УДК 004.414.23

Клеха О. В.
Луцький національний технічний університет

# ОСНОВНІ ПРОБЛЕМИ ПРИ ПОБУДОВІ МОДЕЛЕЙ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ МЕРЕЖІ АВТОМАТИЗОВАНИХ СИСТЕМАХ

*У статті розкриваються основні проблеми при побудові моделей захисту інформації в комп'ютерній мережі автоматизованих системах. Наведені складові частини забезпечення АС. Розкриті основні методи забезпечення інформаційної безпеки АС.*

**Ключові слова:** *захист інформації, автоматизовані системи, комп'ютерні мережі, інформаційна безпека, комплексна система захисту інформації, система.*

**Постановка проблеми та завдання дослідження.** На даний час в галузі захисту інформації розроблено багато моделей захисту інформації. Існує низка проблем при побудові моделей захисту інформації. Дані проблеми пов'язані з не стандартизованими різнорідними за будовою та призначенням автоматизованими системами. Головним завданням даного дослідження є проведення повного аналізу проблем побудови моделей захисту інформації в комп'ютерних мережах автоматизованих систем.

**Аналіз останніх досліджень і публікацій.** Принципи інформаційної безпеки в автоматизованих системах в Україні регламентуються низкою нормативних документів. Основним законом слід вважати Закон України «Про інформацію» від 02.10.1992 № 2657-XII, Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.07.1994 № 80/94-ВР, ДСТУ 3396.0-96, ДСТУ 3396.1-96, ДСТУ 3396.2-97 та ДБН А.2.2-2-96. Що стосується захисту інформації в автоматизованих системах основним нормативним документом є Закон України «Про захист інформації в автоматизованих системах» від 05.07.94 № 81/94-ВР. Дані нормативні документи є директивними та регламентують правила організації захисту інформації тільки для систем в яких обробляється інформація, яка несе у собі державну таємницю, або інші види таємниці. Дослідження проведені у галузі інформаційної безпеки та захисту інформації охоплюють в основному напрямки захищеності інформації будь-якої з видів таємниці. Отже існує потреба в аналізі основних проблем при побудові моделей захисту інформації, що не суперечать нормативним документам та задовольняють міжнародним стандартам з захисту інформації таким як ISO/IEC 17799:2005, ISO/IEC 27001:2005 та ін..

**Метою дослідження** є всебічний аналіз проблем, що дозволить розробити рекомендації, методи та моделі захисту для конкретних автоматизованих систем різного практичного використання та будови.

**Виклад основного матеріалу.** Існує багато моделей захисту інформації в комп'ютерних мережах автоматизованих систем. Слід зауважити, що в залежності до загального підходу до політики безпеки локальної мережі та загальних нормативних та директивних документів, що присутні на підприємстві існує багато підходів до вибору конкретної моделі захисту. Насамперед необхідно дослідити саму інформаційну систему. Дане дослідження повинне охоплювати не тільки комп'ютерні ресурси, а також усі суміжні інформаційні та інші ресурси. Для цього необхідно побудувати модель функціонування самої системи адже як зазначив Джордж Клір «система – це множина елементів, що знаходяться у відносинах або зв'язані один з одним та утворюють цілісність або органічне об'єднання»[1]. Тобто необхідно підходити до аналізу інформаційної системи як системи загалом.

Як було сказано Крістіаном Норберг-Шульцом «Тільки при повному розумінні задач можна знайти відповідні способи їх вирішення. Для результатів важливіше поставити правильні запитання чим правильно відповісти на хибні». Тому необхідно строго визначити усі області і задачі що охоплює автоматизована система, а також визначити усі суміжні з нею інші системи та їх складові підсистеми.

Системи інформаційної безпеки в автоматизованих системах (АС), в тому числі в загальних і корпоративних мережах, призначені для забезпечення безпеки інформаційних технологій, тобто забезпечення конфіденційності, цілісності, доступності інформаційних та інших ресурсів АС.

Конфіденційність — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем.

Цілісність — означає неможливість модифікації неавторизованим користувачем.

Доступність — властивість інформації бути отриманою авторизованим користувачем, за наявності у нього відповідних повноважень, в необхідний для нього час.

Для запобігання можливості реалізації загроз ресурсам АС необхідна розробка і використання в АС комплексної системи захисту інформації (КСЗІ). Вимоги до такої системи передбачають централізоване управління засобами та механізмами захисту на основі політики інформаційної безпеки.

Згідно закону України «Про захист інформації в автоматизованих системах» (ст.1) м. Київ, 5 липня 1994 року N 80/94-ВР (В редакції Закону N 2594-IV від 31.05.2005) комплексна система захисту інформації – це взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації. Саме на неї нормативними документами системи КСЗІ покладається завдання забезпечення вже згаданих функціональних властивостей захищених АС. Це завдання вирішується як технічними, так і програмними засобами базового і прикладного програмного забезпечення (ПЗ), а також з використанням спеціально розроблених програмних і апаратних засобів.

Для кожної конкретної інформаційної системи склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи та умовами її експлуатації.

Організаційно-правовими заходами реалізується комплекс відповідних в нормативно-правовій базі держави адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом аналізу загроз, регламентації діяльності персоналу і визначення порядку функціонування засобів забезпечення інформаційної діяльності та засобів ТЗІ, а також шляхом створення служб (або призначення адміністраторів ТЗІ), відповідальних за їх реалізацію. До таких заходів належать також визначення контрольованих зон та організація контролю доступу в ці зони. Для реалізації заходів цієї групи в більшості випадків немає необхідності використання засобів, що є компонентами АС.

Специфікація області в якій відбувається моделювання системи захисту інформації, а саме комп'ютерна мережа автоматизованої системи розуміє під собою дві області, які тісно пов'язані між собою. Основною областю слід вважати АС, як клієнта та основного керуючого елемента комп'ютерної мережі, що належить до технічного забезпечення АС (рис. 1). Необхідно розпочинати аналіз захищеності з найменшої логічної структури загального комплексу.

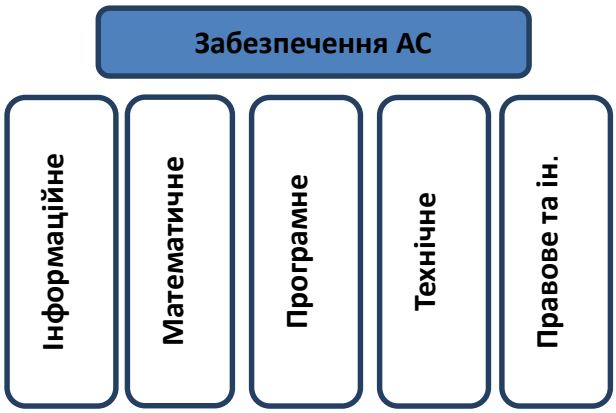


Рис 1. Складові частини забезпечення АС

Комп'ютерна мережа будь-якої сучасної організації – це різнорідна багатокомпонентна система. Захист одного або декількох компонентів не може забезпечити необхідний рівень захищеності інформаційних ресурсів підприємства. Головною проблемою захисту інформації в комп'ютерних мережах є те, що питаннями безпеки починають цікавитись коли інформаційна та технічна структура мережі уже розгорнута, тобто сформований не тільки функціонал мережі, а також і технічний потенціал. Дана ситуація викликає проблему в правильному підході до -

побудови комплексної системи захисту, адже часто спеціалістів, що розуміють усю структуру функціонування підприємства немає, не говорячи уже про висококваліфікованих спеціалістів в галузі захисту інформації.

Одним з методів правильної організації з урахування усіх нюансів функціонування комп'ютерної мережі в умовах визначеної АС є залучення спеціалістів з захисту інформації ще на етапі проектування інформаційної системи в склад якої буде входити комп'ютерна мережа як складовий елемент АС. Залучення даних спеціалістів та побудова ними моделі захисту інформації дозволить заощадити як на етапах експлуатації системи так і підвищити рівень захищеності системи. У разі якщо система уже функціонує необхідно провести усесторонній аналіз захищеності мережі. Існує декілька методів аналізу захищеності мережі, серед яких слід виділити наступні: аналітичний, імітаційний та експертний. Жоден з цих методів не має переваги над іншим. Основними джерелами атак є атаки, що проведені з локальної мережі та з глобальної мережі (рис. 2)

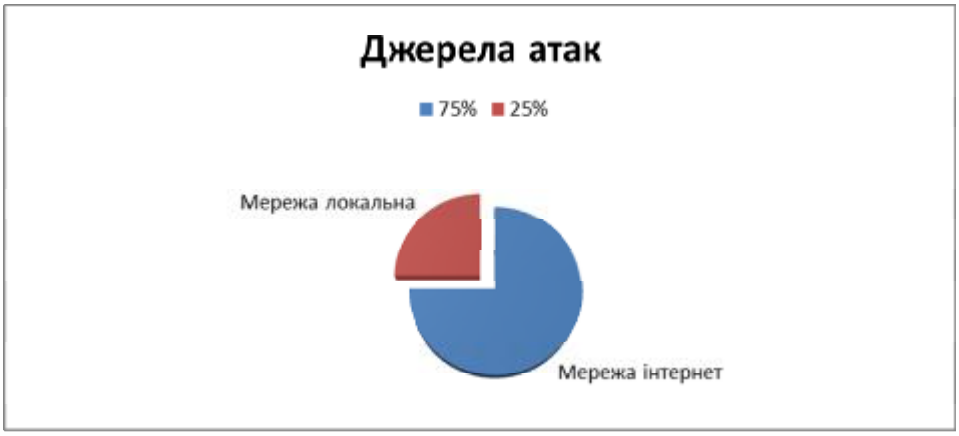


Рис.2. Джерела атак на локальний комп'ютер

У зв'язку з тим, що для організації мереж необхідно базуватись на моделях та стандартах у мережевих технологіях таких як модель OSI. Модель OSI представляє рівневий підхід до мережі. Основні атаки, що були реалізовані у відповідності до мережевої моделі OSI показані на рис. 3.


Рис. 3. Реалізовані атаки у системі OSI

Інформаційна безпека АС розглядається як стан системи, при якому[2]:

1. Система здатна протистояти дестабілізуючого впливу внутрішніх та зовнішніх загроз.
2. Функціонування і сам факт наявності системи не створюють загроз для зовнішнього середовища і для елементів самої системи.

З існуючих методів розрахунку інформаційної безпеки слід виділити вказані на рис. 4. Це дозволить підійти до проблеми організації захисту інформації в АС, як до комплексу.

При виборі та використанні методів і моделей тієї чи іншої групи слід спиратися тільки на їх відповідність розв'язуваній задачі і застосовувати ті методи, які в даній ситуації найбільш виправдані. Що стосується самого методу оцінки захищеності, то тут можна сказати наступне.

Дійсно, з методичної точки зору аналітичні та імітаційні моделі, які розроблені до цього часу, виглядають кращими, оскільки ґрунтуються на формалізованому поданні предметної області. Експертні методи дозволяють знаходити рішення в умовах слабо структурованої предметної -

області. Проте відзначимо, що існуючі на сьогоднішній день моделі та методики оцінки багато в чому орієнтовані на вузького фахівця-професіонала, який добре розбирається в даній конкретній проблематиці. Що ж стосується питання визначення необхідного набору вимог і критеріїв оцінки та їх дотримання, то тут основна проблема полягає в складності вироблення повного і достовірного їх безлічі і повторюваному характері процедури їх конкретизації протягом усього життєвого циклу комп'ютерної мережі.


Рис. 4. Основні методи забезпечення інформаційної безпеки АС

Кожна автоматизована система має унікальну будову та складові частини, які не можливо підвести до якогось одного топологічного характеру. Дані частини функціонують в комплексі. Таким чином, АС являє собою складну систему, яку доцільно розділяти на окремі блоки (модулі) для полегшення її подальшого проектування. У результаті цього, кожен модуль буде незалежний від інших, а в комплексі вони будуть складати цілісну систему захисту.

Виділення окремих модулів АІС дозволяє службі захисту інформації:

- своєчасно і адекватно реагувати на певні види загроз інформації, які властиві певному модулю;
- в короткі терміни впроваджувати систему захисту інформації в модулях, які щойно з'явилися;
- спростити процедуру контролю системи захисту інформації в цілому (під системою захисту інформаційної інфраструктури підприємства в цілому слід розуміти сукупність модулів систем захисту інформації).

Поступово нарощуючи кількість модулів, а також ускладнюючи структуру захисту, АС набуває певної комплексність, яка має на увазі використання не одного типу захисних функцій у всіх модулях, а їх добуток. Таким чином, побудова КСЗІ стає невід'ємним фактором у розробці ефективної системи захисту від несанкціонованого доступу.

**Висновки:** Згідно вище викладеного слід зауважити особливу увагу на необхідності формування правильного підходу до розробки моделей захисту інформації комп'ютерної мережі автоматизованих систем, як складової частини загальної комплексної системи захисту інформації. Основними проблемами при розробці моделей є низький рівень аналітичної діяльності і хибність підходу, що пов'язаний у відсутності розгляду усіх структурних елементів та зв'язків між ними як системи. Необхідно строго усвідомлювати, що основні складові системи є також взаємопов'язаними системами, що створює додаткові проблеми при розробці моделей, та вимагає залучення висококваліфікованих та вузькоспеціалізованих спеціалістів з предметних областей, що

охоплює система загалом. Необхідно використовувати уже існуючі методи та моделі інформаційної безпеки, а також модернізувати їх та розробляти нові для конкретної задачі.

**Бібліографія:**

1. Закон України «Про інформацію» від 02.10.1992 № 2657-XII
2. -
3. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.07.1994 № 80/94-ВР
4. ДСТУ 3396.0-96
5. ДСТУ 3396.1-96
6. ДСТУ 3396.2-97
7. ДБН А.2.2-2-96
8. Закон України «Про захист інформації в автоматизованих системах» від 05.07.94 № 81/94-ВР.
9. Клир Дж. Системология. Автоматизация решения системных задач / Дж. Клир – М.: «Радио и связь», 1990. – 200 с
10. Цирлов В. Л. Основы информационной безопасности автоматизированых систем / В. Л. Цирлов – М.: «Феникс», 2008. – 320 с.
11. Шаньгин В. Комплексная защита информации в корпоративных системах. Учебное пособие. М.: «Форум», 2010. - 592 с