УДК 004.056: 004.942

ОРГАНІЗАЦІЙНО-ПРАКТИЧНІ АСПЕКТИ ПОБУДОВИ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ СИСТЕМИ З ІНФОРМАЦІЄЮ, ЩО ПУБЛІКУЄТЬСЯ В ГЛОБАЛЬНІЙ МЕРЕЖІ

Носов Віталій; Манжай Ірина

Харківський національний університет внутрішніх справ,
Харківський економіко-правовий університет

ORGANIZATIONAL AND PRACTICAL ASPECTS OF CONSTRUCTION OF INFORMATION SECURITY COMPLEX SYSTEM FOR THE SYSTEM WITH INFORMATION WHICH IS PUBLISHED IN GLOBAL NETWORK

Nosov Vitalii; Manzhai Irina

Kharkiv National University of Internal Affairs

Анотація: **Проаналізовано нормативно-правову базу в сфері побудови комплексної системи захисту інформації. Розглянуто коло суб'єктів, можливі варіанти та послідовність дій власника інформаційно-телекомунікаційної системи щодо розробки та впровадження комплексної системи захисту інформації. Визначено послуги, які надаються виконавцем при створенні та супроводженні комплексної системи захисту інформації. Окреслено окремі елементи контролю відповідної системи, а також проаналізовано орієнтовні час і витрати на її розробку.**

Ключові слова: **відкрита інформація, організація захисту, комплексна система захисту інформації, час і витрати, глобальна мережа**

Summary: **The normative and legal base is analyzed in the field of construction of the information security complex system. The circle of subjects, possible variants and sequence of executions of owner of the informatively-telecommunication system, is considered on development and introduction of the information security complex system. Services which are given a performer at creation and accompaniment of the information security complex system are certain. The separate elements of control of the proper system are outlined, and also tentatively is analyzed time and costs for its development.**

Keywords: **public data, organization of security, information security, information security complex system, time and costs, global network.**

Вступ

Потужна інформатизація українського суспільства вочевидь експоненційно збільшує кількість інформаційно-телекомунікаційних систем (ІТС), доступ до ресурсів яких здійснюється через глобальну мережу Інтернет. У загальному випадку такі системи не містять інформацію з обмеженим доступом але у визначених законодавством випадках потребують захисту цілісності і доступності інформації, що оприлюднюється, шляхом створення комплексної системи захисту інформації (КСЗІ).

Власник (розпорядник) такої ІТС, який раніше системно не вирішував задачі захисту інформації, стикається з такими організаційно-практичними питаннями:

– які є релевантні нормативно-правові акти в Україні щодо КСЗІ для ІТС з відкритою інформацією і доступом до неї через Інтернет?

– які існують правові підстави у необхідності створення КСЗІ?

– хто розробляє і впроваджує КСЗІ?

– чи є варіанти створення КСЗІ?

– якою є послідовність дій власника (розпорядника) ІТС із організації розробки КСЗІ?

– які надаються послуги виконавцем при створенні та супроводженні КСЗІ?

– яким чином і ким підтверджується якість створеної КСЗІ?

– яким чином і хто контролює функціонування КСЗІ?

– яким є орієнтовний час та витрати на розробку КСЗІ?

Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язок) надає загальний опис порядку створення КСЗІ, проведення експертизи та видачі Експертних висновків і Атестатів відповідності [1], який або не в повній мірі або зовсім не надає відповіді на поставленні вище організаційно-практичні питання.

Дослідження відповідних нормативно-правових актів і ринку послуг із створення КСЗІ дозволив встановити наступне.

Основна частина

Релевантні нормативно-правові акти щодо КСЗІ для ІТС з відкритою інформацією і доступом до неї через Інтернет.

Аналіз нормативно-правової бази України, яка регламентує розробку та функціонування КСЗІ для ІТС з відкритими інформаційними ресурсами дозволив розділити її на такі акти:

– концептуальні (20 актів);

– основні (4 акти);

– суміжні (17 актів);

– проведення експертних робіт (4 акти);

– державного контролю (3 акти).

У зв'язку із обмеженням обсягу публікації повний перелік актів не наводиться.

Правові підстави створення КСЗІ для ІТС з відкритою інформацією.

ІТС з відкритою інформацією і доступом до неї через Інтернет належить до автоматизованої системи класу 3 (є багатомашинним багатокористувачевим комплексом, який характеризується необхідністю передачі інформації через незахищене середовище) [2].

Захист відкритої інформації в Україні регламентує:

1. Концепція технічного захисту інформації в Україні [3].

2. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [4].

Згідно з Концепцією одним з принципів формування і проведення державної політики у сфері технічного захисту інформації (ТЗІ) є обов'язковість захисту інженерно-технічними заходами інформації, яка становить державну та іншу передбачену законом таємницю, службової інформації, *відкритої інформації, важливої для держави*, незалежно від того, де зазначена інформація циркулює, а також *відкритої інформації, важливої для особи та суспільства*, якщо ця інформація циркулює в органах державної влади та органах місцевого самоврядування, Національній академії наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ, на державних підприємствах, в державних установах і організаціях. Для відкритої інформації захисту потребують такі її властивості як *цілісність* та *доступність*.

Віднесення тієї чи іншої інформації до категорії відкритої проводиться згідно із законом «Про інформацію» [5] та Правилами [4].

Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом. До відкритої інформації, що підлягає захисту, зокрема відносять інформацію, яка належить до *державних інформаційних ресурсів* (інформація, яка є власністю держави та (або) необхідність захисту якої визначено законодавством), а також *про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті*, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами.

В окремих випадках відкриту інформацію доцільно захищати від несанкціонованого копіювання. З правової точки зору мова насамперед йде про використання інституту захисту інтелектуальної власності.

В інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах для захисту відкритої інформації створюється КСЗІ та *підтверджується її відповідність*. Відповідно до ч. 2 ст. 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [6] підтвердження відповідності здійснюється за результатами *державної експертизи* в порядку, встановленому законодавством. Також відповідно до ч. 3. ст. 8 цього ж закону для створення КСЗІ використовуються *засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок* за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

Завдання, які вирішує КСЗІ, для відкритої інформації:

1. Захист від несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів (*обов'язковий елемент*).

2. Захист інформації від витоку технічними каналами (*забезпечується в системі у разі, коли в ній обробляється інформація, що становить державну таємницю, або коли відповідне рішення щодо необхідності такого захисту прийнято розпорядником інформації*).

3. Захист від спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування (*забезпечується в системі, якщо рішення про необхідність такого захисту прийнято розпорядником інформації*).

Між Концепцією [3] та Правилами [4] існує певна неузгодженість, оскільки перша наголошує на необхідності захисту відкритої інформації, важливої для держави, особи та суспільства. Правила ж зобов'язують захищати всю відкриту інформацію [7, с. 46-49]. Враховуючи те, що Правила мають розпорядчий характер можна дійти висновку, що *захисту мають підлягати усі відкриті державні інформаційні ресурси*.

Основні процедурні моменти створення КСЗІ викладено у нормативних документах системи технічного захисту інформації, а саме у НД ТЗІ 3.7-003-05 [8]. КСЗІ створюється на підставі Технічного завдання, розробленого згідно з вимогами НД ТЗІ 3.7-001-99 [9].

Для ІТС з відкритою інформацією, що підлягає обов'язковому захисту, відповідно до НД ТЗІ 3.7-003-2005 [8] має бути також передбачено створення *комплексу засобів захисту від несанкціонованого доступу*. Комплекс засобів захисту інформації включає в себе програмні, апаратні, програмно-апаратні засоби та засоби криптографічного захисту інформації.

Розробці КСЗІ передує створення служби захисту інформації, вимоги до якої визначені в НД 1.4-001-2000 [10].

Виконавці розробки і впровадження КСЗІ.

Виконавцем робіт із створення (експертизи) КСЗІ може бути суб'єкт господарської діяльності або орган виконавчої влади, який має *ліцензію або дозвіл* на право провадження хоча б одного виду робіт у сфері ТЗІ, необхідність проведення якого визначено технічним завданням на створення системи захисту [4, ст. 23].

Відповідно до вимог [11] ліцензуванню підлягає надання послуг з:

1. Оцінювання захищеності інформації, що не становить державної таємниці.

2. Оцінювання захищеності інформації усіх видів, у тому числі інформації, що становить державну таємницю.

3. Виявлення закладних пристроїв.

Під час створення (експертизи) КСЗІ для відкритої інформації має бути ліцензія або дозвіл за першим або другим напрямом.

Варіанти створення КСЗІ для ІТС з відкритою інформацією і доступом до неї через Інтернет.

Можна виділити два основних варіанти створення КСЗІ для ІТС, яка розроблялася без комплексу засобів захисту від несанкціонованого доступу:

1) розробка засобів захисту для вже розробленого програмного забезпечення;

2) адаптація розробленого програмного забезпечення під вже розроблені і сертифіковані засоби захисту.

У першому випадку потрібно буде проводити більш тривалу та вартісну оцінку захищеності силами відповідних підрядників-ліцензіатів та адаптувати програмний код системи до вимог нормативних документів у сфері ТЗІ.

У другому випадку слід враховувати, що на теперішній час є два відповідних сертифікованих засоби, які потенційно можуть бути використані у системі ІТС з відкритою інформацією і доступом до неї через Інтернет та які мають діючий експертний висновок на відповідність вимогам законодавства в сфері ТЗІ, це:

– комплекс засобів захисту Web-ресурсів від несанкціонованого доступу «Тайфун-Web» версії 1.хх, виробництва ТОВ «Інститут комп'ютерних технологій» (функціональний профіль: КА-2, КВ-2, ЦА-1, ЦВ-2, ДС-1, ДЗ-1, ДВ-1, НР-1, НИ-1, НО-1, НЦ-1, НТ-2, НВ-2 з рівнем гарантії Г-4 оцінки коректності його реалізації згідно з НД ТЗІ 2.5-004-99). Інформацію про комплекс можна дізнатись за адресою: http://www.ict.com.ua;

– комплекс засобів захисту системи управління порталом «Портал Менеджер 1.0» виробництва ТОВ «Софтлайн-ІТ», яке постачає ТОВ "Айкюжн" (функціональний профіль: КА-2, ЦА-1, ЦО-1, ДВ-1, НР-2, НИ-1, НИ-2, НК-1, НО-2, НЦ-1, НТ-2, НВ-1 з рівнем гарантії Г-2 оцінки коректності його реалізації згідно з НД ТЗІ 2.5-004-99). Інформацію про комплекс можна дізнатись за адресою: http://www.iqusion.com.

Таким чином, ліцензіат-виконавець на етапі побудови КСЗІ після оцінки наявного стану захищеності ІТС:

– або надає рекомендації розробнику системи для самостійної розробки засобів захисту і модернізації системи відповідно до вимог нормативних документів у сфері ТЗІ;

– або пропонує вже існуючі сертифіковані засоби захисту і бере участь в адаптації розробленого програмного забезпечення системи під надані засоби захисту.

Послідовність дій власника (розпорядника) ІТС із організації розробки КСЗІ.

Організація-власник (розпорядник) ІТС:

а) визначає правові підстави у необхідності створення КСЗІ для ІТС;

б) визначає для ІТС відповідальну за захист інформації особу (службу захисту інформації), яка буде у подальшому забезпечувати функціонування КСЗІ і повноваження якої визначено у [10];

в) здійснює вибір ліцензіата-виконавця робіт із створення КСЗІ для ІТС та заключає із ним договір на виконання робіт:

– вимоги, що пред'являються до ліцензіатів наведено в [11];

– перелік ліцензіатів наведений на веб-сторінці Держспецзв'язку [12].

Обсяг послуг виконавця із розробки КСЗІ.

Ліцензіат-виконавець згідно [8] поетапно створює КСЗІ для ІТС:

а) формує загальні вимоги до КСЗІ;

б) розробляє політику безпеки інформації в ІТС;

в) розробляє технічне завдання на створення КСЗІ;

г) розробляє проект КСЗІ;

д) вводить КСЗІ в дію;

е) за узгодженням із Адміністрацією Держспецзв'язку оцінює захищеність інформації (проводить державну експертизу) в ІТС;

ж) виконує роботи з організаційного забезпечення функціонування КСЗІ та управління засобами захисту інформації відповідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ, гарантійному і післягарантійному технічному

обслуговуванню засобів захисту інформації.

Більш розгорнутий перелік послуг зі створення та супроводження КСЗІ може виглядати наступним чином [13; 14].

1. *Підготовка організаційно-розпорядчої документації*. У рамках цього етапу спочатку проводиться аналіз існуючої організаційно-розпорядчої документації (організаційна структура, штатний розклад, положення про відділи і посадові інструкції співробітників, пов'язаних з експлуатацією системи, документи, що регламентують доступ до системи тощо). За результатами проведеного аналізу готуються проекти документів, які визначають організаційну складову КСЗІ (проект наказу про створення КСЗІ, проект положення про службу захисту інформації, проекти посадових інструкцій і процедур тощо), які затверджуються Замовником.

2. *Обстеження інформаційної інфраструктури Замовника*. На цьому етапі аналізується архітектура системи, її топологія і складові елементи. Визначаються типи користувачів системи, типізується інформація, що обробляється в системі. У результаті розробляються акт обстеження системи (містить її опис, принципи побудови і архітектуру) та перелік об'єктів системи, що підлягають захисту, які затверджуються Замовником.

3. *Розробка «Плану захисту інформації»*. За підсумками цього етапу мають бути підготовлені наступні документи: «Модель загроз інформації. Модель порушника», «Положення про Службу захисту інформації», «Політика безпеки інформації». Вказані документи мають бути затверджені Замовником.

4. *Розробка «Технічного завдання на створення КСЗІ»*. У технічному завданні викладаються вимоги до функціонального складу і порядку розробки і впровадження технічних засобів, які забезпечують безпеку інформації в процесі її обробки в обчислювальній системі, а також вимоги до організаційних, фізичних та інших заходів захисту, які реалізуються поза обчислювальною системою в доповнення до комплексу програмно-технічних засобів захисту інформації. Технічне завдання може розроблятися для вперше створюваних систем, а також під час модернізації вже існуючих у вигляді окремого розділу технічного завдання на створення системи, окремого (часткового) технічного завдання або доповнення до технічного завдання на створення системи.

5. *Розробка «Технічного проекту на створення КСЗІ»*. Цей документ розробляється після узгодження технічного завдання з Держспецзв'язком. До цього комплекту документів входить частина документів розроблених на попередніх етапах і низка нових, в яких описано, як саме створюватиметься, експлуатуватиметься і, у разі потреби, модернізуватиметься КСЗІ. Технічний проект на створення КСЗІ розробляється на підставі і відповідно до технічного завдання. Під час розробки проекту КСЗІ обґрунтовуються і приймаються проектні рішення, які дають можливість реалізувати вимоги технічного завдання, забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і способів захисту інформації. В результаті створюється комплект робочої і експлуатаційної документації, необхідної для забезпечення тестування, проведення пусконалагоджувальних робіт, випробувань та управління КСЗІ.

6. *Приведення інформаційної інфраструктури Замовника у відповідність з «Технічним проектом на створення КСЗІ»*. Особливістю цього етапу є те, що на момент ухвалення рішення про створення КСЗІ вартість цього етапу є невідомою як для Замовника, так і для Виконавця. Також, зважаючи на великий можливий спектр виконання робіт, на цьому етапі існує велика вірогідність підключення до його виконання Підрядників. На цьому етапі можуть виконуватися монтажні, будівельні, пусконалагоджувальні роботи, роботи, пов'язані зі встановленням необхідних технічних або криптографічних засобів захисту інформації, засобів фізичного

захисту елементів системи (встановлюється необхідне устаткування і програмне забезпечення, засоби контролю доступу, охоронна і пожежна сигналізації) тощо.

7. *Розробка «Експлуатаційної документації на КСЗІ»*. По завершенню цього етапу мають бути підготовлені наступні документи: інструкції експлуатації КСЗІ і її елементів; процедури регламентного обслуговування КСЗІ; правила і положення проведення тестування і аналізу роботи КСЗІ; керівництво адміністраторів і користувачів; формуляр КСЗІ системи.

8. *Впровадження КСЗІ*. На цьому етапі здійснюється організація захисту інформації від несанкціонованого доступу та антивірусного захисту інформації, розробка програми і методики попередніх випробувань, проведення попередніх випробувань.

9. *Випробування КСЗІ*. В процесі випробувань виконуються тестові завдання і контролюються отримані результати, які є індикатором працездатності спроектованої КСЗІ. За результатами випробування КСЗІ робиться висновок про можливість представлення КСЗІ на державну експертизу. Під час дослідної експлуатації: відпрацьовують технології обробки інформації, облік машинних носіїв інформації, управління засобами захисту, розмежування доступу користувачів до ресурсів системи і автоматизованого контролю за діями користувачів; співробітники служби захисту інформації і користувачі системи набувають практичних навичок використання технічних і програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних і розпорядчих документів з питань розмежування доступу до технічних засобів і інформаційних ресурсів; здійснюється (за потреби) доопрацювання програмного забезпечення, додаткове налагодження і конфігурація комплексу засобів захисту інформації від несанкціонованого доступу; здійснюється (за потреби) коректування робочої і експлуатаційної документації.

10. *Проведення державної експертизи КСЗІ і отримання «Атестата відповідності»*.

11. *Підтримка і обслуговування КСЗІ*.

Підтвердження якості створеної КСЗІ.

Після введення КСЗІ у дію і проведення випробувань необхідно провести державну експертизу КСЗІ, порядок організації і проведення якої регламентується в [15].

Експертиза КСЗІ є процедурою підтвердження відповідності КСЗІ вимогам нормативних документів ТЗІ і проводиться шляхом *експертних випробувань* або шляхом *аналізу декларації про відповідність КСЗІ вимогам нормативних документів із ТЗІ*.

Метою проведення первинної державної експертизи у сфері технічного захисту інформації КСЗІ є отримання Експертного висновку про відповідність КСЗІ вимогам нормативних документів у сфері технічного захисту інформації та Атестату відповідності КСЗІ вимогам нормативних документів у сфері технічного захисту інформації.

Державна експертиза проводиться для визначення відповідності КСЗІ технічному завданню, вимогам нормативних документів із захисту інформації та визначення можливості введення КСЗІ в складі інформаційно-телекомунікаційної системи в промислову експлуатацію.

Державна експертиза КСЗІ для ІТС з відкритою інформацією і доступом до неї через Інтернет проводиться шляхом експертних випробувань. Порядок її організації і проведення можна представити як на рис. 1 [16, с. 156-157].

Експертиза включатиме наступні послуги:

– *аналіз технічної документації на КСЗІ, середовища її функціонування*;

– *розробка Програми і методик проведення експертизи* (документи: Програма та методика проведення державної експертизи);

– *проведення експертного оцінювання КСЗІ* (документи: Протокол експертних випробувань);

– *оформлення результатів експертизи та* підготовка *експертного висновку відповідно до вимог НД ТЗІ*;

– *супроводження розгляду в Державній службі спеціального зв'язку та захисту* інформації *результатів проведення експертизи* (документи: Атестат відповідності, Акт введення в дію КСЗІ).

Рис. 1. Порядок організації і проведення державної експертизи шляхом експертних випробувань

Виявлені під час державної експертизи недоліки повинні усуватися до її завершення. Якщо в силу якихось причин усунути недоліки під час експертизи неможливо, це оформлюється актом, до якого вноситься перелік необхідних доробок та рекомендації щодо їх виконання. Після завершення передбачених актом заходів проводиться повторна експертиза.

Якщо інтегрована КСЗІ має у своєму складі типові модулі, які створювались за єдиним технічним завданням, то експертиза таких модулів КСЗІ виконується в два етапи: на першому проводиться у повному обсязі експертиза одного обраного типового модуля, а на другому – здійснюється перевірка відповідності умов експлуатації типовим на кожному конкретному об'єкті для всіх модулів КСЗІ цього типу.

Після завершення державної експертизи власнику системи надається атестат відповідності КСЗІ, зареєстрований в Державній службі спеціального зв'язку та захисту інформації України, та позитивний експертний висновок, якщо під час проведення експертизи не було виявлено недоліків, які не було усунуто до її завершення.

Отже, у результаті проведення державної експертизи КСЗІ шляхом експертних випробувань необхідно мати:

– *Протоколи* виконання робіт відповідно до окремої методики експертизи КСЗІ;

– *Експертний висновок*, зареєстрований і затверджений Експертною радою Держспецзв'язку;

– *Атестат відповідності*, зареєстрований і виданий Держспецзв'язком.

Для того, щоб ввести в дію КСЗІ проводяться відповідні заходи з підготовки організаційної структури та розробки розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в системі, якщо цього не було зроблено на попередніх етапах. Також на етапі введення в дію КСЗІ виконуються заходи з організаційного забезпечення функціонування КСЗІ та управління засобами захисту відповідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ, гарантійному і післягарантійному технічному обслуговуванню засобів захисту інформації.

Контроль за функціонуванням КСЗІ.

Після проведення державної експертизи згідно з нормативними документами [17; 18] передбачається контроль за функціонуванням КСЗІ ІТС з боку Держспецзв'язку. Ця діяльність здійснюється шляхом організації і проведенням контрольно-інспекторської роботи з питань ТЗІ.

Порушення встановлених норм і вимог ТЗІ, що можуть бути виявлені під час проведення перевірок, розділяються на *три категорії порушень*. Для КСЗІ ІТС з відкритою інформацією і доступом до неї через Інтернет може бути порушення тільки третьої категорії, яка не пов'язана із загрозою порушення конфіденційності.

Ліцензіат-виконавець, який створював КСЗІ для ІТС, у подальшому може бути залучений або для вдосконалення стану ТЗІ, або для усунення недоліків, виявлених в ході проведення Держспецзв'язком перевірок.

Орієнтовний час та витрати на розробку КСЗІ.

Для аналізу ринку послуг в сфері розробки та експертизи КСЗІ ІТС з відкритою інформацією і доступом до неї через Інтернет було використано наступні методи:

– безпосереднє звернення до компаній, які мають ліцензію у сфері створення КСЗІ та її експертизи;

– аналіз пропозицій компаній в мережі Інтернет;

– аналіз тендерної документації державних закупівель послуг у сфері створення та експертизи КСЗІ.

Виходячи з проведеного аналізу встановлено наступне:

1) розробка документації на створення КСЗІ здійснюється в середньому протягом 1-4 місяців в залежності від складності системи, в якій планується її створити. Вартість відповідних робіт становить 27000-36000 грн (в окремих випадках розробити КСЗІ пропонують за ціною 64000, 158000 грн без наведення розшифровки виконуваних робіт). Відповідні послуги включають:

– обстеження середовища функціонування системи;

– розробку документації на комплекс технічного захисту інформації *об'єкта інформаційної діяльності*. Для ІТС з відкритою інформацією і доступом до неї через Інтернет – це приміщення, де розташовуватиметься серверне обладнання та саме обладнання (1500 - 2000 грн);

– налаштування комплексу засобів захисту інформації від несанкціонованого доступу (6000 - 10000 грн);

– розробку технічного завдання на створення КСЗІ (3000 - 4000 грн);

– розробку документації на КСЗІ для декларування в галузі технічного захисту інформації, що потрібно для проведення експертизи (15800 - 19000 грн);

– розробку декларації на КСЗІ для реєстрації в Держспецзв'язку (700 - 1000 грн).

2) експертизу КСЗІ (як правило виконується незалежною третьою стороною) відбуватиметься протягом 2-6 місяців в залежності від складності

системи. Строк перебування заяви на розгляді в Держспецзв'язку становить до 30 днів. Вартість експертизи орієнтовно становитиме 48000 - 73000 грн:

– попереднє ознайомлення з об'єктом експертизи (10000 - 19000 грн);

– поглиблене обстеження об'єкту експертизи (3000 - 4000 грн);

– формування програми та методики проведення експертизи (6000 - 10000 грн);

– проведення експертних випробувань та досліджень за розробленими програмою та методикою (20000 - 29000 грн);

– документування та затвердження результатів експертизи (91000 - 11000 грн).

Окремо можна зазначити, що простий аналіз декларації допускається лише для автоматизованої системи класу 1 (локальна робоча станція без підключення до комп'ютерної мережі). Вартість цієї послуги становитиме орієнтовно 6000 - 15000 грн.

Висновки

Підбиваючи підсумки, варто зазначити, що процедура створення КСЗІ загалом та для систем з відкритою інформацією зокрема є доволі заплутаною. Відсутній єдиний нормативно-методичний документ, у якому було б в повній мірі, послідовно викладено описаний процес. Це створює певні обмеження та незручності для осіб, які не мають профільної освіти або відповідного досвіду роботи, адже вони не можуть швидко зрозуміти без сторонньої допомоги, «Що»? і «Як»? їм робити для розбудови КСЗІ. Пропозиції відповідних програмних комплексів для створення КСЗІ в системах з відкритою інформацією також є доволі обмеженими, а вартість відповідних послуг доволі високою, що говорить про неконкурентність середовища та надмірну заорганізованість процесу розбудови КСЗІ.

Перелік посилань

[1] Порядок створення комплексних систем захисту інформації, проведення експертизи та видачі Експертних висновків і Атестатів відповідності. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=39479&cat_id=38689&ctime=1127824089206 (дата звернення: 11.09.2017).

[2] НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407 (дата звернення: 12.07.2017).

[3] Концепція технічного захисту інформації в Україні: постанова Кабінету Міністрів України № 1126 від 8.10.1997. // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/1126-97-%D0%BF (дата звернення: 12.07.2017).

[4] Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: постанова Кабінету Міністрів України № 373 від 29.03.06 // Офіційний вісник України. - 2006. - № 13 (12.04.2006), стор. 164, стаття 878.

[5] Про інформацію: закон України від 02.10.1992; [із змінами і доповненнями на 01.01.2017] // Відомості Верховної Ради України. – 1992. – № 48 (01.12.1992). – ст. 650.

[6] Про захист інформації в інформаційно-телекомунікаційних системах: закон України від 05.07.1994; [із змінами і доповненнями на 19.04.2014] // Відомості Верховної Ради України. – 1994. – № 31 (02.08.1994). – ст. 286.

[7] **Манжай О. В.** *Правові засади захисту інформації: навчальний-посібник*. Харків : Ніка Нова, 2014. 104 с.

[8] НД ТЗІ 3.7-003-05. Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. URL: http://dstszi.kmu.gov.ua/dstszi/doccatalog/doc

ument?id=106350 (дата звернення: 12.07.2017).

[9] НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. URL: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106349 (дата звернення: 12.07.2017).

[10] НД 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. URL: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106341 (дата звернення: 12.07.2017).

[11] Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України: постанова Кабінету Міністрів України № 821 від 16.11.2016; // Офіційний вісник України від 02.12.2016. – 2016. – № 93, стор. 39, стаття 3033.

[12] Перелік суб'єктів господарювання, що мають ліцензії на провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації, за переліком, що визначається Кабінетом Міністрів України. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=277736&cat_id=266373 (дата звернення: 12.07.2017).

[13] Побудова Комплексних Систем Захисту Інформації (КСЗІ). URL: http://www.iqusion.com/ua/produkti-i-servisi/zakhist-informatsiji/120-kszi.html.

[14] Етапи побудови КСЗІ. URL: http://altersign.com.ua/korysna-informacija/pobudova-kszi/etapy-pobudovy-kszi.

[15] Положення про державну експертизу в сфері технічного захисту інформації: наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України № 93 від 16.05.2007 року // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/z0820-07 (дата звернення: 12.07.2017).

[16] **Носов В. В.**, **Манжай О. В.** *Організація та забезпечення інформаційної безпеки: навчальний посібник*. Х. : Вид-во Харк. нац. ун-ту внутр. справ, 2007. 216 с.

[17] Положення про державний контроль за станом технічного захисту інформації: наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України №87 від 16.05.07. // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon5.rada.gov.ua/laws/show/z0785-07 (дата звернення: 12.07.2017).

[18] Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних, та інформаційно-телекомунікаційних системах: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України № 660 від 02.12.2014. // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/z0090-15 (дата звернення: 12.07.2017).

References

[1] Porjadok stvorennja kompleksnykh system zakhystu informaciji, provedennja ekspertyzy ta vydachi Ekspertnykh vysnovkiv i Atestativ vidpovidnosti. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=39479&cat_id=38689&ctime=1127824089206 (access date: 11.09.2017).

[2] ND TZI 2.5-005-99. Klasyfikacija avtomatyzovanykh system i standartni funkcionaljni profili zakhyshhenosti obrobljuvanoji informaciji vid nesankcionovanogho dostupu. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407 (access date: 12.07.2017).

[3] Koncepcija tekhnichnogho zakhystu informaciji v Ukrajini No 1126 (8.10.1997). //

Baza danykh «Zakonodavstvo Ukrajiny» / Verkhovna Rada Ukrajiny. URL: http://zakon3.rada.gov.ua/laws/show/1126-97-%D0%BF (access date: 12.07.2017).

[4] Pravyla zabezpechennja zakhystu informaciji v informacijnykh, telekomunikacijnykh ta informacijno-telekomunikacijnykh systemakh: Cabinet of Ministers of Ukraine enactment No 373 (29.03.06) // Oficijnyj visnyk Ukrajiny. 2006. No 13 (12.04.2006). p. 164, art. 878.

[5] Pro informaciyu: law of Ukraine (02.10.1992); [with changes and amendments on 01.01.2017] // Vidomosti Verkhovnoji Rady Ukrajiny. 1992. No 48 (01.12.1992). art. 650.

[6] Pro zakhyst informaciji v informacijno-telekomunikacijnykh systemakh: law of Ukraine (05.07.1994); [with changes and amendments on 19.04.2014] // Vidomosti Verkhovnoji Rady Ukrajiny. 1994. No 31 (02.08.1994). art. 286.

[7] **Manzhai O. V.** *Pravovi zasady zakhystu informaciji: tutorial*. Kharkiv : Nika nova, 2014. 104 p.

[8] ND TZI 3.7-003-05. Porjadok provedennja robit zi stvorennja kompleksnoji systemy zakhystu informaciji v informacijno-telekomunikacijnij systemi. URL: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106350 (access date: 12.07.2017).

[9] ND TZI 3.7-001-99. Metodychni vkazivky shhodo rozrobky tekhnichnogho zavdannja na stvorennja kompleksnoji systemy zakhystu informaciji v avtomatyzovanij systemi. URL: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106349 (access date: 12.07.2017).

[10] ND 1.4-001-2000. Typove polozhennja pro sluzhbu zakhystu informaciji v avtomatyzovanij systemi. URL: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106341 (access date: 12.07.2017).

[11] Dejaki pytannja licenzuvannja ghospodarsjkoji dijaljnosti z nadannja poslugh u ghaluzi kryptoghrafichnogho zakhystu informaciji (krim poslugh elektronnogho cyfrovogho pidpysu) ta tekhnichnogho zakhystu informaciji za perelikom, shho vyznachajetjsja Kabinetom Ministriv Ukrajiny: Cabinet of Ministers of Ukraine enactment No 821 (16.11.2016) // Oficijnyj visnyk Ukrajiny (02.12.2016). 2016. No 93, p. 39, art 3033.

[12] Perelik sub'jektiv ghospodarjuvannja, shho majutj licenziji na provadzhennja ghospodarsjkoji dijaljnosti z nadannja poslugh u ghaluzi kryptoghrafichnogho zakhystu informaciji (krim poslugh elektronnogho cyfrovogho pidpysu) ta tekhnichnogho zakhystu informaciji, za perelikom, shho vyznachajetjsja Kabinetom Ministriv Ukrajiny. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=277736&cat_id=266373 (access date: 12.07.2017).

[13] Pobudova Kompleksnykh System Zakhystu Informaciji (KSZI). URL: http://www.iqusion.com/ua/produkti-i-servisi/zakhist-informatsiji/120-kszi.html (access date: 12.07.2017).

[14] Etapy pobudovy KSZI. URL: http://altersign.com.ua/korysna-informacija/pobudova-kszi/etapy-pobudovy-ksz (access date: 12.07.2017)i.

[15] Polozhennja pro derzhavnu ekspertyzu v sferi tekhnichnogho zakhystu informaciji: order of Administration of State Service of Special Communications and Information Protection of Ukraine No 93 (16.05.2007) // Baza danykh «Zakonodavstvo Ukrajiny» / Verkhovna Rada Ukrajiny. URL: http://zakon3.rada.gov.ua/laws/show/z0820-07 (access date: 12.07.2017).

[16] **Nosov V. V.**, **Manzhai O. V.** *Orghanizacija ta zabezpechennja informacijnoji bezpeky: tutorial*. Kharkiv : KNUIA, 2007. 216 p.

[17] Polozhennja pro derzhavnyj kontrolj za stanom tekhnichnogho zakhystu informaciji: order of Administration of State Service of Special Communications and Information Protection of Ukraine No 87 (16.05.07) // Baza danykh «Zakonodavstvo Ukrajiny» / Verkhovna Rada Ukrajiny. URL: http://zakon5.rada.gov.ua/laws/show/z0785-07 (access date: 12.07.2017).

[18] Porjadok ocinky stanu zakhyshhenosti derzhavnykh informacijnykh resursiv v informacijnykh,

telekomunikacijnykh, ta informacijno-telekomunikacijnykh systemakh: order of Administration of State Service of Special Communications and Information Protection of Ukraine No 660 (02.12.2014) // Baza danykh «Zakonodavstvo Ukrajiny» / Verkhovna Rada Ukrajiny. URL: http://zakon3.rada.gov.ua/laws/show/z0090-15 (access date: 12.07.2017).

Реферат

Носов Віталій, Манжай Ірина. ***Організаційно-практичні аспекти побудови комплексної системи захисту інформації для системи з інформацією, що публікується в глобальній мережі.*** У роботі проаналізовано нормативно-правову базу в сфері побудови комплексної системи захисту інформації. Розглянуто коло суб'єктів, можливі варіанти та послідовність дій власника інформаційно-телекомунікаційної системи щодо розробки та впровадження комплексної системи захисту інформації. Визначено послуги, які надаються виконавцем при створенні та супроводженні комплексної системи захисту інформації. Окреслено окремі елементи контролю відповідної системи, а також проаналізовано орієнтовні час і витрати на її розробку.

Носов Виталий, Манжай Ирина. ***Организационно-практические аспекты построения комплексной системы защиты информации для системы с информацией, публикуемой в глобальной сети.*** В работе проанализирована нормативно-правовая база в сфере построения комплексной системы защиты информации. Рассмотрен круг субъектов, возможные варианты и последовательность действий собственника информационно-телекоммуникационной системы по разработке и внедрению комплексной системы защиты информации. Определены услуги, которые предоставляются исполнителем при создании и сопровождении комплексной системы защиты информации. Очерчены отдельные элементы контроля соответствующей системы, а также проанализированы ориентировочные время и расходы на ее разработку.

Nosov Vitalii, Manzhai Irina. **Organizational and Practical Aspects of Construction of Information Security Complex System for the System with Information which is Published in Global Network.** The paper presents the normative and legal base analysis in the field of construction of the information security complex system. The circle of subjects, possible variants and sequence of executions of owner of the informatively-telecommunication system, is considered on development and introduction of the information security complex system. Services which are given a performer at creation and accompaniment of the information security complex system are certain. The separate elements of control of the proper system are outlined, and also tentatively is analyzed time and costs for its development.

Відомості про авторів

Носов Віталій Вікторович. Освіта - вища, спеціальність – «Авіаційні радіотехнічні засоби» (1993). Кандидат технічних наук (1998), доцент (2002); місце роботи – професор кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ. Область знань і/або наукові інтереси: кібербезпека, цифрова криміналістика Email: vitnos@ukr.net.

Манжай Ірина Андріївна. Освіта – вища, спеціальність: «Захист інформації з обмеженим доступом та автоматизація її обробки» (2010). Місце роботи – завідувач навчального відділу Харківського економіко-правового університету. Область знань і/або наукові інтереси: інформаційні технології, кібербезпека Email: ir.lily@i.ua