УДК 004.056.5

О.К. Юдін, д-р техн. наук, проф.;
С.С. Бучик, к.т.н, доц.,
О.І. Варченко

АВТОМАТИЗОВАНА СИСТЕМА ЯК ОБ`ЄКТ "ТРИЄДИНОЇ" СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

*Національний авіаційний університет, м. Київ, kszi@ukr.net
** Житомирський військовий інститут імені С.П. Корольова
Державного університету телекомунікацій, м, Київ

У статті досліджуються питання забезпечення захисту інформації в автоматизованих системах. Проаналізовані і показані деякі протиріччя, які існують в термінології і вимогах нормативно-правових актів з технічного захисту інформації. Приведені основні відомості про функціональні профілі, класифікацію автоматизованих систем і механізми захисту від несанкціонованого доступу в автоматизованих системах. Структурно представлена автоматизована система як об'єкт "триєдиної" системи захисту інформації згідно з нормативною базою.

Ключові слова: *автоматизована система, захист інформації, об'єкт захисту.*

Постановка проблеми. Сьогодні, за умов глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень та боротьби конкуруючих сторін стає інформаційний простір. Сучасні інформаційні технології надають інформаційній складовій дедалі більшої ваги і стають одним із найважливіших елементів забезпечення захисту інформації, тому завдання захисту інформації, яка зберігається в автоматизованих комп'ютерних системах, є досить актуальним. Для вирішення цього завдання використовується цілий комплекс засобів, що включає в себе нормативно-правові, організаційні та інженерно-технічні напрямки захисту інформації [1].

Сучасні методи обробки, передачі й накопичення інформації сприяли появі загроз, що забезпечують можливість втрати, перекручування та розкриття даних. Тому завдання побудови надійного захисту комп'ютерної системи залишається актуальним, звідки виникає необхідна задача високоякісного забезпечення безпеки автоматизованої системи (АС), яку неможливо виконати без попереднього аналізу можливих загроз безпеки системи. Для вирішення цього питання виникає необхідність чіткого визначення АС як об'єкта захисту інформації.

Аналіз останніх досліджень і публікацій. Останнім часом проблеми, пов'язані з використанням різного роду захисту інформації в повсякденній діяльності, стали особливо актуальними завдяки широкому розвитку АС. Цим проблемам присвячені праці Мельникова В.В.[2], Завгороднева В.И. [3], Горбенка І.Д., Гриненка Т.О. [4], Когаловского М.Р. [5]. Також значний внесок в розробку питань із оцінки захисту комп'ютерних систем внесли роботи докторів наук Корченка О.Г. [6], Дудикевича В.Б.[7].

Мета дослідження. Метою дослідження є розкриття АС як об'єкту "триєдиної" системи захисту інформації, визначення класифікації АС відповідно до існуючої нормативної бази. Структурно визначити АС як об'єкт "триєдиної" системи захисту інформації.

Виклад основного матеріалу. У процесі конструктивного поєднання діяльності держави, громадянського суспільства і людини захист інформації є одним з трьох головних напрямів діяльності органів виконавчої влади у сфері забезпечення інформаційної безпеки України [8].

В Законі України «Про інформацію» (від 02.10.1995 року №2658-XII-ВР//ВВР) визначено, що головними напрямами державної інформаційної політики в Україні, яку розробляють і здійснюють органи державної влади, а також відповідні органи спеціальної компетенції, є сприяння зберіганню національних інформаційних ресурсів, створення загальної системи охорони інформації та гарантування інформаційного суверенітету України. Для того щоб визначити АС як об'єкт захисту потрібно детальніше розглянути це поняття.

В нормативно-правових актах України представлено декілька таких понять.

Так, в ДСТУ 2226-93 «Автоматизовані системи. Терміни та визначення», якій установлює терміни та визначення основних понять у галузі автоматизованих систем, автоматизована система є: " організаційно-технічна система, що складається із засобів автоматизації певного виду (чи кількох видів) діяльності людей та персоналу, що здійснює цю діяльність ".

В той же час, звертаючись до сучасних нормативно-правових актів з технічного захисту інформації, а саме Закону України «Про захист інформації в автоматизованих системах» (від 05.07.1994 року №81/94-ВР//ВВР) *автоматизована система* – система, що здійснює автоматизовану обробку даних і до складу якої входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури,

програмне забезпечення. В НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» (Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 року № 22) *автоматизована система* є організаційно-технічна система, що реалізує інформаційну технологію і об'єднує обчислювальну систему, фізичне середовище, персонал і інформацію, яка обробляється.

Зрозуміло, що починаючи вже з ключових термінів АС немає однозначних визначень цих понять, діюча нормативна база з ТЗІ потребує доопрацювання та впровадження єдиної термінології.

Для розгляду АС як об'єкту захисту інформації скористуємось визначенням АС з НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», в зв'язку з тим, що воно найбільш повно на думку авторів розкриває суть поняття АС. Тепер, коли визначено поняття АС потрібно розглянути поняття суб'єкта і об'єкта інформації.

В Законі України «Про інформацію» визначено, що *суб'єктами* інформаційних відносин є: фізичні особи; юридичні особи; об'єднання громадян; суб'єкти владних повноважень. *Об'єктом* інформаційних відносин є інформація.

Згідно Закону України «Про захист інформації в автоматизованих системах» *об'єктом* захисту є інформація, що обробляється в АС, права власників цієї інформації та власників АС, права користувача. Захисту підлягає будь-яка інформація в АС, необхідність захисту якої визначається її власником або чинним законодавством.

Цим же законом визначено, що *суб'єктами* відносин, пов'язаних з обробкою інформації в АС, є: власники інформації чи уповноважені ними особи; власники АС чи уповноважені ними особи; користувачі інформації; користувачі АС. Як бачимо, в Законі України «Про захист інформації в автоматизованих системах» ширше розкривається зміст об'єкта захисту інформації і суб'єкта інформаційних відносин, що повинно використовуватись для розгляду АС як об'єкта захисту інформації. Зрозуміло, для узагальнення всіх понять необхідно розглянути, що являє собою *захист інформації в АС*.

Зі змісту Закону України «Про захист інформації в автоматизованих системах» випливає, що з*ахист інформації* – це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією. Таким чином, захист інформації в АС — діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації та АС в цілому, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків внаслідок реалізації загроз [НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»].

Для вирішення завдання захисту інформації використовується цілий комплекс засобів, що включає технічні, програмно-апаратні засоби та адміністративні заходи захисту інформації. Побудова надійного захисту комп'ютерної системи неможлива без попереднього аналізу класифікації АС та можливих загроз безпеки системи.

Вимоги до гарантій АС визначаються насамперед характером і важливістю оброблюваної інформації і призначенням АС. Згідно з НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» (Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999) за сукупністю характеристик АС виділено три ієрархічні класи АС, вимоги до функціонального складу комплекс засобів захисту (КЗЗ) яких істотно відрізняються.

Клас «1» — одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох ступенів обмеження доступу.

Клас «2» — локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.

Клас «3» — розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.

Розглянемо істотні особливості і приклади.

В кожен момент часу з комплексом (Клас «1») може працювати тільки один користувач, хоч у загальному випадку осіб, що мають доступ до комплексу, може бути декілька, але всі вони повинні мати однакові повноваження (права) щодо доступу до інформації, яка оброблюється; технічні засоби (носії інформації) з точки зору захищеності відносяться до однієї категорії і всі можуть використовуватись для збереження всієї інформації. Прикладом такого класу може бути персональна автономна ЕОМ, доступ до якої контролюється шляхом використання організаційних заходів.

Клас «2» являє собою локалізований багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності. Істотна відміна від класу «1» — наявність користувачів з різними повноваженнями по доступу і/або технічних засобів, які можуть одночасно здійснювати обробку

інформації різних категорій конфіденційності. Прикладом даного класу є звичайна локальна обчислювальна мережа (ЛОМ).

Клас «3» має істотну відмінну особливість від попереднього класу — необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки. Приклад — глобальна мережа.

Таким чином, підсумовуючи всі попередньо розглянуті питання, АС, як об'єкт "триєдиної" системи захисту інформації може бути представлена наступним чином (рис.1).

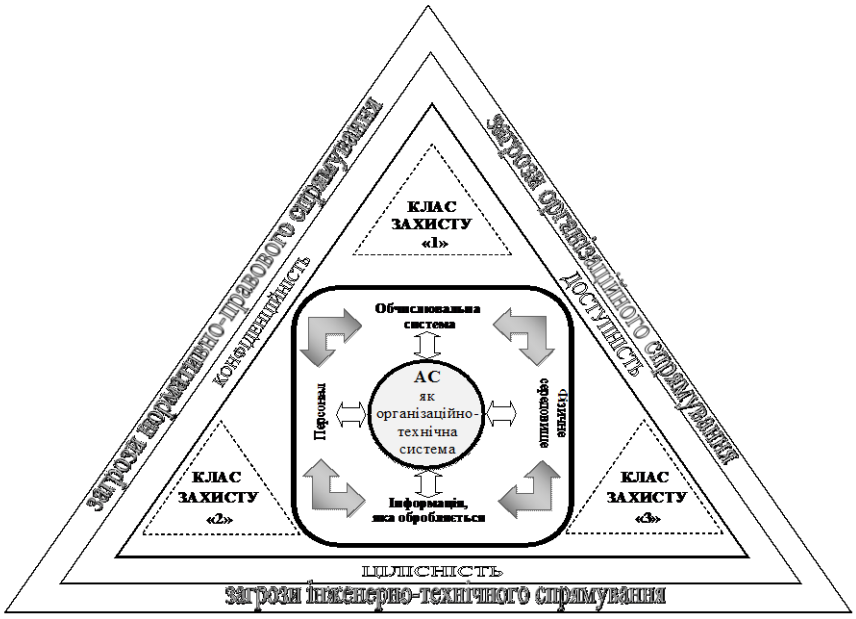

Рис.1. АС, як об'єкт "триєдиної" системи захисту інформації

Висновки. Аналізуючи стан класифікації АС, як об'єкту "триєдиної" системи захисту інформації, можна зробити висновок, що узагальнена класифікація (згідно класів захисту 1,2,3) використовується в межах кожного класу на підставі вимог, які забезпечують певні властивості інформації: конфіденційність, цілісність і доступність. Така класифікація корисна для полегшення вибору переліку функцій, які повинен реалізовувати КЗЗ АС. Цей підхід дозволяє мінімізувати витрати на початкових етапах створення захисту АС. Проте слід визнати, що для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної АС, необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків. Це в свою чергу показує шляхи для подальшої класифікації загроз нормативно-правового, організаційного та інженерно–технічного спрямування, їх розподіл за основними властивостями інформації, які впливають на стан безпеки АС. Розглянуті в статті та інші впроваджені в державі нормативно-правові акти (НПА), що стосуються інформації та її захисту, а також внесення змін та доповнень до діючих, потребують вжиття певних заходів з метою приведення нормативної бази системи технічного захисту інформації у відповідність до вимог цих НПА, що, в свою чергу, відображається на захисті АС в цілому.

Список використаних джерел

1. Інформаційна безпека. Нормативно-правове забезпечення: підруч. / О.К. Юдін. – К.: НАУ, 2011. – 640 с.
2. Мельников В.П. Информационная безопасность и защита информации / В.П. Мельников. – М.: Издательский центр «Академия», 2008. – 336 с.
3. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос, 2001. – 264 с.
4. Горбенко І.Д. Гриненко Т.О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації. – Харків: ХНУРЕ, 2004.– 368 с.
5. Когаловский М. Р. Перспективные технологии информационных систем. – М.: ДМК Пресс; Компания АйТи, 2003. – 288 с.
6. Корченко О.Г. Оценка безопасности компьютерных систем на базе методов и моделей нечетких множеств. Сборник научных трудов «Защита информации» – К.: КМУГА. – 1998.– 232 с.
7. Дудикевич В.Б., Зачепило А.В., Пархуць Л.Т., Хома В.В., Яструбецький О.В., Термінологічний словник з інформаційної безпеки. – Режим доступу: http://megalib.com.ua/content/8805_Terminologichnii_slovnik.html
8. Доктрина інформаційної безпеки України: затв. Указом Президента України від 8 липня 2009 р. № 514/2009 // Офіц. вісн. України. – 2009. – № 52. – Ст. 1783.