вольчої галузі європейськими країнами та "трансплантація" ефективних механізмів регулювання є невідкладним завданням у адаптації національної системи регулювання до міжнародних вимог.

Список використаних джерел

1. *Білик Ю. Л.* Продовольча безпека України: стан, проблеми та використання потенційних резервів продовольчого забезпечення населення / Ю. Л. Білик. - К. : Фенікс, 2000. - 56 с.

2. *Гойчук О. І.* Продовольча безпека : монографія / О. І. Гойчук. - Житомир : Полісся, 2004. - 348 с.

3. Деякі питання продовольчої безпеки : Постанова Кабінету Міністрів України від 5 груд. 2007 р. № 1379. - Режим доступу : http://www.uazakon.com/documents/date_bv/pg_gxcxoh.htm

4. Інформаційно-аналітична записка Міністерства економіки України "Оцінка стану продовольчої безпеки України у 2008 році". - Режим доступу : http://me.kmu.gov.ua/control/uk/publish/category/main?cat_id=32844

5. Офіційний сайт Державного комітету статистики України. - Режим доступу : http://www.ukrstat.gov.ua

6. Закон України про державну підтримку сільського господарства України. - Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1877-15

7. Состояние продовольственной необеспеченности в мире. 2008 / Продовольственная и сельскохозяйственная организация Объединенных Наций. - Режим доступа : http: www.fao.org

Віктор Янчук,
аспірант кафедри інформаційної політики НАДУ,
начальник відділу режиму і захисту інформації
Адміністрації Держприкордонслужби України

Підходи до вирішення завдання оцінювання ефективності захисту інформації в системі електронного урядування

У статті запропоновано порівняльний, системний та модельний підходи до вирішення завдання оцінювання ефективності захисту інформації в системі електронного урядування. В основу підходів покладено організаційно-методичний аспект оцінювання ефективності захисту інформації.
Ключові слова: державне управління, захист інформації, організаційно-методичний аспект, порівняльний підхід, системний підхід, модельний підхід.

In this article the correlative, systematic and model approaches are proposed with the aim of solving the task on informatin protection effectiveness assesment in the system of state governing electronic. The organisational-methodilogikal aspect of the information protection effectiveness assesment is the background of the approaches.
Key words: state governing, information protection, organizational methodological aspect, correlative approach, systematical approach, model approach.

Постановка проблеми. Результативність аналізу та повнота обробки все зростаючих обсягів відкритої інформації, яка є власністю держави, та інформації з обмеженим доступом (конфіденційної та секретної), вимога щодо захисту якої встановлена законом у системі електронного урядування (далі - ІСЕУ), можливі лише за умов застосування різноманітних інформаційно-комунікаційних технологій і загальнодержавних інформаційно-аналітичних систем різного рівня та призначення, чим пояснюється об'єктивність та невідворотність розвитку процесу інформатизації державного управління. При цьому розв'язання проблем щодо захисту зазначеної інформації з позиції мінімізації витрат і виділених ресурсів потребує нових підходів до вирішення питань оцінювання ефективності захисту ІСЕУ.

Необхідність визначення таких підходів пов'язана з головними напрямами державної інформаційної політики в Україні, яку розробляють і здійснюють органи державної влади загальної компетенції та відповідні органи спеціальної компетенції, а також із одним із трьох головних напрямів діяльності органів виконавчої влади у сфері забезпечення інформаційної безпеки України - захистом інформації [1].

Аналіз останніх досліджень та публікацій. Проведений аналіз останніх публікацій показав, що наукові дослідження щодо розв'язання зазначеної проблеми у сфері охорони державної таємниці та стосовно конфіденційної інформації проводять О.Є.Архипов, С.А.Архипова, І.Т.Бородавко, В.П.Ворожко, В.М.Луценко [2; 3]. Публікації присвячені розв'язанню проблеми розроблення методів та способів оцінки ефективності захисту відкритої інформації, яка є власністю держави, в науковій літературі не зустрічаються. В аспекті інформаційної політики на зазначену проблему звернули увагу В.В.Балюк [4], Г.Г.Почепцов, С.А.Чукут [5].

Невирішені раніше частини загальної проблеми. Варто зазначити, що незважаючи на активні дослідження проблеми оцінювання ефективності стану захисту ІСЕУ, у працях науковців недостатньо уваги приділяється питанню вивчення та визначення підходів до розв'язання зазначеної проблеми. Тому встановлення підходів до оцінювання ефективності стану захисту ІСЕУ потребує додаткових наукових досліджень.

Мета наукового дослідження - визначення підходів до розв'язання завдання оцінювання ефективності захисту ІСЕУ.

Поставленій меті відповідають такі *завдання*: аналіз організаційно-методичного, етичного та технологічного аспектів, визначення можливих підходів до вирішення завдання оцінювання ефективності захисту ІСЕУ.

Виклад основного матеріалу дослідження. Основною метою використання інформаційних технологій є підвищення ефективності механізмів державного управління. Відомо, що сучасні інформаційні технології, у тому числі й високоефективні технічні засоби, за допомогою яких можна легко здобувати, пересилати та аналізувати ІСЕУ, дають змогу іноземним держа-

вам реалізувати власні інтереси без застосування воєнної сили, послабити або завдати значної шкоди безпеці Україні. Разом з тим на фоні загального динамічного розвитку систем захисту інформації, інтенсивної гармонізації національної нормативної бази із світовими та європейськими стандартами у галузі інформаційної безпеки ситуація щодо захисту ІСЕУ виглядає стабільно консервативною, відстороненою щодо сприйняття і використання нових напрямів, технологій та ідей. Тому актуальним і важливим завданням є забезпечення інформаційної безпеки діяльності органів державної влади, елементів інформаційно-технологічної інфраструктури держави, а також розвитку єдиної захищеної телекомунікаційної інфраструктури для державних потреб та ефективного захисту ІСЕУ в умовах постійно діючих реальних та потенційних загроз [1; 6; 7].

Характеристики цих загроз суттєво залежать від видів та типів інформаційно-телекомунікаційних систем та інших технічних засобів органів державного управління, їх просторового розміщення один відносно іншого, ступеня взаємної сумісності, що ускладнює процедуру визначення конкретного переліку реально існуючих загроз, формалізацію цієї процедури, можливості використання шаблонів чи каталогів типових загроз, вимагає проведення індивідуального поглибленого аналізу інформаційного середовища та факторів, що впливають на функціонування зазначених систем та засобів, а також призводить до створення неефективних систем захисту ІСЕУ.

Проблема забезпечення оцінювання ефективності захисту ІСЕУ також загострюється жорсткими фінансовими умовами, у яких здійснюється державне управління.

Зважаючи на викладене, завдання оцінювання ефективності захисту ІСЕУ розглянуто з позицій аналізу організаційно-методичного, етичного та технологічного аспектів.

Так, аналіз організаційно-методичного аспекту показав, що ситуація в державі щодо електронного урядування ускладнюється поки що безсистемним розвитком українського законодавства, яке регулює відносини в інформаційній сфері із запізненням у часі (орієнтовно на 5-20 років відносно часу видання аналогічних актів законодавства в інших країнах), а також відсутністю єдиної базової методики оцінювання ефективності захисту ІСЕУ. Розглянувши структуру закріплення чинними нормативно-правовими актами правових норм на доктринальному, концептуальному, стратегічному, програмному та плановому рівнях, бачимо, що вони за сукупністю не дають змоги розв'язувати проблеми методичного забезпечення захисту ІСЕУ й інформаційної безпеки держави в усіх їх складових [1; 7-12].

Аналіз етичного аспекту показав, що існує досить поширена думка щодо неможливості (або недоречності з етичних міркувань) використання грошового виміру для визначення збитків (шкоди), що виникли внаслідок

втрат чи витоку ІСЕУ. Застосування умовних бальних оцінок (розрахункових або експертних) шкоди, заподіяної повною чи частковою втратою інформації, певною мірою дає змогу зняти цей проблемний аспект. Зворотна процедура визначення за відомим ступенем обмеження доступу до певної інформації її умовно-бальної вартості дає змогу розрахувати можливу шкоду від втрати цієї інформації внаслідок реалізації тієї чи іншої загрози (частково або в повному обсязі). Умовні бальні оцінки можуть бути використані при визначенні шкоди, заподіяної втратою секретної, конфіденційної та відкритої інформації, що є складовими частинами ІСЕУ, чи у їх комбінаціях [3; 7].

Аналіз технологічного аспекту показав, що складання повного переліку загроз, специфічних для кожного конкретного органу державного управління, підприємства, установи, а також міністерств, відомств чи держави загалом само по собі є досить складним завданням, а в деяких випадках і не завжди можливим і економічно доцільним. Разом з тим для полегшення вирішення завдання аналізу загроз доцільно розробити та використовувати спеціальні базові переліки загроз для певних типових ситуацій, у тому числі й окремо для кожного конкретного органу державного управляння, підприємства установи, а також міністерств, відомств чи держави загалом.

З огляду на результати аналізу різних аспектів вирішення завдання оцінювання ефективності захисту ІСЕУ вбачається найбільш доцільним розглянути можливість такого вирішення з позиції підходів, притаманних організаційно-методичному аспектові, пов'язавши ці підходи з визначенням об'єктів системи державного управління, стосовно яких і буде вирішуватися зазначене завдання.

Такими об'єктами у системі державного управління визначимо:

• локальні об'єкти - органи державного управляння, підприємства чи установи, а також їх окремі підрозділи, що функціонують на нижньому рівні державного управління і забезпечують впровадження державної політики в тій чи іншій сфері діяльності держави;

• об'єкт "сфера-галузь" - органи державного управління, міністерства чи відомства, а також їх окремі органи, організації чи установи спеціальної компетенції, що функціонують на середньому рівні державного управління і забезпечують розроблення та впровадження державної політики у тій чи іншій сфері чи галузі діяльності держави;

• об'єкт "держава" - органи державного управління загалом, що за сукупністю складають вищий рівень державного управління, якому притаманний широкий спектр функціональних завдань.

Залежно від того, що розуміємо під об'єктом системи інформатизації системи електронного урядування, запропоновано застосування порівняльного, модельного та системного підходів до вирішення завдання визначення ефективності захисту ІСЕУ, впровадженого на відповідному об'єкті.

Порівняльний підхід пропонується застосовувати для вирішення завдання оцінювання ефективності захисту інформації на локальних об'єктах системи електронного урядування. Зазначений підхід базується на зіставленні переліку загроз інформації, що циркулює на локальному об'єкті, з комплексом заходів та засобів, які пропонується застосувати для нейтралізації визначених загроз. Надійність функціонування зазначеного комплексу заходів та засобів, рівень нейтралізації сукупності загроз та вартість захисту ІСЕУ власне і визначатимуть ефективність захисту інформації на локальних об'єктах системи електронного урядування.

Модельний підхід пропонується застосовувати для вирішення завдання оцінювання ефективності захисту інформації на об'єктах "держава" системи електронного урядування. Зазначений підхід базується на побудові моделі ефективності функціонування захисту ІСЕУ держави, яка пов'язує ступінь ефективності захисту ІСЕУ з певним нечисленним набором діагностичних показників такого захисту, таких як захищеність, значущість. Останні є опосередковано залежними від комплексу захисних функцій, притаманних захисту об'єкта "держава" системи електронного урядування. Діагностичні показники припускають ту чи іншу змістову інтерпретацію і можуть бути кількісно обчислені через певні об'єктивні дані, що характеризують функціонування системи інформаційної безпеки держави, наприклад, становлять результати моніторингу стану захисту ІСЕУ. Застосування модельного підходу принципово не може бути зведено до типової процедури і в кожному випадку потребує проведення спеціальної наукової розробки. Разом з тим застосування математико-статистичних методів скорочення розмірності набору вхідних даних (факторний, дисперсійний аналіз, інші), реально дає можливість отримати прозору інтерпретацію властивостей діагностичних показників, установити їх зв'язок із функціями захисту ІСЕУ. При цьому порівняльний підхід до оцінювання ефективності захисту ІСЕУ об'єкта "держава", на думку автора, не може бути застосований через занадто довгий перелік загроз, у зв'язку з чим можливість дослідити або хоча б відстежити вплив кожної окремої загрози на стан захисту інформації в країні є завданням вкрай проблематичним.

Системний підхід (оцінювання та керування інформаційними ризиками) пропонується застосовувати для вирішення завдання оцінювання ефективності захисту інформації на об'єктах "сфера-галузь", зважаючи на те, що такий підхід дає можливість визначити склад ІСЕУ, оцінити необхідний ступінь захисту ІСЕУ, обрати стратегію розвитку інформаційної структури об'єкта "сфера-галузь" й підтримувати на відповідному рівні її безпеку. Зазначений підхід базується на зіставленні вихідних та залишкових ризиків для ІСЕУ, які розраховуються через оцінки можливих збитків, що можуть виникнути внаслідок ймовірної реалізації загроз зазначеній інформації до або після впровадження захисту ІСЕУ. За результатами порівняння робиться

висновок щодо доцільності використання тих чи інших механізмів захисту ІСЕУ, їх ефективності та ефективності функціонування захисту ІСЕУ в цілому. Крім того, встановлено, що в умовах сучасної ринкової економіки системний підхід дає змогу враховувати аспект економічної доцільності, зважаючи на можливість зіставлення витрат на створення захисту ІСЕУ на об'єктах "сфера-галузь", який забезпечує певні вимоги до рівня захисту ІСЕУ, із загальноекономічними характеристиками об'єктів "сфера-галузь" чи показниками інформаційної діяльності, що ними забезпечується.

За результатами аналізу застосування порівняльного, модельного та системного підходів до визначення ефективності захисту ІСЕУ, впровадженого на відповідному об'єкті державного управління, визнано ефективним тільки активні системи захисту ІСЕУ, які мають прогностичні якості й забезпечують успішний випереджальний захист щодо можливих атак і мають, таким чином, практично нульові втрати. Разом з тим встановлено, що активний захист ІСЕУ принципово не може будуватися за єдиним шаблоном, має індивідуальні властивості, залежні від напряму діяльності конкретного об'єкта державного управління, його інформаційної структури, рівня й особливостей інформаційних ресурсів, кадрового забезпечення тощо. Крім того, активний прогностичний захист вимагає постійного пошуку та аналізу інформацій про наміри і можливості потенційного зловмисника, моніторингу загроз в умовах постійних змін інформаційного середовища. Очевидно, що при цьому враховуються і певні загальні тенденції, і рекомендації, які відпрацьовуються на рівні державного управління та залежать від встановлених вимог ефективності захисту ІСЕУ об'єкта "держава".

Завдання оцінювання ефективності захисту ІСЕУ є багатоаспектним і достатньо фінансово затратним, тому наявність економічного зіставлення витрат на захист ІСЕУ, його окремих складових із можливими наслідками від втрат ІСЕУ є необхідною умовою створення ефективного захисту ІСЕУ, обов'язковим зворотним зв'язком, який дасть змогу оцінити доцільність і достатність реалізації того чи іншого елемента захисту ІСЕУ, дієвість функціонування захисту ІСЕУ в цілому, його адекватність існуючим зовнішнім та внутрішнім загрозам.

Висновки. У статті для вирішення завдання оцінювання ефективності захисту ІСЕУ запропоновано використати порівняльний, системний та модельний підходи, які, на відміну від існуючих, повністю враховують усі види об'єктів державного управління, що дає змогу підвищити рівень об'єктивності та ефективності захисту інформації на локальних об'єктах, об'єктах "сфера-галузь" та "держава" системи електронного урядування.

Правові норми щодо забезпечення захисту ІСЕУ на доктринальному, концептуальному, стратегічному, програмному та плановому рівнях у їх прямому значенні на сьогодні фактично не мають достатнього законодавчого закріплення.

Перспективи подальших розвідок у даному напрямі полягають у необхідності проведення спеціальної наукової розробки можливості застосування системного та модельного підходів для вирішення завдання оцінювання ефективності захисту інформації на об'єктах "сфера-галузь" та "держава" системи електронного урядування.

Також вбачається за доцільне провести подальшу розвідку щодо складання типової методики оцінювання стану захисту інформації локальних об'єктів системи електронного урядування та розробленні доктринальних, концептуальних, стратегічних і програмних документів з метою обґрунтування принципів, методів та засобів ефективного управління захистом ІСЕУ, адекватних новим політичним, соціальним та економічним відносинам у державі.

Список використаних джерел

1. Доктрина інформаційної безпеки України : Указ Президента України від 8 лип. 2009 р. № 514/2009 // Офіц. вісн. України. - 2009. - № 52. - Ст. 1783.

2. *Архипов А. Е.* Особенности использования средств технической защиты информации от утечки за счет побочных электромагнитных излучений и наводок / А. Е. Архипов, В. Н. Луценко, В. А. Худяков // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - 2002. - № 4. - С. 178-182.

3. *Архипов О. Є.* Оцінювання ефективності системи охорони державної таємниці : монографія / О. Є. Архипов, І. Т. Бородавко, В. П. Ворожко. - К. : Наук.-вид. відділ НА СБУ України, 2007. - 63 с.

4. *Балюк В. В.* Стан інформатизації органів виконавчої влади як фактор до широкого впровадження електронного врядування в Україні / В. В. Балюк // Вітчизняний і зарубіжний досвід впровадження електронного урядування : зб. матеріалів наук.-практ. конф. / за заг. ред. д-ра наук з держ. упр. проф. С. А. Чукут, канд. наук з держ. упр. О. В. Загвойської. - К. : Майкрософт, 2008. - С. 11-15.

5. *Почепцов Г. Г.* Інформаційна політика : навч. посіб. / Г. Г. Почепцов, С. А. Чукут. - 2-ге вид., стер. - К. : Знання, 2008. - 663 с.

6. *Гринберг А. С.* Защита информационных ресурсов государственного управления / А. С. Гринберг, Н. Н. Горбачев, А. А. Тепляков. - М. : ЮНИТА-ДАНА, 2003. - 327 с.

7. Закон України про основи національної безпеки України. - Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=964-15

8. *Змитрович А. И.* Интеллектуальные информационные системы / А. И. Змитрович. - Минск : НТОО "Тетра Системс", 1997. - 368 с.

9. *Мусиенко Д. М.* Защита электронного оборудования от деструктивного воздействия беспроводных технических средств / Д. М. Мусиенко // Бизнес и безопасность. - 2005. - № 5. - С. 37-42.

10. Закон України про інформацію. - Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12

11. Закон України про державну таємницю. - Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3855-12

12. Закон України про захист інформації в інформаційно-телекомунікаційних системах. - Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=80%2F94-%E2%F0