УДК 681.3.06 **Хлапонін Ю.І., Криховецький В.Я., Процюк Ю.О.**

ОСНОВНІ НЕДОЛІКИ ФОРМУВАННЯ ПАКЕТУ ДОКУМЕНТІВ ДЛЯ ПРОВЕДЕННЯ ДЕРЖАВНОЇ ЕКСПЕРТИЗИ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Наведено порядок та досліджено особливості проведення державної експертизи комплексних систем захисту інформації в ІТС та шляхи їх розв'язання. За результатами дослідження запропоновані рекомендації щодо розв'язання цих проблем та своєрідний стислий алгоритм проведення державної експертизи, що враховують вимоги нормативних документів з цих питань та набутий позитивний досвід.

Ключові слова: інформаційно-телекомунікаційна система (ІТС), автоматизована система (АС), технічний захист інформації (ТЗІ), комплексна система захисту інформації (КСЗІ), державна експертиза.

Інформація, що є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації (КСЗІ) з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством України та нормативними документами системи технічного захисту інформації (ТЗІ).

Введення процедури експертного оцінювання комплексних систем захисту інформації в ІТС, технічних і програмно-апаратних засобів захисту інформації обумовлено логічною складністю сучасних програмно-апаратних комплексів, а також суттєвим впливом на безпеку інформації конкретних умов експлуатації ІТС, іншими словами такі об'єкти не повторюють один одного і кожний з них має тільки йому притаманні особливості.

Державна експертиза в сфері технічного захисту інформації (далі – експертиза) проводиться з метою дослідження, перевірки, аналізу та оцінки об'єктів експертизи щодо можливості їх використання для забезпечення ТЗІ.

Державна експертиза проводиться згідно з вимогами [1]. Сторонами, які приймають безпосередню участь в проведенні експертизи є об'єкти та суб'єкти експертизи.

Суб'єктами експертизи є:

— Замовники – юридичні та фізичні особи, які виступають замовниками експертизи;

— Держспецзв'язку – Адміністрація Державної служби спеціального зв'язку та захисту інформації України (*контролюючий орган*);

— Організатори – підрозділи Державної служби спеціального зв'язку та захисту інформації України, підприємства, установи та організації, які проводять експертизу (далі – Організатори);

— Експерти – фізичні особи, виконавці експертних робіт з ТЗІ;

— Державні органи, які проводять експертизу в сфері свого управління.

Об'єктами експертизи є:

— комплексні системи захисту інформації (далі – КСЗІ), які є невід'ємною складовою частиною інформаційної, телекомунікаційної або інформаційно-телекомунікаційної системи (далі - ІТС);

— технічні та програмні засоби, які реалізують функції ТЗІ (далі – засоби ТЗІ).

На даний час перед Експертом постає завдання проаналізувати надані Замовником десятки документів, перевірити їх відповідність нормативним документам системи технічного захисту інформації. Робота Експерта ускладнюється ще й тим, що в Україні є дійсними (діючими) державні стандарти та нормативні документи ще радянського періоду та нормативно-правові акти, видані вже Адміністрацією Держспецзв'язку України (або ще їх попередниками). Різноманітність цих документів, неузгодженість між собою окремих положень, що в них міститься, не дозволяє у повному обсязі реалізувати єдину політику в

проектуванні та експлуатації КСЗІ в АС, ускладнює роботу Експерта, а отже створює передумови для можливих невиправданих інтелектуальних й економічних втрат.

Метою даної статті є дослідження основних проблем **проведення державної експертизи** комплексних систем захисту інформації в ІТС та шляхів їх розв'язання. Дослідження базується на визначенні та врахуванні існуючих загальносистемних проблем, які враховують внутрішні загрози і виклики в інформаційній сфері. За результатами дослідження запропоновані рекомендації щодо розв'язання цих проблем та своєрідний стислий алгоритм проведення державної експертизи, що враховують вимоги нормативних документів з цих питань та набутий позитивний досвід.

Відповідно до [1] експертиза може бути первинною, додатковою та контрольною.

Детальніше зупинимося на первинній експертизі, яка проводиться на заключному етапі створення КСЗІ або перед початком використання технічних та програмних засобів, які реалізують функції ТЗІ (засобів ТЗІ).

Первинна експертиза є основним видом експертизи і передбачає виконання Організатором усіх потрібних заходів, визначених у розділі 3 [1], для підготовки та прийняття рішення щодо об'єкта експертизи.

Для проведення експертизи КСЗІ в ІТС або засобу технічного захисту інформації (засобу ТЗІ) Замовник надсилає заяву встановленої форми на ім'я Голови (заступника Голови) Державної служби спеціального зв'язку та захисту інформації України. В заяві дозволяється висловлювати побажання щодо Організатора Експертизи. За результатами розгляду заяви у місячний термін приймається рішення про можливість й доцільність проведення експертизи та визначення підрозділу Держспецзв'язку, підприємства, установи або організації, які проводитимуть експертизу (далі – Організатор експертизи).

Права та обов'язки всіх сторін, які приймають участь в проведенні експертизи визначаються в [1, 4].

Замовник надає Організатору експертизи комплект організаційно-технічної документації на КСЗІ в ІТС або засіб ТЗІ, необхідний для проведення експертних випробувань.

Організатор, за результатами аналізу наданих документів і з урахуванням загальних методик оцінювання задекларованих характеристик засобів ТЗІ та КСЗІ, формує програму і окремі методики проведення експертизи об'єкта.

Робота Експерта виконується у відповідності до програми проведення державної експертизи комплексної системи захисту інформації в автоматизованій системі, яка узгоджується з Замовником та Департаментом з питань захисту інформації в інформаційно-телекомунікаційних системах Адміністрації, та окремих методик, які узгоджуються з зазначеним департаментом.

Умовно роботу Експерта можливо поділити на кілька етапів:

***І етап*:** Аналіз документів зі створення КСЗІ в АС.

— аналіз технічного завдання на створення КСЗІ та проектної документації;

— перевірка відповідності комплекту документації на КСЗІ вимогам НД ТЗІ;

— перевірка повноти та змісту документів.

На цьому етапі Експерт також має пересвідчитися, що враховані вимоги щодо розміщення поблизу об'єкта іноземних представництв [8] та з'ясувати, що електроживлення об'єкта здійснюється від трансформаторної підстанції, яка розташована в межах контрольованої зони та не має сторонніх споживачів.

ІІ етап: Аналіз проведених робіт зі створення КСЗІ в АС.

— перевірка реальних умов експлуатації;

— перевірка відповідності реально встановлених технічних засобів (ТЗ) та додаткових технічних засобів та систем (ДТЗС) вказаним в Акті обстеження ОІД;

— перевірка впроваджених заходів захисту інформації від витоку технічними каналами;

— перевірка впроваджених заходів захисту інформації від НСД до інформаційних ресурсів;

— перевірка виконання вимог щодо функціонування системи антивірусного захисту.

На цьому етапі Експерт вимагає від Замовника та перевіряє:

— протокол вимірювання опору контуру заземлення;

— специфікації апаратних та апаратно-програмних засобів ОІД;

— опис програмного забезпечення з номерами ліцензій та підтвердженням, що ПЗ придбане без порушення авторських прав, (підтвердити рахунками-фактурами, ліцензіями (паспортами), серійними номерами). На встановлене антивірусне програмне забезпечення робочих станцій, серверів Замовник повинен надати експертні висновки Адміністрації Держспецзв'язку України та підтвердити, що оновлення баз даних проводиться у відповідності до [7].

— відповідність комплексу засобів захисту інформації від несанкціонованого доступу (КЗЗ від НСД) з визначеним рівнем гарантії вимогам нормативних документів системи технічного захисту інформації у обсязі функцій, сукупність яких визначається функціональним профілем захищеності [2] та наявність експертного висновку Адміністрації Держспецзв'язку України.

III етап: Аналіз організаційно-розпорядчих та програмно-експлуатаційних документів.

— перевірка наявності відповідних наказів керівника Замовника на різних етапах створення та впровадження КСЗІ;

— перевірка наявності інструкцій, які регламентують функціонування КСЗІ в АС.

На цьому етапі Експерт перевіряє:

— наказ про проведення робіт зі створення КСЗІ на ОІД з висновками щодо обмеження грифу обмеження доступу до інформації, що обробляється в АС та призначення відповідальних осіб;

— наказ щодо створення служби захисту інформації;

— наказ про створення комісії з проведення випробувань КСЗІ в АС;

— наказ про забезпечення захисту інформації в АС;

— наказ про введення АС в дослідну експлуатацію тощо;

— інструкцію про порядок введення в експлуатацію КСЗІ в АС;

— інструкцію про порядок модернізації КСЗІ в АС;

— інструкцію системному адміністратору;

— інструкцію адміністратору безпеки при роботі в АС;

— інструкцію користувачу.

Результати роботи Експерта оформлюються у вигляді протоколу виконання експертних робіт, приклад якого наведено в [1] (додаток 5) за підписом Експертів, які її виконували. Протокол затверджується Організатором.

Результати робіт, визначених окремою методикою, узагальнюються Організатором в Експертному висновку.

За результатами проведених робіт Організатор складає Експертний висновок відповідного змісту [1] (додатки 6, 7) щодо відповідності об'єкта експертизи вимогам нормативних документів з ТЗІ, підписує його і подає до Адміністрації.

На підставі позитивного рішення щодо експертизи КСЗІ Замовнику видається зареєстрований Атестат відповідності [1] (додаток 8) за підписом Голови (заступника Голови) Держспецзв'язку.

Атестат відповідності є підставою для Замовника видати наказ про введення КСЗІ в ІТС в постійну експлуатацію та оформити Паспорт-формуляр по захисту секретної інформації на ОІД.

Для виконання такого значного обсягу робіт, Експерт повинен володіти великим

обсягом знань з технічних, юридичних питань, добре знати нормативні документи не тільки в галузі технічного захисту інформації, але й побудови інформаційно-телелекомунікаційних систем взагалі. Як зазначалося на початку статті робота Експерта ускладнюється ще й тим, що в Україні є дійсними (діючими) державні стандарти та нормативні документи ще радянського періоду та нормативно-правові акти, видані вже Адміністрацією Держспецзв'язку України (або ще їх попередниками). Вимоги зазначених документів в деяких питаннях можуть суперечити один одному.

Прикладом різного тлумачення нормативної бази може бути наступне.

Є два локалізованих багатомашинних багатокористувачевих комплекса (наприклад, розміщені в різних містах філії підприємства) та для роботи їм необхідно обмінюватися інформацією за допомогою електронної пошти (поштовими повідомленнями). Чи підпадає така АС під визначення АС класу 3 згідно [2] ? На думку деяких експертів, достатньо створити КСЗІ для АС класу 2 та захистити інформацію, що передається існуючими засобами захисту.

Інший приклад. Законом [9] внесено зміни до Закону [3] (навіть змінено його назву), та вводиться визначення інформаційної (автоматизованої) та інформаційно-телекомунікаційної систем (ІТС). Але в той же час чинними залишаються нормативні документи системи ТЗІ, наприклад [2], де наводиться визначення автоматизованої системи (АС) та виділено три ієрархічні класи АС. Тому при виконанні робіт зі створення КСЗІ використовують обидва ці визначення.

Впровадження в усі сфери життєдіяльності особи, суспільства та держави інформаційних технологій зумовило широке розгортання інформаційно-телекомунікаційних систем, різке збільшення обсягів інформації, яка обробляється, зберігається в цих системах, значне збільшення кола користувачів, які мають безпосередній доступ до інформаційних ресурсів тощо.

За відсутності конкурентоспроможних вітчизняних засобів обробки інформації та програмного забезпечення вітчизняної розробки перевага надається інформаційним технологіям та технічним засобам іноземного виробництва, які здебільшого не забезпечують захист інформації, а також створюють передумови неконтрольованого використання спеціальних програмних та апаратних засобів („закладних пристроїв").

Також, як показує досвід, під час експлуатації КСЗІ необхідно контролювати дієздатність системи, тому що з часом параметри можуть змінюватися або якийсь вузол системи може вийти з ладу. Сьогодні – це не робиться. Деякі підприємства-виробники засобів ТЗІ пропонують вирішити це питання за рахунок підвищення ціни. Крім того, такий контроль функціонування необхідно узгодити з Держспецзв'язку. Відповідно, впровадження контролю функціонування засобів ТЗІ може призвести до необхідності проведення чергової атестації, а це знову ж таки призведе до додаткових витрат Замовника.

Досвід проведення державної експертизи КСЗІ в ІТС дозволяє віднести до основних недоліків формування пакету документів на експертизу наступні:

1. Замовник серед інших документів надає Експерту Акт обстеження АС згідно [5], але інший нормативний документ, а саме, [6] вимагає проведення обстеження вже на об'єкті інформаційної діяльності (далі – ОІД). В самому ж акті відображаються:

— категорія об'єкта ЕОТ;

— перелік основних технічних засобів (ОТЗ) (найменування, тип, заводський номер);

— перелік додаткових технічних засобів та систем (ДТЗС) і комунікацій, що знаходяться на об'єкті ЕОТ.

Часто в акті відсутній перелік ДТЗС і комунікацій, що знаходяться на об'єкті ЕОТ та не в повній мірі розкриті характеристики складових ОІД.

Процедура проведення обстеження повинна враховувати вимоги [8] щодо розміщення поблизу об'єкта іноземних представництв. Інформацію про іноземні представництва мають такі органи як місцева податкова інспекція, місцева державна адміністрація, відділи віз та

реєстрацій та відповідні компетентні органи. Чи існує зведена інформація від цих органів? А як бути з фізичними особами-іноземцями, які можуть проживати (орендувати квартири) на визначеній в [8] відстані до об'єкта. Чи всі іноземці офіційно реєструються? Як бачимо, це питання не є врегульованим.

2. Іноді в комплекті документів на КСЗІ відсутній ,,Протокол про визначення вищого ступеня обмеження доступу до інформації", зміст якого впливає на обґрунтований вибір необхідного рівня захисту ІзОД від витоку технічними каналами, використання тих або інших норм, положень, методик і рекомендацій, викладених в нормативній базі системи ТЗІ.

3. Документ ,,Окрема модель загроз для інформації на ОІД, де розміщено АС", що містить питання можливих технічних каналів витоку ІзОД на ОІД для подальшого створення комплексу ТЗІ на об'єкті, часто плутається з документом ,,Модель загроз та модель порушника в АС", який, зазвичай, входить окремим розділом до Плану захисту і містить формалізований опис всіх можливих загроз безпеці інформації від не санкціонованого доступу (НСД) для подальшого створення комплексу засобів захисту (КЗЗ).

На жаль, розглянуті недоліки формування необхідного пакета документів, зазвичай, виявляються вже на етапі проведення державної експертизи КСЗІ та можуть значно загальмувати процес отримання дозвільних документів на експлуатацію АС певних класів. Тому, на нашу думку, єдиним шляхом розв'язання цієї проблеми є чітке додержання розробником КСЗІ вимог нормативних документів з питань ТЗІ та формування повного переліку необхідних документів.

Але також зрозуміло, що діюча нормативна база з ТЗІ потребує доопрацювання та вдосконалення з метою підвищення ефективності захисту інформації, впровадження єдиного порядку виконання заходів та спрощення процедури проведення державної експертизи КСЗІ в ІТС. Закони України мають вищу юридичну силу, тому необхідно забезпечити приведення існуючих нормативних документів системи ТЗІ у відповідність із Законами, які регулюють відносини у сфері захисту інформації в інформаційно-телекомунікаційних системах.

ЛІТЕРАТУРА

1. Положення про державну експертизу в сфері технічного захисту інформації (Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України № 93 від 16.05.07).

2. НД ТЗІ 2.5-005 -99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

3. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 5.07.1994 року № 80/94-ВР.

4. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

5. ТР ЕОТ – 95. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок.

6. НД ТЗІ 3.1-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи.

7. Порядок оновлення антивірусних програмних засобів, які мають позитивний Експертний висновок за результатами державної експертизи в сфері технічного захисту інформації (Наказ ДССЗЗІ України від 26.03.07 № 45).

8. ТПКО-95. Тимчасове положення про категоріювання об'єктів 10.07.95 № 35.

9. Про внесення змін до Закону України ,,Про захист інформації в автоматизованих системах". Закон від 31.05.2005 року № 2594-IV.

Надійшла: 21.09.2011

Рецензент: д.т.н., проф. Петров О.С.