передавати мультимедійний трафік (голос, дані та відео), перетворюються на універсальних операторів та починають надавати своїм абонентам цілий комплекс конвергентних послуг – комунікаційних, інформаційних, розважальних, навчальних тощо. Так, наприклад, life:) – GSM-оператор мобільного зв'язку, представлений компанією «Астеліт» в Україні, ще у 2009 р. поставив перед собою мету стати єдиним джерелом комунікації та самостійно надавати своїм абонентам комунікаційні, інформаційні, розважальні, освітні послуги тощо [12].

Той факт, що напрям масової перепідготовки кадрів невід'ємно присутній в антикризових програмах як розвинутих країн світу, так і тих країн, що розвиваються, ставить на порядок денний нагальну потребу організації аналогічної новаторської перепідготовки і в Україні.

З урахуванням обмеженості державних коштів, що можуть бути в умовах кризи виділені на виконання цих робіт, питання економії коштів та їх ефективного використання стає дуже актуальним. Досвід провідних іноземних компаній ("Cisco", "PricewaterhouseCoopers", IBM) свідчить що існує можливість значної економії коштів при використанні для підготовки кадрів систем дистанційного навчання (e-learning). Так, наприклад, після впровадження системи "e-learning" компанії "Cisco" вдалося зменшити витрати на навчання з 1500 дол. США на місяць на людину до 120, "PricewaterhouseCoopers" – з 706 дол. США до 106. А у 2001 р. за рахунок використання системи електронного навчання компанії IBM вдалося заощадити 395 млн дол. США. На даний час кожна компанія застосовує свої особисті технічні рішення і запроваджує свій унікальний підхід до навчання персоналу. Як виявило опитування фахівців найбільших компаній при створенні курсів дистанційного навчання використовуються не тільки розробки західних постачальників контенту, але й теоретичні знання провідних ВНЗ [16].

Підсумовуючи все зазначене можна зробити висновок, що за підтримки центральних органів державної влади України, співпраця провідних операторів телекомунікацій із провідними вітчизняними вищими навчальними закладами, такими, наприклад, як НТУУ «Київський політехнічний інститут», Одеська національна академії зв'язку ім. О.С. Попова, Державний університет телекомунікацій, Національна академія управління, не тільки дозволить дієво сприяти реалізації ефективного вектору прискореного розвитку – мобілізації новаторського арсеналу країни, але й, як наслідок, досягти суттєвого збільшення ВВП України.

Беручи до уваги, що у XXI ст. цифрова грамотність стала найважливішим особистим і професійним активом, оскільки глобальна економіка перетворюється у відкриту і конкурентну цифрову економіку, і країни з високим рівнем цифрової грамотності є новаторськими і продуктивними, і на них припадає більша частка в світових торгівлі, інвестиціях і робочих місцях, використовуючи позитивний досвід провідних країн світу, враховуючи, що у підґрунті будь якого успішного IT-проекту міжнародного рівня, передуючи його втіленню у вигляді технічної чи програмної реалізації, завжди існує оригінальна новаторська ідея, очевидно, що принципово необхідним є створення як невід’ємної складової інноваційного середовища нового для України типу, новаторської системи дистанційного навчання та перепідготовки населення, що:

- забезпечить впровадження в Україні переліку нових інформаційно-освітніх послуг;
- прискорить створення в країні інвестиційно-привабливого клімату для побудови у державі національної інформаційно-комунікаційної інфраструктури нового покоління;
- закладе потужний фундамент для прискореної побудови в Україні новаторської і продуктивної економіки, організації у країні масового виробництва інноваційної продукції та підвищення конкурентоспроможності України у світі.

Література

1. Директива 2002/22/ЄС Європейського Парламенту та Ради від 7.03.2002 Про універсальні послуги та права користувачів стосовно електронних мереж зв'язку і послуг (Директива про універсальні послуги): Міністерство юстиції України, Центр європейського та порівняльного права / Пер. офіц. // nkrzi.gov.ua.
2. Про затвердження Положення про дистанційне навчання: Наказ Міністерства освіти і науки України від 25.04.2013 №466 // zakon.rada.gov.ua.
3. ВОИС: Украина в первую очередь должна поддерживать новаторов // proit.com.ua.
4. Всеукраїнська школа новаторства – школа професійної майстерності й творчості // naps.gov.ua.
5. Всеукраїнська школа новаторства на Рівненщині // www.mon.gov.ua.
6. Гейтс Б. Дорога в будущее // book-online.com.ua.
7. ГРАМ ТРИЗ // www.gramtriz.com.
8. Индия бьет рекорды роста // www.ng.ru.
9. Инновационный ресурс человечества // Репортер.– 2013.– №2. – С. 58–59.
10. Кабмин настроен максимально поддерживать IT-отрасль //economics.unian.net.
11. Леви С. Хакеры: Герои компьютерной революции // iknigi.net.
12. Лубнина Н. Видение нашей компании предполагает объединение множества услуг в одно целое // Сети и телекоммуникации.– 2009.– №10. – С. 50.
13. МСЭ. 8-й Глобальный симпозиум для регуляторных органов (ГСР). Паттайя, Таиланд, 11–13 марта 2008 года. Отчёт председателя. Май 2008.
14. Наука та інновації в умовах форс-мажору // kpi.ua.
15. Новий Закон «Про вищу освіту» ухвалено! // kpi.ua.
16. Овчаренко О.М., Сафонов В.Р. Використання в Україні новітніх інформаційних технологій та Інтернет під час світової фінансової кризи // Вісник Державного університету інформаційно-комунікаційних технологій.– 2009.– Спец. вип. – С. 117–120.
17. Работа над нормированием вопросов дистанционного образования продолжается // www.mon.gov.ua.
18. Стартував Десятий всеукраїнський конкурс «Вчитель-новатор» // www.microsoft.com.
19.Трансформування України у країну новаторів: Концепція національної інноваційної стратегії / Підготували М.М. Єрмошенко, Г.М. Луцький, О.В. Нестеренко, В.Р. Сафонов // Актуальні проблеми економіки.– 2012.– №12. – С. 250–254.
20.Третій ресурс України / Підготували М.М. Єрмошенко, В.Р. Сафонов // Актуальні проблеми економіки. – 2013.– №10. – С. 228–237.
21. У столиці презентовано Національний освітній проект «Розумна дитина» // www.mon.gov.ua.
22.Украина вошла в число наиболее инновационных стран мира // news.eizvestia.com.
23.Украина заняла 13-е место в мире по развитию науки и технологий // proit.com.ua.
24. Широкосмуговий доступ до Інтернету в Україні: поточний стан та перспективи: Аналітичне дослідження (скорочений виклад) // www.ticon.com.ua.
25. Шпотов Б.М. Генри Форд: жизнь и бизнес. – М.: КДУ, 2005. – 384 с.
26. Эксперты рассказали о будущем образования // ria.ru.
27. E-learning: будущее среднего образования // www.elw.ru.
28. В НТУУ «КПІ» відкрито регіональний Міжуніверситетський навчально-виробничий центр аутсорсингу «ITSEA» // kpi.ua.

УДК 621.3

Рыбальский О.В. д.т.н., профессор,
Тимошенко Л.Н. к.э.н., доцент
Национальная академия внутренних дел,
Соломенская площадь, 1,
03034 Киев, Украина
rybalsky_ol@mail.ru

ПОДГОТОВКА СПЕЦИАЛИСТОВ ДЛЯ БОРЬБЫ С КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТЬЮ

В статье рассмотрены вопросы организации обучения кадров для следственных, оперативных и экспертных подразделений правоохранительных органов Украины. Особое внимание обращено на необходимость получения такими работниками как специального технического и юридического образования, так и получения серьезной научной подготовки. Показана необходимость обеспечения высокой мотивации работы в таких подразделениях, чтобы обеспечить высокую квалификацию и заинтересованность в работе подготавливаемых специалистов.
Ключевые слова: *компьютерная преступность, следствие, эксперты, компьютерная экспертиза.*

У статті розглянуті питання організації навчання кадрів для слідчих, оперативних і експертних підрозділів правоохоронних органів України. Особлива увага звернена на необхідність отримання такими працівниками як спеціальної технічної та юридичної освіти, так й отримання серйозної наукової підготовки. Показана необхідність забезпечення високої мотивації роботи в таких підрозділах, щоб забезпечити високу кваліфікацію та зацікавленість в роботі фахівців, що готуються.
Ключові слова: *комп'ютерна злочинність, слідство, експерти, комп'ютерна експертиза.*

In the article the questions of organization of educating of shots are considered for inquisitional, operative and expert subdivisions of law enforcement authorities of Ukraine. The special attention is turned on the necessity of receipt by such workers of both the special technical and legal education and receipt of serious scientific preparation. The necessity of providing of high motivation of work is shown for such subdivisions, to provide high qualification and personal interest in-process the prepared specialists.
Keywords: *computer criminality, investigation, experts, computer examination.*

Вступление

Широкое применение вычислительной техники во всех сферах общественной жизни сопровождается, к сожалению, все более широким ее использованием при совершении разного рода преступлений. Естественно, что совершение практически всех хозяйственных преступлений совершается с использованием информационных технологий хотя бы потому, что ведение современной бухгалтерии без компьютера невозможно. Но диапазон преступлений, совершаемых с использованием информационных технологий, достаточно широк. Он охватывает и взлом банковских компьютерных систем и кражи денежных средств со счетов клиентов, и взлом компьютерных сетей государственных учреждений и кражу сведений, содержащих государственную тайну. В этот диапазон укладывается также и промышленный шпионаж.

Для раскрытия такого рода преступлений требуется специальная подготовка как оперативных и следственных работников, так и экспертов, проводящих компьютерную экспертизу, а сама экспертиза, как было показано в [1], может рассматриваться как один из аспектов информационной безопасности.

Ситуация осложняется тем, что, во-первых, в нашей стране не готовят квалифицированных специалистов ни для расследований компьютерных преступлений, ни для проведения такой экспертизы, которых, кстати, катастрофически не хватает. Во-вторых, при подготовке таких специалистов (как и специалистов для ряда других видов экспертиз, связанных со сложными техническими объектами) возникают сложности образовательного и организационного характера.

Некоторые аспекты подготовки таких специалистов для правоохранительных органов являются предметом рассмотрения этой статье.

Основная часть

В сложившихся традициях в Украине (как и в странах бывшего СССР) следователей широкого профиля готовят либо юридические факультеты университетов, либо специализированные высшие учебные заведения (ВУЗы) МВД и СБУ. Кадры оперативных работников подготавливаются или при стационарном обучении в ВУЗах МВД и СБУ, или путем привлечения на работу специалистов других специальностей с последующим заочным обучением юриспруденции.

Экспертов по традиционным экспертным специальностям (дактилоскопия, почерковедение и т.п.) готовят ВУЗы МВД. Для ряда сложных технических экспертиз подготовка экспертов в научно-исследовательских институтах судебных экспертиз (НИИСЭ) проводится традиционным методом. Это набор молодых специалистов из технических ВУЗов с их последующим обучением основам юриспруденции на курсах по месту работы. Затем сдается экзамен и присваивается квалификация эксперта. Аналогичным образом поступают и в экспертных подразделениях МВД и СБУ.

К сожалению, такой способ набора кадров для проведения розыскных мероприятий и экспертиз зачастую себя не оправдывает. Во-первых, в оперативных и экспертных подразделениях МВД и Минюста наблюдается большая текучка кадров. Молодые специалисты, пройдя дополнительное обучение и получив некоторый практический опыт, стараются найти более высокооплачиваемую работу. Во-вторых, набор новых кадров часто осуществляется отнюдь не на конкурсной основе.

Очевидно, эти моменты были учтены при организации ряда новых подразделений МВД при переходе от милиции к полиции. Но эти изменения коснулись только части следствия, связанного с информационными технологиями. Однако при этом не учтена необходимость обучения новых работников основам юриспруденции.

В 2010 г. была предпринята попытка предложить организацию подготовки специалистов для подразделений борьбы с преступлениями в сфере компьютерных технологий МВД Украины. В то время мы также предложили двухэтапную организацию такой подготовки [2]. Но такая организация требовала приложения значительных усилий и дополнительных средств, то есть именно того, что всегда не нравится некоторым лицам, принимающим решения. Поэтому, несмотря на наши возражения, было принято решение об отборе на отдельную подготовку курсантов Национальной академии внутренних дел (НАВС), имеющих тяготение к информационным технологиям, и подготовки из них нужных специалистов. Как мы и ожидали, из такой подготовки ничего не вышло – мы получили правоведов с углубленными пользовательскими знаниями, но никак не специалистов в отрасли компьютерных технологий. То есть, не было учтено, что нужное количество специалистов такого плана всегда ограничено, они не могут быть продуктом “массового производства”. В результате произошло то, что и должно было произойти при

подготовке таких специалистов в ВУЗе МВД Украины без предоставления им основательной научно-технической подготовки.

Образовательные сложности подготовки экспертов для проведения компьютерных экспертиз заключаются в том, что такой специалист должен в совершенстве знать и понимать научно-технические и технологические тонкости построения исследуемой техники, т.е. компьютеров, программирования и программного обеспечения [3]. Но при этом эксперт должен владеть основами криминалистики, в частности теорией криминалистической идентификации, и другими теоретическими принципами правоведения, что необходимо для проведения экспертиз с учетом всех законодательных норм [4]. При этом, учитывая недостаточную разработанность методической и программной базы такой экспертизы, будущим экспертам необходимо предоставить теоретическую техническую и юридическую научную подготовку. Только так можно обеспечит в будущем для нашей страны возможность развития в разработке новых отечественных методологий, методик, методов и средств проведения такой экспертизы, созданных на основе научного подхода. Обеспечить такое развитие необходимо, принимая во внимание быстрое развитие информационных технологий и, соответственно, постоянного появления новых способов осуществления правонарушений с использованием вычислительной техники [1; 3]. Таким образом, будущие эксперты должны получить достаточно основательную теоретическую и практическую подготовку как в отрасли математики, вычислительной техники, программирования, так и общих и специальных разделах юриспруденции. Очевидно, что следует готовить специалистов, которые были бы как инженерами, так и правоведами. Соответственно готовить таких специалистов нужно в два этапа – техническую подготовку должны предоставлять технические ВУЗы, а правовую – юридические.

Подготовка таких специалистов требует проведения определенных организационных мероприятий, в частности, создание нормативных принципов для взаимодействия и объединения усилий ВУЗов двух разных профилей. Но, как показывает практика, особенности организации такого взаимодействия может стать серьезным препятствием при решении этой проблемы. Дело в том, что на настоящее время такая экспертиза наиболее развита в подразделениях Государственного научно-исследовательского экспертно-криминалистического центра МВД Украины (ГНИЭКЦ). Эта экспертная служба имеет свои региональные ячейки и выполняет “львиную” часть экспертиз из всех, что проводятся в Украине. Поэтому мы будем рассматривать особенности организации первоочередной подготовки специалистов по компьютерной экспертизе для подразделений ГНИЭКЦ, что не исключает возможность параллельной подготовки экспертов для подразделений Министерства юстиции Украины.

Мы полагаем, что для обеспечения комплектования кадрами подразделений компьютерной экспертизы необходимо пойти по пути отбора специалистов из числа выпускников технических ВУЗов с обязательным уровнем квалификации “магистр” и дальнейшим предоставлением им необходимых правовых знаний в НАВС. Эти знания им можно предоставлять в рамках ускоренного второго высшего образования или курсов повышения квалификации.

Но для организации такого специализированного кадрового набора необходимо на государственном уровне решить ряд задач:

1. Создать такие условия работы в этих подразделениях, чтобы лучшие выпускники технических ВУЗов пытались туда попасть. Для этого, в свою очередь, необходимо:

- обеспечить высокий начальный уровень оплаты труда и социального пакета для таких специалистов, чтобы перспективные специалисты не искали работы в частных структурах;

- ввести жесткие критерии отбора для кандидатов в такие подразделения и организовать сам отбор так, чтобы исключить возможность принятия на должности

людей, его не прошедших (и этим исключить возможность коррупционного принятия недостойных кандидатов на высокооплачиваемые должности);

- обеспечить такие условия, чтобы эксперты таких подразделений были заинтересованы работать как можно дольше и не освобождались через несколько лет;
- поощрять техническую и научную деятельность работников таких подразделений.

2. Организовать и провести законодательное обеспечение набора кадров и деятельности таких подразделений.

3. Организовать широкое взаимодействие с Министерством образования и науки и с ведущими техническими ВУЗами, готовящих специалистов по информационным технологиям в регионах, что обеспечит возможность комплектования подразделений местными кадрами. Для этого необходимо определить ВУЗы, способные готовить студентов по этими специальностями с высоким уровнем профессиональной подготовки [2].

Мы полагаем, что решение этих задач позволит быстро провести комплектацию кадрами таких подразделений.

Выводы

1. Стране необходимо создать новую систему подготовки кадров для подразделений по борьбе с компьютерной преступностью.
2. Эта система должна готовить специалистов с технической, юридической и научной подготовкой.
3. Необходимо обеспечить высокую мотивацию работы в таких подразделениях, чтобы обеспечить высокую квалификацию и заинтересованность в работе подготавливаемых специалистов.

Литература

1. Рибальський О.В. До зв’язку між компьютерно-технічною експертизою та інформаційною безпекою / О.В.Рибальський, Л.М.Тимошенко, А.Я. Мушак // Сучасна спеціальна техніка. – К., № 1 (36), 2014. – С. 86 – 90.
2. Рибальський О.В. Комплектування кадрами підрозділів боротьби зі злочинами у сфері високих технологій / О.В. Рибальський, В.О. Хорошко, В.І. Шакун // Протидія злочинам, які вчиняються з використанням комп’ютерних мереж: Матеріали науково-практичної конференції 1 – 2 жовтня 2010 р., м. Севастополь.
3. Федотов Н.Н. Форензика – компьютерная криминалистика / Н.Н. Федотов. – М.: Юридический Мир, 2007. – 432 с.
4. Рыбальский О.В. Основы технологии создания инструментария проведения экспертизы сложных технических объектов/ О.В.Рыбальский, Т.А. Татарникова // Закон и жизнь : международный научно-правовой журнал. – Молдова. – 2013. – № 11 (263). – С. 29–31.

УДК 004.5

Додонов А.Г. д.т.н., профессор,
Ландэ Д.В. д.т.н. с.н.с.
Институт проблем регистрации информации Национальной академии наук Украины,
ул. М.Шпака, 2, 03113 г.Киев, Украина
e-mail: dodonov@ipri.kiev.ua , dwl@vist.net

МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННЫХ РЕЗЕРВАЦИЙ

Рассматриваются понятия «информационная резервация», «внешняя информационная изоляция», «информационная самоизоляция» и сопутствующие им. Исследуются модели, соответствующие типовым информационным сюжетами, информационным операциям и информационным резервациям. Предложена методологическая основа для выявления информационных резерваций, базирующаяся на исследовании динамики тематических информационных сюжетов.

Ключевые слова: *Информационные резервации, Информационные сюжеты, Информационные операции, Информационное пространство, Моделирование*

Розглядаються поняття «інформаційна резервація», «зовнішня інформаційна ізоляція», «інформаційна самоізоляція» і супутні ним. Досліджуються моделі, що відповідають типовим інформаційним сюжетам, інформаційним операціям і інформаційним резервціям. Запропоновано методологічна основа виявлення інформаційних резервацій, що базується на дослідженні динаміки тематичних інформаційних сюжетів.

Ключові слова: *Інформаційні резервації, Інформаційні сюжети, Інформаційні операції, Інформаційний простір, Моделювання*

The concepts "information reservation", "external information isolation", "information self-isolation" and accompanying them are considered. The models corresponding standard information plots, to information operations and information reservations are investigated. A methodological basis for identification of information reservations which is based on research of dynamics of thematic information plots is offered.

Keywords: *Information Reservation, News Items, Information Operations, Information Space, Modeling*

В этой работе обсуждается понятие «информационной резервации», которое может ассоциироваться с индейскими резервациями эпохи «Дикого Запада». Резервация – место, с одной стороны отрезанное от мира (сегодня чаще добровольно), в котором действуют свои порядки, чаще всего сегодня более широкие, чем в окружающем мире. Резервации устанавливают собственные правила владения землей, на их территориях в ряде штатов даже разрешен игорный бизнес. Информационные резервации, в отличие от реальных индейских резерваций сегодня, отнюдь не расширяют прав своих обитателей.

Речь идет об информационной самоизоляции и сопутствующих процессах, – так называемом «информационном гетто». Примеры самоизоляции – Северная Корея (достаточно привести пример с ложным освещением чемпионата мира по футболу 2014,

согласно которому в финале будто бы участвовали Северная Корея и Бразилия). В качестве примера информационной блокады можно привести отключение СМИ неприятеля из своего информационного пространства. Информационной изоляцией можно считать, например, недоступность информации по языковому признаку – так изолирован Китай от остального мира, хотя это явление нельзя однозначно трактовать как информационную резервацию.

Определим информационную резервацию (ИР) как фрагмент информационного пространства, находящийся в:

1) в блокаде (внешней изоляции);
2) внутренней изоляции, исходящей от некоторой администрации (государства);
3) направленной самоизоляции, исходящей непосредственно от участников информационных отношений (акторов) в рамках данного фрагмента;
4) ненаправленной самоизоляции, являющейся следствием отличий рассматриваемого фрагмента от всего остального информационного пространства (язык или, например, другой общественный уклад);
5) самоизоляции, заключающейся в ограничении распространения собственных информационных потоков за границу ИР.

Рассмотрим некоторые механизмы, которые могут приводить к формированию информационных резерваций.

1. Внешнее блокирование доступа к некоторой информации.
2. Внутреннее блокирование доступа к внешней информации со стороны администрации. Административное блокирование доступа к внешней информации (со стороны государства, правящей партии, руководства секты, администрации корпоративной информационной системы), начиная от элементарного глушения радиостанций, таможенных ограничений на ввоз литературы, и вплоть до ограничений доступа к сети Интернет, средствам мобильной связи. Большую роль, как известно, при блокировании «нежелательной» информации отводится и цензуре.
3. Блокирование может исходить от самих акторов в рамках данного фрагмента информационного пространства. Блокирование может исходить от самих граждан – объектов и субъектов информационного воздействия, воспитанных в рамках информационной резервации направленными на них внутренними информационными потоками.
4. Формирование виртуальных образов внутри ИР, фактически препятствующих акторам объективно воспринимать внешние информационные потоки. В информационных резервациях государством могут формироваться виртуальные образы, фактически препятствующие гражданам объективно воспринимать внешние информационные потоки, формироваться фантомы, разрушение которых зачастую очень сложная задача.
5. Из информационной резервации в общее информационное пространство администрацией ИР также могут не пропускаться информационные потоки определенной тематики, объективно отражающие реальные процессы.

Информационная резервация обладает внутренними информационными потоками, правилами, определяемыми некоторой административной политикой. Внешняя среда, в которой функционирует такая информационная резервация, не подчиняется ее административной политике и, таким образом, может вырабатывать негативные или непредвиденные воздействия на связанную с информационной резервацией реальность, а также негативно или непредвиденно реагировать на воздействия информационной резервации на нее. Отсутствие в системе процесса обмена информацией с внешней средой приводит систему к деградации, нарушению условия устойчивости.

Практически во всех странах, включая Украину, Россию, США, существуют правовые основы, фундамент для реализации понятия «информационная резервация». Например, в законодательстве о средствах массовой информации везде существует понятие «территория распространения», которое, по-видимому, уже перестало соответствовать реалиям нового времени и может вести к появлению информационных резерваций, т.е. зон вне заданной территории. К примеру, территория распространения для телевизионных программ или контента сети Интернет весьма условна.

Более десяти лет региональные власти Донецка создавали так называемый «информационный зонтик», что им в результате удалось. В регионе с помощью различных (прежде всего, экономических механизмов) целенаправленно ограничивалось распространение центральной украинской прессы, телепрограмм с целью обеспечения следования выбранным администрацией Донбасса «курсом» и поддержки населения.

Проблемы, связанные с получением достоверной информации неизбежно привели регион к информационной изоляции – теряя связь с реальностью. В результате сформировалась типичная информационная резервация, население в своей массе утратило связь с информационным пространством, реально отражающим действительность, и, как следствие, способность принимать адекватные решения. Логическим следствием этих процессов (наряду с другими, в том числе и внешними факторами) стали устойчивые и массовые сепаратистские настроения, приведшие регион к катастрофе. А ведь еще два столетия тому назад Наполеон пришел к выводу, что пресса не должна принадлежать власти, и внес поправки в Конституцию о свободе средств массовой информации.

Информационные резервации не всегда сразу приводят катастрофам в реальном мире, так например, в условиях идеологического противостояния СССР и западного мира информационная изоляция вначале была мощным стимулом развития высоких технологий, но затем стала основным тормозом развития.

Предлагаемое Европарламенту и временно отложенное Торговое соглашение по борьбе с контрафактной продукцией (ACTA) также могло служить формированию информационных резерваций в странах с небольшим доходом населения, не давая им (вполне оправданно с точки зрения авторского права) доступа к наиболее объективным информационным ресурсам. Вместе с тем, в январе 2012 года двадцать две страны, входящие в Евросоюз, подписали это соглашение.

Внутри информационной резервации циркулируют внутренние информационные потоки, подчиняющиеся правилам, определенным некоторой административной политикой. Внешняя по отношению к ИР среда не подчиняется ее административной политике, и, таким образом, может непредвиденно реагировать на воздействия на нее.

Некоторая живучесть информационной резервации обеспечивается, с одной стороны, административным контролем за ее взаимодействием с внешней средой (реакции на воздействия с внешней среды, на последствия воздействий ИР на внешнюю среду), а, с другой стороны, контролем и коррекцией внутреннего состояния, связанного как с субъектами информационного воздействия (акторами), так и с состоянием

информационного наполнения ИР [1]. При этом практика показывает, что отсутствие в системе процесса обмена информацией с внешней средой приводит ее к деградации, нарушению условия устойчивости.

Каковы размеры информационной резервации, и чем они отличаются от общего информационного пространства? Казалось бы, что ИР может представлять собой лишь небольшой островок по отношению к внешнему информационному пространству, небольшую зону информационной связности, оторванную от всего остального мира. Порой информационные пространства крупных государств могут представлять собой ИР. В рамках этих резерваций их собственное информационное пространство может восприниматься как самое объективное, открытое, общее, а весь остальной мир, наоборот, как информационная резервация.

Похоже, единственное принципиальное отличие информационной резервации от общего информационного пространства заключается в объективности отражения в нем информации о реальном мире, процессах происходящих в реальности. При этом всегда возникает вопрос, кто может выступать арбитром такой объективности? Если в качестве арбитра выбрать диктатора какой-либо небольшой страны, то общим информационным пространством, конечно же, будут объявлены его средства массовой информации в виде единственной придворной газеты и центрального телевизионного канала.

Поэтому, если изучать информационные резервации с научной точки зрения, необходимо определить максимально объективные критерии, и в качестве одного таких, можно рассматривать динамику распространения информационных сюжетов в соответствующем фрагменте информационного пространства. Исследованию динамики информационных потоков посвящены многочисленные научные работы [2-5] показано, что в типовых ситуациях динамике распространения новостей, информационного сюжета присущ характер «всплеска», волны с явным периодом возрастания его влияния и плавным спадом.

В результате анализа многочисленных диаграмм поведения ТИП, были выявлены наиболее типичные, базовые профили их поведения (рис. 1) [6]. Некоторые сюжеты развиваются следующим образом: после быстрого информационного всплеска подготовки идет плавный спад (например, публикации о стихийных бедствиях, рис. 1 а), некоторые, напротив предполагают длительную плавную информационную подготовку, после чего идет резкий спад (например, публикации об планируемых заранее мероприятиях). Существуют также тематические потоки, характеризующиеся симметричной кривой динамики, как узкие, кратковременные, так и растянутые во времени (рис. 1 в).

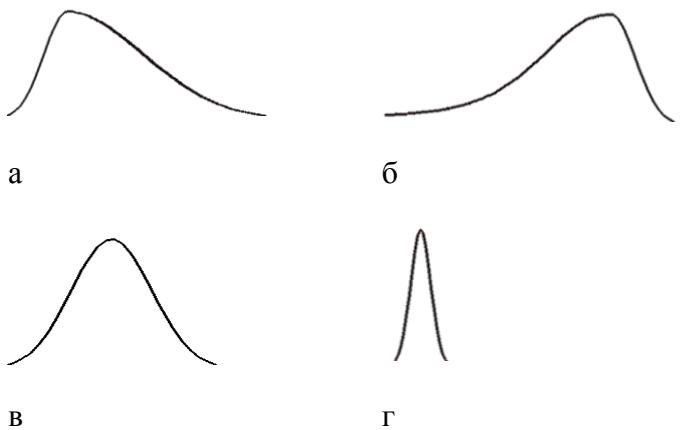


Рис. 1 – Базовые профили динамики тематических сюжетов новостей

В случае информационных потоков, которые ассоциируются с конкретными тематическими информационными потоками, необходимо описывать динамику каждого из таких потоков отдельно, принимая во внимание то, что рост одного из них может автоматически приводить к уменьшению других и наоборот. Поэтому ограничение на объемы информации по всем тематикам распространяется и на совокупность всех информационных сюжетов. В случае изучения общего информационного потока наблюдается явление «перетекания» объемов публикаций из одних, теряющих актуальность информационных сюжетов, в другие.

Следует отметить, что выбор тематики информационных сюжетов, позволяющих детектировать ИР, является содержательно сложной, неоднозначной задачей.

Мультиагентная модель распространения информации

Для создания правдоподобной виртуальной модели распространения информации, прежде всего, необходимо сформировать приближенное к реальности виртуальное информационное пространство, населенное виртуальными информационными агентами. Основной задачей компьютерного моделирования является создание информационного виртуального мира (модели информационного пространства), населенного индивидуальными информационными агентами.

Одной из основных проблем моделирования информационного пространства является проблема описания взаимодействия информационных агентов. Каким образом происходит формирование социумов агентов? Что влияет на отношение агента к той или иной информации? Каковы динамика падения и восстановления информационной репутации, величина информационного следа (остаточная мощность), критическая масса информационного влияния.

Как предположение, можно рассмотреть возможность сравнения информационного воздействия агентов с моделью распространения вирусов, как простейший случай. Информация как вирус может распространяться в общем случае:

- от агента агенту;
- от агента группе (социальные сети, вербальный обмен и др.);
- от информационных центров (производства информации) к отдельному агенту или к группе агентов.

Рассмотрим предложенную авторами мультиагентную модель распространения информации в информационном пространстве. Базовые профили динамики тематических информационных потоков (ТИП) были получены с помощью предложенной авторами мультиагентной модели, в рамках которой отдельные документы, образующие информационный сюжет, ассоциируются с агентами, жизненный цикл агентов – с жизненным циклом документов в информационном пространстве. Предполагается, что в течение времени происходит эволюция популяции агентов, т.е. отдельные агенты могут:

1) самозарождаться (рождаться по причинам, возникающим вне рассматриваемого мультиагентного пространства);
2) порождать новых агентов;
3) «умирать» – исчезать из пространства агентов;
4) получать ссылки от других агентов.

Каждый агент обладает «потенциалом», зависящим от его возраста (времени жизни на текущий момент), авторитетности (ссылок, проставленных на него) и плодовитости (количества порожденных непосредственно им агентов).

Управляющие параметры модели следующие:

1) вероятность «самозарождения» P_1;

2) потенциал агента Pot, зависящий от количества ссылок на него (ns), времени его жизни (t), и количества порожденных им агентов (k): $Pot = \frac{ns + k}{t}$;

3) вероятность «рождения» от существующего: $P_2 \cdot Pot$;

4) вероятность «смерти» агента: P_3 / Pot;

5) вероятность ссылки на агента: $P_4 \cdot Pot$.

Варьирование параметрами управления P_1, P_2, P_3 и P_4 позволили смоделировать профили поведения информационных сюжетов. На рис. 2 приведена пример возможной динамики мультиагентой системы: процессы рождения новых агентов от существующих обозначены сплошными стрелками, процессы проставления ссылок на агентов представлены пунктирными стрелками, живые агенты – черными кругами, «метрвые» агетнты к моменту t = 5 – незаполненными окружностями.

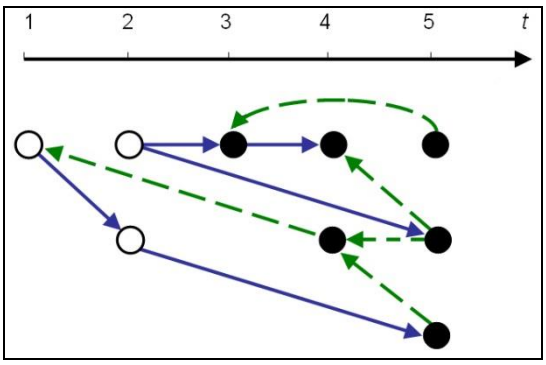


Рис. 2 – Фрагмент мультиагентного пространства

В предложенной модели учитывается общеизвестная практика проведения информационных кампаний в социальных сетях, заключающаяся в регистрации большого числа аккаунтов-роботов (роя), от имени которых проставляются ссылки (лайки) на материалы, публикуемые от имени аккаунтов из того же роя и на целевые информационные страницы – документы.

В результате проведенных исследований была реализована программа эволюции пространства агентов, исследована эволюция мультиагентной системы при различных значениях параметров, найдены аналогии с реальными тематическими информационными потоками.

Модель диффузии информации

Жизненный цикл тематических информационных потоков (информационных сюжетов) может описываться, например, моделью диффузии информации (МДИ), построенной с помощью методов клеточных автоматов [7].

Клеточные автоматы являются полезными дискретными моделями для исследования динамических систем. Дискретность модели, а точнее, возможность представить модель в дискретной форме, может считаться важным преимуществом, поскольку открывает широкие возможности использования компьютерных технологий.

Модель диффузии информации является двумерной, поэтому вся система клеточных автоматов для этого случая будет описываться двумерным массивом. В случае двумерной решетки, элементами которой являются квадраты, ближайшими соседями, входящими в окрестность элемента, можно считать или только элементы, расположенные вверх-вниз и

влево-вправо от него, либо добавленные к ним еще и диагональные элементы (окрестность Мура).

В рамках данной модели, которая относится к распространению новостей в информационном пространстве, применяются окрестность Мура и вероятностные правила распространения новостей по заданной тематике.

В рамках МДИ, которая относится к распространению информационных сюжетов в информационном пространстве, применяются вероятностные правила распространения новостей по заданной тематике. Предполагается, что каждая клетка клеточного автомата может иметь различные статусы информированности, а именно, быть в одном из трех состояний: 1 – «свежая новость» (клетка окрашивается в черный цвет); 2 – новость, устаревшая, но сохраненная в виде сведений (серая клетка); 3 – клетка не имеет информации, переданной новостным сообщением (клетка белая, информация не дошла или уже забыта).

МДИ предполагает следующие правила развития информационного сюжета (рис. 3):

1) изначально все поле состоит из белых клеток за исключением нескольких стоящих рядом черных, которые первыми «приняли» новость;
2) белая клетка может перекрашиваться только в черный цвет или оставаться белой (она может получать новость или оставаться «в неведении»);
3) белая клетка перекрашивается, если выполняется условие: $pm > 1$, где p – псевдослучайная величина $(0 < p < 1)$, m – количество черных клеток в окрестности;
4) если клетка черная, а вокруг нее черные и серые ($s > x$, s – количество черных и серых клеток, x – заданная константа, то она перекрашивается в серый цвет (новость устаревает, но сохраняется как сведения);
5) если клетка серая, а вокруг нее исключительно черные и серые ($s > y$, y – заданная константа), то она перекрашивается в белый цвет (забывание сведений при их общеизвестности).

Типичные зависимости количества клеток (последовательности количества однотипных клеток), пребывающих в различных состояниях, в зависимости от шагов итерации приведены на рис. 4.

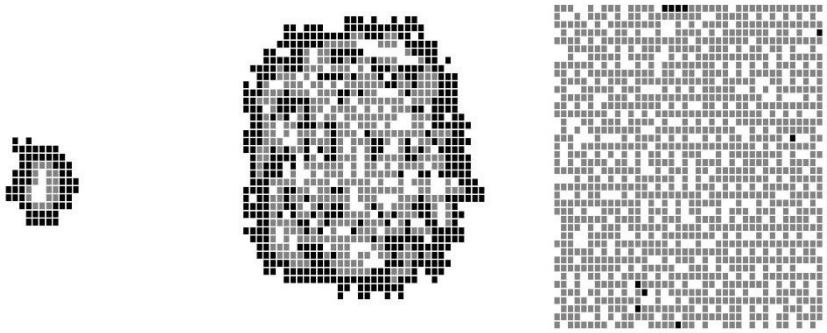


Рис. 3 – Состояния эволюции системы клеточных автоматов

При анализе приведенных графиков следует обратить внимание на такие особенности: 1 – суммарное количество клеток, пребывающих во всех трех состояниях на каждом шагу итерации постоянно и равно размеру поля; 2 – при стабилизации клеточных автоматов соотношение количества серых, белых и черных клеток приблизительно

составляет: 0.75 : 0.25 : 0; существует точка пересечения кривых, определяемых всеми тремя последовательностями на уровне 33 % каждая.

Именно черные клетки образуют актуальный информационный сюжет, динамика которого представлена на рис. 4.

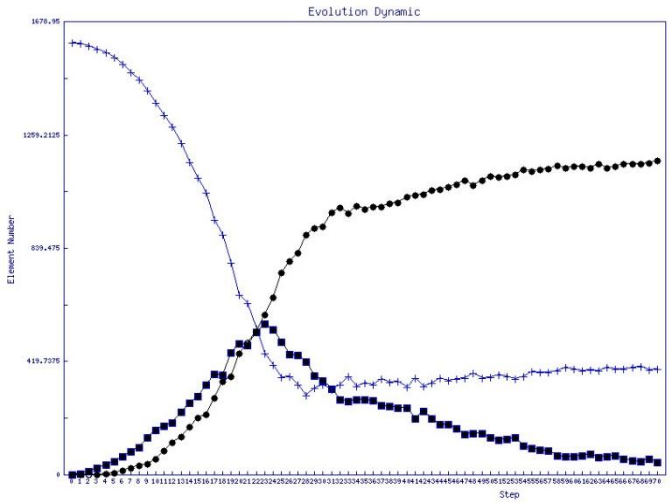


Рис. 4 – Распределение клеток в зависимости от такта системы клеточных автоматов: белые клетки – (+); серые клетки – (•); черные клетки – (■)

Полученные в результате аналитического моделирования зависимости количества серых x_g, белых x_w и черных x_b клеток от шага эволюции системы клеточных автоматов, выражаются формулами:

$$x_g = \frac{1}{1+e^{-\alpha(t-\tau_1)}};$$

$$x_w = 1 - \frac{1}{1+e^{-\beta(t-\tau_2)}};$$

$$x_b = \frac{1}{1+e^{-\beta(t-\tau_2)}} - \frac{1}{1+e^{-\alpha(t-\tau_1)}}.$$

Базовые профили динамики информационных сюжетов, соответствующие значениям $x = y = 8$ в правилах 4 и 5 модели, были получены при значениях параметров $\alpha = 0.15,\ \beta = 0,25$.

Модель динамики информационных операций

Предполагается, что системное нарушение типовой динамики некоторых информационных сюжетов в открытом информационном пространстве может свидетельствовать как об информационных операциях [8], так и о наличии существовании информационной резервации. При исследовании информационных операций также большое внимание уделяется анализу динамики информационных сюжетов [9], пользоваться доступными аналитическими средствами, например, вейвлет-анализом. При этом следует ориентироваться на возможные модели информационных атак, например, если эта модель охватывает фазы: «фоновые публикации» — «затишье» — «артподготовка» — «затишье» — «атака», то уже по первым трем компонентам можно с большой вероятностью предсказать будущие события.

Объединяя участки графика, соответствующие началу информационной операции и трендам, связанным с инновационной деятельности (внедрение инноваций можно условно также считать информационными операциями), был получен полный график, соответствующий отображению информационных операций в информационном пространстве (рис. 5). При этом следует ориентироваться на возможные модели информационных атак, однако уже по первым трем компонентам (фазам) можно с большой вероятностью предсказать будущие события.

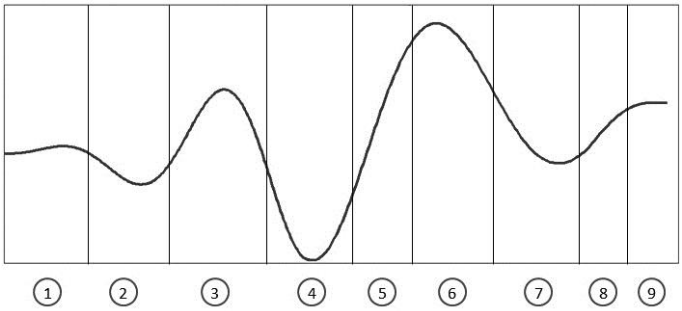


Рис. 5 – Обобщенная диаграмма, соответствующая всем этапам жизненного цикла информационных операций: 1 – фон; 2 – затишье; 3 – «артподготовка»; 4 – затишье; 5 – атака/триггер роста; 6 – пик завышенных ожиданий; 7 – утрата иллюзий; 8 – общественное осознание; 9 – продуктивность/фон

Предложенные модели соответствуют реальным данным, которые экстрагируются системами контент-мониторинга. Такким образом, приведенные зависимости могут быть использованы в качестве шаблонов для выявления информационных операций – как путем анализа ретроспективного фонда сетевых публикаций, так и путем оперативного мониторинга появления некоторых их признаков в реальном времени.

Отметим, что предложенная модель позволяет отличать информационные потоки, поведение которых определяется естественными закономерностями информационного пространства, от потоков, вызванных влиянием внешних факторов. В частности, в случае информационных резерваций, в качестве индикатора может рассматриваться отклонение трендов динамики некоторых информационных сюжетов от характерных форм распределения, появление периодических зон нестабильности значений, или, наоборот, удивительная локальная стабильность этих значений.

Модель информационной резервации в рамках МДИ

Информационную резервацию можно также охарактеризовать как область информационного пространства, находящуюся под непрерывным воздействием информационных операций. В результате этого динамике важнейших информационных сюжетов, протекающих в ИР, свойственны отклонения от характера плавного «всплеска», а именно:

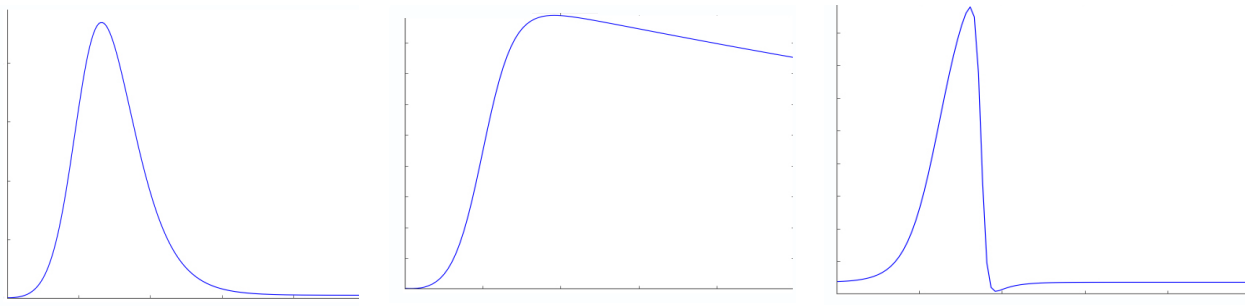
- быстрое прекращение «нежелательного» информационного сюжета (*S*-эффект);
- растягивание периода подъема информационного сюжета (*L*-эффект) с «угодной» администрации ИР тематикой.

Указанные отклонения получаются в том случае, когда изменяются параметры правил, определяющих поведение модели диффузии информации, соответствующие некоторым жизненным наблюдениям за информационными резервациями. Если сопоставить черным клеткам модели (сообщение активно) нахождение сообщения в оперативной памяти, а серым – нахождение сообщения в архивной памяти, то *S*- или *L*-эффектам будет соответствовать соотношение времен нахождения сообщения в

оперативной или архивной памяти, что регулируется параметрами x и y правил 4 и 5. Как уже было отмечено, при значениях параметров $x = y = 8$ модель соответствует естественной динамике развития информационного сообщения вне информационной резервации – ее график принимает вид колоколообразной кривой. При сохранении параметра оперативной памяти ($x = 8$) и уменьшении параметра архивной памяти y, (до $y = 2$), чаще освобождаемые от информации серые ячейки, затем интенсивней принимают ранее забытую информацию, перекрашиваясь в результате в черный цвет, т.е. происходит эффект «проталкивания» нового сообщения (соответствующего «политике» информационной резервации) – L-эффект.

С другой стороны, при сохранении параметра оперативной памяти ($x = 8$) и уменьшении параметра архивной памяти x (до $x = 2$) происходит быстрое «забывание» не соответствующего информационной резервации сообщения и перевод его основной части в архив – S-эффект.

Обобщение аналитической интерпретации МДИ, связанное с изменением коэффициентов в приведенных выше уравнениях (связанных с восприятием информации), которое приводит к искажению типовой динамики, что можно объяснять наличием эффекта информационной резервации (рис. 6).



а *б* *в*

Рис. 6 – Динамика количества клеток в состоянии «свежая новость»:
а – типовая динамика ($\alpha = 0.15,\ \beta = 0,25$); *б* – растягивание периода актуальности информации ($\alpha = 0.01,\ \beta = 0,25$); *в* – немедленное прекращение распространения информации ($\alpha = 0.15,\ \beta = 1,5$).

Выводы

Таким образом, рассмотрено понятие «информационной резервации», приведено его определение, основные свойства и механизмы обеспечения живучести. В качестве методологической основы детектирования ИР предложено исследование динамики информационных потоков.

Рассмотрены некоторые модели информационных потоков, предложена модификация модели диффузии информации, приводящая к типовым профилям динамики информационных потоков в информационных резервациях. Показано, что в информационной резервации, как в изолированной части информационного пространства, плохо связанной с глобальным информационным пространством, быстро блокируются внешние по отношению к ней информационные потоки и продолжительно циркулируют собственные информационные потоки, не соответствующие актуальным событиям во внешней среде.

Литература

1. Додонов А.Г., Флейтман Д.В. Корпоративные информационные системы: обеспечение живучести // Математичні машини і системи, 2005. – № 4. – С. 118-130.

2. G. M. Del Corso, A. Gulli, F. Romani. Ranking a stream of news. InProceedings of 14th International World Wide Web Conference, pp. 97-106, Chiba, Japan, 2005.

3. Kleinberg J. Temporal dynamics of on-line information streams // Data Stream Management: Processing High-Speed Data Streams. – Springer, 2006.

4. Ландэ Д.В., Фурашев В.Н., Брайчевский С.М., Григорьев А.Н. Основы моделирования и оценки электронных информационных потоков: Монография. – К.: Инжиниринг, 2006. – 176 с.

5. Rakesh V., Singh D., Vinzamuri B., Reddy C.K. Personalized Recommendation of Twitter Lists Using Content and Network Information // Association for the Advancement of Artificial Intelligence (Proceedings of the Eighth International AAAI Conference on Weblogs and Social Media, 2014.

6. Ландэ Д.В., Брайчевский С.М. Моделирование поведения тематических сюжетов новостей в веб-пространстве // Тринадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2012 (16-20 октября 2012 г., г. Белгород, Россия): Труды конференции. – Т. 1. – Белгород: Изд-во БГТУ, 2012. – С. 197-204.

7. Ландэ Д.В. Модель диффузии информации // Информационные технологии и безопасность. Менеджмент информационной безопасности. Сборник научных трудов Института проблем регистрации информации. – Вып. 10. – 2007. – С. 51-67.

8. Горбулін В.П., Додонов О.Г., Ланде Д.В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. – К.: Інтертехнологія, 2009. – 164 с.

9. Додонов А.Г., Ландэ Д.В. Мультиагентная модель поведения тематических информационных потоков // Материалы VI Всероссийской мультиконференции по проблемам управления (30 сентября – 5 октября 2013 г.) – Т. 4. – Ростов-на-Дону: Издательство Южного федерального университета, 2013. – С. 102-107.

УДК 004.942.519.87(045)

А. І. Кузьмичов, к.т.н., доцент, **В. В.Бочаров**
Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2б 03113 Київ, Україна
e-mail: akuzmychov@gmail.com

ОПЕРАТИВНА РЕКОНФІГУРАЦІЯ КОМУНІКАЦІЙ У МЕРЕЖІ ІЗ ЗАСТОСУВАННЯМ ОПТИМІЗАЦІЙНИХ ЕТ-МОДЕЛЕЙ

Пропонується комп'ютерна модель, побудована у доступному й потужному середовищі електронних таблиць (ЕТ), для підготовки до прийняття організаційно-управлінських рішень щодо забезпечення прийнятного режиму експлуатації сервісної комунікаційної мережі шляхом її реконфігурації – процедури визначення оновлених функцій складових мережі в залежності від щойно утворених умов – за певним критерієм оптимізації.
Ключові слова: *задачі розміщення серверів та призначення клієнтів (location/allocation problems), реконфігурація мережі, системи та центри надання послуг, електронно-табличне моделювання та оптимізація (spreadsheet modeling and optimization).*

Предлагается компьютерная модель, построенная в доступной и мощной среде электронных таблиц (ЭТ), для подготовки к принятию организационно-управленческих решений по обеспечению приемлемого режима эксплуатации сервисной коммуникационной сети путем ее реконфигурации – процедуры определения обновленных функций составляющих сети в зависимости от вновь образованных условий – по определенному критерию оптимизации.
Ключевые слова: *задачи размещения серверов и назначения клиентов (location/ allocationproblems), реконфигурация сети, системы и центры предоставления услуг, электронно-табличное моделирование и оптимизация (spreadsheetmodelingandoptimization).*

Proposed computer model which built on the powerful and accessible environment of spreadsheets for prepare the organizational and management decisions to ensure acceptable usage service communications by reconfiguration of network - procedures for updated features network components based on the newly created conditions - with certain criterion of optimization.
Keywords*: location/allocation problems, reconfiguration of network, service systems and centers, spreadsheet modeling and optimization.*

Вступ

Мережева організація процесу надання послуг складається з тих, хто надає (сервери, центри обслуговування, постачальники), й тих, кому вони надаються (клієнти, замовники, споживачі) із відповідними комунікаціями між ними та витратами для їх забезпечення.

Це важлива складова сервіс-менеджменту – сучасної науково обґрунтованої технології з організаційного управління інфраструктурними об'єктами, що за своїми будь-якими показниками перевищує аналогічні параметри у структурах виробничого та операційного менеджменту (залучений персонал, обіг коштів, матеріальна база). На практиці сервіс-менеджмент охоплює торгівлю, транспорт, освіту, охорону здоров'я, безпеку, банкінг, це: управління різноманітними організаціями чи службами із розподілу,

зберігання чи постачання будь-чого (склади підприємств, оптові бази, логістичні центри), що функціонують відповідними комунікаціями. Його клієнти, це замовники послуг – регіони,

населені пункти та їх складові, організації, групи зі специфічних категорій людей аж до усіх нас: пасажирів, покупців, власників техніки, школярів, хворих тощо**.**

Ділення усіх вузлів мережі на два класи – сервери й клієнти – тимчасове й досить штучне, бо у складно-організованих сервіс-системах зі змінюваною оргструктурою й функціями у часі чи просторі для розв'язання функціональних задач завжди формуються потоки (матеріалів, послуг та їх носіїв) із різними властивостями, де певний вузол мережі може неодноразово змінювати свій статус й бути одночасно сервером певного призначення із відповідною клієнтурою чи клієнтом певного сервера. Наприклад, магазин роздрібної торгівлі є сервером для мешканців прилеглих будинків й клієнтом міжрегіонального логістичного центру, підприємства чи оптового ринку.

На етапі проектування мережевої структури визначаються кількість й місця розміщення у певних вузлах мережі обслуговуючих об'єктів чи засобів (серверів), що надають послуги прикріпленим до них вузлам-клієнтам згідно їх попиту на споживання цих послуг. Таким чином, чітко визначені функції усіх вузлів (джерела, стоки, транзит) й зв'язки між ними для передачі потоків відповідними комунікаціями, приклади: магістральні та розподільчі нафто-, газо- та водопроводи, шляхове господарство, ЛЕП, телефонний зв'язок тощо.

При експлуатації мережі постачання можливі звичайні чи, рідше, але із більш впливовими наслідками, т. зв. нештатні чи надзвичайні ситуації, події зі стихійним характером, коли вусталеній хоча б тимчасово конфігурації «сервери-клієнти» вимушено перерозподіляються функції серверів та клієнтів із одночасною перемаршрутизацією, бож різко змінилися ресурсні можливості серверів, попит клієнтів на споживання відповідних послуги властивості комунікацій. Причини виникнення таких ситуацій різні, це: непередбачувані погодні умови, аварії, вихід з ладу обладнання й перенавантаження як їх наслідок, порушення договірної дисципліни чи некваліфіковане обслуговування аж до терористичних актів, свідомо направлених на пошкодження чи навіть знищення певних складових мережі.

Й завжди виникає проблема якнайкращого зваженого реагування на ці ситуації шляхом проведення відповідних оперативних розрахунків для формування відповідальних й зважених оптимальних рішень, які мають бути прийняті.

Оптимізаційні задачі, що виникають у таких ситуаціях, належать, зокрема, класу комбінованих задач (*location*/*allocation problems*) про:

- ***розміщення*** (*location*) серверів шляхом визначення місць їх розташування (у вузлах чи поза ними) та
- ***призначення*** (розподіл, прикріплення, *allocation*) клієнтів-споживачів до розміщених серверів, виконавців й постачальників їхніх замовлень,

ці задачі розв'язуються спільно, бо одночасно враховуються параметри усіх складових мережі – вузлів (у певних з них розташовуються сервери) та дуг (що зв'язані із цими вузлами), далі, коротко, «Задачі про розміщення».

Критерій оптимізації може один, а може бути й більше, коли у багатокритеріальній задачі оптимізації одночасно треба прийняти рішення щодо його здійснення за несумісних умов: скажімо, клієнти бажають, аби надання послуги обійшлося якнайдешевше й з якістю високого рівня, й тоді в режимі діалогу відшукується компромісне зважене рішення.

Найчастіше критерієм оптимальності задач про розміщення центрів обслуговування є *мінімум*, де мінімізується сума зважених витрат чи ризиків із надання комунікаційних послуг серверами оточуючим їх вузлам-клієнтам. Інші критерії: *мінімакс*, коли мінімізуються витрати в інтересах найвіддаленіших клієнтів при розміщенні

«корисних» центрів, чи *максимін*, якщо треба розмістити якнайдалі розміщувані об'єкти із шкідливими чи небезпечними властивостями від ближчих до них клієнтів.

Звичайно *кількість розміщуваних серверів* різна, від одного загального для усіх до кількох (k) для обслуговування виокремлених груп клієнтів, відповідно, відшукуються місця розташування k центрів обслуговування, де k – задана чи шукана їх кількість серверів: як

задана, то потенційними місцями розташування є усі або визначені вузли-кандидати, якщо ж шукана, то треба знайти координати цих місць, що зробити значно складніше.

Суттєву роль при розробці оптимізаційної моделі відіграють *характеристики простору рішень* (неперервний, дискретний),це: площина X,Y (евклідів простір) із доступною точкою з координатами(x_i, y_i) будь-де й мережа із дискретними властивостями потенційних точок для розміщення у потенційних i-их вузлах: бути/не бути у них серверу. У першому випадку маємо теоретичну можливість ідеально розмістити сервер, правда, за допомогою моделі «важкого» нелінійного програмування й де не завжди знайдений ідеал стане прийнятним на практиці, дискретний варіант більш розповсюджений й краще пристосований для обчислень з використанням моделі лінійного цілочислового програмування. У свою чергу, мережа (типу повного графа) може бути представлена квадратною матрицею відстаней (МВ), побудованою за координатами вузлів, де потенційно існують зв'язки між усіма парами вузлів. Інший варіант, кращий для практики, коди мережа відтворює існуючі комунікації, наприклад, неорієнтовану чи змішану транспортну чи інформаційну систему, тоді у розрахунках використовується квадратна матриця найкоротших шляхів (МНШ) між усіма парами вузлів (яку ще треба знайти за одним із відомих алгоритмів).

Цільова функція, значення якої зазвичай мінімізується, це загальна вартість розміщення серверів та прикріплення клієнтів, яка складається із комунікаційних витрат «сервер → клієнти» на дугах й витрат на створення й облаштування самих серверів у вузлах, які розрізняються в залежності від попиту й властивостей (природних, демографічних, економічних) клієнтів та від типу й властивостей розміщуваного сервера, наприклад, необхідної системи енергопостачання, мобільного чи поштового зв'язку. Тож звичайно відшукується оптимальна конфігурація мережі за критерієм мінімізації загальних витрат із врахуванням обмежень на шукані невідомі змінні.

В умовах реконфігурації мережі, тобто, вимушеного відхилення від оптимуму, загальні витрати неодмінно зростуть й розв'язанням оптимізаційної задачі із оновленими початковими даними визначається найкращий вихід із ситуації, що склалася.

1.Розміщення центрів у повному графі

Стандартна постановка задачі

Задана мережа $G = (N, A)$ із $|N| = n$ зважених вузлів та $|A| = m = n^2$ зважених дуг, початкові дані:

- $V = \{v_{ij}\}$, $i, j = 1, \ldots, n$ – вагові коефіцієнти дуг, це повна матриця відстанейміж вузлами розміром $(n \times n)$,
- k – кількість серверів $(1 \le k \le n)$ та
- $P = \{p_i\}$ –вагові коефіцієнти(попит) n вузлів.

Треба розмістити у певних k вузлах із n вузлів-кандидатів сервери для задоволення попиту m клієнтів, визначивши:

- вектор розміщення $Y = \{y_i\}, i \in N$, де $y_i = 1$, якщо у i-му вузлі розміщено сервер, й 0 у іншому випадку, та
- матрицю призначення $X = \{x_{ij}\}$, де $x_{ij} = 1$, якщо i-ий сервер обслуговує j-го клієнта, й 0 у іншому випадку,

щоб мінімізувати суму зважених відстаней між серверами й клієнтами.
Це задача лінійного цілочисельного (булева) програмування.

Задача оптимізації

I. Знайти $Y = \{y_i\}$ *та* $X = \{x_{ij}\}$, щоб

II. ЦФ $F(X,Y) = \sum_{i=1}^{n}\sum_{j=1}^{n} p_i v_{ij} x_{ij} \to \min$

III. За обмежень:

$$\sum_{i=1}^{n} x_{ij} = 1 \quad i = \overline{1,n}$$

$$\sum_{j=1}^{n} x_{ij} \le n y_i \quad i, j = \overline{1,n}; c \in N$$

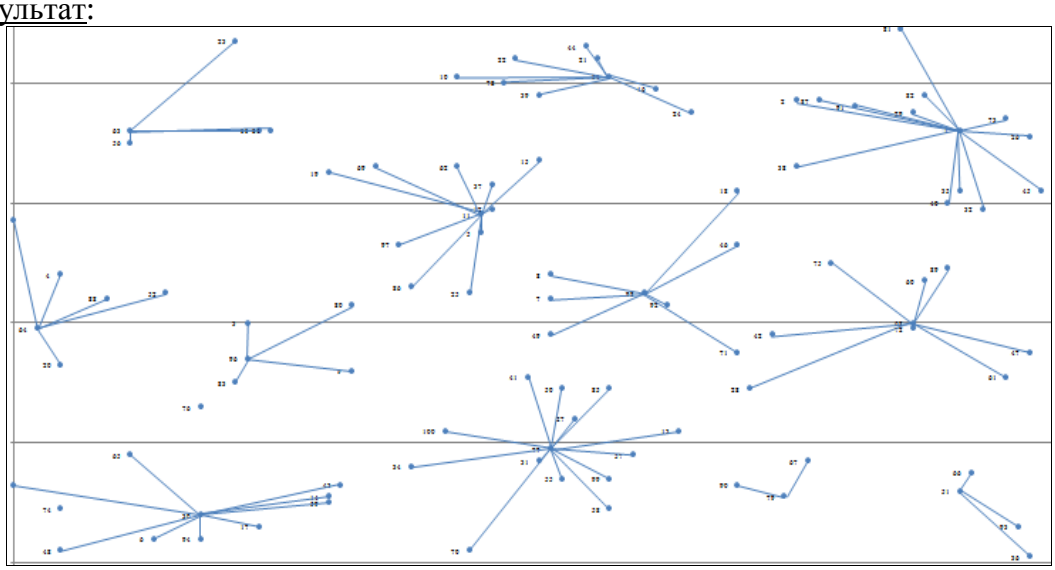
$$\sum_{i} y_i = k$$

та граничних умов: x_{ij}, $y_i \in \{1,0\}$.

Приклад.

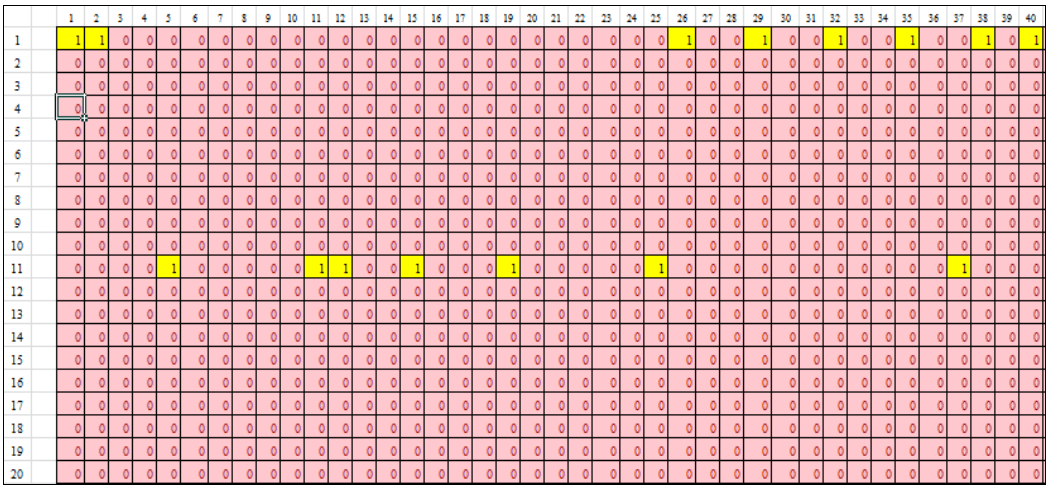
Задана мережа зі100 вузлів, де кожен вузол має попит, визначенаматриця відстаней розміром(100×100) між ними, k = 12.

Результат:



Аналіз результату

I. Визначено вектор розміщення:Y = (1, 11, 30, 51, 54, 63, 64, 68, 77, 79, 96, 98) та матрицю призначення X (на рис. фрагмент 20×40)



призначення: «сервер→кількість клієнтів», список клієнтів, сума витрат:

1→ 14 (1-2-26-29-32-35-38-40-45-73-81-82-87-91), 5398 од.

11→ 11 (5-11-12-15-19-25-37-62-69-86-97), 3599 од.

30→11 (6-14-17-30-43-48-59-65-74-94-95), 4972 од.

51→4 (36-51-66-93), 1129 од.

54→9 (10-16-21-22-24-39-44-54-78), 2951 од.

63→5 (23-33-56-63-84), 2140 од.

64→6 (4-20-52-53-64-88), 1698 од.

68→9 (28-42-47-60-61-68-72-75-89), 2866 од.

77→14 (13-27-31-34-41-50-55-57-58-70-77-85-99-100), 5631 од.

79→3 (67-79-90), 850 од.

96→6 (3-9-76-80-83-96), 2449 од.

98→8 (7-8-18-46-49-71-92-98), 3618 од.

ІІ. Загальні мінімальні витрати (ЦФ) S = 37301 од.

Модифікація моделі

Мета: визначити змінену конфігурацію мережі згідно умов, що склалися.

Умова 1: за ситуацією, що виникла, сервер у вузлі 1, який обслуговував 14 клієнтів, припиняє своє існування, тож цей вузол є звичайним клієнтом іншого сервера, результат:

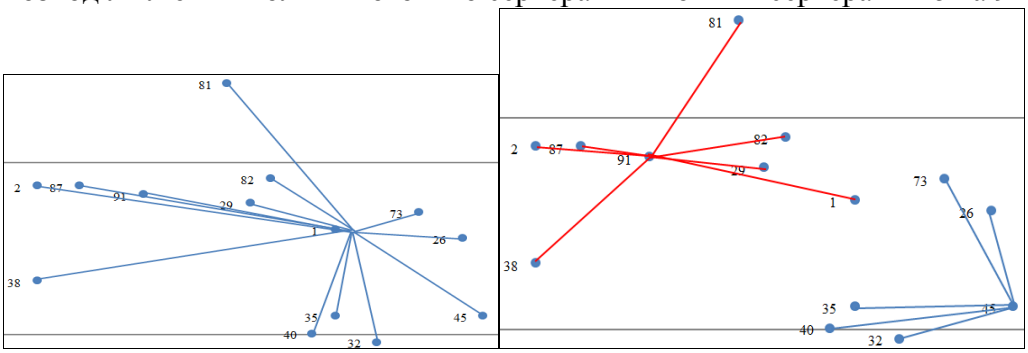
Розміщення:Y = (11, 30, **45**, 51, 54, *63*, 68, 77, 79, **91**, *96*, *98*), S = 37662 од.

Оновлений розподіл клієнтів (на заміну сервера, що вибув):

нові сервери:91 → (**1**-2-29-38-81-82-87-91), 45 → (26-32-35-40-45-73),

зміни розподілу (клієнтів: стало/було): 63 - 6/5, 96 - 11/6, 98 - 7/8, вибули: 1, 64.

Розподіл клієнтів колишнього 1-го сервера між новими серверами 45 та 91:



Умова 2: сервер у вузлі 64 за попереднім розміщенням не чіпати, результат:

Розміщення:Y = (11, 30, 45, 51, 54, **57**, 63, **64**, 68, 91, 96, 98), S = 37687од.

Для цієї «ідеальної» моделі характерна властивість – чим більше серверів, тим меншими будуть комунікаційні витрати, при k =1 вони найбільші, один центр для усіх, при $k = n$ – дорівнюють нулю, де кожен вузол є одночасно клієнтом й власним сервером.

Тож методом параметричного програмування для 1 ≤k≤nможна побудувати залежність $F(X, Y) = f(k)$, де k – параметр.

2.Розміщення зважених серверів у повному графі

Ідеалізована задача розміщення/розподілу (№ 1) «приземлюється» додаванням реальних умов, бо кожен вузол-кандидат має власні властивості/можливості у вигляді вагових коефіцієнтів, які мають враховуватися в обмеженнях на шукані змінні чи у цільовій функції для обчислення витрат при шуканому розміщенні серверів.

Так, коефіцієнт r_i–це необхідний запас споживаного клієнтами ресурсу, який повинен мати сервер, якщо його розміщувати у i-му вузлі, наприклад, питної води, електрики, обігових коштів чи необхідного кваліфікованого персоналу (лікарні, школи, підприємства). Відповідно, у модель задачі оптимізації додається обмеження $\sum_{j=1}^{n} p_i x_{ij} \le r_i y_i$ для прикріплених j-их клієнтів, які будуть отримувати послуги від щойно утвореного сервера у i-му вузлі.

Або, принципово важливий ваговий коефіцієнт, що визначає окремий тип задачі, задане значення z_i, це фіксовані витрати на будівництво й облаштування сервера у i-му вузлі. Для їх врахування змінюється ЦФ задачі оптимізації: $S = \sum_{i=1}^{n}\sum_{j=1}^{n} p_i v_{ij} x_{ij} + \sum_{i=1}^{n} z_i y_i \to \min$, тож в результаті пошуку необхідного бюджету буде неявно визначена оптимальна кількість центрів $k_o \le k$.

Для майбутнього сервера слід додати у якості вагового коефіцієнта його зону покриття, звичайно зображується колом із заданим діаметром, що застосовується у задачі про максимальне покриття клієнтів оптимально розміщеними серверами.

Результат.

Із додаванням деяких вказаних початкових даних виявилося, що для обслуговування достатньо 4-ох серверів, їхнє розміщення:Y = (29, 34, 37, 90) й розподіл:29→19 вузлів, 34→29 вузлів, 37→33 вузла, 90→19 вузлів.

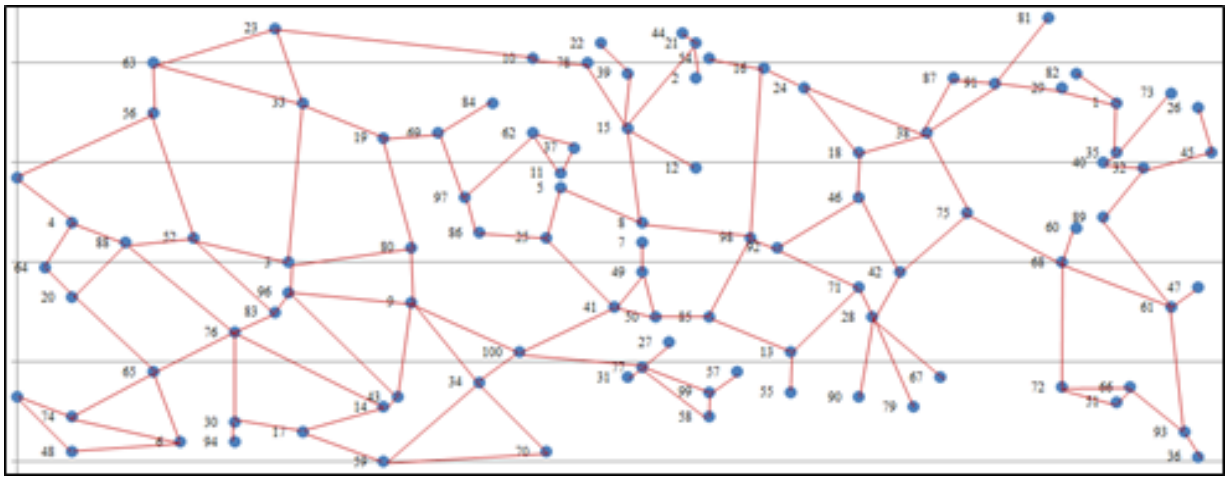
S = 95246 (комунікації) + 41244 (сервери) = 136490 од.

Фрагмент табличної моделі:

DJ	DK	DL	DM	DN	DO	DP	DQ	DR	DT	DU	D	DW	D	DY	DZ	EA
71	30	29	0	23	35	36	20									
70	51	51	23	0	22	42	31									
50	55	62	35	22	0	31	28									
35	36	51	36	42	31	0	16									
51	27	38	20	31	28	16	0									
93	94	95	96	97	98	99	100			№		Ком. витр.		Витрати дод.	Витрати	Разом
0	0	0	0	0	0	0	0	19	1	29		9683,0		8576,4	8576,4	18259,4
0	1	1	1	0	0	0	1	29	1	34		29634,0		10710,0	10710,0	40344,0
0	0	0	0	1	1	0	0	33	1	37		33851,0		10659,6	10659,6	44510,6
1	0	0	0	0	0	1	0	19	1	90		22078,0		11298,0	11298,0	33376,0
								100	4			95246,0		41244,0		136490,0
1	1	1	1	1	1	1	1		≤ 12							ЦФ
									задано центрів							

3. Розміщення центрів у мережі (аналог класичної постановки)

Задана ненаправлена мережа з n вузлів та mненаправлених дуг, що відтворює діючу комунікаційну систему:

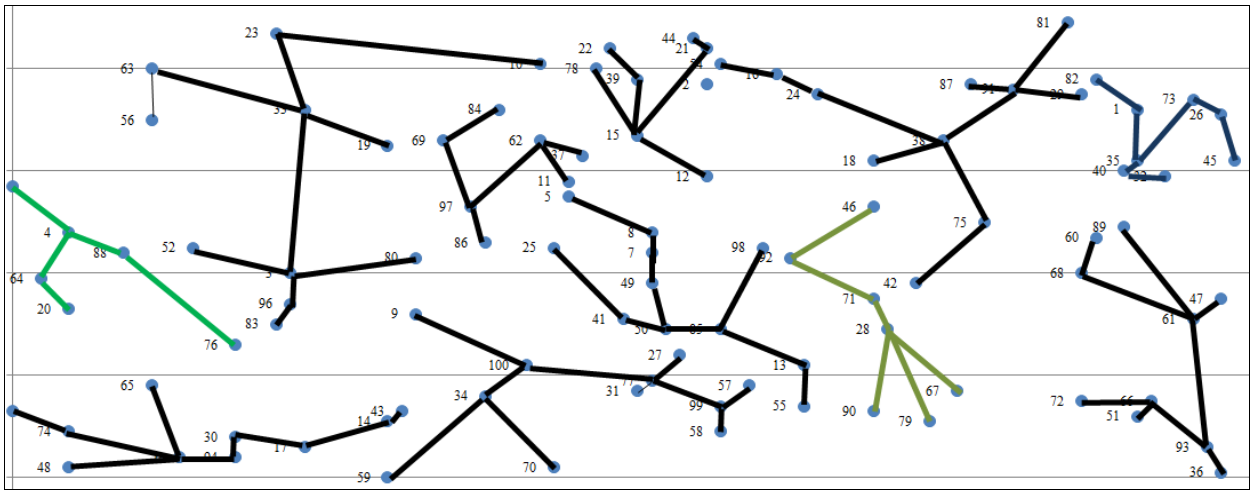


За спеціальною процедурою й алгоритмом сформована матриця найкоротших відстаней між усіма парами вузлів-кандидатів вже для направленої мережі, де треба визначити місця розташування:

- заданої кількості (k) серверів із врахуванням ваги клієнтів,
- мінімальної кількості серверів із врахуванням ваги серверів та клієнтів

із відповідним розподілом клієнтів між ними за мінісумним критерієм.

Приклад. n = 100, k = 12:

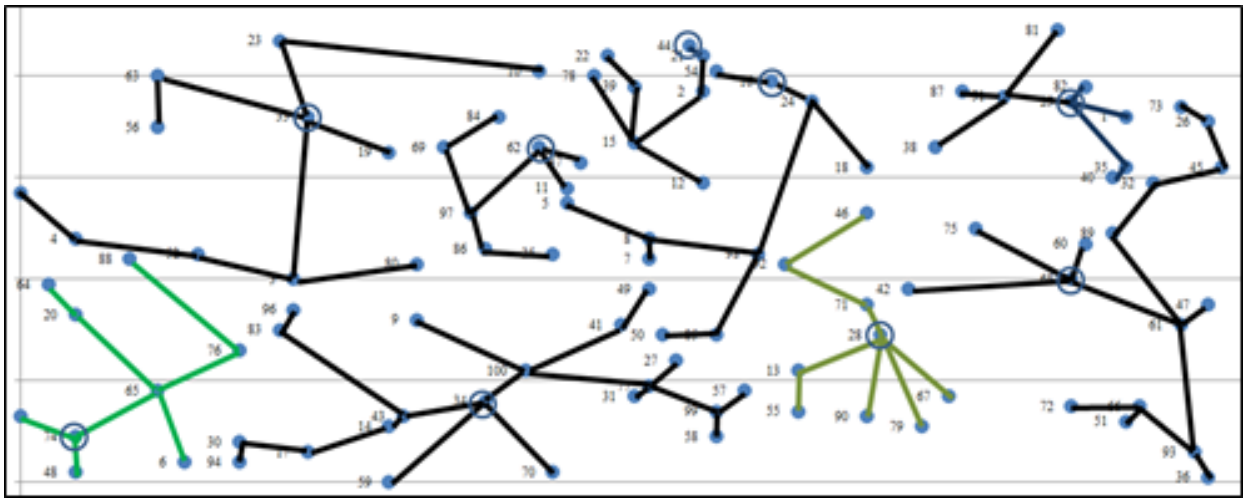


Для кожного сервера визначено дерево найкоротших шляхів до оточуючих їх серверів.

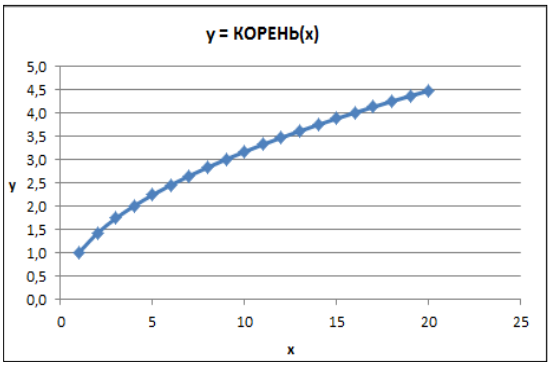
Модифікацією моделі можна змінити конфігурацію мережі згідно вимог, що склалися.

4. Розміщення зважених серверів у мережі

Достатня кількість – 9.



5.Розміщення центрів на площині (*X*, *Y*)



На відміну від стандартної задачі, де усі *n*вузлів є місцями-кандидатами на розміщення серверів, серед яких й треба вибирати, маючи матрицю відстаней, у цій постановці треба відшукати такі місця будь-де, зокрема, поза заданих вузлів, так би мовити, «у чистому полі».Ця умова суттєво ускладнює задачу, бо відповідна модель цієї задачі оптимізації належить до класу нелінійного (негладкого) програмування, де отримання глобального оптимуму не гарантується. Нелінійність виникає з-за використання степеневої функції при обчисленні відстані між двома точками $a(x_a, y_a)$, $b(x_b, y_b)$ в евклідовому просторі, зокрема, в Excel для цього використана нелінійна функція $d(a,b) = КОРЕНЬ((x_a - x_b)^2 + (y_a - y_b)^2)$ із (1/0)-коефіцієнтами.

Приклад.

Матриця відстаней від шуканих серверів до вузлів *n* вузлів-клієнтів графа формується за заданими координатами (*x*, *y*) вузлів, *n* = 45, треба визначити координати місць розташування *k*серверів, *k*= 4 за умови, що кожен клієнт прикріплений до одного зі знайдених центрів.

Задача нелінійної оптимізації

I. Знайти розміщення серверів у вигляді набору координат$\{x_i, y_i\}$ й матрицю призначення

$A = \{a_{ij}\}$, $i = 1, \ldots, 4$; $j = 1, \ldots, 45$, за якими

II. ЦФ $S = \sum_{i=1}^{4}\sum_{j=1}^{45} a_{ij} r_{ij} \to \min, \quad r_{ij} = \sqrt{\left((x_i - x_j)^2 + (y_i - y_j)^2\right)}$

III. за обмежень:

$$\sum_{i=1}^{4} a_{ij} = 1, \; j = \overline{1,45}$$

та граничних умов: $a_{ij} \in \{1/0\}$.

Результат

20,8	45,0
12,0	14,0
66,3	76,8
50,8	27,1

I. Координати розміщення центрів:

Розподіл:

z1 (3,6,7,8,9,22,25,34,38,39) = 10;

z2(1,2,4,5,10,28) = 6;

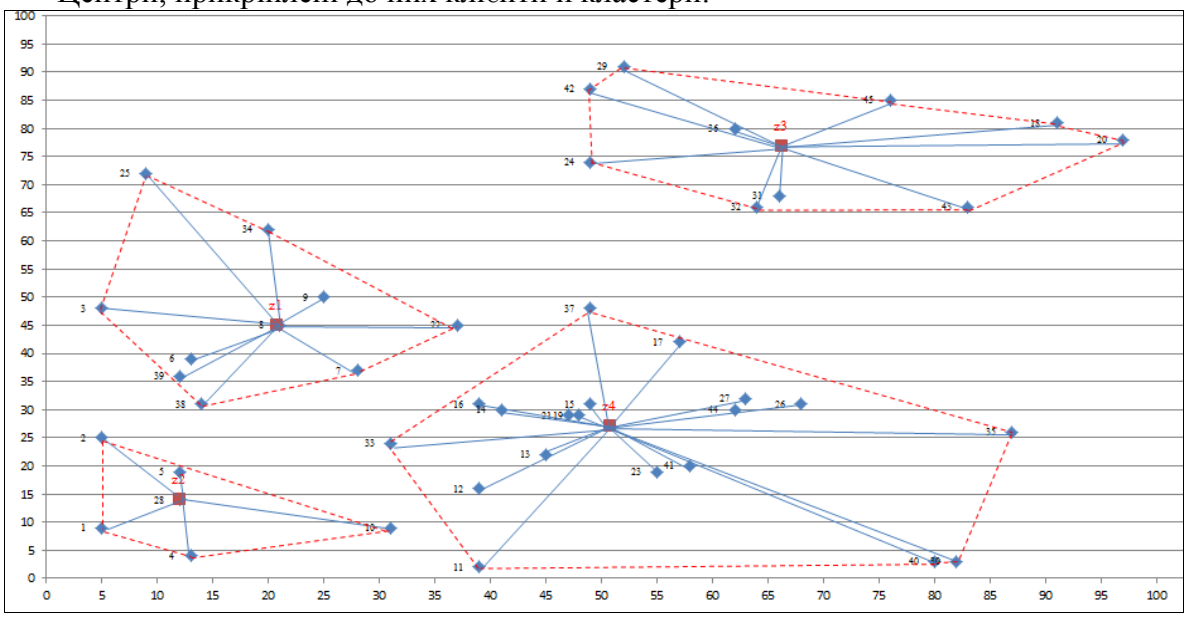
z3(18,20,24,29,31,32,36,42,43,45) = 10;

z4 (11-17,19,21,23,26,27,30,33,35,37,40,41,44) = 19.

II. S = 680, 4 од.

Отриманий результат дозволяє розв'язати непряму задачу із розбиття області розміщення/розподілу на кластери (Districting Problems).

Центри, прикріплені до них клієнти й кластери:



6. «Найкраще» розміщення корисного центру на площині

За критерієм *мінімакс* визначається розташування загального центру, за яким мінімізуються витрати для найвіддаленіших клієнтів, знайдені координати центру визначають т. зв. діаметр мережі – у відповідному колі сконцентровані усі її вузли.

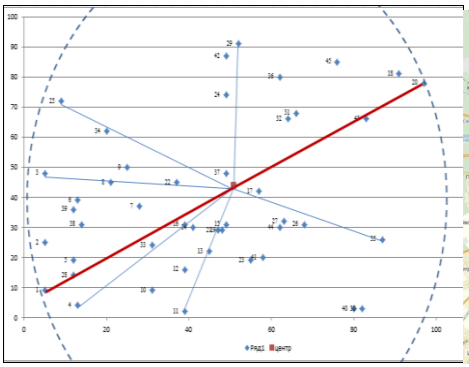
Задача нелінійної оптимізації

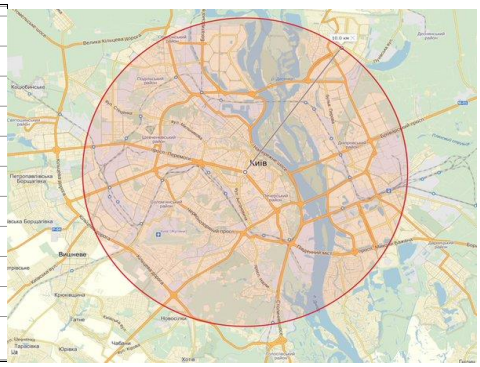
I. Знайти координати $\{x_ц, y_ц\}$ центру, за якими

II. ЦФ $S = \max_i \left(\sqrt{\left((x_i - x_ц)^2 + (y_i - y_ц)^2\right)} \right) \to \min$

за граничних умов: $x_ц, y_ц \geq 0$.

Результат: $(x_ц, y_ц)$ = (50,9; 43,7), ЦФ = 57,5, аналогічний діаметр визначено для Києва:





7. «Найгірше» розміщення небезпечного центру на площині

За критерієм *максмін* визначається найгірше серед можливих розташування загального центру, за яким максимізуються витрати для клієнтів, розташованих найближче до майбутнього центру.

Задача нелінійної оптимізації

I. Знайти координати $\{x_ц, y_ц\}$ центру, за якими

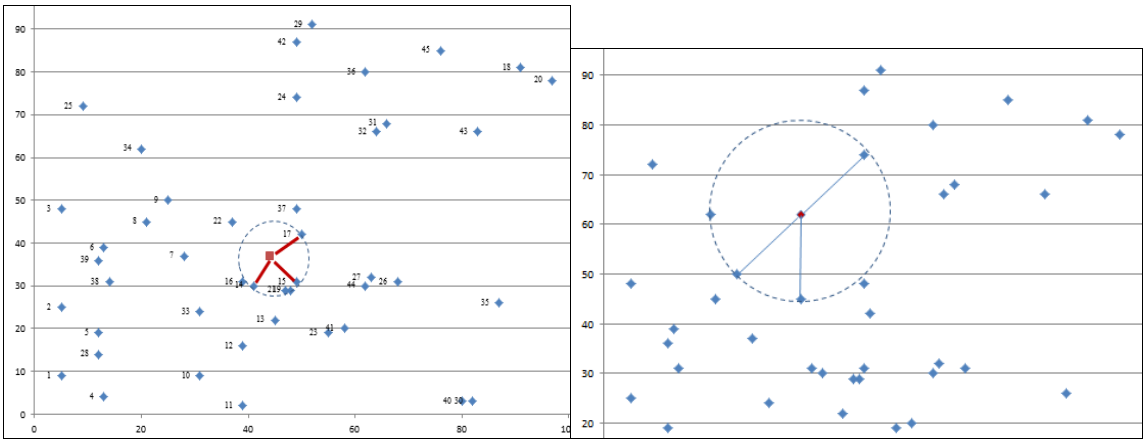
II. ЦФ $S = \min_i \left(\sqrt{\left((x_i - x_ц)^2 + (y_i - y_ц)^2\right)} \right) \to \max$

за граничних умов: $x_ц, y_ц \geq 0$.

Результат:

найгірше місце: $(x_ц, y_ц) = (44{,}2;\ 37{,}0)$, ЦФ = 7,68 од.

найкраще із таких місць: $(x_ц, y_ц) = (37;\ 62)$, ЦФ = 16,97 од.



Висновки

Запропонована ЕТ-модель розрахована на застосування будь-якою особою, що готує пропозиції щодо рішень, які мають прийматися, на власному АРМ. Оптимізаційні задачі, що розв’язуються у цій моделі, дозволяють врахувати певні специфічні властивості ситуації, що склалася, шляхом уведення відповідних початкових даних й обмежень. Єдина

пересторога – реалізація моделі залежить від програмних засобів оптимізації, якими обладнано АРМ, у першу чергу, це стосується дозвільних обмежень оптимізатора на розмір задачі.

Література

1. Кристофидес Н. Теория графов: Алгоритмический подход. Пер. с англ./ Н.Кристофидес. – М.: Мир, 1978. – 432 с.

2. Daskin M. Network and Discrete Location: Models, Algorithms, and Application/M.Daskin. – Wiley, 1995. – 517 p.

3. Daskin M. Service Science/M.Daskin. – Wiley, 2011. – 576 p. (Ch. 4. Location and Districting Problems is Services)

4. Aiselt H. Foundations of Location Analysis/H.Aiselt, V.Marianov. – Springer, 2011. – 524 p.

5. Кузьмичов А. І. Оптимізаційні методи і моделі: Практикум в Excel/А. І. Кузьмичов. – АМУ, 2013.- 438 с.

УДК 004.056.2

О.Я. Матов[1], д.т.н., професор,
В.С. Василенко[2] к.т.н., доцент
[1]Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна
[2]Національний авіаційний університет
вул. Космонавта Комарова, 1, 03058 Київ, Україна

МЕТОДИКА ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ

Для оцінки захищеності інформації автоматизованих систем запропоновано моделі відповідних систем захисту інформації та застосування ймовірностей подолання порушником засобів захисту тих чи інших властивостей захищеності – величин залишкового ризику, наведені вирази для їх розрахунків.

Ключові слова: *Загроза, порушник, ресурси, модель.*

Для оценки защищенности информации информационных систем предложены модели соответствующих систем защиты информации и использование вероятностей преодоления нарушителем средств защиты тех или иных свойств защищенности – величин остаточного риска, приведены выражения для их расчетов.

Ключевые слова: *Угроза, нарушитель, ресурсы, модель.*

To assess the information security of information systems offered model corresponds to the information security systems and the use of the probability of overcoming the infringer protection of certain security features - the quantities of residual risk, given the expressions for their calculation.

Keywords: *The threat, the offender, the resources model.*

Вступ

Головна тенденція розвитку сучасного суспільства тісно пов'язана із зростанням інформаційної складової (інформаційні ресурси, інформаційні технології тощо) і, як наслідок, зростанням вимог щодо інформаційної безпеки. Питання інформаційної безпеки на сучасному етапі розглядаються як пріоритетні у державних структурах, у наукових установах і в комерційних фірмах. Інформаційні системи (ІС) спеціального призначення (банківські системи, силові відомства і т. п.), будучи пріоритетними в структурі держави, не можуть залишатися в питаннях забезпечення інформаційної безпеки тільки на рівні традиційних засобів: криптографічний захист, вдосконалення систем розділення доступу, реалізація спеціальних вимог для абонентського трафіку, проведення організаційних заходів щодо посилення режиму.

Немає сенсу перераховувати всі переваги, які отримує організація, підключившись до глобальної мережі Інтернет. Однак при цьому необхідно враховувати і негативні сторони такої акції. У загальнодоступної мережі - це можливі атаки на підключені до неї локальні мережі і комп'ютери.

Загальновизнано, що щорічні збитки через недостатньо захищених корпоративних інформаційних систем обчислюються десятками мільйонів доларів. Бачачи свої переваги від використання мережних технологій, спочатку користувачі часто не надають значення вибору засобів захисту інформації, реально ставлячи під загрозу своє фінансове становище, репутацію і конкурентоспроможність.

Інформаційна безпека, як і захист інформації, завдання комплексне, спрямоване на забезпечення безпеки шляхом впровадження системи безпеки. Проблема захисту інформації є багатоплановою і комплексною і охоплює ряд важливих завдань. Проблеми інформаційної безпеки постійно поглиблюються процесами проникнення в усі сфери суспільства технічних засобів обробки і передачі даних і, насамперед, обчислювальних систем.

Захист інформації - це лише одна складова завдання забезпечення інформаційної безпеки. Інша її частина - це забезпечення безперебійної роботи обладнання. Вихід з ладу того чи іншого вузла в результаті хакерської атаки приводить як до витрат на його відновлення, коли потрібно оновити або замінити програмне забезпечення, так і до втрати частини клієнтури. Тому при включенні комп'ютера в мережу, при інтеграції корпоративної інформаційної системи в мережу необхідно в першу чергу продумати питання забезпечення захисту цієї системи.

На сьогоднішній день відомими є вимоги щодо захисту ресурсів інформаційних систем. Наприклад, у відповідності з Законом України "Про захист інформації в автоматизованих системах" (від 5.07.1994 року) необхідним є застосування в ІС спеціальних засобів захисту, які слід спрямовувати на досягнення певного поєднання чотирьох властивостей інформаційних систем [1, 2, 3, 4]:

1. Цілісності (інформація, на основі якої приймаються рішення, повинна бути достовірною та повною, повинна бути захищеною від ненавмисних на зловмисних спотворень. Загрози, що відносяться до можливостей несанкціонованої модифікації інформації, є загрозами цілісності);
2. Конфіденційності (конфіденційна чи таємна інформація повинна бути доступною лише тому, кому вона є призначеною. Загрози, що відносяться до можливостей несанкціонованого ознайомлення з інформацією є загрозами конфіденційності);
3. Доступності інформації (інформація та відповідні ресурси повинні бути доступними для користувачів та, в разі необхідності, готовими до обслуговування. Загрози, що відносяться до порушення можливостей використання елементів ІС або оброблюваної інформації є загрозами доступності).
4. Спостереженості (можливості фіксувати діяльність користувачів і процесів. Загрози, що відносяться до приховування чи імітації такої діяльності є загрозами спостереженості).

При цьому оцінка, а ще краще, прогнозування захищеності ресурсів інформаційних систем є надзвичайно актуальними при організації, побудові чи оцінці відповідних систем захисту.

Для визначення вимог, оцінки чи прогнозування захищеності інформації використовуються певні показники оцінки захищеності. Відомо також, що досягнуті результати із забезпечення ефективності захисту можна оцінювати або величиною можливих збитків по кожному з класів порушень, або з допомогою залишкового ризику [1] чи інших показників ефективності захищених систем, застосування яких рекомендується в [1]. Їх основний недолік полягає в тому, що вони є якісними а не кількісними, що на етапах проектування чи вибору засобів системи технічного захисту інформації потрібної якості звужує можливості оцінки рівня та ефективності захищеності ресурсів, насамперед, захищеності інформації, наприклад з погляду оптимального співвідношення витрат на засоби захисту та досягнутих при цьому результатів (можливості з оптимізації параметрів систем захисту).

На відміну від цього в даній статті пропонується методика використання кількісних показників захищеності інформації в ІС – величин залишкових ризиків .

Як величини залишкового ризику в цій методиці використовуються ймовірності порушення: конфіденційності – $q_{пк}$, цілісності – $q_{пц}$, доступності – $q_{пд}$ та подолання, злому комплексної системи захисту – q.

В роботі показано, що для визначення залишкового ризику за допомогою відповідних методик необхідно:

визначити (побудувати) моделі порушників та загроз відповідним ресурсам ІС, визначити найбільш суттєві із цих загроз;

детально проаналізувати взаємодію загроз (засобів реалізації атак), спрямованих на подолання механізмів забезпечення захищеності інформації ІС, із засобами протидії цим загрозам.

У цій методиці враховано те, що службою захисту інформації відповідного підприємства моделі порушників та загроз побудовані, найбільш суттєві загрози відповідним ресурсам ІС визначені [1]. До найбільш суттєвих загроз віднесено: різноманітні спроби несанкціонованого, у тому числі фізичного, доступу (з подоланням засобів організаційного обмеження доступу, засобів охоронної сигналізації, засобів адміністрування доступу операційних систем, систем керування базами даних, використання витоків інформації за рахунок побічних електромагнітних випромінювань та спеціальних впливів на інформаційні ресурси ІС тощо), загрози з боку впроваджених тим чи іншим чином вірусів.

Виходячи з цього, методика оцінки захищеності інформаційних ресурсів ІС складається із наступних етапів:

1. Побудова графічних моделей взаємодії загроз функціональним властивостям захищеності інформаційних ресурсів ІС;
2. Оцінки величин залишкових ризиків у ІС;
3. Визначення вихідних даних для оцінки залишкових ризиків у ІС.

1 Графічні моделі взаємодії загроз функціональним властивостям захищеності інформаційних ресурсів ІС

Для побудови графічних моделей взаємодії загроз функціональним властивостям захищеності інформаційних ресурсів ІС слід виконати наступні етапи:

1. Сформулювати моделі порушників та загроз (здійснюється службою захисту інформації підприємства);
2. Визначити, хоча б у загальному вигляді, засоби протидії загрозам – моделі захисту інформаційного об’єкту;
3. Розробити графічні моделі взаємодії загроз із засобами протидії цим загрозам.

За наслідками першого етапу та з урахуванням [2 –4] доцільно здійснити додаткову класифікацію порушників на:

- “Випадкових порушників” – авторизованих користувачів, які порушили політику безпеки тієї чи іншої послуги ненавмисно, а помилково шляхом виконання непередбачених дій з об’єктом захисту шляхом випадкового подолання засобів управління (адміністрування) доступом до нього та т.п.;
- “Терплячих зловмисників” – авторизованих користувачів, які порушили політику безпеки тієї чи іншої послуги навмисно, але без рішучих дій, маскуючись, шляхом підбору атрибутів доступу інших користувачів з метою прихованого подолання засобів управління (адміністрування) доступом до нього та т.п.;
- "Рішучих зловмисників”, які мають на меті будь-що порушити ту чи іншу властивість захищеної інформації. Для цього такі зловмисники прагнуть подолати засоби організаційного обмеження доступу, охоронної сигналізації, управління доступом до фізичних ресурсів, елементи будівельних конструкцій тощо й отримати змогу фізичного доступу до засобів оброблення, зберігання чи передавання інформаційних об’єктів з метою виведення їх з ладу, зміни режимів функціонування, крадіжки носіїв, наприклад, накопичувачів на жорстких чи гнучких магнітних дисках тощо;
- Зловмисників, які використовують засоби віддаленого доступу до інформаційних об’єктів: витоки інформації технічними каналами, спеціальні впливи на інформацію

- технічними каналами, мережне обладнання локальних чи розподілених мереж, у тому числі й засоби телекомунікаційних мереж.

Така класифікація дозволяє більш чітко визначати способи унеможливлення несанкціонованих дій порушників та засоби, які потрібні для побудови моделей взаємодії засобів реалізації атак із засобами захисту відповідних властивостей захищеності інформації (чи взагалі ресурсів ЛОМ).

Такий підхід дозволяє визначити деяку узагальнену графічну модель загроз ресурсам локальних обчислювальних мереж (ЛОМ), у вигляді, який наведено на рис. 1.

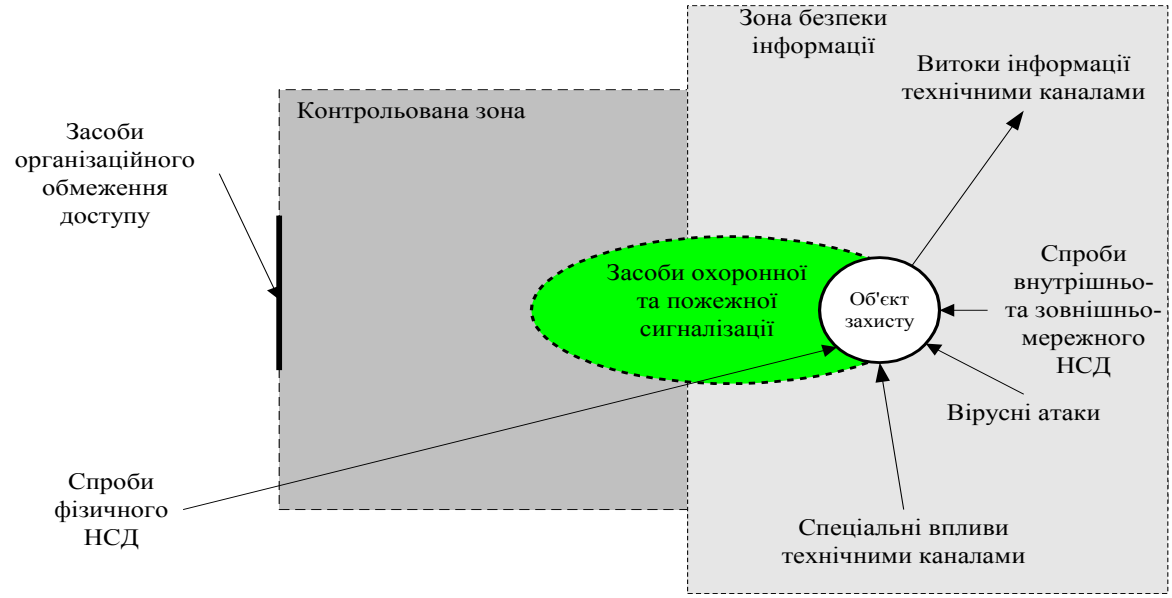


Рис.1 Узагальнена графічна модель загроз інформаційному об’єкту ЛОМ

На другому етапі (визначення моделей захисту інформаційного об’єкту) з урахуванням інформаційної відокремленості (ізольованості) локальних обчислювальних мереж підприємства, будемо вважати, що об’єктом захисту є інформаційні ресурси певної ЛОМ, а засоби технічного захисту ресурсів такої ЛОМ, виходячи із наданої на рис. 1 узагальненої моделі загроз інформаційному об’єкту ЛОМ, складаються із засобів організаційного обмеження доступу, охоронної сигналізації, адміністрування доступу – внутрішньомережних засобів управління доступом до ресурсів ЛОМ, засобів захисту від витоків інформації технічними каналами, засобів захисту від спеціальних впливів на інформацію технічними каналами та засобів антивірусного захисту і забезпечують реалізацію певного набору функцій по обслуговуванню множини запитів.

З розглянутого витікає, що загрози об’єкту захисту (інформаційним ресурсам певної ЛОМ) можуть здійснюватися шляхом несанкціонованого доступу (НСД), тобто шляхом подолання порушником:

1. Засобів організаційного обмеження доступу;
2. Засобів управління фізичним доступом;
3. Засобів охоронної сигналізації;
4. Внутрішньомережних засобів управління доступом – засобів адміністрування доступу (проблемно – орієнтованих засобів захисту базового програмного забезпечення – операційних систем та систем керування базами даних (при їх наявності);
5. Засобів захисту в телекомунікаційних мережах (в разі підключення ЛОМ до розподілених чи глобальних інформаційно – телекомунікаційних мереж);
6. Засобів антивірусного захисту (засобів захисту від впровадження комп'ютерних вірусів).

Окрім того, впливи на інформаційні об’єкти можливі за рахунок використання:

- технічних каналів побічних електромагнітних випромінювань і наведень;
- каналів спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту чи порушення цілісності інформації.

Після розгляду такої узагальненої графічної моделі загроз інформаційному об’єкту ЛОМ можна розробити графічні моделі взаємодії загроз із засобами протидії цим загрозам по відношенню до кожної з властивостей захищеності інформації ЛОМ.

Третій етап методики розглядається по відношенню до кожної з функціональних властивостей захищеності інформації ЛОМ.

1.1. Графічна модель взаємодії засобів реалізації атак із засобами забезпечення конфіденційності інформації

Графічна модель взаємодії засобів реалізації атак із засобами протидії цим загрозам - засобами забезпечення конфіденційності інформації представлена на рис. 2. На цьому рисунку ЗК - загрози конфіденційності.

Примітка 1. У цій графічній моделі передбачено наявність загроз та відповідних засобів захисту конфіденційності за рахунок подолання засобів захисту в телекомунікаційній мережі, що не завжди є притаманним ЛОМ підприємств, оскільки в деяких із них можуть використовуватися лише відокремлені ЛОМ підрозділів чи , навіть відокремлені ПЕОМ. Але з урахуванням можливого об’єднання окремих ЛОМ у розподілену обчислювальну мережу підприємства, чи приєднанні окремих ЛОМ до інших обчислювальних мереж (наприклад, деяких глобальних обчислювальних мереж) цей підхід може бути корисним і для цих підприємств.

Як витікає із даної графічної моделі, несанкціоноване отримання користувачем інформації чи ознайомлення з нею тим чи іншим чином є можливим при умові:

1. Подолання неавторизованим користувачем засобів криптографічного захисту;

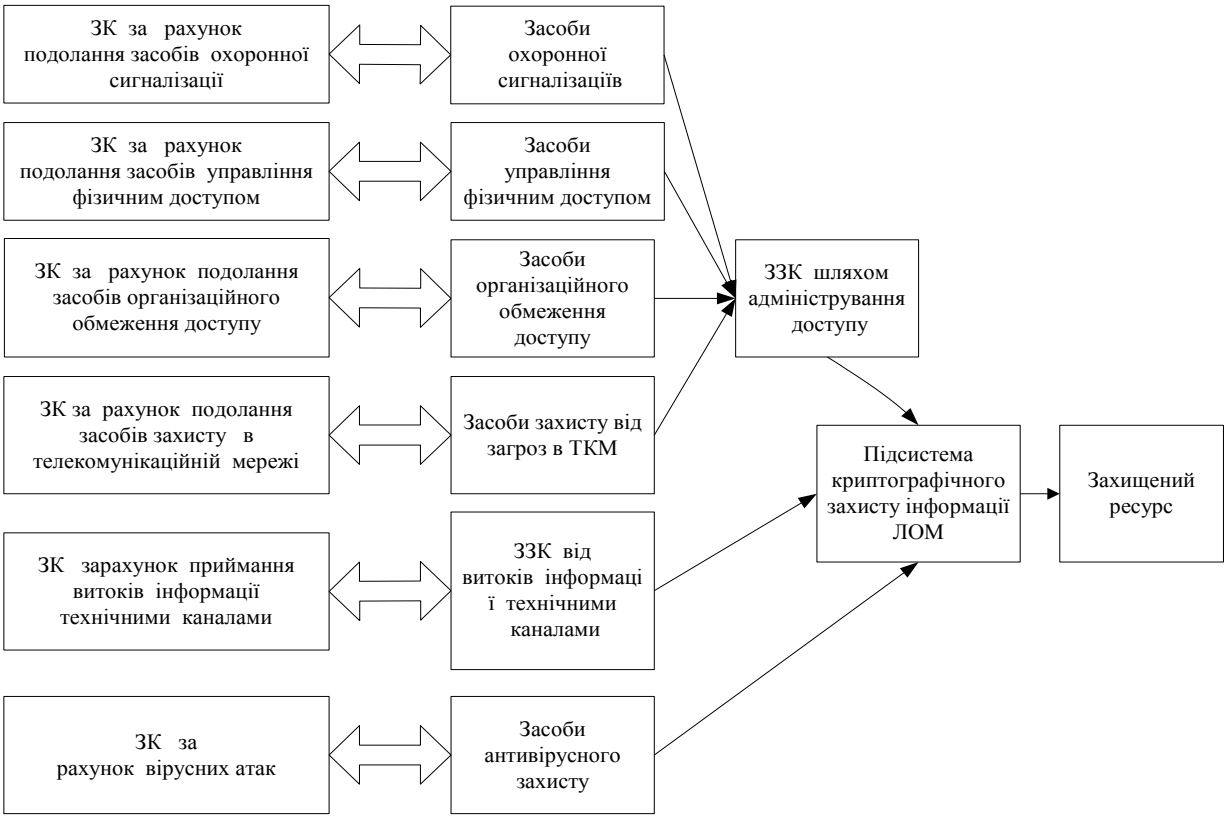


Рис 2. Графічна модель процесу взаємодії засобів реалізації атак із засобами забезпечення конфіденційності інформації в ЛОМ

2. Несанкціонованого доступу до інформаційних ресурсів з подоланням, в свою чергу, засобів:

- охоронної сигналізації (тобто шляхом “обходу” засобів організаційного обмеження доступом. Такі дії слід очікувати, скоріше за все, від “рішучих зловмисників”, які мають на меті будь-що порушити ту чи іншу властивість захищеної інформації;
- організаційного обмеження доступу – недотримання порушниками, у тому числі персоналом відповідних підрозділів підприємства, у яких використовуються ЛОМ, посадових інструкцій, наказів та розпоряджень керівництва щодо забезпечення безпеки інформації тощо;
- управління доступом, включаючи засоби управління фізичним доступом (дозвіл чи блокування доступу до приміщень, терміналів, системних блоків, клавіатури та інших фізичних засобів) та адміністрування доступу (адміністрування суб’єктів, об’єктів, побудови і реалізації моделі захищеної системи, розмежування доступу тощо). Такі дії слід очікувати, скоріше за все, від “терплячих зловмисників”, які порушують політику безпеки даної послуги навмисно, але без рішучих дій, маскуючись, шляхом підбору атрибутів доступу інших користувачів з метою прихованого подолання засобів правління доступом до інформації, або від “випадкових порушників” – авторизованих користувачів, які порушують конфіденційність не навмисно а помилково – шляхом випадкового подолання засобів управління (адміністрування) доступом до об’єкту захисту, виконання непередбачених дій відносно цього інформаційного об’єкту та т. п.;
- засобів захисту в телекомунікаційній мережі (в разі використання ЛОМ, яка є підключеною до інших ЛОМ підприємства чи є елементом розподіленої мережі більш високого рівня);
- засобів захисту від витоків інформації технічними каналами;
- засобів захисту від вірусних атак (засобів антивірусного захисту), спроможних перевести захищений інформаційний ресурс із розряду конфіденційного до розряду відкритого.

1.2. Графічна модель взаємодії засобів реалізації атак із засобами забезпечення цілісності та доступності інформації

Графічна модель взаємодії засобів реалізації атак із засобами протидії цим загрозам – засобами забезпечення цілісності та доступності інформації з урахуванням наведеної вище примітки 1 щодо загроз із телекомунікаційних мереж та відповідних засобів захисту представлена на рис. 3 (на цьому рис. ЗЦ – загрози цілісності).

Використати для оцінки цілісності і доступності інформації єдину графічну модель дозволяє наведене вище трактування Нормативними документами Системи технічного захисту України цих функціональних властивостей захищеності, коли доступність розглядається, зокрема, як властивість інформації, що полягає в тому, що інформація знаходиться у вигляді, необхідному користувачеві (тобто є не модифікованою), і в той час, коли вона йому необхідна. Тобто порушення цілісності є, одночасно, і порушенням і доступності.

При цьому, як і для моделі взаємодії засобів реалізації загроз конфіденційності інформації та засобів протидії цим загрозам, подолання неавторизованим користувачем системи захисту цілісності з імовірністю $q_{пц}$ можливе, якщо:

1.Подолано засоби захисту від несанкціонованого доступу (охоронної сигналізації, організаційного обмеження доступу, засоби управління фізичним доступом (дозвіл чи блокування доступу до приміщень, терміналів, системних блоків, клавіатури та інших фізичних засобів) та адміністрування доступу (адміністрування суб’єктів, об’єктів, побудови і реалізації моделі захищеної системи, розмежування доступу тощо))

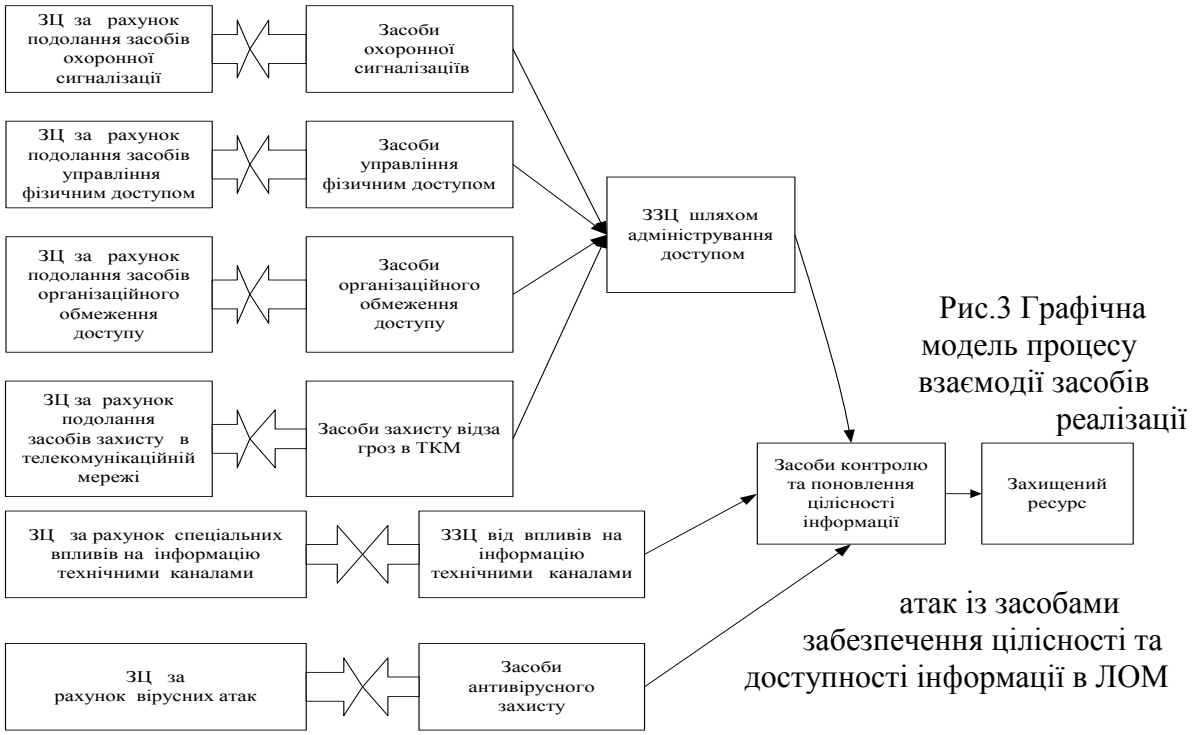


Рис.3 Графічна модель процесу взаємодії засобів реалізації атак із засобами забезпечення цілісності та доступності інформації в ЛОМ

1. З імовірністю $q_{св}$ подолано засоби захисту від спеціальних впливів на інформацію технічними каналами;

2. З імовірністю $q_{ав2}$ подолано засоби антивірусного захисту, спроможних здійснити ту чи іншу модифікацію (порушення цілісності) інформаційного об'єкту;

3. З імовірністю $q_{кц}$ подолано засоби контролю та поновлення цілісності інформації.

З урахуванням наведених вище зауважень, слід вважати, що подолання неавторизованим користувачем системи захисту доступності з імовірністю $q_{пд}$ можливе, якщо:

- з імовірністю $q_{пц}$ порушено цілісність інформаційного об'єкту;
- порушено правила, встановлені політикою безпеки, щодо часу очікування авторизованим користувачем доступу до інформації (користувач очікує довше заданого (малого) проміжку часу або інформація не знаходиться користувачем в той час, коли вона йому необхідна).

Остання ситуація в методиці розглядається як штучна відмова в обслуговуванні, а порядок розрахунку відповідної ймовірності викладено нижче.

2. Методики оцінки залишкових ризиків

2.1. Оцінка залишкового ризику при забезпеченні конфіденційності

Для оцінки залишкового ризику при забезпеченні конфіденційності (ймовірність отримання інформації порушником з розкриттям змісту) із врахуванням висновків, отриманих при розгляді графічної моделі взаємодії засобів реалізації атак із засобами протидії цим загрозам – засобами забезпечення конфіденційності інформації (рис. 2), подію, пов'язану з порушенням конфіденційності, слід розглядати як складну та таку, що складається з подій:

Несанкціонованого отримання користувачем інформації тим чи іншим чином (несанкціонований доступ) з метою ознайомлення з нею чи будь-якого подальшого використання;

Розкриття змісту інформації з обмеженим доступом (ІзОД) після отримання її тим чи іншим. Останнє слід трактувати як можливість подолання порушником відповідних засобів криптозахисту.

При цьому ймовірність несанкціонованого доступу q_1 можна визначити з виразу:

$$q_1 = q_{ад}\cdot[1-(1-q_{ос})\cdot(1-q_{уфд})\cdot(1-q_{оод})\cdot(1-q_{кткм})],$$

де: $q_{ад}$ – ймовірність подолання засобів адміністрування доступом;
$q_{ос}$ – ймовірність подолання засобів охоронної сигналізації;
$q_{уфд}$ – ймовірність подолання засобів управління фізичним доступом;
$q_{оод}$ – ймовірність подолання засобів організаційного обмеження доступу;
$q_{кткм}$ – ймовірність порушення конфіденційності в засобах телекомунікаційної мережі (в разі використання ЛОМ, яка є підключеною до інших ЛОМ підприємства чи є елементом розподіленої мережі більш високого рівня).

Примітка 2. Тут і надалі ймовірність подолання відповідного захисту при відсутності певних загроз того чи іншого виду вважається такою, що дорівнює нулю, а при відсутності засобів захисту від таких загроз – такою, що дорівнює одиниці.

Окрім того, несанкціоноване отримання користувачем інформації є можливим і через засоби віддаленого доступу до інформаційних об'єктів, використовуючи витоки інформації технічними каналами, вірусні атаки та засоби телекомунікаційної мережі при умові подолання неавторизованим користувачем відповідних засобів захисту. Нехай імовірність подолання засобів захисту від витоків інформації технічними каналами дорівнює $q_{зві}$, а ймовірність подолання засобів антивірусного захисту – $q_{ав1}$.

Після отримання ІзОД тим чи іншим шляхом порушнику необхідно здійснити розкриття її змісту. Подія, яка полягає в тому, що порушник може розкрити зміст ІзОД (при умові подолання системи захисту даного інформаційного об'єкту) є також складною і складається з трьох подій: першої – порушник знає мову, якою інформація представляється; другої – порушник знає і може застосувати програмні засоби або апаратуру для криптографічного перетворення (для дешифрування закритої інформації); третьої – має необхідні ключі (ключові набори) для такого перетворення. Імовірності цих подій $P_{зм}$, $P_{зкп}$, $P_{кн}$ відповідно.

При цьому $q_{кзі}$ – ймовірність подолання неавторизованим користувачем засобів криптозахисту (можливість розкрити зміст ІзОД) інформації можна визначити з виразу:

$$q_{кзі} = P_{зм}\cdot P_{зкп}\cdot P_{кн}.$$

Тоді вираз для розрахунку ймовірності $q_{пк}$ порушення конфіденційності інформації з подоланням розглянутих засобів захисту можна записати у вигляді

$$q_{пк} = q_{кзі}\cdot[1-(1-q_1)\cdot(1-q_{зв})\cdot(1-q_{ав1})]$$

Розглянута в методиці модель дозволяє зробити, висновок про те, що для забезпечення конфіденційності за рахунок унеможливлення доступу неавторизованих користувачів до інформації та розкриття її змісту необхідно застосовувати засоби (апаратурні чи програмні) для адміністрування доступу, для криптографічного перетворення (для шифрування та дешифрування закритої інформації, а також засоби генерації та розповсюдження ключів), засоби управління фізичним доступом, засоби охоронної сигналізації, організаційного обмеження доступом та засоби антивірусного захисту.

2.2 Оцінка залишкового ризику при забезпеченні цілісності

Для оцінки залишкового ризику при забезпеченні цілісності подію, пов'язану з її порушенням, слід розглядати як складну та таку, що складається з подій:

- виведення з ладу, зміни режимів функціонування або несанкціонованого використання засобів зберігання носіїв інформації і порушення, таким чином, її цілісності;

- несанкціонованої модифікації (зміни, підміни, знищення та т. п.) ІзОД у середовищах її оброблення, зберігання чи передавання з метою унеможливлення подальшого її використання чи нанесення іншої шкоди власнику даного ресурсу.

Тоді, з використанням застосованих вище підходів, імовірність порушення цілісності $q_{пц}$ можна знайти з виразу

$$q_{пц} = q_{кц} \cdot [1 - (1 - q_1) \cdot (1 - q_{св}) \cdot (1 - q_{ав2})].$$

Використана у цій формулі величина q_1 визначена у попередньому підрозділі.

Розглянута в методиці модель дозволяє зробити, по-перше, висновок про те, що для забезпечення цілісності за рахунок унеможливлення доступу до інформації та модифікації неавторизованим користувачем змісту інформаційного об'єкту необхідно застосовувати засоби (апаратурні чи програмні) для адміністрування доступу, контролю цілісності, управління фізичним доступом, засоби охоронної сигналізації та організаційного обмеження доступом.

По-друге, з останнього витікає необхідність, на відміну від моделі взаємодії засобів реалізації загроз та засобів забезпечення конфіденційності, застосування для забезпечення цілісності інформаційних об'єктів засобів з відповідними механізмами контролю цілісності та замість засобів захисту від витоків – засобів захисту від спеціального впливу. Окрім того, для унеможливлення порушення цілісності за рахунок отримання неавторизованим користувачем доступу до інформації з обмеженим доступом слід застосовувати такі ж засоби управління доступом (апаратурні чи програмні), як і для забезпечення конфіденційності.

Примітка 3. Звернемо увагу на те, що із наведеного вище визначення цілісності, як функціональної властивості захищеності інформації, не витікає ніяких часових обмежень щодо тривалості процесу поновлення цілісності, у разі виявлення засобами контролю наявності її порушення. Це дає змогу для забезпеченні цілісності використовувати і ручні методи, наприклад, поновлення із застосуванням резервних копій інформаційних об'єктів чи шляхом забезпечення відкоту процесів у разі виявлення порушення цілісності.

2.3. Оцінка залишкового ризику при забезпеченні доступності

Виходячи із наведеного вище визначення функціональної властивості доступності інформації та графічної моделі взаємодії засобів реалізації атак із засобами протидії цим загрозам – засобами забезпечення цілісності та доступності інформації (рис. 3), для оцінки залишкового ризику при забезпеченні доступності подію, пов'язану з її порушенням, слід розглядати як наслідок впливу на інформаційний об'єкт загроз, найбільш суттєвими з яких є:

1. Несанкціонована модифікація інформаційного ресурсу (порушення цілісності – вигляду ресурсу, необхідного користувачеві), включаючи зміни режимів його функціонування, місця зберігання, необхідного чи заданого користувачем, що потребує поновлення цілісності ресурсу шляхом, наприклад, використання його резервної копії. Така подія передбачає можливість фізичного доступу до джерел чи носіїв інформаційних ресурсів, наявність реалізованої спроби несанкціонованого доступу до інформаційного ресурсу, в тому числі каналами ТКМ та каналами спеціального впливу (порушник зумів здійснити маскування під авторизованого користувача чи модифікація не виявлена засобами контролю цілісності);

2. Перевід ресурсу в режим штучної відмови шляхом:

- несанкціонованого використання інформаційного ресурсу в той час, коли ресурс є необхідним користувачеві, та протягом часу довше заданого (малого) проміжку – шляхом захоплення ресурсів (неконтрольованого використання, утримання, занадто тривалого використання) і створенню, таким чином перешкод іншим користувачам в використання цих ресурсів;
- постійного використання ресурсу, наприклад, шляхом генерації потоку заважаючих запитів (несправжніх запитів на обслуговування, несправжніх пакетів вхідної інформації, спроб підбору паролів та т.п. – завад процесу обслуговування справжніх запитів) з такою інтенсивністю, коли їх період (середня тривалість проміжку часу між двома сусідніми

запитами) не перевищує тривалості обслуговування кожного з таких запитів, тобто такого потоку, коли захищений ресурс призначається для обслуговування лише заважаючих запитів;

- постійного порушення цілісності з періодичністю меншою ніж час відновлення інформаційного ресурсу. Така подія передбачає наявність порушень цілісності за рахунок впливу природних факторів (збої, відмови), а також наявність реалізованих спроб несанкціонованого доступу до інформаційного ресурсу каналами спеціального впливу (без спроб маскування).

Імовірність першої із цих подій визначено вище (з використанням моделі, представленої на рис. 3) і вона дорівнює $q_{пц}$.

Для оцінки ймовірності порушення доступності шляхом переводу ресурсу в режим штучної відмови необхідно визначити інтенсивність потоку впливів на доступність ресурсу. Для цього скористаємося відомими підходами для розрахунку результуючої інтенсивності як природних, так і штучних впливів на інформаційні ресурси технічними каналами. Під природними впливами будемо розуміти потоки будь-яких подій, які здатні вивести ЛОМ з ладу тимчасово (збої, для яких є характерним самоусунення), чи на тривалий термін (відмови, усунення яких вимагає втручання персоналу), тобто потоки відмов. Причинами таких впливів може бути недостатня спроможність уже згаданих первинних технічних засобів запобігти дії таких впливів, недостатня надійність засобів ЛОМ, виходи за межі допустимих значень температури, вологості, радіаційного чи електромагнітного випромінювання, яке впливає на елементи ЛОМ, та т.п. Такі події впливають як безпосередньо на інформаційні ресурси ЛОМ, так і на засоби технічного захисту цієї системи. При цьому стійкість ЛОМ до природних загроз визначається в основному такою її властивістю як надійність і забезпечується відповідними заходами (резервування – гаряче та холодне, застосування елементів підвищеної надійності та т. інш.). Для боротьби зі збоями, які призводять до порушення цілісності програмних засобів та оброблюваної інформації, можна застосовувати засоби контролю та поновлення цілісності чи інші засоби поновлення після збоїв.

Під штучними впливами розуміються ті події, які є наслідком діяльності користувачів, як авторизованих, так і неавторизованих по відношенню до ресурсів ЛОМ, що є з якихось причин забороненими для даних користувачів. Такі впливи – спроби НСД можуть бути випадковими (в наслідок помилки користувача) або зловмисними, тобто спеціальними, з метою використання чи то ресурсів, чи то інформації ЛОМ.

Таким чином, на інформаційні ресурси ЛОМ можуть впливати як спроби несанкціонованого доступу, при умові подолання систем управління доступом та фільтрації, так і безпосередньо природні впливи.

Будемо вважати потік загроз найпростішим з інтенсивністю $\lambda_з$. Зрозуміло, що цей потік складається зі штучних загроз з інтенсивністю $\lambda_ш$ та природних з інтенсивністю λ, так що $\lambda_з = \lambda_ш + \lambda$. У свою чергу, штучні загрози можуть бути внутрішніми з інтенсивністю $\lambda_{шв}$ (з боку авторизованих чи неавторизованих користувачів ЛОМ чи її елементів) та зовнішніми з інтенсивністю $\lambda_{шз}$. Виявлення і подальша протидія загрозі (ймовірність захисту ЛОМ від загроз) залежить від того, чи запобігла (не допустила) система ТЗІ впливу цієї загрози, чи установила факт її впливу і ліквідувала відповідні наслідки.

Ця задача вирішується, по-перше, шляхом управління доступом до інформаційних ресурсів ЛОМ (ідентифікація, автентифікація, надання певних повноважень чи привілеїв, з наступною їх перевіркою під час кожної зі спроб доступу до ресурсів). Для цього в системі ТЗІ повинен виділятись адміністратор (адміністратор безпеки), який і вирішує усі ці питання, зрозуміло з використанням засобів системи захисту, можливо через спеціальним чином обладнане автоматизоване робоче місце (АРМ) адміністратора безпеки. Зауважимо, що оскільки адміністратор безпеки має, як правило, найширші права

щодо управління доступом до ресурсів ЛОМ, то захопивши його повноваження можна порушити процес надання цією ЛОМ будь–якої функціональної послуги.

Тому слід уважати, що стійкість (в розумінні ймовірності не подолання) системи управління доступом $p_д = 1 - q_1$ визначається стійкістю процесів ідентифікації та автентифікації самого адміністратора безпеки, як користувача з найширшими повноваженнями. Останнє визначається можливостями системи ідентифікації та автентифікації (наприклад, кількістю можливих варіантів ідентифікаторів та кількістю можливих варіантів паролів і надійністю їх конфіденційного зберігання). У наслідок відсіву (фільтрації) внутрішніх впливів системою управління доступом на її виході інтенсивність завад буде дорівнювати $\lambda_{шв} \cdot q_1$.

Ця задача може вирішуватися, по-друге, застосуванням у ЛОМ засобів фільтрації зовнішніх штучних впливів (від елементів розподіленої обчислювальної мережі через засоби телекомунікаційної мережі в разі наявності підключення даної ЛОМ до розподілених чи глобальних інформаційно – телекомунікаційних мереж), які впливають на дану ЛОМ (засоби фільтрації типу міжмережних екранів (firewall, брандмауерів), сервісів – посередників (proxy services) та т. п.). Якщо стійкість таких засобів (в розумінні ймовірності не подолання) дорівнює $p_ф = 1 - q_ф$, то в наслідок відсіву (фільтрації) зовнішніх впливів на виході системи фільтрації інтенсивність завад буде дорівнювати $\lambda_{шз} \cdot q_{фі}$, а інтенсивність $\lambda_р$ штучних впливів, які не відфільтровані системами управління доступом та фільтрації, складе:

$$\lambda_{рш} = \lambda_{шв} \cdot q_1 + \lambda_{шз} \cdot q_ф + \lambda.$$

З урахуванням інтенсивності справжніх запитів $\lambda_{сз}$ загальна інтенсивність $\lambda_з$ впливів дорівнює

$$\lambda_з = \lambda_{сз} + \lambda_{шв} \cdot q_1 + \lambda_{шз} \cdot q_ф + \lambda$$

При середній тривалості обслуговування в ЛОМ одного запиту (середньому значення часу використання ресурсу $t_{вр}$) і пуассонівському законі розподілу ймовірностей впливу ймовірність того, що під час звернення до ресурсу він уже використовується (ймовірність звернення до ресурсу на даному інтервалі $t_{вр}$ більше ніж однієї заявки – ймовірність порушення доступності шляхом переводу ресурсу в режим штучної відмови) дорівнює

$$q_{пз} = 1 - p_0 = 1 - \exp\{-t_{вр} \bullet \lambda_з\},$$

де p_0 – ймовірність відсутності впливів (ймовірність того, що на даному часовому інтервалі виникне рівно нуль впливів), а, отже ймовірність порушення доступності ресурсу

$$q_{пд} = 1 - (1 - q_{пз}) \bullet (1 - q_{пц}).$$

Розглянута модель дозволяє:

по–перше, запропонувати вирази для оцінки залишкового ризику при захисті доступності ресурсів у вигляді ймовірності порушення доступності та сформувати умову переходу захищеного ресурсу в режим штучної відмови;

по–друге, зробити висновок про те, що для забезпечення доступності за рахунок унеможливлення доступу до інформації та модифікації неавторизованим користувачем змісту інформаційного об’єкту необхідно застосовувати засоби (апаратурні чи програмні) для управління доступом, для контролю та поновлення цілісності, для фільтрації пакетів, блокування засобів генерації безперервних запитів та т.п., засоби управління фізичним доступом, охоронної сигналізації та організаційного обмеження доступом;

по–третє, зробити висновок про необхідність, на відміну від захисту від порушення конфіденційності та цілісності, передбачати й можливість недопущення переводу ресурсу в режим штучної відмови – порушення доступності об’єкту за рахунок унеможливлення вчасного використання того чи іншого ресурсу авторизованим користувачем, тобто необхідно передбачати механізми запобігання постійного чи занадто тривалого

використання цього ресурсу чи засобів його отримання порушником (установка квот – кількості звернень поспіль, допустимої тривалості чи допустимих часових інтервалів використання ресурсу, установка пріоритетів на використання ресурсів та інше), механізми забезпечення стійкості та відновлення процесів в умовах збоїв, механізми резервування інформаційних об'єктів, механізми аналізу потоків запитів від суб'єктів ЛОМ та ТКМ, контролю та поновленню цілісності інформаційних об'єктів (наприклад, в каналах ТКМ) та т.п.

Змінну $t_{вр}$, при цьому, слід розглядати як середній час використання захищеного ресурсу в умовах обслуговування ЛОМ усіх можливих запитів (для інформаційних об'єктів це - контроль цілісності, при необхідності її поновлення, виконання програмного засобу, читання чи запис інформації та все таке інше). В якості першого, грубого, наближення можна використати значення $t_{вр} = (T_{ki} - \Delta T_{ki})/ n_{зк}$, де: $n_{зк}$ – кількість інформаційних об'єктів, що потребують використання на інтервалі часу $(T_{ki} - \Delta T_{ki})$, T_{ki}, ΔT_{ki} – періодичність та тривалість контролю відповідно. При цьому, якщо середнє значення часу використання ресурсу перевищить середнє значення часового інтервалу між сусідніми запитами (інтенсивність запитів перевищує інтенсивність обслуговування), то кількість будь-яких запитів у черзі на використання ресурсу буде зростати до нескінченності, що є ознакою штучної відмови захищеного ресурсу.

Тобто умову, коли $1/\lambda_з > t_{вр}$ слід розглядати як умову переходу захищеного ресурсу в режим штучної відмови.

2.4. Оцінка загального залишкового ризику

Розглянуті вище моделі дозволяють отримати, окрім розглянутих кількісних характеристик – ймовірностей порушення конфіденційності, цілісності та доступності також величину загального залишкового ризику.

Неважко показати, що величину загального залишкового ризику у вигляді ймовірності порушення (подолання, злому) комплексної системи захисту можна при цьому розрахувати з виразу

$$q = 1 - (1 - q_{пк}) \cdot (1 - q_{пц}) \cdot (1 - q_{пд}).$$

Таким чином, наведені методики надають змогу здійснення досить глибокого і достовірного аналізу та оцінки величин залишкових ризиків, які забезпечують застосовані засоби захисту та зробити оцінку впливів можливих порушників та загроз ресурсам інформаційних систем на величини цих залишкових ризиків. Це, у свою чергу, дозволяє визначити можливі контрзаходи для протидії цим загрозам, в тому числі, визначити чи уточнити склад необхідних засобів захисту з метою забезпечення припустимої захищеності ІС.

Література

1. "Типове положення про службу захисту інформації в автоматизованій системі" (НД ТЗІ 1.4 – 001 – 2000);

2. Матов О.Я. Теорія інформації та кодування. / О.Я. Матов, В.С. Василенко // Монографія, ISBN 978-966-02-7096-1, "Експрес-книга", Україна, Харків, - 2014. – с. 440.

3. Василенко В. С. Целостность и доступность информационных объектов. / В.С. Василенко, О.Я. Матов // Монографія, ISBN 978−3−659− 47333−3, LAMBERT Academic Publishing, Saarbrücken, Deutschland. − 2013. – с. 95.

4. Василенко В.С. Методология оценки защищенности информационных объектов. / В.С. Василенко, О.В. Дубчак // Монографія, ISBN 978−3−659− 43968−1, LAMBERT Academic Publishing, Saarbrücken, Deutschland. − 2013. – с. 84.

5. Матов О.Я. Целостность и доступность информационных объектов. / В.С. Василенко, О.Я. Матов, О.В. Дубчак // ISBN 1561−6886, Современный научный вестник. −

УДК 004.5

Сенченко В.Р. к.т.н.
Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна

МЕТОДИ ТА ТЕХНОЛОГІЇ ОБРОБКИ ДАНИХ У СИСТЕМІ МОНІТОРИНГУ ТА АНАЛІЗУ ДЕРЖБЮДЖЕТУ

Розглянуто особливості семантичної обробки даних в системі моніторингу та аналізу держбюджету. Як основа аналізу даних розглянута інформаційна модель, яка охоплює всі основні сутності бюджетного процесу та їх взаємозв'язки. На підставі запропонованої інформаційної моделі розроблено програмні засоби та технології обробки даних в системі моніторингу, включаючи спеціалізовані ETL-засоби.
Ключові слова: *інформаційна модель, фінансові показники, інформаційні технології, бази даних, витяг даних, семантична обробка даних, державний бюджет.*

Рассмотрены особенности семантической обработки данных в системе мониторинга и анализа госбюджета. В качестве основы анализа данных рассмотрена информационная модель, которая охватывает все основные сущности бюджетного процесса и их взаимосвязи. На основании предложенной информационной модели разработаны программные средства и технологии обработки данных в системе мониторинга, включая специализированные ETL-средства.
Ключевые слова: *информационная модель, финансовые показатели, информационные технологии, базы данных, извлечение данных, семантическая обработка данных, государственный бюджет*

Features of semantic data processing in system of monitoring and the analysis of the state budget are considered. As a basis for data, analysis examined the information model, which covers all the basic entities of the budget process and their relationships. Based on the proposed information model software was developed and data processing technology in the monitoring system, including the specialized ETL-tools.
Keywords: *informationmodel, financialperformance, informationtechnology, database, extractdata, semanticprocessing, thestatebudget.*

Вступ

Аналіз виконання держбюджету та оцінка його ефективності є ключовою проблемою в галузі державного управління. В України, де частина бюджетних відносин складає майже 30 відсотків від ВВП країни, ця проблема ускладнена значним впливом тіньового сектору на державні відносини. Якісний контроль та аналіз неможливий без застосування методів та технології обробки даних, які включають всі етапи оброки даних, починаючи з витягу та очищення і закінчуючи аналізом та осмисленням. Ось чому, незважаючи на достатню кількість наукових досліджень у цьому напряму, створення якісної системи моніторингу і досі є дуже актуальною проблемою як у науковому, так і в практичному аспектах.

На сучасному ринку спеціалізованих програмних засобів (ПЗ), які позиціонуються як засоби фінансового контролю та аналізу, пропонуються таки засоби як Financial Observer, Hyperion Pillar, Microsoft Business Solutions, Audit Expert, Парус-Бюджет, Audit Expert, RS – Казначейство, Прогноз, а також компоненти у складі ERP- систем. Аналіз можливості побудови системи моніторингу та аудиту на базі існуючих ПЗ, показав, що процеси в

суміжних областях базуються на моделях типових бізнес-процесів організаційних структур, які не є адекватними процесам моніторингу держбюджету і дозволяють розв'язати лише окремі функції. Тобто комп'ютерною підтримкою забезпечена, в основному, сфера бухгалтерського обліку малих та середніх підприємств, характерною ознакою якої є формалізовані процедури підготовки бухгалтерської звітності.

Другім фактором є низька ефективність використання існуючих програмних засобів (Oracle Financial Services Applications, Adaytum e.Planning, Hyperion Pillar, Scala, Navision та інших) [8-11], тому що функціональність програмних рішень або не сприймається користувачами, або є надлишковою для обраної предметної області. Загальними недоліками цих засобів є надмірна складність процесу створення гіперкубів, нерозкритість механізмів аналізу даних, Крім того, вони є занадто коштовні, а також потребують додаткових ресурсів на доведення програмної платформи під рішення визначеного переліку функцій.

Використання ERP-засобів [8] для створення ядра системи моніторингу держбюджету на їх базі є теж недоцільним, оскільки занадто висока вартість кінцевої системи та етапів її впровадження. У більшості випадків це є наслідком великої складності взаємозв'язків між різними програмними застосуваннями та надмірності їх функціональних можливостей.

Аналогічна картина спостерігається й в ETL-засобах. Із звітів дослідницьких компанії Gartner і Forrester Research [3, 4] випливає, що лідерами серед засобів витягу, обробки та завантаження даних (extract-transform-load) є два – IBM та Informatica (рис. 1.). За функціональністю обидва ETL-засоби перекривають потреби бізнесу так, що більшість клієнтів цих систем не використовують і половини наявного функціоналу. Іншим фактором є надвисока вартість ETL-інструментарію, його обслуговування та ліцензування, що робить їх майже не доступними для використання в державних установах країни.

Дослідження Gartner

Дослідження Forrester Research

Рис. 1. Рейтинги відомих ETL-засобів за даними компанії Gartner і Forrester Research

Постановка задачі

Світовий і вітчизняний досвід побудови спеціалізованих застосувань для аналітичних систем показує, що більша частина застосувань, які складають аналітичне ядро системи, або створюється зусиллями фахівців організації, або силами сторонній компаній за технічним завданням цієї організації [13]. Тому більш прийнятною стратегією побудови системи моніторингу держбюджету України є стратегія системної інтеграції, де умовою успішної реалізації є створення спеціалізованих технологій, здатних до швидкої доробки моделей предметної області, та їх інтеграція з базовими інформаційними технологіями, за рахунок чого й досягаються позитивні результати при фінансових обмеженнях. При цьому, більшою мірою, ефективність створюваної системи пов'язана з якістю моделі предметної області.

Метою статті є розробка формалізованого підходу до побудові системи моніторингу виконання держбюджету України, якій ґрунтуються на розробці інформаційних моделей та технології витягу, очищення та завантаження даних, а також типових сценаріях семантичної обробки даних при здійсненні функцій аналізу.

Об'єктом дослідження є методи і засоби семантичної обробки даних, а предметом дослідження — бізнес-процеси створення моделі системи аналізу даних.

Побудова інформаційної моделі моніторингу та аналізу державного бюджету

Якщо говорити про застосування в Україні інформаційних технологій (ІТ) при здійсненні моніторингу та аналізу бюджетних процесів, то ситуація є складною [1]. Це підтверджує також аналіз вітчизняних публікацій, пов'язаних із застосуванням ІТ в аудиті та внутрішньогосподарському контролі, проведений Івахненковим С.В. [2]. Автор показує практичну відсутність комплексних досліджень у цієї сфері.

Моніторинг стану виконання бюджету визначається як систематичний збір та обробка інформації, яка застосовується для оцінки ефективності використання бюджетних коштів, а також підготовки та прийняття управлінських рішень [14].

Інформаційна модель системи моніторингу держбюджету (надалі - інформаційна модель) будується на базі формування багатовимірних даних, які описують бюджетні відносини, та складається з наступних компонент:

P_z^{fip} - множина фінансових показників, через які визначають стан бюджетних відносин в країні, і які згруповані відповідним чином і підтримуються певними методами та технологіями обробки;

F^{adb} - напрями і функції фінансового моніторингу та аналізу показників, що визначають бюджетні відносини;

$\mathbf{Pr}_m^{\circ}$ - сукупність спеціалізованих ETL-інструментів витягу, семантичної обробки та завантаження до баз даних фінансових та економічних показників, які визначають стан виконання держбюджету.

В основі моделі даних предметної області - P_z^{fip} закладена структура бюджетних відносин, яка визначається показниками доходів, видатків та кредитування, фінансування бюджету та показників, що характеризують боргові зобов'язання [7]

$$P_z^{fip} = \{P_{inc}^{fip}, P_{\exp}^{fip}, P_{fin}^{fip}, P_{deb}^{fip}\};$$

Показники множини $\{P_{inc}^{fip}\}$ відображають доходи бюджету і розрізняються за податковими та неподаткові надходженнями, доходами від операцій з капіталом та трансфертами тощо. Показники множини $\{P_{\exp}^{fip}\}$ - видатки та кредитування, які класифікуються за бюджетними програмами, головними розпорядниками бюджетних коштів та функціями, з виконанням яких пов'язані видатки та кредитування бюджету.

Множина показників $\{P_{fin}^{fip}\}$ характеризує категорію кредитора, а також типи боргових зобов'язань, $\{P_{deb}^{fip}\}$ систематизує інформацію про всі боргові зобов'язання держави, територіальної громади міст та класифікується за типом кредитора і типом боргового зобов'язання.

Основним поняттям багатовимірної моделі даних бюджетного процесу є поняття гіперкуба даних, що представляє собою множину осередків $H^{fip}(P^{fip},M)$, що відповідають множині вимірів (напрямам та функціям дослідження фінансових показників держбюджету: зведеного бюджету, місцевих бюджетів в цілому та у розрізі регіонів, а також заборгованості бюджетних установ). У свою чергу майже кожен з вимірів має ієрархічну структуру і описується за допомогою методу семантичної мережі пов'язаних понять (сутностей предметної області). Наприклад, ієрархічна структура «бюджет» має, як мінімум, два види ієрархічних рівнів «бюджет – державний – місцевий – загальний фонд – спеціальний фонд» та «бюджет – доходи – видатки – заборгованість – трансфери» і таке інше.

Отже $P^{fip}=\{p_1,p_2,...,p_z\}$ являє собою множину значень вимірів (яка асоціюється зі станом фінансових показників, та відповідає кодам бюджетної класифікації, прийнятою у державі). Тоді $M=M_{p_1}\cup M_{p_2}\cup...\cup M_{p_z}$, де $M_{p_z}=\{m_{1_z},m_{2_z},...,m_{kz}\}$ – множина позначок виміру p_z (наприклад, множина позначок виміру у регіональному розрізі з розбивкою по місяцям, кварталам, рокам).

Моніторинг та аналіз виконання бюджету базується на методології бухгалтерського обліку, основою якого є бюджетна класифікація – систематизоване згрупування показників (доходів, видатків, кредитування, фінансування бюджету, боргу) відповідно до законодавства України та міжнародних стандартів [7, 10]. Завдяки бюджетній класифікації кожний окремий показник P_z^{fip} має відмінний від інших кількісний набір цифр, тобто будь-який показник може бути однозначно ідентифікований у багатовимірної моделі даних (**наприклад, Податки на доходи, податки на прибуток, податки на збільшення ринкової вартості – 11000000** (Код бюджетної класифікації), або **Податок на доходи фізичних осіб – 11010000**).

Отже, бюджетна класифікація в інформаційній моделі описується виразом

$$BC_z^{fip}=\{BC_{inc}^{fip},BC_{\exp}^{fip},BC_{fin}^{fip},BC_{deb}^{fip},\}$$

Де $\{BC_{inc}^{fip}\}$ - класифікація доходів бюджету;

$\{BC_{\exp}^{fip}\}$ - класифікація видатків та кредитування бюджету;

$\{BC_{fin}^{fip}\}$ - класифікація фінансування бюджету;

$\{BC_{deb}^{fip}\}$ - класифікація боргу.

Для побудови інформаційної моделі скористаємося методом декомпозиції за рівнями. У межах рівня здійснюється опис характерних елементів і процесів функціонування системи. При цьому кожен рівень може містити свою власну сукупність перемінних. В залежності від повноти інформаційної моделі кількість рівнів може відрізнятися. Для спрощення сприйняття моделі в цілому обмежимось 4 рівнями (рис. 2.).

Рівень 1 визначає та описує джерела та потоки інформації, які надходять до системи та формується на підставі фінансової звітності розпорядників бюджетних коштів - Q_η^{ap}, звітності фіскальних органів - Q_η^{fo}, на основі казначейської звітності - Q_η^{ac}.

Порядок надання та склад звітних форм визначаються відповідними нормативними документами.

Рівень 2 охоплює процеси та методи вилучення даних, очищення від помилок, валідації даних та їх завантаження в відповідні БД, а також ETL – технології, що реалізують ці процеси і методи.

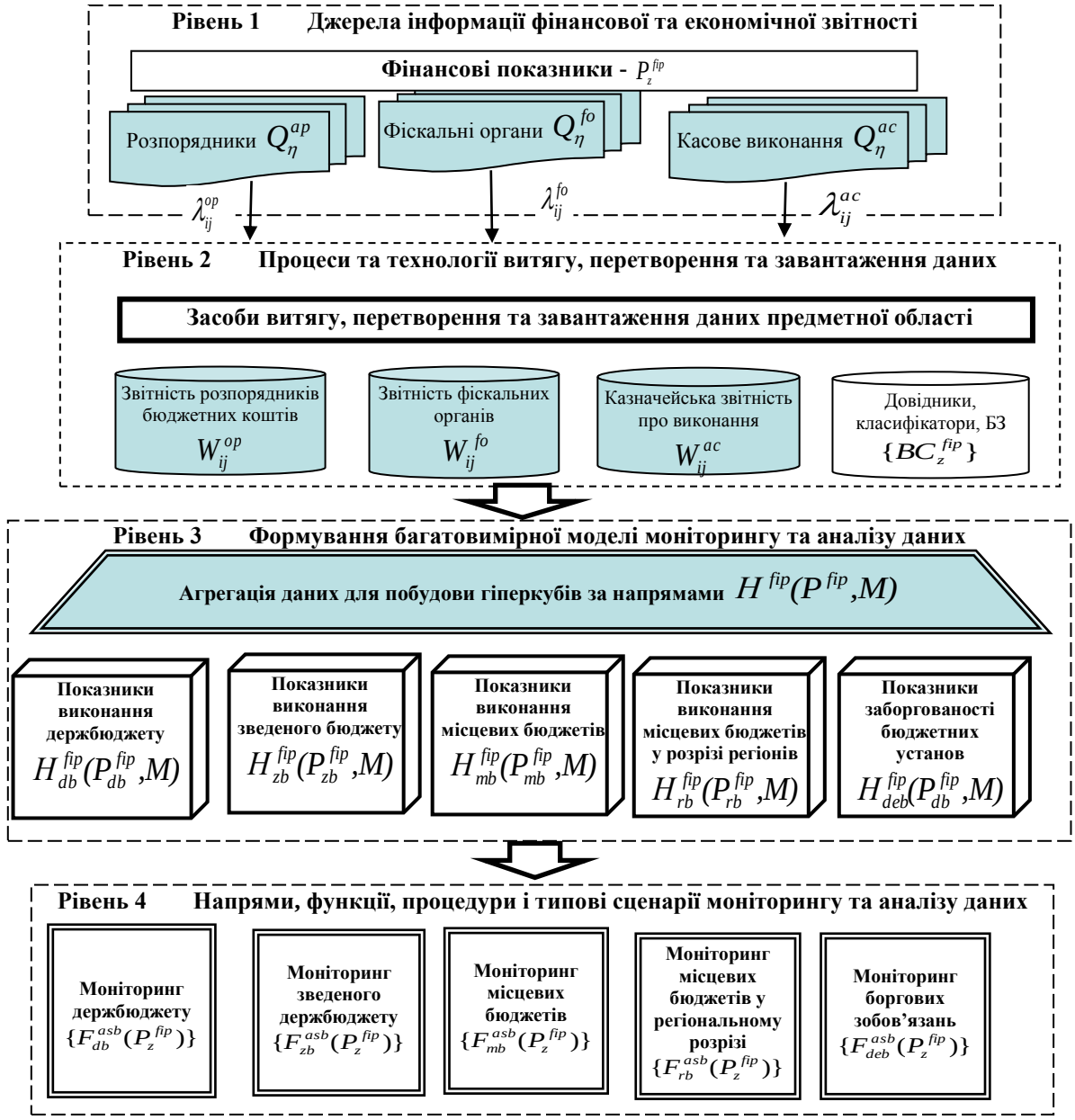


Рис. 2. Інформаційна модель моніторингу та аналізу бюджетних процесів в Україні.

Рівень 3 формування та актуалізації багатовимірної моделі даних моніторингу та аналізу виконання бюджетних процесів. Враховуючи особливості бюджетного устрою України, та маючи на увазі спеціалізацію кінцевих користувачів системи, гіперкуб даних $H^{fip}(P_z^{fip},M)$ можна представити як сукупність проблемно-орієнтованих гіперкубів, які відповідають визначеним напрямам моніторингу та аналізу держбюджету. А саме:

$H_{db}^{fip}(P_{db}^{fip},M)$ - гіперкуб фінансових показників виконання державного бюджету;

$H_{zb}^{fip}(P_{zb}^{fip},M)$ - гіперкуб фінансових показників виконання зведеного бюджету;

$H_{mb}^{fip}(P_{mb}^{fip},M)$ - гіперкуб фінансових показників виконання місцевих бюджетів;

$H_{rb}^{fip}(P_{rb}^{fip},M)$ - гіперкуб фінансових показників виконання місцевих бюджетів у розрізі регіонів;

$H_{deb}^{fip}(P_{db}^{fip},M)$ - гіперкуб показників заборгованості бюджетних установ.

Використання OLAP-технології (On-Line Analytical Processing) надає можливість користувачу (аналітику, експерту, керівнику) оперативно (за кілька секунд) отримувати потрібні (агреговані) дані, які кількісно описують процеси, що досліджуються. Під терміном агрегація розуміється процес формування меншої кількості значень (агрегатів) на основі більшої кількості первинних значень (багатовимірних даних), що містяться у сховищі даних (Data Warehous).

Рівень 4 розглядає напрями і функції фінансового моніторингу та аналізу. У відповідності з структурою бюджету та територіальним устроєм України в інформаційної моделі моніторингу визначені таки напрями:

- моніторинг виконання державного бюджету;
- моніторинг виконання зведеного бюджету;
- моніторинг виконання місцевих бюджетів;
- моніторинг виконання місцевих бюджетів у розрізі регіонів;
- моніторинг заборгованості бюджетних установ.

Структура аналітичного ядра системи моніторингу

Відомо, що при сприйнятті програмного застосування кінцевим користувачем значну роль відіграє людський фактор, якій опосередковано пов'язують з кількістю «кліків» мишкою користувачем при отриманні бажаного результату [8]. Світовий досвід успішного впровадження програмних продуктів показує, що поширення та розповсюдження досягають ті програмні застосування, які потребують мінімальної кількості «кліків» [12]. Виходячи з цих вимог архітектура аналітичного ядра системи моніторингу має являти собою трирівневу модель взаємовідносин між кінцевим користувачем (експертом) та створюваною системою. Трирівнева модель взаємовідносин вважається більш оптимальною (у сенсі подання бажаного результату кінцевому користувачу) оскільки вона не містить зайвих «кліків».

Таким чином, архітектура програмних засобів моніторингу та аудиту бюджетних процесів представлена наступними рівнями (рис. 3.):

- Рівнем, який надає механізми та інтерфейс вибору напряму дослідження бюджетного процесу – державного та місцевих бюджетів, заборгованості тощо;
- Рівнем, який представляє множину функції – типових завдань для дослідження доходів, видатків, боргових зобов'язань, наприклад – «дослідження видатків за КФК» (дослідження звіту Держказначейства за видатками КФК за будь-який період місяці, квартали, роки, регіони);
- Рівень, який надає безпосередньо експерту множину аналітичних процедур з прив'язкою до особливостей предмета дослідження (порівняльні діаграми, картограми, структури тощо).

Технологія витягу, очищення, валідації та завантаження показників виконання держбюджету

Під витягом даних (Extract-Load-Transform) – процес отримання даних з неструктурованих (зазвичай слабко структурованих) даних для подальшої їх обробки в системах моніторингу або аналізу даних [11, 15, 16]. Як відомо, інформаційна технологія витягу та семантичної обробки даних складається з низки процедур: отримання даних; збір і реєстрація даних; машинне кодування даних; збереження.

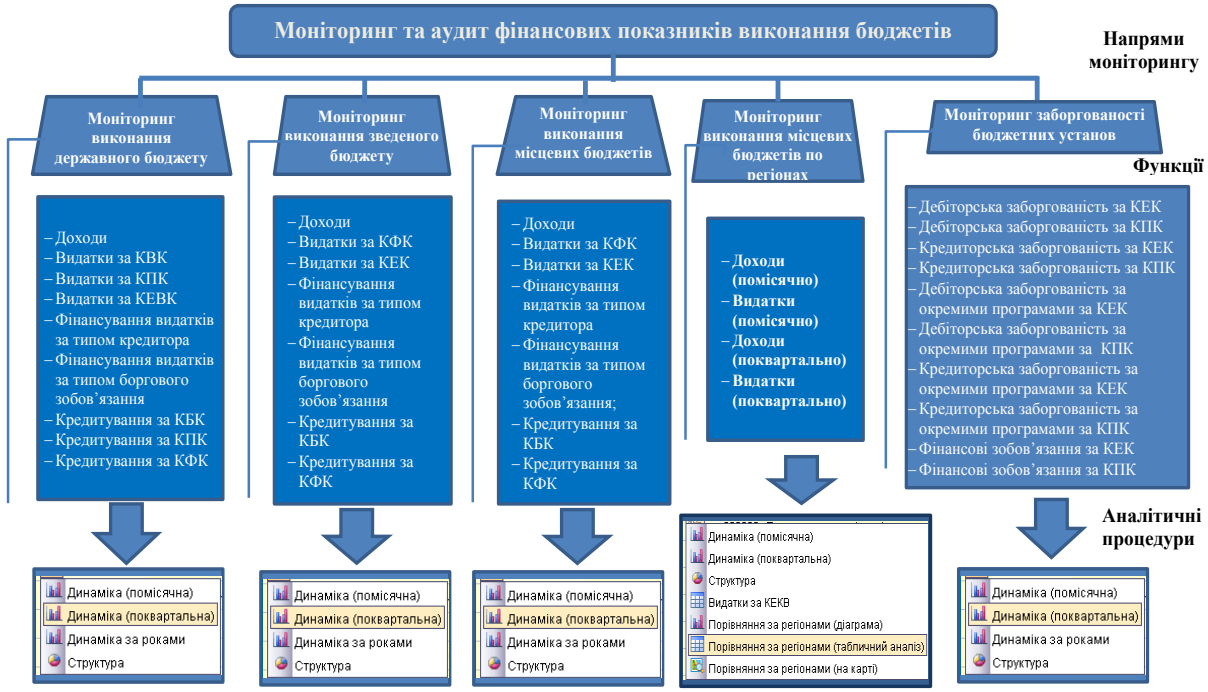


Рис. 3. Архітектура аналітичного ядра системи моніторингу держбюджету України

Сьогодні засоби ETL інструментів постачаються як крупними компаніями виробниками (SSIS від Microsoft, IBM Cognos Data Manager, BusinessObjects, Oracle BI, Informatica, IBM Data Stage), так і невеликими компаніями (third-party company). Як показує аналіз, більшість ETL інструментів виробляється невеликими компаніями. Такі компанії в силу обмеженості своїх ресурсів часто не можуть забезпечити розробку і супровід продуктів на різних платформах. ETL інструменти часто модифікуються, їх життєвий цикл обмежений, тому важливо, щоби технологія їх створення припускала швидку розробку і внесення змін при виникненні такої необхідності. Випадки використання готових програмних застосувань, які налаштовуються для потреб організації, наприклад, IBM Cognos Data Manager SAP, є винятковими у порівнянні з практикою створення спеціальних програмних застосувань. Ще один важливий момент – це доплати за різні програмні конектори і додаткові функції, які потрібні для впровадження адаптації ETL інструментів до потреб організації. Так, SAP- конектор від Informatica коштує близько 100 тис. доларів.

Системи моніторингу, які використовують багатовимірну модель даних, коректне працюють тільки з однорідними, чітко структурованими даними. Саме з метою систематизації та приведення даних до одного типу, розроблені засоби автоматичного вводу документів фінансової звітності $\mathbf{Pr}_m^{\circ}$,

Звітність про виконання держбюджету Q_{η}^{ac}, яка надходить до системи, є оперативною (місячна, квартальна, річна) та представлена чисельними звітними формами

(понад 30 форм). Відповідно до Бюджетного кодексу, Державним казначейством України встановлюються єдині форми звітності, які, в свою чергу, теж застосовують бюджетну класифікацію для визначення показників. Саме тому, бажано щоб ETL-інструменти для семантичної обробки та автоматичного завантаження документів фінансової звітності, підтримували модель бюджетної класифікації, $BC_z^{fip} = \{BC_{inc}^{fip}, BC_{\exp}^{fip}, BC_{fin}^{fip}, BC_{deb}^{fip}, \}$, оскільки це суттєво спрощує ідентифікацію показників в процесі їх обробки і завантаження до БД системи моніторингу.

Виходячи із запропонованої структури багатовимірних даних інформаційної моделі, яка відбиває модель бюджетного устрою держави, бажано щоби ETL-інструменти теж підтримували модель бюджетних відносин. Саме тому, для спрощення алгоритмів семантичної обробки даних, які застосовують словники, побудовані на бюджетних класифікаторах, доцільно щоби ETL-інструменти оперували із звітними документами, згрупованими за напрямами:

- Звіти про виконання доходної частини бюджетів всіх рівнів, включаючи й регіональні;
- Звіти про виконання видаткової частини бюджетів всіх рівнів, включаючи й регіональні;
- Звіти про фінансування бюджетів всіх рівнів за типом боргового зобов'язання;
- Звіти про заборгованості бюджетних установ.

Одним із засобів зменшення помилок в процесі вводу документів фінансової звітності є застосування **методу автоматичної ідентифікації та корекції типових помилок** (при визначенні назви показника P_z^{fip} та співставлені його коду). Метод засновано на використанні словника припустимих слів (словосполучень) та визначенні імовірності появи типових помилок. В якості словників для вищезазначених напрямів звітності використовуються відповідні бюджетні класифікатори: $\{BC_{inc}^{fip}\}$ - доходів бюджету; $\{BC_{\exp}^{fip}\}$ - видатків та кредитування бюджету; $\{BC_{fin}^{fip}\}$ - фінансування бюджету; $\{BC_{deb}^{fip}\}$ - класифікації боргу та боргових зобов'язань.

Враховуючи специфіку предметної області, слід нагадати, що деякі показники P_z^{fip} можуть мати назву, яка складається з кількох слів, наприклад, «**Податок на прибуток банківських організацій, включаючи філіали аналогічних організацій, розташованих на території України – 11020600».** Тобто при виникненні багатократних помилок таки висловлювання потребують семантичного аналізу. Крім того, поточне значення показника P_z^{fip} може містити неприпустимі символи або суттєве відрізнятися від припустимого діапазону значень. Тобто при вводі показника повинна виконуватися валідація показника - семантична перевірка на числове значення. Випадки валідації можуть бути пов'язані ні тільки з визначенням значень самого показника, а також з наявністю в звітах зайвих строк, колонок та інших непередбачених випадків. На рис. 4. наведений приклад наявності скритих колонок у звіті, який підлягає вводу до системи.

Отже, ймовірність $P(g)$ появи помилок при ідентифікації та валідації показника P_z^{fip} може бути викликана наступними умовами:

E_1 – появою однократної помилки (граматична помилка) в назві показника P_z^{fip} при співпадінні кодів показника із словником (відповідним бюджетним класифікатором);

E_2 – появою багатократних помилок в назві показника P_z^{fip} (скорочення, неприпустимі символи, помилковий регістр вводу тощо) при співпадінні кодів показника із словником (відповідним бюджетним класифікатором);

E_{cod} – невідповідністю назви показника P_z^{fip} його коду за бюджетною класифікацією;

E_{val} – появою неприпустимого значення показника P_z^{fip} - валідація показника не виконана.

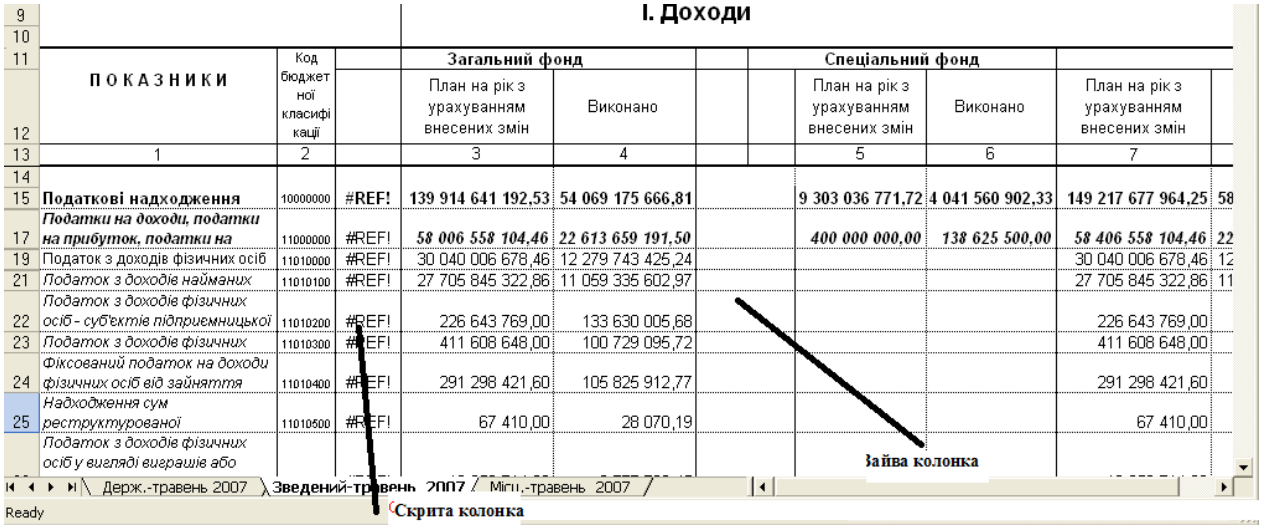


Рис. 4 Приклад наявності скритих колонок у звіті, які призводять до помилкової валідації

Сутність методу полягає в генерації V варіацій помилкового слова у визначеному звіті і перевірці припустимості значення варіації у назві показника P_z^{fip} з відповідним бюджетним класифікатором.

Залежно від обмежень словника (бюджетного класифікатора) для автоматичної ідентифікації показника та корегування помилок, а також валідації показника можуть бути запропоновані 4 основних алгоритми, а саме:

- Автоматичне коригування по варіації з максимальною імовірністю помилки;
- Автоматичне однозначне коригування по єдиній варіації, що співпала;
- Напівавтоматичне коригування за участю експерта по варіації, що відповідає максимальній імовірності помилки;
- Комбіноване коригування, як правило, виконується при виявлені помилок валідації показника або групи показників, причиною яких є також й технічні помилки (наприклад, вставки зайвих строк або колонок, що дуже часто трапляється у реальному житті).

Можливі такі загальні результати процесу ідентифікації та валідації показника:

$R_{AK}, R_{ПАК}$ - помилка правильно ідентифікована й автоматично (імовірність P_{AK}) або напівавтоматично (імовірність $P_{ПАК}$) виправлена;

$R_{РК}$ - помилка не ідентифікована, і вона виправляється «вручну» (імовірність $P_{РК}$);

$R_{ЛК}$ - помилка ідентифікована невірно і виправлена хибно (імовірність $R_{РК}$).

Визначення та аналіз значень $P_{АК}, P_{ПАК}, P_{РК}, P_{ЛК}$ для різних рішень (конкретних алгоритмів) є основною метою побудови відповідних логіко-імовірнісних моделей, які враховують особливості структури фінансового звіту. Логіко-імовірнісні моделі застосовувалися на методі побудови семантичних графів, які описують структуру можливих подій і визначають частки складових імовірностей виникнення типових помилок з урахуванням особливості кожного типу фінансового звіту.

Кінцевим результатом впровадження методу автоматичної ідентифікації, корекції та валідації типових помилок є формування спеціалізованих ETL інструментів, які враховують особливості кожного типу фінансового звіту і надають зручний інтерфейсі адміністратору даних. В реальної ситуації, документи, які надходять до системи, можуть містити десятки тисяч показників та бути представлені різноманітними типами даних – doc, xls, Access, що створює додаткові складнощі при їх обробці. З метою систематизації та приведення даних до єдиного типу, робочим типом прийнято дані в форматі MS Excel. Для конвертації даних з інших типів застосовуються серійні засоби, які здатні конвертувати дані типу doc або Access до формату MS Excel, для подальшого їх введення спеціалізованими ETL-інструментами.

Робочим середовищем, в якому реалізовані спеціалізовані ETL-інструменти, обрано MS Excel. У цьому контексті, кожної формі звіту відповідає МАКРОС, який виконує вісь цикл автоматичного введення даних звіту, починаючи з витягу даних, очищення від типових помилок, валідації даних та завантаження даних в реляційні таблиці БД фінансових показників в середовищі СУБД Oracle 11g. Кожний МАКРОС реалізує **метод автоматичної ідентифікації та корекції типових помилок** та налаштовується на особливості фінансового звіту, оскільки звіт може складатися з кількох частин (ЛИСТІВ).

На рис. 5. наведено приклад головного меню ETL-інструментів для введення звітів за різними формами видатків. Аналогічні засоби розроблені й для введення фінансових звітів за всіма вищепереліченими напрямами.

Занесення звітів про виконання бюджетів всіх рівнів до бази даних ФЕП		МАКРОСИ
ВВЕДЕННЯ ЗВІТІВ ПО ВИДАТКАХ ЗА КПК		
Для введення звіту про виконання видатків ДЕРЖАВНОГО бюджету за КПК натисніть "Виконати " та відкрийте файл W_ммрr.xls	Виконати	INPUT_EXPENS
ВВЕДЕННЯ ЗВІТІВ ПО ВИДАТКАХ ЗА КЕКВ		
Для введення звіту про виконання видатків ДЕРЖАВНОГО бюджету за КЕКВ по ЗАГАЛЬНОМУ фонду натисніть "Виконати " та відкрийте файл zvitrrмм.xls	Виконати	INPUT_ZAGKEK
Для введення звіту про виконання видатків ДЕРЖАВНОГО бюджету за КЕКВ по СПЕЦІАЛЬНОМУ фонду натисніть "Виконати " та відкрийте файл zvc_rrмм.xls	Виконати	INPUT_SPECKEK
Для введення звіту про виконання видатків ДЕРЖАВНОГО, ЗВЕДЕНОГО та МІСЦЕВИХ бюджетів за КЕКВ натисніть "Виконати " та відкрийте файл W_ммek.xls	Виконати	INPUT_BUDGKEK
ВВЕДЕННЯ ЗВІТІВ ПО ВИДАТКАХ ЗА КФК		
Для введення звіту про виконання видатків ДЕРЖАВНОГО, ЗВЕДЕНОГО та МІСЦЕВИХ бюджетів за КФК натисніть "Виконати " та відкрийте файл W_ммf.xls	Виконати	INPUT_BUDGKFK
ВВЕДЕННЯ ЗВІТІВ ПРО ВИКОНАННЯ ЗАХИЩЕНИХ СТАТЕЙ ВИДАТКІВ БЮДЖЕТУ		
Для введення звіту про виконання захищених статей видатків ДЕРЖАВНОГО бюджету натисніть "Виконати "та відкрийте файл ZAH_STррмм.xls	Виконати	INPUT_ZAHSTAT

Рис. 5. Приклад головного меню ETL-інструментів для введення звітів за різними формами видатків

Для ініціювання введення звіту адміністратор даних має натиснути на кнопку ВИКОНАТИ відповідної форми звіту та обрати відповідний файл. Далі виконується

автоматичне введення даних та занесення до відповідної БД у середовищі СУБД Oracle 11g. Фрагмент роботи інтерфейсу ETL-інструментів при налаштуванні на визначену форму звіту, показано на рис. 6.

Спеціалізовані ETL інструменти входять до складу системи моніторингу Рахункової палати України та встановлюються на робочому місці адміністратора даних. Станом на грудень 2015 року ETL інструменти дозволяють обробляти понад 30 різних форм фінансової звітності. Так, завдяки впровадженню спеціалізованих ETL-інструментів введення даних самий великий за обсягом звіт за доходами та видатками бюджетів всіх рівнів (понад 120000 записів/на місяць) виконується за 1 – 2 хвилини та завантажується до БД Oracle 11g. Ручне введення такої кількості показників з наступною їх верифікацією потребує декілька робочих днів.

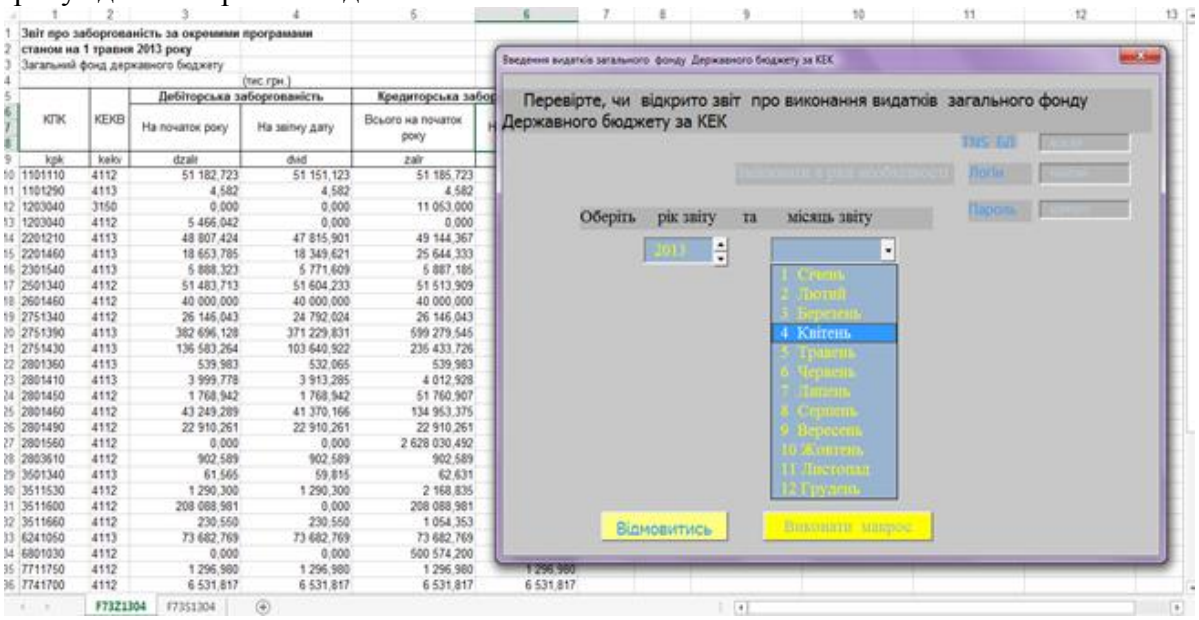


Рис. 6. Фрагмент роботи ETL інтерфейсу при введенні звіту

Метод аналізу даних бюджетних процесів

Користувачем системи моніторингу є людина, що приймає рішення. Природно вимагати від розроблюваної системи, щоб фахівець працював у звичних для нього умовах та оперував з даними у вигляді, приємному для сприйняття та осмислення. Методом, який дозволяє вирішити проблеми обробці багатовимірних даних (гіперкубів), є **метод реалізація типових сценаріїв поведінки експерта** без застосування занадто складних аналітичних процедур, які притаманні кубічним сховищам та OLAP-технологіям [17].

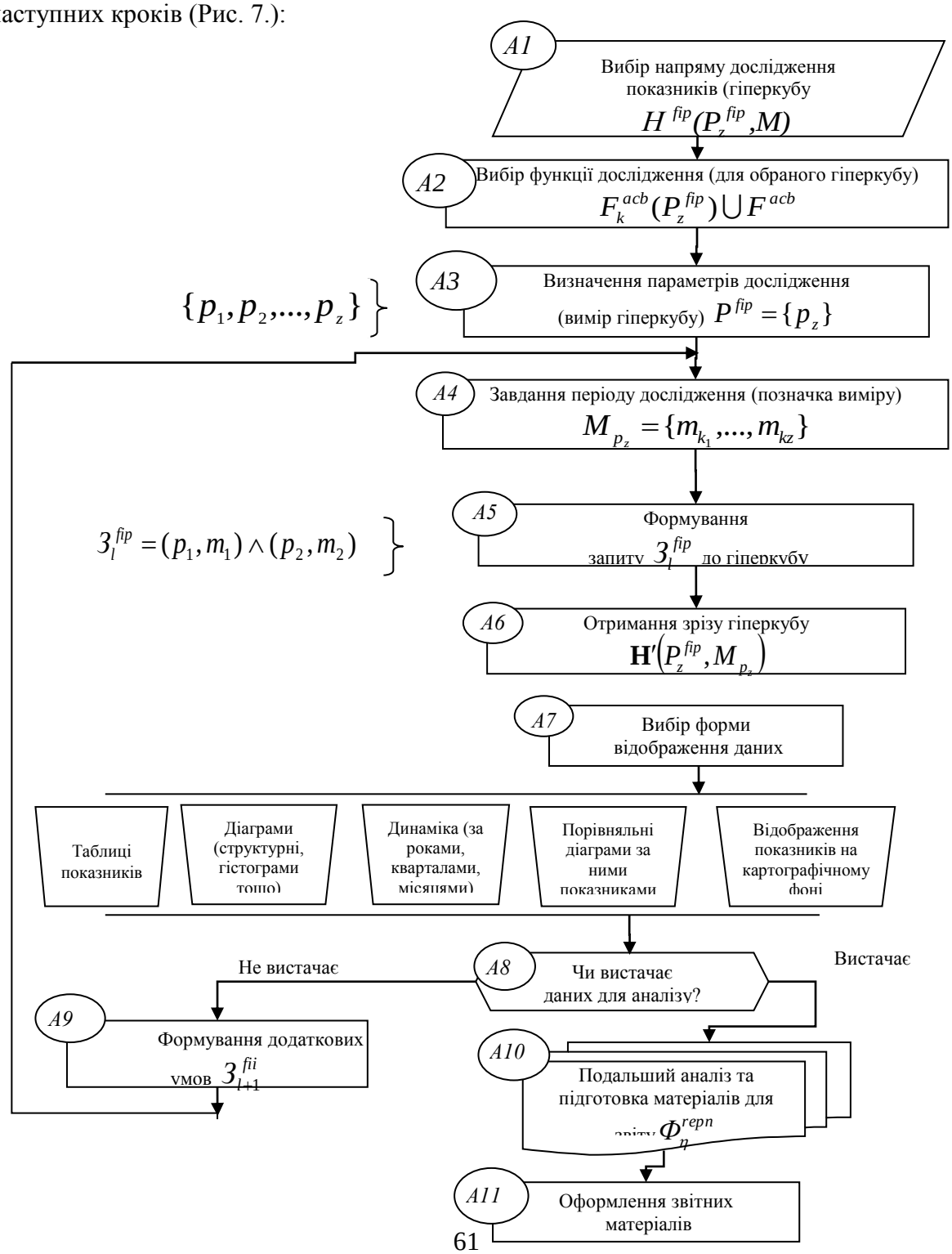
Іншим фактором, що впливає на комфортність роботи експерта, є час відгуку, який бажано мати настільки малим, щоб не встигали розмикатися асоціативні зв'язки, які виникають в аналітика в процесі осмислення проблеми. У більшості OLAP-систем процеси формування запитів до багатовимірних даних рознесені в часі та відокремлені від процедур відображення зрізів даних у зручному для сприйняття виді [20]. Тому запропоновано метод, який на відміну від існуючих методів, дозволяє об'єднувати процедури агрегації даних (формування зрізів гіперкубів) з процедурами їх візуалізації в одному програмному застосуванні для подальшого семантичного осмислення отриманих даних.

Такий підхід дає можливість представляти процес моніторингу у вигляді сукупності типових сценаріїв поведінки експерта при досліджені даних ПрО. Засобом досягнення цієї мети є інтуїтивно-зрозумілий інтерфейс, організований у такий спосіб, що **експерт оперує ні з базами даних або інформаційними ресурсами системи, а з типовими сценаріями аналітичної діяльності**, та отримує потрібні зрізи даних,

фактично, за один «дотик». Переваги такого підходу очевидні. Експерту надається Web-інтерфейс, якій віддзеркалює предметну область в цілому, тобто напрями дослідження, аналітичні функції, процедури маніпулювання даними.

Графічний інтерфейс користувача побудований у такий спосіб, що аналітик без використання мови програмування може формувати складний запит $З_l^{fep} = (p_1, m_1) \wedge (p_2, m_2)$ за будь-якими параметрами (бюджети, доходи, видатки, розписи, призначення, звіти, роки, квартали, коди показників КЕК, КФК, КВК в бюджетній класифікації) для вибірки потрібного для дослідження зрізу даних $\mathbf{H}'\left(P_z^{fip}, M_{p_z}\right) | \mathbf{H}' \subseteq \mathbf{H}$.

Типовий сценарій моніторингу та аналізу бюджетного процесу складається з наступних кроків (Рис. 7.):



Крок 1. Початком роботи застосування є вибір напряму дослідження фінансових показників (блок А1), тобто вибору проблемно-орієнтованого гіперкубу $H^{fip}(P_z^{fip},M)$. Наприклад, необхідно дослідити заборгованість бюджетних установ на звітну дату. Для цього застосування підключається до гіперкуб показників заборгованості бюджетних установ - $H_{deb}^{fip}(P_{db}^{fip},M)$.

Крок 2. У блоці А2, на підставі обраного гіперкубу, розкривається список типових функцій $F_k^{acb}(P_z^{fip})\bigcup F^{acb}$, доступних експерту при досліджені обраного напряму. Експерт визначає функцію моніторингу, наприклад, моніторинг фінансових зобов'язань $F_{deb}^{asb}(H_{deb}^{fip}(P_{obl}^{fip},M))$.

Крок 3. У блоці А3 та А4 визначається перелік показників $P_1^{fip}\wedge P_2^{fip}\wedge P_z^{fip}$ (наприклад, боргові зобов'язання РБК) та вимір $\{p_1,p_2,...,p_z\}$ за якими має виконуватися запит до гіперкубу та встановлюються позначки виміру $M_{p_z}=\{m_{k_1},...,m_{kz}\}$ (рік, квартал, місяць).

Крок 4. У блоці А5 формується автоматичний запит до сервера БД з визначеними параметрами $З_l^{fip}=(p_1,m_1)\wedge(p_2,m_2)$.

Крок 5. Далі (блок А6) сервер БД виконує витяг даних з визначеними параметрами запиту $З_l^{fip}=(p_1,m_1)\wedge(p_2,m_2)$ та передає дані $\mathbf{H}'\left(P_1^{fip},M_{p1}\wedge P_2^{fip},M_{p2}\wedge P_z^{fip},M_{pz}\right)$ на комп'ютер експерта для подальшого аналізу.

Крок 6. Після отримання зрізу даних $\mathbf{H}'\left(P_1^{fip},M_{p1}\wedge P_2^{fip},M_{p2}\wedge P_z^{fip},M_{pz}\right)$ (блок А7), експерт переходить до аналізу даних за допомогою спеціалізованих процедур, які дозволяють виконувати різні форми аналізу: у вигляді таблиць, гістограм, кругових діаграм, порівняльних діаграм, діаграм динаміки за кількаами вимірами, діаграм з прив'язкою до картографічної основи. Для зменшення надлишкової функціональності кількість аналітичних процедур корелюється з напрямом та функцією моніторингу. Наприклад, процедура відображення даних на картографічному фоні притаманна тільки дослідженням місцевих бюджетів у регіональному розрізі – гіперкуб $H_{rb}^{fip}(P_{rb}^{fip},M)$.

Крок 7. У блоці А8 здійснюється оцінка якості аналізу на отриманому зрізі даних. Якщо ціль аналізу не досягнута – здійснюється перехід до блоку А9 для завдання додаткових умов формування зрізу, наприклад, з іншим періодом дослідження $M_{p_z}^{new}=\{m_{k_1},...,m_{kz}\}$. Якщо даних вистачає – перехід до блоку А10.

Крок 8. У блоці А9 виконується формування нового періоду дослідження з позначкою $M_{p_z}^{new}=\{m_{k_1},...,m_{kz}\}$, наприклад, для порівняння показників за роками в іншому періоді.

Кроки 3 – 8, як правило, виконуються в циклі, доки не отримаємо зріз даних $\mathbf{H}'\left(P_1^{fip},M_{p1}\wedge P_2^{fip},M_{p2}\wedge P_z^{fip},M_{pz}\right)$, якій задовольняє умовам аналізу.

Крок 9. Кінцевим кроком типового сценарію аналітичної діяльності є експорт даних до обраної форми звіту – Φ_{η}^{rep}: доповідна записка, звіт, аналітична довідка, експертний висновок та інші.

Цикл повторюється для всіх актуальних показників. Після завершення моніторингу показників виконується генерація узагальненого звіту. Як правило, узагальнений звіт містить як текстові, так і графічні фрагменти аналітичних матеріалів.

Система моніторингу входить до складу інформаційно-аналітичної системи Рахункової палаті України. ПЗ моніторингу реалізовані за технологією «клієнт – Intranet-сервер – сервер баз даних». Дані зберігаються на сервері БД під керуванням СУБД Oracle 11g, яка забезпечує їх цілісність, збереження та доступ (на запис, корегування або читання) згідно з повноваженнями кожного користувача. Intranet-сервер обслуговує запити з метою отримання зрізів даних від сервера БД, проводить необхідні обчислення і перетворення інформації, формує та публікує у власній файловій системі Web-сторінку, яка відображається на АРМі користувача стандартними засобами WEB-браузера (Microsoft Internet Explorer). Оскільки обсяг БД моніторингу постійно зростає та за станом на рпень 2015 року становить більш 15 000 000 записів, для прискорення обміну використовуються сучасні Web-браузери Internet Explorer 9, 10, 11. Цей Web-браузер оснащений новим движком JavaScript «Chakra», що збільшує продуктивність виконання сценаріїв на мові JavaScript в окремих випадках до 10 разів у порівнянні з Internet Explorer 6. Web-браузер також оснащений процесором підтримки мови ECMAScript 5, яка застосовується як мова опису сценаріїв взаємодії різноманітних Web-сервісів.

Висновки

Запропоновано інформаційну модель моніторингу виконання держбюджету, яка відрізняється від «детермінованих» моделей тим, що враховує особливості національного устрою бюджетних процесів (змінюваність у часі організаційної структури суб'єктів процесу, номенклатури і контенту інформаційних ресурсів) та забезпечує порядок здійснення аналізу бюджетного процесу на всіх стадіях.

На підставі інформаційної моделі визначено структуру аналітичного ядра системи моніторингу та запропоновано методи семантичної обробки даних, які враховують особливості предметної області, а саме:

Удосконалений метод оперативного аналізу даних дозволяє поєднати процедури формування OLAP-зрізів даних за будь-якими вимірами з широким спектром процедур візуалізації даних (включаючи картографічну основу).

Метод автоматичної ідентифікації та корекції типових помилок, на базі якого розроблено спеціалізовані ETL-інструменти витягу, очищення, валідації та завантаження показників виконання держбюджету, що дозволяє в автоматичному режимі виконувати введення даних фінансових звітів, які містять сотні тисяч показників.

Результати випробувань ПЗ на базі типових сценаріїв поведінки експерта показали підвищення швидкості обробки багатовимірних даних до 20 разів у порівнянні з роздільним методом обробки.

Представлені результати досліджень є базою для подальшої розробки та реалізації вторинних, у тому числі прогнозних, сценаріїв аналізу бюджетного процесу в Україні.

Література

1. Назаренко О.О., Михайленко Ю.В. Автоматизація аудиту в Україні: підходи і програмне забезпечення http://www.rusnauka.com/2_KAND_2009/Economics/39554.doc.htm

2. Івахненков С.В. Інформаційні технології в аудиті та внутрішньогосподарському контролі [Электронный ресурс] http://www.ivakhnenkovaudit.info/IvakhnenkovDoctOfSciences.pdf
3. Gartner research: available at http://www.gartner.com/technology/home.jsp
4. Forrester Research: available at https://www.forrester.com/home/
5. Шмаков А. Сервис-ориентированный подход в бизнес-аналитике от Oracle Электронный ресурс] // – Режим доступу до журн.: http://citforum.ru/database/oracle/soaway/
6. Чубукова И.А. Data Mining: [учебное пособие] / Чубукова И.А. — 2-е изд., испр. — М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2008. — 382 с. — (Серия «Основы информационных технологий»)
7. Бюджетний Кодекс України [Электронный ресурс] http://zakon1.rada.gov.ua/laws/
8. Методы анализа и прогнозирования, применяемые в процессе исполнения бюджета в США http://bujet.ru/article/22524.php
9. Анализ исполнения сводного бюджета http://www.cis2000.ru/cisBudgetingTwo/
10. "Финансовая модель и архитектура системы бюджетирования» http://www.intellect-capital.ru/text/69.htm
11. Анализ зарубежного опыта организации исполнения бюджета http://bibliofond.ru/view.aspx
12. Джозеф Джарратано, Гари Райли, Экспертные системы: принципы разработки и программирование, 4-е издание, Пер. с англ. – М.: Издательский дом "Вильямс", 2007. – 1152 с.:
13. David J. DeWitt, Ph.D.; Samuel Madden, Ph.D.; Michael Stonebraker, Ph .D How to Build a High-Performance Data Warehouse : available at http://db.csail.mit.edu/madden/high_perf.pdf
14. Коваль О.В., Сенченко В.Р., Построение системы анализа выполнения госбюджета на основе сценарного похода // Сборник тезисов 14-ой международной научно-технической конференции «Системный анализ и информационные технологи» SAIT 2012, - К.: ИПСА НТУУ «КПИ», 2012 – 202-203 сс.
15. Мелащенко А.О. Использование технологий ETL и OLAP в анализе финансовых организаций http://dep145.org.ua/ru/node/153
16. Обзор ETL- и ELT-инструментов для обработки данных http://www.ibm.com/developerworks/ru/library/bd-hivetool/
17. Реализация OLAP http://www.basegroup.ru/library/dw_olap/olap_core_part2/

СПЕЦІАЛЬНА БЕЗПЕКА

УДК 330:631.1

І.М.Демчак, директор НДІ ”Украгропромпродуктивність”,
О. П. Кучеров, к. ф.-м. н., с.н.с., завідувач лабораторії,
О.П.Савицька, завідувач відділом НДІ ”Украгропромпродуктивність”

ЕКОНОМІКО-МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ СІЛЬСЬКИХ НАСЕЛЕНИХ ПУНКТІВ ЯК ОСНОВА ДЛЯ ФОРМУВАННЯ АГРАРНОЇ ПОЛІТИКИ

В роботі запропоновано методику математично точної об’єктивної категоризації сільських населених пунктів по кожному з показників паспорту методом економіко-математичного моделювання,для ефективного управління сільськими територіями та формування аграрної політики.
Ключові слова: *паспортизація сільських населених пунктів, структурні числа, економіко-математичне моделювання.*

В работе предложена методика математически точной объективной категоризации сельских населенных пунктов по каждому из показателей паспорту методом экономического и математического моделирования, для эффективного управления сельскими территориями и формирования аграрной политики.
Ключевые слова: паспортизация сельских населенных пунктов, структурные числа, экономико-математическое моделирование.

Mathematically exact objective categorizing of rural settlements methodology is offered on each of the passport’s indexes by the method of economic and mathematical design, for an effective management and forming of agrarian politics rural territories.
Keywords: passport system of rural settlements, structural numbers, economic and mathematical design.

Постановка проблеми. Сільськогосподарський і сільський розвиток - ключова сфера політики України. Формування аграрної політики неможливо здійснити без попереднього ґрунтовного моделювання сільських поселень. Моделювання дозволяє уточнити концептуальні положення, деталізувати, визначити вузькі місця, відхилення від концептуальних засад, оцінити їх масштаби та загрози для реалізації всього комплексу заходів. Проведення моделювання дозволяє здійснити аналіз сукупності сільських поселень, визначити їх спільності та відмінності, прорахувати профіль сільських поселень та розробити рекомендації до законодавства, у першу чергу бюджетного, у частині розроблення соціальних нормативів на базі модельних сільських поселень.

Аналіз останніх джерел і публікацій. Аграрну систему слід розглядати як суцільний соціально-економічний комплекс, який має в своєму складі не лише природні елементи (матеріальні об’єкти), але і колективи людей, що виконують певні функції, приймають управлінські рішення. Потрібне створення міжнародної статистичної бази даних для економіко-математичного моделювання і категоризації сільських територій по всьому комплексу параметрів.

Це задача інтернаціонального рівня і для її вирішення потрібні об’єднані зусилля декількох країн. Тому рішення цієї проблеми почали шукати зусиллями Організації економічного співробітництва та розвитку (OECD) англ. Organisation for Economic Co-operation and Development — це міжнародна організація, що об'єднує 34 країни світу, більшість з яких є країнами з високим доходом громадян та високим рівнем життя і мають

статус розвинених економік. Місія організації полягає в підтримці політики, яка поліпшить економічне і соціальне благополуччя людей у всьому світі. Докладніше дивиться на сайті: www.oecd.org.

В результаті було створено проект: Створення Сільських Індикаторів для Формування Аграрної Політики (Creating Rural Indicators for Shaping Territorial Policies) – це піонерська робота, яка направлена на створення міжнародної статистичної бази даних для класифікації міжнаціональних територій. Вона повинна дати змогу робити обчислення наборів територіальних індикаторів розвитку, щоб виявити величезну різноманітність демографічних, економічних, соціальних і екологічних умов і тенденцій, зазвичай прихованих. З'єднані міжнаціональні економіко-математичні моделі і індикатори дозволять робити порівняння, покращать аналітичні можливості і прозорість і таким чином сприятимуть більш ефективному формуванню аграрної політики.

На Рис.1 наведено перелік ключових проблем і тем, для яких повинні збиратися територіальні дані і робитися індикатори для того, щоб сприяти управлінню прогресом у напрямку до інтегрального життєздатного розвитку країн в межах OECD і поза спільнотою (наприклад Франція) [6].

Територіальні *повинні надати*	**Індикатори** *інформацію по:*
ЕКОНОМІЧНІ	**СОЦІАЛЬНИЙ**
СТРУКТУРИ & МОДЕЛІ	*ЗАБЕЗПЕЧЕНІСТЬ&БЛАГОПОЛУЧЧЯ*
Продуктивність	Прибуток і Бідність
Зростання виробництва	Праця і Зайнятість
Інвестиції	Освіта і Кваліфікація
Нововведення	Здоров'я і Безпека
Регіональна взаємодія	Культура і Суспільство
ДЕМОГРАФІЧНИЙ	**ЕКОЛОГІЧНИЙ**
НАРОДЖУВАНІСТЬ & МІГРАЦІЯ	*ЯКІСТЬ & БЛАГОУСТРІЙ*
Щільність	Топографія і Клімат
Природний баланс	Ґрунти, Вода, Різновиди
Юність і Старіння	Житла і Ландшафти
Міграція	Поселення і Устаткування
Сім'я	Культурна спадщина
Дають інтегральну оцінку умов розвитку і тенденцій	

Рис.1. Територіальні індикатори - ключові проблеми і теми [6].

Категоризація сільських населених пунктів і їх адміністративно-територіальних об'єднань за показниками є базовою проблемою для кожної країни світу.

Виконання цієї програми різними країнами проводиться в різних напрямках, розглянемо їх.

1.Господарська діяльність, у тому числі сільське господарство: В рамках проекту OECD при дослідженні господарської діяльності пропонується брати до уваги високий ступінь спеціалізації економічного розвитку сільського господарства в "традиційних" сільських областях, та велике різноманіття господарської діяльності з відповідною вагою секторів послуг в "сучасних" сільських областях. Щоб описати економічний профіль області розглядаються такі чинники, як пересіченість землі (пагорби, передгір'я, схили, яри, каміння таке інше), зайнятість населення, особливості виробництва, продукція і використання землі (Cecchi, Sweden; Bryden, Luxembourg; FAO, Italy)[15,16,17,18,19].

2.Соціально-економічні структурні характеристики: Інші дослідники пропонують використовувати соціо-економічні (Socio-economic) структурні характеристики, такі як, наприклад, інфраструктури (Plessis, Canada; Albrecht, Norway)[20,10] або людський капітал (Cecchi, Sweden)[15]. Освітній рівень населення в області - один з вимірів, що характеризує людські ресурси і професійний рівень.

3.Просторовий вимір соціальної інфраструктури: індикатори ґрунтуються на просторовому вимірі соціального життя, бо в сільських областях відстані більші, а можливості нижчі відносно міських областей (Plessis, Canada; UNECE, Switzerland; Albrecht, Norway)[20,22,10]. Це робить послуги менш доступними. В цьому випадку знайти адекватну і зручну модель не завжди легко, тому автори, що пропонують цей підхід, використовують декілька альтернативних моделей. Беруться відстані до певних ключових послуг, кількість послуг на квадратний кілометр або на душу населення.

4.Природні характеристики: Деякі дослідники пропонують розглядати природні характеристики земної поверхні і довкілля. На приклад -European Joint Research Centre (JRC) Європейський Об'єднаний Центр Досліджень пропонує базуватися на територіальній класифікації, яка розглядає територіальні профілі (рілля, пасовища, ліс, і т.п.), пересіченість місцевості (гора, пагорб, яр, долина) і сприятливість клімату (Gallego, Italy; Vard, Belgium) [23,24]. Сільські області головним чином мають сільськогосподарські землі, ліси і невигідні області для людської діяльності(гора, екстремальні умови клімату, і т.п.). Ідея полягає в тому, що природне довкілля значно диференціює людські можливості і його поведінку і, з цього приводу, сільські області повинні бути глибоко різним. Важливим є втручання у біосферні процеси через впровадження людиною культурного землеробства – заміна частини природних біогеоценозів на штучні. З введенням культурного землеробства виникає новий тип чинників – агроекосистеми (Рамад;РФ) [5].

5.Інтегральний критерій: Інший шлях розвитку – представити інтегральний критерій, який складається з декількох критеріїв або змінних для територіальної класифікації, як додаток до щільності населення. Прикладом є національна статистика Великобританії, де для визначення 8 сільських / міських типів поселень використовується 8 чинників (DEFRA, UK; Bibby, UK)[13,14].

Територіальні угрупування виробників поєднаних спільною діяльністю прийнято називати кластерами. Актуальним на сьогодні є створення кластерів для зростання виробничих потужностей територій, стимулювання їхнього технічного прогресу та підвищення конкурентоспроможності регіонів. Світовий і український досвід демонструє низку переваг виробничих систем, побудованих на основі кластерної моделі. Кластери будуються на використанні ефекту масштабу сільських територій. Кластери - це точки зросту, стимулятори технічного прогресу, які являють собою механізм підвищення регіональної і національної конкурентоспроможності (Кропівко, Україна)[4].

З наведеного можна побачити, що в рамках проекту OECD Створення Сільських Індикаторів для Формування Аграрної Політики було залучено фахівці з багатьох країн світу, виконаний величезний об'єм роботи, але цей проект поки що не привів до своєї мети: створення єдиної всеохоплюючої системи моделей і індикаторів сільських територій, що сумісно сприяють формуванню аграрної політики. Така задача є грандіозною і для її вирішення у вище названих авторів не вистачило потужностей інформаційної системи.

Із викладеного випливає, що для ефективного управління сільськими територіями перш за все слід вирішити проблему категоризації сільських населених пунктів по кожному з показників.

Вирішення такої задачі можливо, як що використовувати суцільну паспортизацію сільських населених пунктів, що була проведена на Україні за 2005 і 2010 роки, і єдину аналітичну інформаційну систему, яка створена НДІ «Украгропромпродуктивність».

Метою роботи є на основі всієї сукупності показників паспортів сільських населених пунктів України шляхом економіко-математичного моделювання знайти методику математично точної та об'єктивної категоризації сільських населених пунктів по кожному з показників паспорту, для ефективного управління сільськими територіями та формування аграрної політики.

Основні результати дослідження. Наведений вище аналіз створення надто великої бази даних показав, що переліченим вище організаціям не вдалось знайти єдиний підхід до створення системи індикаторів через перешкоду, яка в кібернетиці добре відома під назвою «інформаційний вибух». Погодимося, що швидкодія сучасних комп'ютерів достатньо велика; об'єм пам'яті комп'ютерів теж достатній.

Проблема полягає в тому, що бази даних побудовані просто у вигляді таблиці, а доступ до даних побудовано у вигляді натурального ряду чисел. Водночас проблема полягає в тому, що об'єктивна реальність (включаючи економічні та соціальні утворення) не описується двовимірною таблицею (якою є бази даних) і вказівником не є натуральний ряд чисел. Об'єктивна реальність має форму ієрархічно організованої системи із відповідною структурою, вказівником до якою є структурні числа.

Для вирішення цих двох проблем в НДІ «Украгропромпродуктивність» було розроблено систему управління базами даних нового покоління, в архітектурну основою якої покладено теорія знань. А доступ до даних реалізовано на структурних числах, які використовуються у вигляді індексів адміністративно територіальних одиниць.

Паспорт сільського населеного пункту включає 16 розділів, в тому числі і 4 розділи з переліку OECD, який представлено на рис.1.

База даних охоплює 930 соціально-економічних показників за 2005 і 2010 роки для 25 тисяч сільських населених пунктів, всього біля 50 мільйонів значень. Аналітична інформаційна система «Село» дозволяє створити біля 50 мільйонів різних таблиць, діаграм та картограм які в різних ракурсах характеризують стан та динаміку сільських населених пунктів.

Було прийнято рішення щодо розробки аналітичної інформаційної системи «Село» (АІС «Село»), яка дала б можливість визначати та прогнозувати пріоритети соціально-економічного стану кожного сільського населеного пункту України, розробляти регіональні програми розвитку сільських територій [1].

Ядром АІС «Село» є процесор, який виконує операції із структурними числами. Основою аналітичної інформаційної системи «Село» є дві структури знань. Перша – структура класифікаторів показників, що групуються в розділи та підрозділи. Друга – структура адміністративно-територіального устрою сільських територій, яка вимагає узагальнення даних у відповідності із цим устроєм. Ці структури містяться в базах знань і управляються методами математики структурних чисел, запропонованої автором [3]. Методологічні переваги такого підходу – системність бачення подій у стані та трансформації села, врахування різноманіття показників.

Структура адміністративно-територіального устрою сільських територій задається геоінформаційними координатами, які вперше були запропоновані І. М. Демчаком [2] і задають повну і однозначну підпорядкованість кожного об'єкта на кожному адміністративно-територіальному рівні. Основу системи складають 4 вісі координат wxyz, де кожна вісь описує свій адміністративний рівень. А саме, w описує області; x описує райони; *y* описує сільські ради; z описує села. Разом із функцією адресації геоінформаційні координати дозволяють а) автоматично узагальнювати дані шляхом проекції об'єктів на відповідну вісь; б) автоматично створювати ієрархічний пошуковий інтерфейс.

Система геоінформаційних координат дозволяє працювати як з первинними даними на рівні села, так і з узагальненими даними на всіх макроекономічних рівнях в розрізі держави, області, району і сільської ради. Запропонована система поєднує мікро і

макроекономіку в єдине ціле, що безумовно дасть потужний поштовх розвитку економічної науки. Далі скористаємось цим механізмом для економіко-математичного моделювання показників на всіх адміністративно-територіальних рівнях одночасно.

Головна панель аналітичної інформаційної системи «Село» показана на рис. 2, яка складається з наступних елементів управління. Панель вибору 2005 або 2010 року, ліворуч. Панель вибору показника, в середині, охоплює 930 показників. Панель вибору адміністративно-територіальної одиниці, всього 40689 областей, районів, сільських рад, сіл.

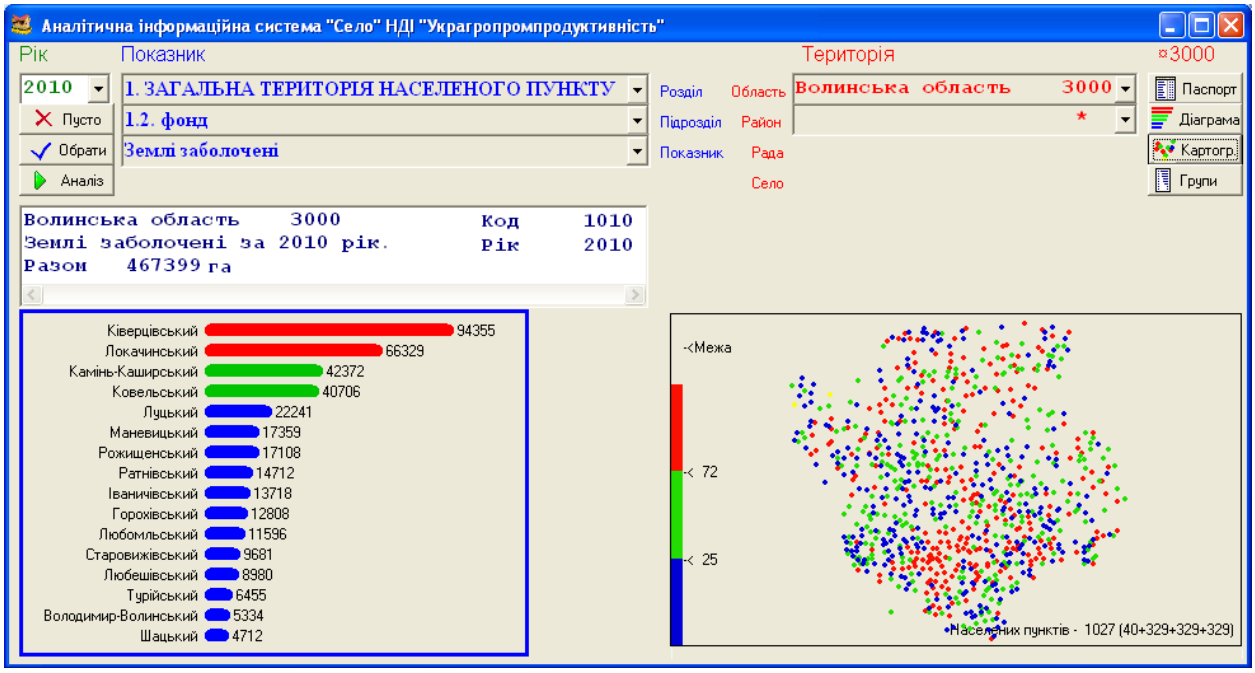


Рис.2. Робоча панель аналітичної інформаційної системи «Село».

Після визначення параметрів аналітична інформаційна система «Село» робить аналіз і результат надає у вигляді діаграми, ліворуч, або у вигляді картограми, праворуч. Система надає таблицю з показниками і автоматично будує картограму по будь-якому обраному показнику. На картограмі кожне село області помічається крапкою одним з чотирьох кольорів. Колір характеризує групу, до якої належить село.

Проведення наукових досліджень за допомогою аналітичної інформаційної системи «Село» на протязі року в 25 наукових центрах України показало, що система дозволяє провести суцільну класифікацію сільських населених пунктів і територій по кожному з 930 показнику. Дуже важливим є той факт, що знайдено спосіб класифікації єдиний для всіх чинників і територій – це економіко-математичне моделювання методом процентилей. Викладемо суть методу, що пропонується.

Розрахунок процентилей. Моделювання є одним з основних засобів наукових досліджень в економіці. Для вирішення поставленої задачі було проведено дослідження методів кореляції, регресії, медіани, моментів, лінійного програмування. Серед цих методів найбільш стійкою до шумів і до наявності не надійних даних є медіана, або процентиль. В економіко-математичному моделюванні процентиль широко використовується, наприклад в MS *Excel* це функція =ПЕРСЕНТИЛЬ(). Її можна використовувати, як критерій категоризації об'єктів дослідження.

Для дослідження візьмемо значення показника в сільському населеному пункті і позначимо його через ***X***. Відповідно до методики розрахунку процентилей всі сільські

населені пункті України впорядковувались за зростанням показника ***X***. Операція виконувалась методом спливаючих бульбашок (Sorting by Exchanging) через його простоту і поширеність. В результаті кожен об'єкт множини отримав свій порядковий номер ***n*** (***n=1.., N***), який визначає кількість об'єктів з показником меншим за X_n.

Цікавим є критерій X_n номером ***n=0.5N,*** це 50-та процентиль, яку називають медіаною ділить всі об'єкти на дві однакових за кількістю групи з низькими та високими значеннями показника ***X***.

Дослідження, результати яких будуть наведені далі, показали, що оптимальним є ділення на 5 категорій. Аналогічно тому, як поділені готелі, кожен з яких має від однієї до п'яти зірочок.

Проведення наукових досліджень за допомогою аналітичної інформаційної системи «Село» на протязі року в 25 наукових центрах України показало, що система дозволяє провести суцільну класифікацію сільських населених пунктів і територій по кожному з 930 показнику. Було перевірено методи кореляції, регресії, моментів, лінійного програмування та нелінійного програмування. В результаті було знайдено, що існує єдина модель, яка дозволяє зробити класифікації всієї сукупності населених пунктів по всіх показниках паспортизації. Це ділення всіх об'єктів на 5 категорій. Критерії, що категоризують поселення задаються 20-тою, 40-вою, 60-тою, 80-тою процентилями (P_{20}, P_{40}, P_{60}, P_{80}). Особливістю такого ділення є те, що кількість поселень кожної категорії за визначенням є константою, і дорівнює 20%. Очевидно, що по кожному показнику межі будуть різні і поселення будуть належати різнім категоріям.

Категорія надається за наступними критеріями: ***надмалі*** поселення з показником ***X*** меншими ніж P_{20}; ***малі*** поселення з показником ***X*** в межах від P_{20} включно до P_{40}; ***середні*** поселення з показником ***X*** в межах від P_{40} включно до P_{60}; ***великі*** поселення з показником ***X*** в межах від P_{60} включно до P_{80}; ***надвеликі*** поселення з показником ***X*** в межах від P_{80} і більше.

На цей час розпочата робота по знаходженню 20, 40, 60, 80-тої процентилей для кожного з 930 показників і наданню відповідної категорії для кожного сільського населеного пункту України. Тобто по кожному показнику в паспорті будуть знайдено критерії і кожному поселенню надана відповідна категорія.

Перелік показників паспорту сільських населених пунктів по яких планується зробити моделювання по розділу 1 "Загальна територія пункту" та розділу 2 "Соціально-демографічна характеристика" наведено в таблиці 2.

Таблиця 2.

Показники розділу 1 "Загальна територія пункту" та розділу 2 "Соціально-демографічна характеристика" для моделювання.

Розробник	Шифр	Показник
НДЦ «Південь-агропромпродуктивність»	1010	площа населеного пункту,га
НДЦ «Лісостеп- агропромпродуктивність»	1033	перелоги
НДЦ «Волинь-агропромпродуктивність»	1050	заболочені землі
НДЦ «Степ-агропромпродуктивність»	1030	Сільськогосподар-ські земелі
НДЦ «Донецьк- агропромпродуктивність»	1031	Сільськогосподарські угіддя
НДЦ «Полісся- агропромпродуктивність»	1041	лісові землі
НДЦ «Закарпат-агропромпродуктивність»	1036	пасовища
НДЦ «Запорізьк - агропромпродуктивність»	3010	населення, зайнятого в усіх сферах діяльності
НДЦ «Івано-франківськ-агропромпродуктивність»	3023	населення,зайняте в особистих селянських господарствах
НДЦ «Київ- агропромпродуктивність»	1150	землі запасу

НДЦ «Кіровоград-агропромпродуктивність»	1170	Зрошувані землі
НДЦ «Луганськ- агропромпродуктивність»	3020	населення, зайняте в сільському господарстві
НДЦ «Львів-агропромпродуктивність»	1190	власники землі та землекористувачі
НДЦ «Миколаїв-агропромпродуктивність»	1060	землі водного фонду
НДЦ «Одес- агропромпродуктивність»	16020	вулиці по селу
НДЦ «Полтав-агропромпродуктивність»	3140	зайняті в соціальній сфері
НДЦ «Рівне- агропромпродуктивність»	1210	земельних паїв
НДЦ «Суми- агропромпродуктивність»	1240	грошова оцінка землі
НДЦ «Захід агропромпродуктивність»	1250	розмір орендної плати
НДЦ «Харків- агропромпродуктивність»	16002	відстань до районного центру
НДЦ «Херсон- агропромпродуктивність»	1170	Зрошувані землі
НДЦ «Хмельницк-агропромпродуктивність»	1260	надходження до місцевого бюджету
НДЦ «Черкаси- агропромпродуктивність»	2010	кількість домогосподарств
НДЦ «Чернівці- агропромпродуктивність»	2030	чисельність постійного населення
НДЦ «Чернігів-агропромпродуктивність»	1035	сіножаті

Запропонований в роботі механізм став можливим завдяки загальній паспортизації, з одного боку, та геоінформаційним координатам, з іншого.

Розроблена система дозволяє виконувати аналіз паспортів сільських населених пунктів та використовувати ці результати для розроблення регіональних програм розвитку, визначення обсягів та джерел фінансування.

Надання кожному сільському населеному пункту категорії, яка об’єктивно оцінює його положення в державі, дасть можливість в кожному конкретному випадку застосовувати оптимальний механізм управління і, відповідно, максимізувати соціально-економічний ефект з мінімальними затратами при формуванні аграрної політики.

Висновки та наступні дослідження. На основі економіко-математичного моделювання кожному селу України пропонується надати одну з 5 категорій і запропоновано механізм управління адміністративними одиницями, оснований на відхиленні від стандарту в 20%. За допомогою запропонованого механізму було досліджено стан областей і районів.

Запропонований в роботі механізм став можливим завдяки загальній паспортизації, з одного боку, та геоінформаційним координатам, з іншого.

Економіко-математичне моделювання, запропоноване в даній роботі на нашу думку є плідним, оскільки воно є першим кроком зробити категорізацію сільських населених пунктів по кожному з показників, як це передбачено програмою OECD.

Другим кроком для ефективного управління сільськими територіями перш за все слід зробити класифікації сільських населених пунктів по кожному з показників, надати кожному об’єкту сукупність категорій, які дозволяють робити порівняння, покращують аналітичні можливості та прозорість, сприяють управлінню прогресом у напрямку до інтегрального життєздатного розвитку сільськими поселеннями.

На підставі проведених досліджень заплановано провести математичне моделювання сільських населених пунктів по цілому ряду показників. Після узагальнення результатів моделювання буде запропоновано блок територіальних індикаторів функціонування сільських територій України.

Література

1. Демчак І.М., Кучеров О.П., Савицька О.П. Аналітична інформаційна система "Село" // Продуктивність агропромислового виробництва. – 2012. – №21. – С. 45–52.
2. Демчак І.М., Кучеров О.П., Риженко Ю.Є. Організація знань як засіб управління сільськими територіями. // ІІІ міжнародний форум «Проблеми розвитку інформаційного суспільства» 20-23 листопада 2012 р., м. Київ – 2012. – Матеріали частина І. – С. 33–37.
3. Кучеров О.П. Теорія управління економікою знань. – К.: НДІ «Украгропромпродуктивність», 2008. – 260 с.
4. Кропивко М. Ф. Концептуальний підхід до кластерної організації та управління розвитком агропромислового виробництва / М. Ф. Кропивко // Економіка АПК. - 2010. - № 11. - С. 3-13.
5. Рамад Ф. Основы прикладной экологии: воздействие человека на биосферу. – Л.: Гідрометеоиздат, 1981. – 543 с.
6. OECD (1994) Creating Rural Indicators for Shaping Territorial Policies, OECD Publications, Paris, France.
7. Lenders, S., Lauwers, L. and Kerselaers, E. (2007) Rural-Urban Delimitation. A Statistical Analysis , ILVA, Merelbeke, Belgium.
8. EC (1999) CORINE Land Cover. Technical Guide, GI&GIS, Luxemburg.
9. Vard, T., Willems, E., Lemmens, T. and Peters, R. (2005) Use of the CORINE Land Cover to Identify the Rural Character of Communes and Regions at EU Level, in Trends of some Agri-environmental Indicators in the EU, Report of the European Commission, Brussels, Belgium.
10. Albrecht, W. (2006) Experiences with Grids at Eurostat, Nordic Forum for Geo-statistics, Kongsvinger, Norway.
11. EUROSTAT (2005) Nomenclature of Territorial Units for Statistics NUTS. Statistical Regions of Europe, Website, Luxemburg. 7. EUROSTAT (2007) European Regional and Urban Statistics. Reference Guide, Luxemburg.
13. DEFRA (2005) Rural and Urban Area Classification 2004. An Introductory Guide, London, UK.
14. Bibby, P., Shepherd, J. (2005) Developing a New Classification of Urban and Rural Areas for Policy Purposes – the Methodology, DEFRA, London, UK.
15. Cecchi, C. (1999) Contextual Knowledge and Economic Exclusion in Rural Local Systems, How to be Rural in Late Modernity, European Society for Rural Sociology XVIII Congress, Lund, Sweden.
16. Bryden, J. (2001) Section 3: Rural Development, in Proposal on Agri-Environmental Indicators (PAIS), Landsis, Luxembourg.
17. FAO (1986) Population and the Labor Force in Rural Economies, Economic and Social Development Paper, No. 59, Rome, Italy.
18. FAO (1993) Rural Poverty Alleviation. Policies and Trends, Economic and Social Development Paper, No. 113, Rome, Italy.
19. FAO (2005) World Program for the Census of Agriculture 2010. A System of Integrated Agricultural Censuses and Surveys, Rome, Italy.
20. Plessis, V., Beshiri, R. and Bollman, R. (2001) Definitions of "Rural", Statistics Canada, Ottawa, Canada.
21. Plessis, V., Beshiri, R. and Bollman, R. (2001) Definitions of Rural, Statistics Canada, Ottawa, Canada.
22.UNECE, FAO, OECD, World Bank (2005) Rural Household's Livelihood and Well-Being:Statistics on Rural Development and Agriculture Household Income, Handbook, Geneva, Switzerland.
23. Gallego, F. J. (2004) Mapping Rural/Urban Areas from Population Density Grids, Institute for Environment and Sustainability, JRC - EC, ISPRA, Italy.

УДК 616.314-76.613

О. П. Кучеров, к. ф.-м. н., с.н.с., завідувач лабораторії,
С.Є. Лавровський, д.псі.н., професор.
Агентство спеціальної безпеки.

ПІКОСКОП, ЯК ІНСТРУМЕНТ ДЛЯ ВИВЧЕННЯ АТОМАРНОЇ СТРУКТУРИ МОЛЕКУЛ

В роботі представлено унікальний електронний пікоскоп з супердифракційною роздільною здатністю, яка складає 10 пикометрів. В роботі вперше отримано зображення форми окремої молекули в деталях, яка складається з електронних оболонок. Першою молекулою, зображення якої отримано пікоскопом, є молекула пентана C_5H_{12}, яка повністю співпадає з відомою реконструкцією цієї молекули. Супердифракційна роздільна здатність отримана за рахунок опорного зображення з подвійною дифракцією, який видаляється з основного сигналу. Розроблена таким чином пікоскопія, дозволяє безпосередньо роздивлятись електронні оболонки атомів в молекулах і може бути інструментом для вимірювання в нанотехнологіях, хімії, фізиці, біології, фармакології таке інше.

Ключові слова: *електронний мікроскоп; роздільна здатність; дифракція, візуалізація молекули.*

В работе представлено уникальный электронный пикоскоп с супердифракционной разрешающей способностью, которая составляет 10 пикометров. В работе впервые получено изображение формы отдельной молекулы в деталях, которая состоит из электронных оболочек. Первой молекулой, изображение которой получено пикоскопом, стала молекула пентана C5H12, вид которой полностью совпадает с известной реконструкцией этой молекулы. Супердифракционная разрешающая способность получена за счет опорного изображения с двойной дифракцией, который удаляется из основного сигнала. Разработана таким образом пикоскопия, позволяет непосредственно видеть электронные оболочки атомов в молекулах и может быть инструментом для измерения в нанотехнологиях, химии, физике, биологии, фармакологии.

Ключевые слова: *электронний микроскоп; разрешение; дифракция, визуализация молекулы.*

The unique electronic picoscope with superdiffraction resolution (~10 picometres) is presented in the publication. The image of separate molecule is obtained. The first molecule is a molecule of pentane C_5H_{12} that fully coincides with the known reconstruction of this molecule. The superdifraction picoscopy allows a direct view into material structure at molecular level and can be used in nanotechnologies, chemistry, physics, biology, pharmacology and other.

Keywords: *electronic microscope; diffraction; deconvolution.*

Актуальність теми. Одним з пріоритетних напрямків розвитку науки, технологій та техніки є індустрія наносистем. На цей час проведено велику кількість досліджень в області синтезу наноматеріалів різного призначення. До матеріалів нанобудови існує велика зацікавленість у зв'язку з реальною можливістю практичної реалізації їх унікальних властивостей в різних галузях.

Головна проблема вивчення наноматеріалів полягає в необхідності вивчати їх структуру і будову де основним інструментом є електронний мікроскоп. Але роздільна здатність сучасних електронних мікроскопів складає сотні пікоментрів, в той час, як відстані між атомами в молекулах складають десятки пікометрів. Тому для подальшого

розвитку нанотехнологій потрібен інструмент з роздільно здатністю біля десяти пікометрів.

Аналіз публікацій. Кожен оптичний прилад не є ідеальним. Спотворення оптичного

зображення виникають як через вади оптичних систем, які викликають аберації, так і через хвильову природу світла, що створює дифракцію. Але незалежно від природи виникнення спотворень всі вони описуються одним рівнянням згортання (convolution). У зв’язку з важливістю проблеми на цей час існує цілий ряд методів усунення результату дії згортання, деконволюції. Найбільш поширеними і ефективними ці методи є в спектроскопії, через одномірність спектрів та їх квантову природу, яка обумовлює нульову ширину спектральної смуги. Найбільш поширеними є методи нелінійного аналізу найменших квадратів [1]. Найбільш швидким та точним є метод диференційних моментів [2], використання якого в різних галузях проаналізоване в [3]. Але ці методи є непридатними для обробки зображень через те, що зображення двовимірні і потрібують надмірну кількість обчислень.

Знання функції розсіювання точки означає, що є можливість усунути цю ваду певною мірою комп'ютерними методами, загальновідомими як деконволюйійна мікроскопія [4]. Ретельний огляд методів деконволюції для зображень наведено в роботі [5], серед яких центральним є метод швидкого фур’є перетворення [6]

Домінуючими в обробці зображень є два алгоритмами, 'CLEAN', запропонований Högbom (1974) [7] і Метод Максимальної Ентропії (MEM) [8], які ґрунтуються на апріорному припущенні існування близьких точкових джерел випромінювання, розташованих на відстані меншої за роздільну здатність визначену Релеєм. Використання методу деконволюції дозволило створити флуоресцентний мікроскоп з нанометровою роздільною здатністю [9] за розробку якого W.E. Moerner, Eric Betzig and Stefan Hell отримали нобелевську премію 2014 року [10].

Всі перелічені методі ґрунтуються на апріорному припущенні, що зображення складається з кінцевої кількості окремих джерел випромінювання. Але в реальності такі випадки поодиноки.

Метою роботи є створення мікроскопу з пікометровою роздільною здатністю, який дозволяє розглянути устрій молекул та електронних оболонок, як валентних, так і ковалентних.

Виклад основного матеріалу. На практиці, кожне джерело випромінювання в мікроскопі виглядає як маленьке кільце (кільце Ері), концентрично до якого видно слабкі світлові кільця, яскравість яких, швидко падає від центру до країв. Обумовлено це хвильовою природою квантів, а явище називається дифракцією. На рис 1 в графічній формі зображено розподіл енергії в самому кільці Ері і в поступово затухаючих дифракційних кільцях навколо нього. Двовимірну функцією розсіяння точки позначимо як *K(x,y).*

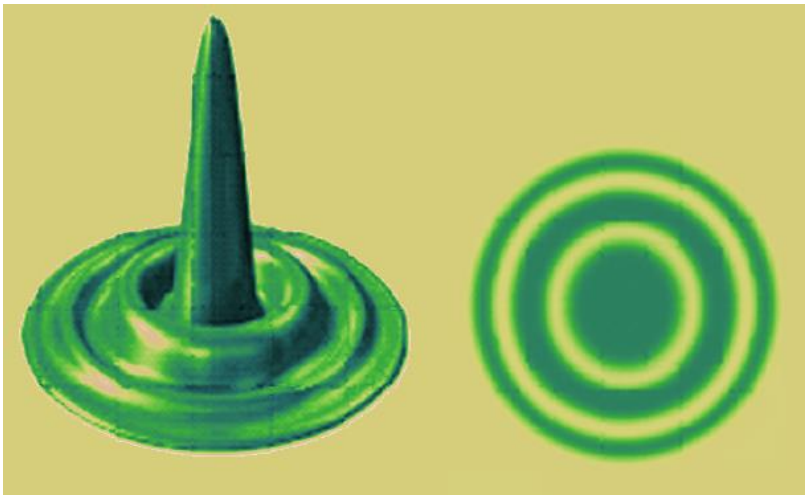


Рис. 1. Функція розсіяння точки *K(x,y)* в фокальній площині мікроскопу, об'ємне зображення, ліворуч, плоске зображення, праворуч.

Таким чином функцію розсіяння точки *K(x,y)* можна знайти, як що отримати зображення окремо розташованого джерела випромінювання. Слід зауважити, що отримана таким чином функція буде включати в себе всі, без винятку, спотворення: і оптичні та

геометричні.

Якість мікроскопа визначається його збільшенням, яке обмежене роздільною здатністю. Найменша відстань між двома точками, починаючи з якої їх зображення зливаються і перестають бути помітними, називається роздільною здатністю. Чим менше ця відстань, тим більше роздільна здатність.

Роздільна здатність мікроскопа, як і будь-якої іншої оптичної системи, підкоряється критерію Релея. Відповідно до умови, введеної Дж. У. Рэлеем (J. W. Rayleigh, 1879), зображення двох точок можна бачити окремо, якщо центр дифракції плями кожного з них перетинається з краєм першого темного кільця іншого (рис.2).

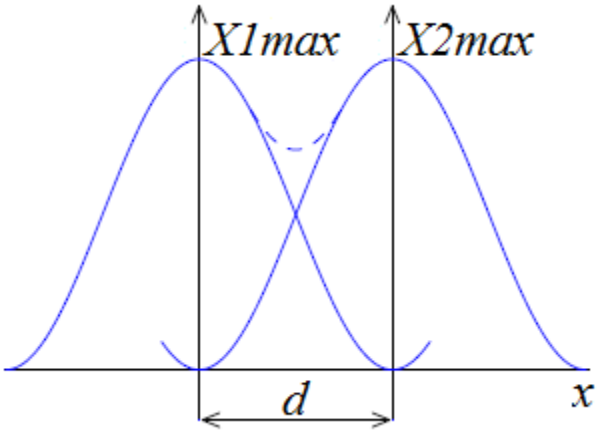


Рис. 2. Визначення роздільної здатності оптичного приладу за Релеєм.

Оскільки в даному випадку дифракція відбувається на круглому отворі, та умова першого мінімуму має вигляд:

$$d=0{,}61\ \lambda / n \sin(u), \qquad 1)$$

де u – апертурний кут (тобто кут, під яким видно радіус вхідної зіниці з точки перетину оптичної осі з площиною предмета), n – показник заломлення середовища, в якому знаходиться предмет, λ – довжина хвилі світла або довжина хвилі електрона.

Враховуючи, що у вакуумі n=1, а апертурний кут не складно встановити таким, що

sin(*u*)=0,61, для роздільної здатності мікроскопа отримуємо робочу формулу:

$$d = \lambda. \qquad (2)$$

Тобто роздільна здатність мікроскопа дорівнює довжині хвилі фотона або електрона.

Нехай «чисте» оптичне зображення об'єкту дослідження має вигляд *f(x,y).* Випромінювання проходячи скрізь оптичну систему мікроскопу створює «грязне» оптичне зображення *F(x,y).* Через дифракцію та аберації кожна точка випромінювання проходячи оптичною системою мікроскопу і потрапляючи на фокальну площину розпливається відповідно функції розсіювання точки *K(x,y).* Математично це перетворення задається інтегралом згортання, або конволюцією:

$$F(x,y) = \int_0^{y_{\max}} \int_0^{x_{\max}} K(x-p, y-q)\, f(p,q)\, dpdq. \qquad (3)$$

де інтегрування виконується по всій площині зображення.

Таким чином, нам відомо «грязне» зображення *F(x,y)* та функція розподілу енергії *K(x,y).* А потрібно знайти «чисте» зображення *f(x,y)*, то б то знайти рішення рівняння (3).

Домінуючими в вирішенні рівняння (3) є два алгоритмами, 'CLEAN', і Метод Максимальної Ентропії (MEM), які ґрунтуються на апріорному припущенні існуванні близьких точкових джерел випромінювання, розташованих на відстані меншої за роздільну здатність визначену Релеєм. Це потужні алгоритми за допомогою яких вдалося вирішити цілу низку складних наукових задач і ми не в змозі запропонувати кращі за них.

Але виявляється, що задачу отримання супердіфракційної пікоскопії можна вирішити, як що змінити парадигму, то б то побачити, що в оптиці слід користуватися іншими правилами, не тими, що встановлено Релеєм для спектроскопії.

Сенс підходу, що пропонується полягає в визначенні іншого критерію роздільної здатності. Справа в тому, що в рамках квантової механіки точковими об'єктами є квантові переходи між енергетичними рівнями. Такі переходи фіксуються спектральними приладами де і був запропонований критерій Релея. Але, на відміну від спектрів, за допомогою мікроскопії ми вивчаємо не переходи між енергетичними рівнями, а самі ці рівні, які називаються термами, або електронними оболонками. Електронні оболонки не є точковими, за визначенням, а мають об'ємну форму, тому роздільну здатність тут треба розуміти як чіткість зображення краю об'єкта дослідження.

Враховуючи вище наведене дамо визначення роздільної здатності оптичного приладу: - це точність, з якою вимірюється краї розділу між світлою та темною смугами.

Для визначеності, на відміну від критерію Релея, в робочому порядку будемо називати його критерієм форми.

В результаті за критерієм форми рівняння (3) має єдине рішення в загальному вигляді і воно має наступний вигляд:

$$f(x) = 2F(x,y) - F_1(x,y). \qquad (4)$$

де *F(x,y)* – знаходиться, як згортання вимірюваного зображення:

$$F_1(x,y) = \int_0^{y_{\max}} \int_0^{x_{\max}} K(x-p, y-q) F(p,q)\, dpdq. \qquad (5)$$

Таким чином знайдено реальну форму об'єкту *f(x,y)*, яка не спотворена дифракцією, а помилки можуть бути обумовлені лише точністю вимірювання оптичного зображення *F(x,y)* та апаратної функції пристрою *K(x,y).*

Запропонований засіб отримання супердіфракційного зображення дозволив створити пікоскоп з роздільною здатністю 10 пікометрів, суттєво меньше за розміри

електронних оболонок атомів в молекулах. Прилад відкриває безмежні можливості дослідження в хімії та інших наук та технологій, що вивчають структури на молекулярному рівні.

За допомогою пікоскопу було отримано зображення окремої молекули пентана C_5H_{12}, зображення якої наведено на рис. 3.

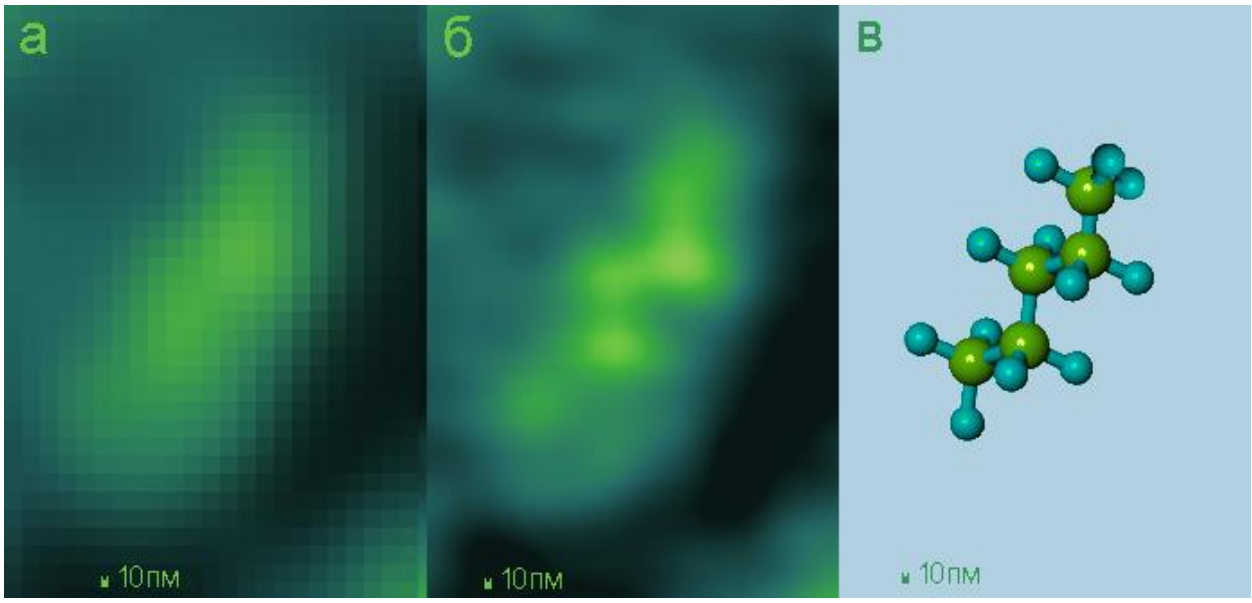


Рис. 3. Зображення окремої молекули пентану C_5H_{12}: а) брудне зображення, роздільна здатність 100 пм; б) чисте зображення, роздільна здатність 10 пм; в) модель з хімічної енциклопедії, відстань між атомами вуглецю 154 пм.

На рис. 3а наведено брудне зображення *F(x,y)*, з роздільною здатністю 100 пм. На рис. 3б наведено чисте зображення *f(x,y)*, яке було отримано за формулою (3), роздільна здатність 10 пм. На зображенні можна бачити всі п’ять електронних хмар навколо атомів вуглецю. Згідно за законами квантової механіки ядра атомів водню позбавлені електронів і їх не можна побачити. На рис. 3в надано реконструкції молекули пентану C_5H_{12} згідно хімічної енциклопедії, яка була отримана методами рентгеноструктурного аналізу. Згідно з енциклопедією, атоми вуглецю в молекулі пентану пов'язані за допомогою ковалентного зв’язку С-С з постійною (для вільних ізольованих молекул в газовій фазі) довжиною, рівного 154 пм, і валентним кутом між С-С-зв'язками, рівним 112°.

Висновки. В результаті багаторічних досліджень, в яких в різні часи приймали участь десятки інститутів та університетів, був створений пікоскоп пікометровою роздільною здатністю, який дозволяє розглянути устрій молекул та електронних оболонок, як валентних, так і ковалентних.

Знайдено спосіб зазирнути за межі, які досі були заборонені дифракцією хвилі. Вчасності, роздільна здатність електронного мікроскопу доведена до декількох пікометрів, що дозволяє роздивитись окрему молекулу в деталях. Запропонований спосіб отримання супердіфракційного зображення дає інструмент для подальшого розвитку нанотехнологій, а також технологій в галузі хімії, фізики, біології, медицини.

Література

1. Pitha J., Jones R. N. A COMPARISON OF OPTIMIZATION METHODS FOR FITTING CURVES TO INFRARED BAND ENVELOPES— Canadian Journal Chemistry, 1966, v. 44, N 24, p. 3031—3050.

2. Кучеров А.П. Элементы теории дифференциальных моментов в задачах обработки спектров // Нові комп'ютерні засоби, обчислювальні машини та мережі.- 2001. – С. 186–192.

3. Кучеров О. П. Теорія управління економікою знань К.: НДІ "Украгропромпродуктивність", 2008 с.252

4. Wallace W, Schaefer LH, Swedlow JR (2001). "A workingperson's guide to deconvolution in light microscopy". BioTechniques 31 (5): 1076–8, 1080, 1082 passim. PMID 11730015.

5. J. L. Starck, E. Pantin, F. Murtagh, Deconvolution in Astronomy: A Review, Publications of the Astronomical Society of the Pacific, 114:1051–1069, 2002

6. Siddharth Shah, FLUORESCENCE AND ELECTRON MICROSCOPY, A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy (Biomedical Engineering) in The University of Michigan, 2006

7. Högbom, J. (1974), Aperture synthesis with a non-regular distribution of interferometer baselines, Astrophys. J. Suppl. Ser., **15**, 417-426.

8. Narayan, R. & Nityananda, R. (1984), "Maximum entropy-flexibility versus fundamentalism", in Indirect Imaging, J.A. Roberts, Ed., Cambridge University Press (Cambridge, England), pp. 281-290.

9. W.E. Moerner, Plenary presentation: Single-molecule spectroscopy, imaging, and photocontrol - foundations for super-resolution microscopy, 5 March 2015, SPIE Newsroom. DOI: 10.1117/2.3201503.17

10. Ritter, Karl; Rising, Malin (8 October 2014). "2 Americans, 1 German win chemistry Nobel". AP News. Retrieved 8 October 2014.

УДК 004.5

Руденко М.П. к.в.н., доцент, с.н.с.,
Інститут проблем реєстрації інформації Національної академії наук України,
вул. М.Шпака, 2, 03113 м. Київ, Україна

Людський фактор у комп`ютерних моделях динамічних процесів складних технічних систем

Розглянуто особливості людського фактора (ЛФ) вскладних динамічних процесах функціонування складних технічних систем (СТС) і особливості його використання при комп`ютерному моделюванні високодинамічних процесів СТС. Досліджено особливості прийняття рішення оператором в нештатних ситуаціях СТС.

***Ключові слова**: людський фактор (ЛФ) в СТС, моделювання, комп`ютерне моделювання, аналіз обставин, особливості прийняття рішення оператором в СТС, нештатна ситуація (НС).*

Рассмотрены особенности человеческого фактора (ЛФ) в сложных динамических процессах функционирования сложных технических систем (СТС) и особенности его использования при компьютерном моделировании высоко динамичных процессов СТС. Исследовано особенности принятия решения оператором в нештатных ситуациях СТС.

***Ключевые слова:** человеческий фактор (ЛФ) в СТС, моделирование, компьютерное моделирование, анализ обстоятельств, особенности принятия решения оператором в СТС, нештатная ситуация (ЧС).*

The features of the human factor (HF) in complex dynamic processes of complex technical systems (CTS)functioning and especially it usein computer modeling highly dynamic processes CTS was considered. Features of making decisions by the operator in emergency situations CTS are discussed.

***Key words**: human factor (HF) in CTS, simulation, computer modeling, analysis of the circumstances, peculiaties especially of decision making by the operator inCTS, an emergency situation .*

Вступ

Кінець XX і початок XXI століть характерні пошуком і впровадженням нових технологій в управлінні складними технічними системами (СТС). Автоматизація процесів управління з одного боку спростила процеси управління, а з іншого проблеми аварій і катастроф через людський фактор (ЛФ) залишилася й досі не вирішеною. Як показує аналіз розслідувань аварій і катастроф, однією із головних їх причин експерти визначають ЛФ. Дослідження характерних змін властивостей ЛФ під час динамічних процесів діяльності операторів в нештатних ситуаціях (НС) є актуальною задачею для професіональної їх підготовки [3].

Об`єктом дослідження статті є типові процеси професіональної діяльності оператора СТС у нештатних ситуаціях, а предметом дослідження - властивості оператора (ЛФ) при виникненні нештатних ситуацій в динамічних процесах функціонування СТС. Метою проведення дослідження є аналіз властивостей оператора і впливу ЛФ на раціональне функціонування в СТС в НС.

Важливість ЛФ у критичних ситуаціях також визначав й видатний льотчик-випробовувач М. Громов: «Мало хто знає, що в ці секунди, що вимагають самих продуманих і точних дій, людина не може розмовляти. Вибух почуттів і вихор думок змушує діяти блискавично, і думка ледве встигає випереджати дії. Зосередженість і

напруга такі великі, почуття такі глибокі і сильні, а розв'язка наближається з такою невблаганною швидкістю, що людина не в змозі говорити. Чим складніше і напруженіше робота, чим глибше переживання, тим коротше час, необхідний для роздумів, тим важче висловлювати свої думки і переживання словами. Тому, як каже У. Бріджмен, пілот одномісного літака часто встигає тільки повідомити про аварійну ситуацію, а потім може замовкнути назавжди» [4].

Аналіз моделей процесів управління СТС дозволяє відображати роль ЛФ, в основному, тільки через його нормативну частину (інструкції, правила використання технологій СТС). На практиці, формування і накопичення знань щодо діяльності оператора критичних технологій здійснюється за рахунок практичного досвіду, який не є ідеальним. Досягнутий й фактичний рівень підготовки не є стабільним. З часом через втому, психологічне «вигорання» діяльність оператора приводить до типової втрати рівня навичок, що відповідно веде до помилок, особливо на критичних етапах функціонування СТС [2,7].

Особливо вищесказане справедливо під час освоєння управління процесами СТС, через значні витрати ресурсу СТС на їх освоєння операторами є нераціональним, оскільки кількість аварій і катастроф після освоєній СТС через помилки операторів не зникає і часто зовсім непередбачені.

Особливості людського фактору при моделюванні технологічних процесів СТС

Особливості моделювання процесів СТС у різних формах: математичних, графічних, вербальних і невербальних, з урахуванням часу і змісту процесів створюють умови для аналізу системи, у тому числі, підготовки операторів критичних технологій. Створення методик удосконалення процесів освоєння та процесів управління вимагає знання особливостей оператора, як ЛФ, що дозволить удосконалити управління СТС. Особливо це важливо для дослідження професіональної діяльності експертів з метою передачі практичного досвіду.

Можливості інформаційних технологій зберігати в базі знань фоновий і піковий рівні нормативних стандартів діяльності оператора дозволяють створювати образ нормативних вимог до властивостей оператора. Відповідно протоколювання процесу підготовки оператора матиме конкретні кількісні результати, а значить і можливість оцінки його готовності до виконання функцій оператора СТС.

Разом з тим, особливість психологічних властивостей особистості під час її діяльності потребує створення протоколу дій, образу і сценарію поведінки оператора у НС. Якості оператора, для якого характерні, крім мотивації, втома, психологічне вигорання, помилкові дії вимагають формування перспективного образу надійності оператора, як людського фактору з його властивостями, в процесах управління СТС.

Особливо актуальним є формування образа оператора (ЛФ) в критичних вузлах процесів СТС в екстремальних професіях.

Врахування людського фактору при моделюванні динамічних процесів у СТС

Суттєво змінилися умови життя сучасного покоління людей: швидкість на транспорті збільшилася в 2-5 разів, швидкість технологічних процесів на автоматизованих виробництвах - в 8-14 разів, необхідність швидко приймати рішення в задачах оборонного значення - в 30-40 разів. Сьогодні психологічна сутність взаємодії оператора, наприклад, пілота літального апарату (ЛА) з машиною, ЛА і технологічними процесами, полягає в тому, що вони можуть ввести його в область позамежних людських можливостей, не знімаючи відповідальності за його дії. Прикладом таких дій може слугувати посадка ЛА в

ручному режиму повітряного судна з пасажирами у вкрай складних погодних умовах в разі несподіваного збою автоматики [5].

При цьому, аналітичне дослідження процесу руху ЛА по глісаді як функціонування складної людино-машинної системи практично неможливо [2,6]. Причиною є множина факторів, що визначаються особливостями роботи пілота одночасно з аеродинамічними системами управління, взаємодією їх складових частин, процесу управління і фактичного положення ЛА в просторі, впливом зовнішнього середовища на роботу його окремих систем.

При цьому певні фактори, що впливають на ефективність управління оператором ЛА, потребують детального аналізу:

- зовнішнє середовища (атмосферні явища (прозорість атмосфери, хмари, турбулентність, температура повітря і т.п.), час доби (день, ніч);
- швидкість літака, яка нормативними документами визначається, як раціональна для пілота з метою безпечного приведення ЛА на посадку;
- динаміка зміни поступальної, вертикальної швидкостей ЛА, робота з механізацією крила і його силовими установками;
- робота авіаційних систем передачі і відображення інформації, яка формує адекватну інформацію щодо положення ЛА і його систем (рис.1).

Інформаційні потоки для оператора є значними по об`єму необхідної роботи з органами і обмежують його час на прийняття рішення і раціональні його дії при появі неочікуваної інформації.

На умови прийняття рішення впливають властивості авіаційної системи:

- управління ЛА відносно 3-х вісей і вектора швидкості;
- управління положенням ЛА відносно Землі-навігація;
- постійне спостереження за станом систем ЛА;
- рішення задачі комунікації відповідно ситуації що склалася;
- прогноз положення ЛА відносно 3-х вісей і вектора швидкості;
- прогноз положення ЛА відносно землі;
- прогнозом стану систем ЛА;
- задача контролю і плану дій інших екіпажів в районі польотів;
- планування своїх дій і дій членів екіпажу у випадку ускладнення умов польоту і розвитку НС.

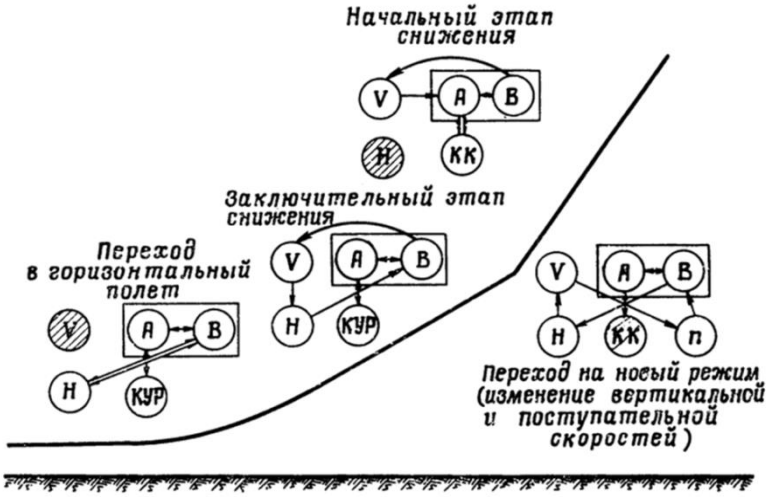


Рис. 1. Розподіл уваги пілота на посадковій глісаді [11].

Аналіз НС, що трапилися з професіоналами, експертами і кількість факторів, що виникли, показують такі епізоди польоту, які іноді вигадати просто неможливо [9]. Наприклад, НС в автоматизованій авіаційній системі через неповну інформацію про динаміку роботи паливної системи привела екіпаж в повітрі і управління на аеродромі до дій, які вийшли за межі безпеки польоту. Ситуація, що склалася, коли літак заправлений паливом, а всі види сигналізації і відображення інформації говорять, що паливо ось-ось закінчиться, призвели до аварійної і катастрофічної ситуації. Практичний досвід, унікальні знання, навички пілота-випробовувача з 30-літнім досвідом перемог, але дефіцит часу виявилися недостатніми для оцінки обставин в управлінні ЛА і виходу з НС. Тобто в критичних технологіях постійно необхідно мати варіанти розвитку процесів і необхідні варіанти в досягненні мети, що може бути під силу тільки за умови використання моделей і комп`ютерних технологій. Знання про помилкові дії вимагають аналізу як варіантів недопустимих дій і виключення їх повторення.

У випадку, коли є час на оцінку НС, екіпажем може бути поетапно переведена ситуація з катастрофічної в аварійну і складну. НС, що виникла навіть технічними нормативними правилами даного ЛА не передбачена [14].

Сьогодні помилка людини, яка управляє складним машинним комплексом, може привести до загибелі сотень людей і/або до мільярдних збитків. Звідси виникає суспільна потреба в формуванні соціальних якостей особистості, готовності прийняти рішення в нестандартній ситуації [5,7].

Аналіз технічного прогресу з позиції ЛФ і його психологічного забезпечення показав необхідність логічної комбінаторики, рефлексивних рішень, візуального мислення, тобто, всього того, що необхідно для надійності операторської діяльності [7,8,10].

В операторських професіях, в яких працює 50-70 млн. осіб, на сьогодні через помилки фахівців відбувається до 70-80% всіх аварій і катастроф. Більш того, за рахунок недостатньо розвиненого навчання фахівців новостворювана техніка протягом 2-3 років використовується лише на 60-70%. Проведені психологічні обстеження понад 300 професіоналів, які страждають невротичними розладами, показали, що однією з провідних причин патології є невідповідність професійної підготовки рівню складності виконуваних завдань[3,6,7,11].

У переважній більшості випадків ненадійні дії людей виникають через відсутність психологічної готовності до нестандартних ситуацій.

Розглядаючи проблему професійної надійності, прийнято вважати, що чим краще підготовлений професіонал до основної діяльності, тим краще він впорається з аварійної обстановкою. Це істина досить умовна: наприклад, висококваліфіковані льотчики, потрапивши в НС, не маючи спеціальної підготовки до екстремальних ситуацій, не завжди забезпечують необхідну надійність [2,7,8,9].

Найбільш складний для людини процес прийняття рішення. Експерименти показали, що в аварійній ситуації більше 3/4 часу витрачається на прийняття рішення. Збільшення часу прийняття рішення обумовлено невмінням застосувати знання в небезпечній обстановці, психологічно взяти відповідальність на себе; в 50-60% випадків людину охоплює страх за наслідки своїх дій, за можливість помилки. Багато затягнуті дії визначаються слабким вольовим імпульсом, звичкою до опікунства, слабохарактерністю [3,5,7].

Крім соціального боку проблеми, є і психологічна: поведінка людини в умовах реальної загрози життю визначається не емоційною напруженістю, а психічними станами, що забезпечують діяльність в екстремальних умовах, і організовується за іншими законами. Приміром, якщо в звичайній професійній діяльності стійкий стереотип як основа автоматизованих навичок сприяє вправності і легкості здійснення операцій, то в

аварійній ситуації він гальмує переключення уваги з режиму репродуктивного функціонування на продуктивний, тобто перешкоджає створенню нового рішення [7, 10].

Аналіз вищерозглянутих процесів, в яких операторська діяльність поєднує необхідність одночасного прийняття рішень пілотом (оператором) по управлінню ЛА адекватно ситуації і НС в технічній системі при дефіциті часу, висоти вимагає завчасного, або точніше, випереджуючого сприйняття динаміки розвитку подій. Яким чином формувати готовність переключення і поєднання діяльності оператора в НС? Поєднання одночасних процесів, що виникли в управлянні ЛА, потребують моделювання процесу для зменшення помилок в прийнятті рішення.

Особливість властивостей поведінки оператора при виникненні нештатної ситуації

Із аналізу вищенаведеного випливає, що дії оператора в критичних технологіях повинні передбачати стійкість до психологічних стрес-факторів:

1. Усвідомлення обстановки під загрозою його здоров'ю і життю.

2. Раптовість - несподівані для людини зміни обставин в ході виконання функцій і завдань.

3. Невизначеність - відсутність, нестача або суперечливість інформації про зміст, або умови виконання професійної діяльності.

4. Новизна - наявність раніше невідомих оператору елементів в умовах виконання, або в самій задачі. Новизна визначається професійним досвідом фахівця, тобто отриманого досвіду в часі, кількості і раціональності власнихдій, а іноді досвід іншого оператора.

5. Збільшення темпу дій - скорочення часу на прийняття рішення і на виконання дій.

6. Дефіцит часу - умови, в яких успішне виконання завдання неможливо простим збільшенням темпу дій, необхідна зміна змісту структури діяльності.

Крім того, виділяються безпосередньо психічно травмуючі фактори екстремальної ситуації із минулого, які викликають негативні психічні реакції в оператора, що знижують або ж повністю обмежують працездатність оператора [7, 8]. До них відносяться:

1. Фактори візуального (зорового) ряду: руйнування будівель, техніки, споруд, ландшафту, вогонь, загоряння, пожежі, вид трупів, поранених і постраждалих.

2. Фактори слухового ряду: гуркіт, рев, гул, тряска, тріск.

3. Фактори тактильного ряду (дотикального): вібрації, удари повітряної хвилі, струсу, падіння.

4. Фактори інтерактивного ряду: смерть близьких, товаришів, контакт з великою кількістю поранених.

Ключовим моментом перерахованих факторів є те, що вони викликають помилки в процесах діяльності оператора.

При аналізі діяльності оператора умовно виділяють фази:

1. Виявлення. Часто залежить від напруги, яка сталась в цей момент управління ЛА, але є очевидною, тому і як такою проблемою не вважається.

2. Оцінка обставин / Локалізація. Перш ніж щось робити, оператору потрібно зрозуміти, в чому саме суть проблеми, і чи треба взагалі щось робити.

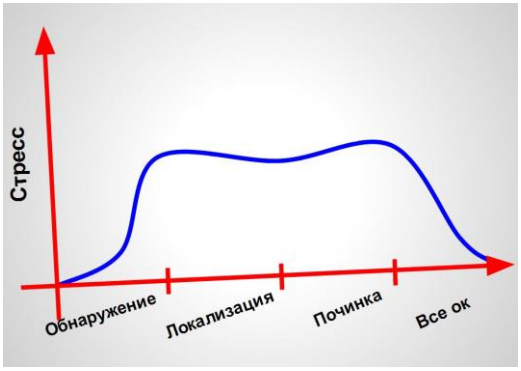
3. Прийняти рішення відповідно до ситуації, що склалася.

4. Відновлення працездатності (починка), практична дія паралельно з управлінням ЛА відповідно до нормативних вимог і ситуації, що склалася.

5. Переконання, що все зроблено. Аналіз того, що зроблено і проблема ліквідована.

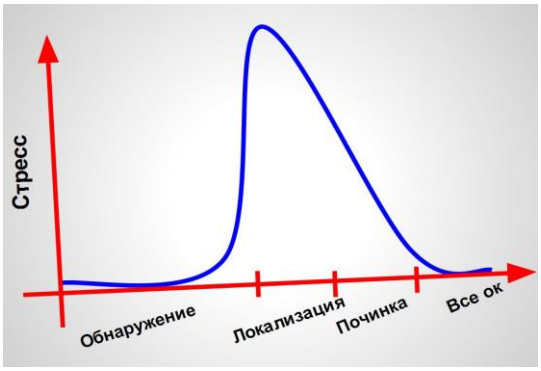
Проведений аналіз досліджень показує, що у звичайній ситуації все виглядає приблизно так (варіант 1,2,3) [2,7]:

Варіант 1.

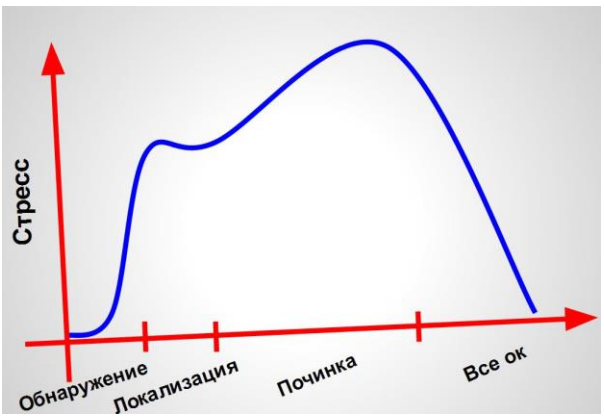


Виявлення проблеми супроводжується тривалим періодом стресу оператора і чим довший процес прийняття рішення і відсутність адекватних обставинам дій, тим довше стрес зберігається. Чим довше оператор вибирає рішення і починає діяти, тим більше наростає напруга. Тільки з початком керованих змін оператор заспокоюється [7].

Варіант 2. Коли є достатньо часу на виявлення проблеми. Зазвичай сама поява чогось непередбаченого в плані оператора лякає дуже сильно, навіть якщо його швидко локалізували і відновили працездатність.



Варіант 3 [7]. Коли час іде на усунення проблеми [2,6,7].



При цьому, стає зрозумілим необхідність оперативного мислення і передбачуваність реакції систем ЛА, здатність оператора до зв'язаних дій, до одночасного виконання завдань різного плану, і це є рівень професіоналізму оператора і рівень його знань, умінь, навичок.

Особливу роль відіграють здібності оператора за окремими ознаками передбачити хід розвитку події, коли ще не розгорнулися події.

Проведені експерименти при моделюванні реальних аварійних ситуацій показали, що після навчання і тренування подібних якостей вдалося знизити емоційну напруженість наполовину, зменшити кількість помилкових рішень на 80%, скоротити час прийняття рішення в 3-5 разів, відповідно підвищити і безпеку діяльності оператора [7,8].

Розвиток в людині здатності передбачати розвиток подій є втраченим або нерозвиненим природним даром. На підставі фізіологічному чутливості людиною розпізнається інформація, яка і створює стійкість діяльності. Відбір людей в екстремальні професії повинен базуватися на якостях розвиненої сенситивності індивіда. Надійність техніки постійно підвищувалася. Тільки людина залишилася джерелом ненадійності, яка дивним чином збільшувалася. Ненадійність оператора породила ідею про необхідність удосконалювати машину, а людину ретельно тренувати і детально контролювати. У цьому випадку вже безнадійно упускається можливість виявлення першопричин неоптимальної діяльності оператора і головне - можливості для створення образу раціональної його діяльності [7,10].

Тобто, питання безпеки діяльності оператора критичних технологій є комплексним і вимагає пошуку комплексу взаємопов`язанних рішень і їх завчасної реалізації у моделях процесів і технологій.

Висновки

Проведений аналіз ролі людського фактора і його вплив на функції оператора екстремальної професії свідчить:

- зростає ролі людського фактору в раціональному функціонуванні СТС;
- необхідно завчасне створення технологічних процесів управління оператором в моделі СТС;
- моделювання дозволяє створювати варіанти сценаріїв поведінки оператора екстремальної професії в критичних точках технологій управління СТС;
- необхідна психологічна підготовка оператора для управління СТС на адекватних моделюючих комплексах;
- питання взаємодії діяльності оператора і технологічних процесів СТС потребують випереджувальних сценаріїв раціонального управління СТС з урахуванням критерію безпеки його діяльності.

Література

1. Квашнина Г.А. Управление познавательной деятельностью персонала на основе модели системной динамики /Г.А. Квашнина // Вестник Воронежского государственного технического университета. 2005. Т.1. № 7.

2. Береговой Г.Т., Пономаренко В.А. Психологические основы обучения человека-оператора готовности к действиям в экстремальных условиях // Вопросы психологии. -1983. - N1. - С. 23-32.

3. Лебедев В.И. Личность в экстремальных ситуациях. — М., 1989[Эл. ресурс]- режим доступа:// www.aquarun.ru.

4. Бриджмєнт У., Азар Ж «Один в безмежному небі»[Эл. ресурс]- режим доступа:// ereading.club/bookreader.php/772/ Azar, _Bridzhmen_-_Od.

5. Додонов А.Г., Кузьмічов А.И., Оперативное принятие решения в нештатних ситуаціях: модель расписания проекта по критерию «время стоимость»// Реєстрація, зберігання і обробка даних. -2014. №2, Том 16. –С. 122-132.

6. Зиньковская С. М. Полет без стрессов: человеческий фактор в авиации / С. М. Зиньковская. – Екатеринбург: УрГПУ, 2005

7. Высоцкий С. «Анатомия ошибки»[Эл. ресурс]- режим доступа:// http://goblingame.blogspot.com/2012/10/blog-post_12.html

8. Ломов Б.Ф., pidruchniki.ws/12631113/psihologiya/lomov_pamyat_antitsipa.

9. Мемореал лётчиков испытателей. http://xn--80akhcovnjb1g.xn-1ai/memo/80/fedotov.htm

10. Психология безопасности труда и эргономика.[Эл.ресурс]- режим доступа://**Ошибка! Недопустимый объект гиперссылки.** bezopasnost_truda

11. Микоян С. А., Корбут А. Г. М59 Заход на посадку по приборам, М.: Воениздат, 1979. — 71 с, ил.15 к.

12. Analysis of factors contributing to 460 “pilot error” experiences in operating aircraft controls Dayton, OH: Aero Medical Laboratory, Air Material Command, Wright-Patterson Air Force Base, 1947.

13. Schmitt E. Navy pilot’s death reflects hazards of job. International New York Times 2015 May 13;6.

14. Планер Гимли.[Эл.ресурс]- режим доступа: //ttps://https://ru.wikipedia.org/wiki/Планёр_Гимли

РЕЦЕНЗІЇ ТА ІНФОРМАЦІЙНІ ПОВІДОМЛЕННЯ

ПРАВИЛА ДЛЯ АВТОРІВ

У науковому журналі «інформаційні технології та спеціальна безпека» друкуються статті, які відповідають профілю журналу і мають наукове та практичне значення. Редколегія просить не надсилати матеріали, раніше надруковані, чи такі, що готуються до друку в інших виданнях. Тексти статей та всі матеріали до них повинні бути ретельно відредаговані, перевірені та підписані авторами.

Надсилаючи статтю до редакції, просимо дотримуватись наступних правил

1. Рукопис надсилається в двох екземплярах, надрукований через 1,5 інтервали шрифтом Times 12 пунктів, набраний у редакторі Word-2003 та в електронному вигляді.

2. Розмір статті разом із рисунками та списком літератури не повинен перевищувати 10–12 сторінок і 5-ти рисунків. Викладення повинно бути чітким, стислим, без довгих вступів, відступів і повторів, а також без дублювання в тексті даних таблиць, рисунків і підписів до них. Реферат і розділ «Висновки», якщо він є, не повинні дублювати один одного. Обсяг реферату — не більше 1000 знаків. На першій сторінці статті має бути зазначено індекс УДК.

3. Назву статті, ініціали та прізвища авторів, повну назву установи та її адресу, де працюють автори, а також текст реферату та ключові слова друкують мовою статті. Окремим файлом подають ті ж самі дані (крім адреси та назви установи) іншими двома мовами (англ., укр./рос.)

4. Рисунки (діаграми, графіки, фотографії тощо) потрібно подавати на окремих сторінках на білому папері, чітко віддруковані (чорно-біле зображення) і підписані на зворотній стороні листа. Рисунки необхідно подавати кожний окремим файлом. Бажана ширина рисунків — 75мм або 150 мм. Надписи на рисунках слід, по можливості, замінити літерними позначками, а криві позначити цифрами, які роз'яснюються в підписах до рисунків або в тексті. Мінімальний розмір надписів на рисунках — 10 пунктів. Не бажано наводити у вигляді рисунків дані, які можна представити в тексті чи в таблиці. Місце рисунків указується на лівому полі рукопису. Підписи до рисунків бажано давати окремим файлом.

5. Таблиці повинні мати номер і назву. Кожний рисунок і таблиця — відповідні посилання в тексті. Скорочення слів у тексті, таблицях і на рисунках не дозволяються.

6. Формули повинні бути набрані у редакторі Microsoft Equation шрифтом 12 пунктів (Italic). Грецькі літери слід підкреслити і на полях написати їхню назву. Розмітити олівцем великі та малі літери, які мають однакове написання ($\underline{\underline{C}}$, $\overline{\overline{c}}$, $\underline{\underline{K}}$, $\overline{\overline{k}}$ тощо). Літери й знаки, які важко відрізнити, слід пояснити на полях олівцем: *J* (йот), *I* (і), 1 (одиниця), *l* (ель), 0 (нуль), О (літера) тощо.

7. Стаття повинна мати список джерел, що цитується. Список оформлюється згідно ДСТУ ГОСТ 7.1.2006 «Система стандартів з інформації, бібліотечної та видавничої справи. Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання. З прикладами складання бібліографічного опису можна ознайомитися в Бюлетені ВАК України № 5 за 2009 рік. Посилання на літературні джерела в тексті статті слід давати в квадратних дужках у вигляді порядкової цифри, надрукованої у рядок.

8. На окремому аркуші подаються відомості про всіх авторів: прізвище, ім'я та по-батькові (повністю), вказується вчена ступінь та звання, посада, повна назва установи, а також домашня та службова адреси із зазначенням індексу, номер телефону кожного автора та e-mail (за бажанням авторів).

Рукописи, що не відповідають цим вимогам, розглядатися не будуть.