УДК 004.056.5(045) **Чунарьова А.В., Чунарьов А.В**.

АНАЛІЗ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ СУЧАСНИХ ІКСМ

В статті проведено аналіз сучасного стану нормативно-правового забезпечення інформаційної безпеки сучасних інформаційно-комунікаційних систем та мереж. Розглянуто основні концептуальні документи з точки зору організації та побудови комплексної системи захисту інформації.

Ключові слова: комплексний захист інформації, інформаційна безпека, несанкціонований доступ, профіль захищеності, нормативно-правове забезпечення.

Вступ. Сучасний етап розвитку суспільства характеризується зростаючою роллю інформаційної сфери, що представляє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, що здійснюють формування, поширення й використання інформації, а також; системи регулювання суспільних відносин, що виникають при цьому. На сьогодні інформаційна сфера є системоутворюючим чинником життя суспільства, активно впливає на стан політичної, економічної, оборонної й інших складових безпеки держави. Сучасні інформаційні технології надають нові можливості з обробки, передачі та зберігання інформації та підвищують рівень доступності інформаційних ресурсів для користувача. Однак нові технології інформації можуть бути не тільки корисними, але й небезпечними для інформаційних систем та мереж.

На даний час приватна й ділова інформація має комерційну вартість і тому важливою є проблема її захисту від несанкціонованого доступу та атак. Нині спостерігається тенденція до підвищення кількості атак та несанкціонованого доступу, які захоплюють контроль над віддаленою інформаційною системою, копіюють та передають зловмисникам персональні дані, іншу конфіденційну або, навіть, секретну інформацію. Проблема комплексного захисту сучасних інформаційно-комунікаційних систем та мереж (ІКСМ) інформації стає ще актуальнішою, якщо мова йде про захист великої кількості оперативної інформації, що обробляється в сучасних комп'ютерних системах.

Постановка задачі. На сьогодні розпочато створення механізмів реалізації законів, підготовку законопроектів, що регламентують суспільні відносини в інформаційній сфері. Разом з тим, аналіз стану інформаційної безпеки України показує, що її рівень не повною мірою відповідає потребам суспільства і держави. Тому, формування бази правового забезпечення інформаційної безпеки є важливою складовою у процесі розвитку законодавства України в інформаційній сфері та захисту інформації в сучасних ІКСМ.

Метою статті є аналіз існуючої нормативно-правової бази в галузі забезпечення інформаційної безпеки сучасних ІКСМ та побудови комплексної системи захисту інформації (КСЗІ).

Система інформаційної безпеки забезпечує цілісність, доступність і конфіденційність критично важливої інформації, а отже, життєздатність і ефективність в цілому самої інформаційної системи. Систему зазначених заходів, що забезпечує захист інформації в ІКСМ, називають комплексною системою захисту інформації. На даний час комплексний захист інформації являє собою сукупність організаційних структур, поєднаних цілями і завданнями захисту інформації, нормативно-правової та матеріально-технічної бази і спрямований на забезпечення інженерно-технічними, апаратними та програмно-апаратними засобами властивостей інформації в сучасних ІКСМ. Під поняттям комплексної системи захисту інформації будемо розуміти сукупність організаційних і технічних заходів, апаратних і програмних засобів, які забезпечують захист інформації в ІКСМ: на автономних робочих станціях (автоматизована система класу 1) і в комп'ютерних мережах (автоматизована система класу 2 і 3) [3].

Напрямки розвитку захищених корпоративних і локальних інформаційно-

комунікаційних мереж та мереж сприяють постійній зміни методів і засобів комплексного захисту інформаційної безпеки шляхом постійного вдосконалення організації захисту інформаційних ресурсів за допомогою програмних і технічних засобів.

Комплексна система захисту інформації включає заходи та засоби, що реалізують способи, методи, механізми захисту інформації від:

1. витоку інформації технічними каналами (побічні електромагнітні випромінювання, акустоелектричних канали і т.д.);
2. несанкціонованих дій та несанкціонованого доступу до інформації (підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, застосування закладних пристроїв чи програм і т.д.);
3. спеціального впливу на інформацію (формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту).

Для кожної конкретної інформаційно-комунікаційної системи склад, структура та вимоги до системи захисту визначаються властивостями оброблюваної інформації, класом автоматизованої системи та умовами її експлуатації. Кінцевою метою всіх заходів щодо захисту інформації, які реалізуються, є забезпечення безпеки інформації під час її оброблення в ІКСМ. Захист інформації має бути забезпечений на всіх стадіях життєвого циклу ІКСМ, на всіх технологічних етапах оброблення інформації і в усіх режимах функціонування.

Інформація та інформаційні ресурси, у процесі функціонування сучасних ІКСМ зазнають впливу цілого ряду загроз, внаслідок чого виникають порушення її цілісності, доступності з боку авторизованих та неавторизованих користувачів. Для забезпечення захисту інформації існує ціла низка напрямів забезпечення інформаційної безпеки, які направлені на зниження ймовірності виникнення загрози та порушення базових властивостей інформації. Нормативно-правове забезпечення, як первинний етап при побудові комплексної системи захисту інформації сучасних ІКСМ є найважливішою складовою для забезпечення ефективного і надійного захисту інформації та інформаційних ресурсів [1,5,9].

Під поняттям **нормативно-правового забезпечення** слід розуміти сукупність правових норм, що визначають порядок створення, правовий статус і функціонування захищених ІКСМ, регламентують порядок одержання, перетворення та використання інформації і інформаційних ресурсів.

Тобто нормативно-правове забезпечення регламентує та визначає порядок захисту визначених політикою безпеки властивостей інформації (конфіденційності, цілісності та доступності) під час створення та експлуатації інформаційної мережі; регламентує порядок ефективного знешкодження і попередження загроз для ресурсів шляхом побудови комплексної системи захисту інформації; статус інформаційної системи з точки зору інформаційної безпеки; права, обов'язки й відповідальність персоналу роботи яких пов'язані з інформаційною безпекою; правові положення окремих видів процесу керування та управління доступом в захищених ІКСМ; порядок створення й використання захищених ІКСМ; етапи побудови КСЗІ [9].

Під час створення комплексної системи захисту інформації, як сукупності організаційних і інженерних заходів, програмно-апаратних засобів слід керуватися низкою нормативно-правових документів та актів. Базовими нормативними документами при організації та побудови комплексної системи захисту інформації в ІКСМ є: Закон України "Про інформацію"; Закон України "Про захист інформації в автоматизованих системах"; НД ТЗІ 1.1-002-99: Загальні положення з захисту інформації в комп'ютерних системах від НСД (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22); НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22); НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі (введено в дію Наказом ДСТСЗІ СБУ від 04.12.2000 р. № 53); НД ТЗІ 2.5-005-99: Класифікація

автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22); НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22).; НД ТЗІ 3.7-001-99: Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (введено в дію Наказом ДСТСЗІ СБУ від 28.04.199 р. № 22) [2-4,6-8,9].

Дослідження показали, що всі вище зазначені нормативні-документи визначають основи та положення організації захисту інформації на всіх етапах життєвого циклу ІКСМ. Основою побудови комплексної системи захисту інформації сучасних ІКСМ, згідно нормативних документів є надання нормативно-методологічної бази для вибору і реалізації вимог до захисту інформації та інформаційних ресурсів в ІКСМ. Порядок вибору вимог до захисту інформації в ІКСМ визначається згідно НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» [3,4].

Основою для надійного та ефективного захисту являється вибір стандартного функціонального профілю захищеності. Під поняттям функціонального профілю захищеності будемо розуміти перелік мінімально необхідних рівнів послуг та механізмів, які повинна реалізовувати система захисту ІКСМ.

Функціональний профіль захищеності повинен задовольняти певні вимоги щодо захищеності інформації, яка обробляється в захищеній ІКСМ. Стандартні функціональні профілі вибираються на основі існуючих вимог щодо захисту інформації та інформаційних ресурсів від певних загроз і відомих на сьогоднішній день функціональних послуг, що дозволяють протистояти даним загрозам і забезпечувати виконання вимог, які пред'являються.

Основними вимогами щодо захищеності інформації в нашому випадку будуть захист цілісності та доступності інформації та інформаційних ресурсів. Тому функціональний профіль захищеності для сучасних розгалужених ІКСМ приймає наступний вид: 3.ЦД.1-3.ЦД.4. Вибраний профіль захищеності дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх передачі через незахищене середовище та включає в себе обов'язкове проведення процедур ідентифікації і аутентифікації.

Цей набір послуг представлений функціональним профілем захищеності забезпечує захист від навмисних та ненавмисних помилок користувача та інших випадкових помилок, а також від модифікації інформації у разі підключенні несанкціонованих користувачів. Також забезпечується виявлення випадкових або навмисних порушень цілісності та доступності не тільки окремих повідомлень, але і потоків повідомлень в цілому. Тобто, метою створення захищених ІКСМ з урахуванням нормативно-правового забезпечення є виявлення та протидія загрозам безпеці інформації, що обробляється, зберігається та передається в них, з метою попередження порушення цілісності та доступності інформації.

Висновки. Отже, в ході роботи було досліджено основні нормативно-правові документи з точки зору побудови КСЗІ в сучасних ІКСМ.

ЛІТЕРАТУРА

1. Анин Б. Защита компьютерной информации. — СПб.: БХВ-Петербург, 2000. — 384 с.

2. Загальні положення з захисту інформації в комп'ютерних системах від НСД: НД ТЗІ 1.1-002-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації).

3. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.5-005-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації).

4. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації).

5. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учеб. пособие. – М.: Горячая линия – Телеком, 2004. – 280 с.

6. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі: НД ТЗІ 3.7-001-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації).

7. Про захист інформації в автоматизованих системах: Закон України від 05.07.1994 № 81/94-ВР//ВВР. — 1994. — № 31. — С. 287.

8. Типове положення про службу захисту інформації в автоматизованій системі: 1.4-001-2000. — [Чинний від 2000.12.04]. — К. : ДСТСЗІ СБУ, 2000. — № 53.— (Нормативний документ системи технічного захисту інформації).

9. Юдін О.К. Інформаційна безпека.Нормативно-правове-забезпечення: Підручник. – К.: Вид-во Видавництво Національного авіаційного університету «НАУ-друк», 2011. – 640 с.

Надійшла: 08.04.2012

Рецензент: д.т.н., проф. Юдін О.К.