КОНСТИТУЦІЙНЕ ТА АДМІНІСТРАТИВНЕ ПРАВО

УДК 35.073

О.О.Бойченко,
ад'юнкт

АНАЛІЗ ФУНКЦІОНУВАННЯ ВІДОМЧИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОВС

У статті розглядаються питання проблематики застосування відомчих інформаційних ресурсів в системі національної безпеки держави. Запропоновані пропозиції щодо удосконалення організаційно-правових заходів застосування відомчих інформаційних ресурсів ОВС, як складової державної безпеки країни.

Ключові слова: інформаційна безпека, відомчі інформаційні ресурси, державна безпека.

Постійне зростання значення інформаційних ресурсів для усіх сторін життєдіяльності суспільства обумовлює необхідність проведення наукових досліджень щодо організаційно-правових заходів регулювання процесів створення, використання та захисту інформаційних даних. Особливого значення набувають наукові дослідження у напрямку захисту відомчих інформаційних ресурсів ОВС, як складових національного інформаційного забезпечення. Це визначено значною кількістю інформаційних даних, що циркулюють у складі інформаційно-аналітичного забезпечення ОВС України (оперативно-розшукова інформація, відомості щодо організації слідчої діяльності і т. ін.). Тому ступінь розвитку відомчих інформаційних ресурсів ОВС, а також рівень функціональності системи інформаційної безпеки визначає спроможність ОВС у протидії злочинності та забезпеченні національної безпеки держави.

Окремі питання щодо становлення інформаційного суспільства, а також ролі інформаційних ресурсів в системі забезпечення національної безпеки розглядаються в роботах таких науковців, як В. М. Брижко, В. Д. Гавловського, В. О. Голубєва, Р. А. Калюжного, В. С. Цимбалюка, М. Я. Швець, В. Г. Афанасьєва, Ю. М. Батуріна, Д. Белл, Н. Вінер, Л. М. Земляновой, М. М. Мазур, А. Д. Урсул та ін.

Однак характеристики відомчих інформаційних ресурсів ОВС в системі забезпечення національної безпеки України залишаються малодослідженими.

Мета публікації полягає в проведенні аналізу організаційно-правових аспектів застосування відомчих інформаційних ресурсів ОВС в контексті забезпечення національної безпеки держави.

Науковий аналіз чинної нормативно-правової бази в Україні та світі доводить дещо невизначеність змісту поняття державної безпеки, що ускладнює підхід до створення ефективної цілісної системи забезпечення національної безпеки як об'єкта управління в політичній системі суспільства. При цьому основною складовою національної безпеки країни слід визначити державну безпеку [1, с. 53].

Тобто державна безпека – це такий стан функціонування державної влади та її інститутів, коли забезпечуються потреби суспільства у нормальній життєдіяльності.

Система забезпечення державної безпеки – це комплекс суспільних відносин, здатний забезпечити захищеність діяльності державної влади та її інститутів від негативного впливу внутрішніх і зовнішніх чинників. При цьому суть суспільних відносин полягає в оптимізації структури державної влади та окремих її функцій з метою прийняття таких управлінських рішень, зокрема в кризових ситуаціях, які мають базуватися на об'єктивному аналізові та врахуванні наявності суспільних ресурсів для їх реалізації. Такі рішення мають бути спрямовані на забезпечення стійкості суспільної системи, підвищення ефективності вирішення суперечностей і конфліктів [2, с. 38].

Сучасний напрям удосконалення суспільних відносин лежить у площині розвитку інформаційних ресурсів, які є базовими для створення ефективних функціонально-інформаційних моделей державного управління як складової політичної системи суспільства. Отже, цей вид ресурсів є водночас об'єктом управління і предметом діяльності державної влади та її інститутів.

Особливого значення в діяльності органів державної влади мають відомчі інформаційні ресурси ОВС, як основного важелю правоохоронної системи країни. Тому захист таких ресурсів також є визначним для становлення й роз-

витку інформаційних ресурсів держави, її політичної та економічної стабільності, а також відповідного іміджу в міжнародних відносинах.

Інформаційні ресурси – це інформаційна інфраструктура та циркулююча в ній продукція інформаційної діяльності, яка дає змогу вирішувати відповідні завдання. Найважливішим при цьому є розуміння того, що дві складові інформаційних ресурсів доповнюють одна одну і не можуть бути використані окремо [3, с. 151].

Планування розвитку інформаційних ресурсів стає визначальним для оптимізації управління підрозділами ОВС з метою підвищення ефективності оперативного реагування на події та злочини, надійну охорону громадського порядку та забезпечення прав і свобод громадян.

Воно повинно здійснюватись за такими основними напрямами:

– удосконалення правових та організаційно-економічних механізмів використання відомчих інформаційних ресурсів ОВС;

– підвищення надійності доступу до інформаційних ресурсів та захисту їх від несанкціонованого використання;

– удосконалення інформаційних технологій та інформаційно-математичних моделей, які використовуються в системі прийняття рішень.

Аналіз стану формування та використання інформаційних ресурсів в ОВС України доводить, що відомча інформаційна політика залишається некоректною (характеризується ознаками безсистемності та непослідовності), що негативно позначається на процесах інноваційного вдосконалення відомчого управління. Визначене обумовлено відсутністю єдиної системи поглядів на реалізацію інформаційної політики та забезпечення відомчої інформаційної безпеки, сформованих у концепцію відомчої інформаційної політики та інформаційної безпеки [4, с. 234].

Ретельний аналіз законопроєктів, що знаходяться на опрацюванні у Верховній Раді України та інших інформаційних джерел свідчить, що концептуально й законодавчо в Україні не визначено поняття "інформаційна безпека" як системний комплекс взаємопов`язаних запобіжних заходів захисту інформаційного суверенітету та інформаційного простору України.

Характерною ознакою підходів до розуміння інформаційної безпеки є наповнення цього поняття різним змістом, наслідком чого є різний зміст заходів щодо її забезпечення. В деяких випадках класифікація загроз інформаційній безпеці України носить яскраво виражений політизований характер – це виявляється в політичній ситуації в Україні постійно, починаючи з кінця 2000 р., а сьогодення вказує на різке його загострення у зв`язку з повною відсутністю взаєморозуміння гілок влади щодо політичних та фінансово-економічних перспектив України. Одні й ті ж самі фактори та умови різні політичні сили розглядали як небезпечні, загрозливі, чи навпаки, як стабілізуючі [5, с. 48].

Проблеми у цій сфері розв`язуються фрагментарно, без належної координації нормотворчої діяльності за цим напрямом. Нині у Верховній Раді України розглядається 27 законопроектів, віднесених до регулювання діяльності у галузі інформаційних ресурсів, 4 законопроекти – у галузі інформаційно-комунікаційних технологій, 6 – інформаційної безпеки.

Безперечно, така кількість законопроектів, з одного боку, засвідчує увагу держави до інформаційної галузі, а з другого – необхідність комплексного підходу до вирішення проблем державного регулювання в національній інформаційній сфері.

На жаль, слід констатувати, що недостатній розвиток національних інформаційних ресурсів унеможливлює їх становлення як визначального чинника соціального та економічного розвитку України. А нерозвиненість інформаційної складової державного управління залишає на малоефективному рівні комунікаційні зв`язки між державною владою і суспільством.

Нині розвинуті держави світу приділяють особливу увагу цій проблемі, розглядаючи її в контексті становлення інформаційного суспільства. Наприклад, у США більшість урядових програм в галузі інформаційних технологій спрямовано на розвиток ресурсів Інтернет. Американський сегмент цієї міжнародної мережі вже сьогодні становить 35 млн. сторінок та 22 тис. сайтів, де найповніше представлені економіка, управління ресурсами та суспільна безпека.

При цьому стратегічна мета впровадження моделі електронного уряду в США полягає у переорієнтації ресурсів та послуг на пересічних громадян, що дало б змогу підвищити якість державних послуг та істотно скоротити термін розгляду їх звернень з кількох днів та тижнів, як це відбувається сьогодні, до кількох годин [6, с. 348].

Електронний уряд в США – це вже не просто наукова теорія або концепція, він став реальністю. Його впровадження вносить революційні зміни у відносини між простими американцями і органами державного управління. Громадяни США стають краще інформованими про державні справи, а новітні мережеві комунікаційні технології дають змогу їм безпосередньо залучатися до управління державою. У практичній площині вирішуються питання скорочення так званого цифрового розриву, тобто надання мож-

ливості доступу громадянам країни, які не мають домашніх комп'ютерів, підключених до мережі Інтернет, до засобів електронної пошти та висловлення у такий спосіб власної позиції з тих чи інших державних рішень.

Водночас, у Сполучених Штатах Америки одним з пріоритетних напрямів розвитку інформаційних ресурсів визначено забезпечення їх безпеки. Впроваджуючи інформаційні технології, держава і суспільство стають критично залежними від їх надійності та захищеності. Тому питання моніторингу, захисту та адаптації інформаційних ресурсів потребують негайного вирішення. Це має своєчасно виявити факт порушення, локалізувати об'єкт, на який здійснюється вплив, нейтралізувати порушника та швидко відновити втрачені функції системи.

У 2003 році США прийняли «Національну стратегію захисту кіберпростору», спрямовану на захист складних і взаємопов'язаних комп'ютерних систем, які мають життєво важливе значення для нинішнього суспільства [7, с. 181].

Вона побудована за п'ятьма пріоритетними напрямами діяльності:

- національна система реагування на загрози для безпеки кіберпростору;
- національні заходи зменшення загрози та уразливості кіберпростору;
- освіта та навчання з питань захисту кіберпростору;
- заходи щодо захисту кіберпростору органів влади;
- співробітництво з питань національної безпеки та безпеки міжнародного кіберпростору.

Перший напрям передбачає створення ефективної системи швидкої ідентифікації, обміну інформацією та заходи щодо зменшення втрат, викликаних зловмисними діями.

Серед основних видів діяльності щодо реагування на загрози для безпеки кіберпростору слід відзначити створення державно-приватної структури для реагування на кіберінциденти національного рівня; забезпечення проведення тактичного та стратегічного аналізу кібератак та оцінку вразливості; координацію управління кризами для захисту кіберпростору.

Другий напрям передбачає оперативне виявлення вразливих місць, які утворилися внаслідок технічної недосконалості та неправильної реалізації технологічних продуктів, а також нагляд за їх використанням. При цьому передбачається здійснення заходів підвищення спроможності правоохоронних органів запобігати атакам у кіберпросторі та переслідувати у судовому порядку тих, хто їх здійснює; розвиток системи виявлення слабких місць кіберсистем і телекомунікацій у масштабах країни з метою належної оцінки потенційних наслідків загроз та їх вразливості; захист механізмів Інтернету шляхом поліпшення протоколів обміну та маршрутизації; впровадження в експлуатацію надійних електронних систем управління та збору даних; скорочення кількості вразливих місць у програмному забезпеченні та їх ліквідацію; вивчення інфраструктурної взаємозалежності та зміцнення фізичної безпеки кіберсистем и телекомунікацій; визначення пріоритетних завдань з досліджень та розробок у галузі кіберпростору; здійснення оцінки та забезпечення безпеки в нових кіберсистемах.

Завдання третього напряму цієї Стратегії – вирішити питання забезпечення високоосвіченими кадрами, здатними працювати над скороченням вразливих місць в кіберпросторі. При цьому передбачається не тільки навчання, а й атестація тих, хто вже використовує комп'ютери, займається системним адмініструванням, розробляє та впроваджує інформаційні технології, а також керує інформаційними службами й установами [8, с. 45].

Найцікавішим для нас у контексті науково-практичної проблематики цієї статті є четвертий та п'ятий напрями: захист кіберпростору органів влади і співробітництво з питань національної безпеки та безпеки міжнародного кіберпростору.

Національна стратегія захисту кіберпростору визначає п'ять основних напрямів діяльності та ініціатив з питань захисту:

– постійний моніторинг й безперервна оцінка загроз та вразливих місць державних кіберсистем;

– встановлення достеменності та облік зареєстрованих користувачів державних кіберсистем;

– захист державних безпровідних локальних мереж;

– підвищення безпеки при розподілі державних підрядів і постачання.

Мережева глобальна структура системи Інтернет істотно ускладнює здійснення заходів окремою державою щодо захисту її національного сектору мережі. Кіберпростір будь-якої держави пов'язаний з усім іншим світом. Тому встановити джерело кібератаки без належного міжнародного співробітництва іноді неможливо.

Американці намагаються вирішити цю проблему шляхом системи заходів, спрямованих на досягнення високої ефективності контррозвідувальної діяльності в кіберпросторі; підвищення спроможності встановлення джерел кібератак та реалізації заходів у відповідь; удосконалення координації діяльності органів національної

безпеки США у питаннях реагування на кібератаки; співробітництво з приватним сектором і робота по лінії міжнародних організацій з метою розвитку діалогу і партнерства з зарубіжними урядами та приватним сектором, з акцентом на захисті інформаційних інфраструктур та популяризації глобальної «культури безпеки»; сприяння створенню національної та міжнародної систем спостереження та попередження, основне завдання яких полягає у виявленні та запобіганні кібератак у міру їх виникнення; заохочення інших держав до приєднання до Конвенції Ради Європи про кіберзлочинність або до того, щоб їх внутрішнє законодавство та процедури відповідали ідеології і цілком охоплювали проблематику цього напряму.

Використовуючи міжнародний досвід формування, використання та захисту національних інформаційних ресурсів, необхідно усвідомлювати, що він відображає реальний рівень експлуатації інформаційних технологій. Водночас формується нова ідеологія та напрями її реалізації, що істотно відрізняються від класичних систем обробки даних (які використовують технології клієнт-сервер та реляційні моделі даних).

Дедалі більшого розвитку набуває принцип організації інформаційних ресурсів на зразок «матриці», коли забезпечується гнучкий, безпечний та централізований розподіл ресурсів в інтересах так званих віртуальних організацій, що створюються для розв'язання завдань, які виникають у складній динамічній ситуації [9, с. 115].

Для оперативного аналізу і прийняття рішень у кризових ситуаціях в системі забезпечення державної безпеки США розробляється віртуальне аналітичне середовище, яке, як передбачається, дасть змогу на основі неструктурованої та неоднорідної (отриманої з різних джерел) інформації формувати об'єктивні дані про ситуацію та забезпечувати спільну роботу усіх зацікавлених учасників незалежно від місця їх розташування.

При цьому наголос робиться на поглибленому та неформальному аналізі передкризової ситуації в інтересах прийняття стратегічних рішень вищим керівництвом держави. Досягнення таким чином переваги у прийнятті рішень дозволить вжити запобіжних заходів щодо нейтралізації загроз державній безпеці. На думку фахівців, нині для Сполучених Штатів Америки ефективність системи забезпечення державної безпеки залежить не лише від кількості комп'ютерів, баз даних, супутників та агентів, а насамперед від ступеня обміну інформаційними даними.

В основу матричного підходу до організації розподілу інформаційних ресурсів між віртуальними організаціями буде покладено принцип організації роботи універсальної еталонної моделі взаємодії відкритих мереж, в якому інформаційна мережа розглядається як сукупність відповідних функцій, що групуються за рівнями.

Це дасть змогу вирішувати питання модернізації будь-якого рівня без істотної переробки інших. При цьому одне робоче місце матиме обмежений програмний ресурс в основному для виконання системних функцій, а усі прикладні програмні модулі завантажуватимуться з мережі. Тобто поступово мережа Інтернет трансформуватиметься в мережу програмних додатків [10, с. 11].

З урахуванням викладеного цілком очевидною є необхідність організації системних досліджень у галузі інформаційної складової державної безпеки, визначення місця та ролі інформаційних ресурсів у системі забезпечення державної безпеки України. Потребують глибокого науково-прогностичного переосмислення структурні та методологічні засади формування й використання інформаційних ресурсів, підходи до розробки інформаційної моделі прийняття рішень у системі забезпечення державної безпеки як невід'ємної складової національної безпеки України.

Практичні результати такої роботи можуть бути покладені в основу державної інформаційної політики, спрямованої на створення ефективної системи інформаційного забезпечення оперативного реагування на кризові ситуації. Необхідно розуміти, що це дасть змогу також прагматично підійти до формування тієї частини інформаційної політики, яка стосується розвитку комп'ютерних технологій та систем телекомунікацій; науково-технічної, технологічної та виробничої бази вітчизняного інформаційно-промислового комплексу; комп'ютерно-технологічної інфраструктури національних інформаційних ресурсів; інтегрованого комунікаційного середовища інформаційної сфери держави і суспільства.

Окремого наукового осмислення потребують підходи до впровадження державних регуляторних механізмів у міжнародній системі Інтернет, які повинні вирішувати завдання захисту державних інтересів з одночасним забезпеченням прав і свобод громадян на свободу інформації. Ці механізми мають захистити особисту інформацію та унеможливити проведення інформаційно-психологічних операцій, спрямованих проти особи, безпеки суспільства та держави, а також запобігти використанню інформаційних ресурсів з метою маніпуляції суспільною свідомістю.

Сьогодні перед науковцями, які працюють у галузі національної безпеки, постає не лише те-

оретичне, а й практичне завдання забезпечити науковий супровід переходу від суто технічного підходу щодо вирішення питань розвитку інформаційної сфери до філософсько-політичного узагальнення досягнутого у світі рівня інформаційного забезпечення життєдіяльності держави, суспільства, особи. Такий підхід повинен допомогти Україні вийти на засади побудови сучасного інформаційного суспільства, основними ресурсами якого є інформаційний, а не природний чи виробничий потенціал. Зволікання з цим може негативно позначитися на місці нашої країни у світі, добробуті й безпеці її громадян.

Література

1. *Брыжко* В. М. Будущее информационное право: учебник [для студ. высш. учебн. учрежд.] / В.М. Брыжко, А.А. Орехов, О.Н. Гальченко и др. [под ред. Р. А. Калюжного, М. Я. Швеца] – К.: Интеграл, 2002. – 264 с.

2. *Гавловський* В. Д. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії й практики / В.Д. Гавловський, М.В. Гуцалюк, Р.А. Калюжний та ін. – Запоріжжя: Просвіта, 2002. – 38 с.

3. *Голубєв* В. О. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: підручник [для студ. вищ. навч. закл.] / В.О. Голубєв, В.Д. Гавловський, В.С. Цимбалюк [за заг. ред. Р. А. Калюжного, М. Я. Швеця]. – Запоріжжя: Просвіта, 2001. – 252 с.

4. *Калюжний* Р.А. Інформатизація управління соціальними системами: організаційно-правові питання теорії і практики: навч. посібник [для студ. вищ. навч. закл.] / Р. А. Калюжний, М. Я. Швець. – К.: МАУП, 2003. – 336 с.

5. *Афанасьев* В. Г. Социальная информация / Афанасьев В.Г. – М.: Гран, 1994. – 164 с.

6. *Белл* Д. Грядущее постиндустриальное общество: Опыт социального прогнозирования / Белл Д. [пер. с англ. В. Иноземцев]. – М.: Academia, 1999. – 956 с.

7. *Винер* Н. Кибернетика и общество / Винер Н. – М.: Наука, 1958. – 282 с.

8. *Землянова* Л. М. Современная американская коммуникативистика: теоретические концепции, проблемы, прогнозы / Землянова Л. М. – М.: Изд-во МГУ, 1995. – 84 с.

9. *Мазур* М. Качественная теория информации / Мазур М. – М.: Прогресс, 1982. – 249 с.

10. *Урсул* А. Д. Информационная безопасность. Сущность, содержание и принципы ее обеспечения // Материалы конференции / Урсул А. Д., Цырдя Ф. Н.. – М.; 1999 – С. 1.

А. А. Бойченко

Анализ функционирования ведомственных информационных ресурсов ОВД.

Рассматриваются вопросы проблематики использования ведомственных информационных ресурсов в системе национальной безопасности государства. Определены предложения относительно усовершенствования организационно-правовых мероприятий применения ведомственных информационных ресурсов ОВС, как составляющей государственной безопасности страны.

A.A. Boychenko

Analysis of operation information resources Institutional ATS.

The questions of problem of the use of department informative resources are examined in the system of national safety of the state. Suggestions in relation to the improvement of organizationollegal measures of application of department informative resources of OIA, as a part of state security of country, are determined.