УДК 004.056.5(045)

Ряба О.І., Черниш Л.Г., Погорілий Ю.В.

ОСОБЛИВОСТІ ЗАХИСТУ РЕСУРСІВ ТА КАНАЛІВ КОРПОРАТИВНИХ МЕРЕЖ

В статті розглянуті загрози корпоративним мережам та основні можливі канали витоку інформації. Розглянуто можливі заходи для покращення дій персоналу з діями в інформаційній мережі.

Ключові слова: мережа, канали зв'язку, інформаційні системи, корпоративні мережі.

Вступ. Забезпечення безпеки в корпоративних мережах, має велике значення в сучасних реаліях. Будь-яка інформація, що обробляється та зберігається в інформаційних системах, чогось варта при умові її достовірності та гарантованості, а тому інформація має бути надійно захищена.

Аналіз останніх досліджень та постановка проблеми. Актуальність проблеми захисту інформації від загроз, можна порівняти на прикладі даних, опублікованих Computer Security Institute [1] (Сан-Франциско, штат Каліфорнія, США), які відображають з якими порушеннями захисту комп'ютерних систем доводиться боротись:

Рис.1 Загрози захисту інформації в % порушень

Основна частина. **З**агрози корпоративній мережі можна поділити на дві групи: внутрішні, що можуть виникати безпосередньо на території та завдяки персоналу установи та зовнішні, що виникають за територією, а іноді на великій відстані, і завдяки сторонньому втручанню в систему [2]. Характеристика основних джерел загроз для функціонування інформаційних систем:

Проникнення у систему через комунікаційні канали зв'язку з присвоєнням повноважень легального користувача з метою підробки, копіювання або знищення даних. Реалізується розпізнаванням або підбором паролів і протоколів, перехопленням паролів при негласному підключенні до каналу під час сеансу зв'язку, дистанційним перехопленням паролів у результаті прийому електромагнітного випромінювання.

Проникнення в систему через комунікаційні канали зв'язку при перекоммутації каналу на модем порушника після входження легального користувача в мережу й пред'явлення ним своїх повноважень з метою присвоєння прав цього користувача на доступ до даних.

Підключення до каналу зв 'язку в ролі активного ретранслятора для фальсифікації платіжних документів, зміни їх утримання, порядку проходження, повторної передачі, затримання доставки.

Вірусні атаки, що можуть знищувати інформацію та виводити з ладу деякі апаратні пристрої. Основний засіб боротьби – використання антивірусного ПЗ, що дозволяє вести профілактичні заходи та лікування у разі необхідності. Вірусні атаки можуть бути проведені ззовні через мережі передачі даних або шляхом внесення вірусів у систему в неробочий час, наприклад використання співробітником "подарунка" у вигляді нової комп'ютерної гри.

Апаратні збої, що загрожують частковим або повним втратам інформації, програмного забезпечення, систем обробки даних. Захист інформації полягає в забезпеченні дублювання інформації на паралельно працюючому сервері, збереженні баз даних в архівах на змінних носіях інформації, як наприклад блоках флеш пам'яті, компакт-дисках, магнітних стрічках тощо [3].

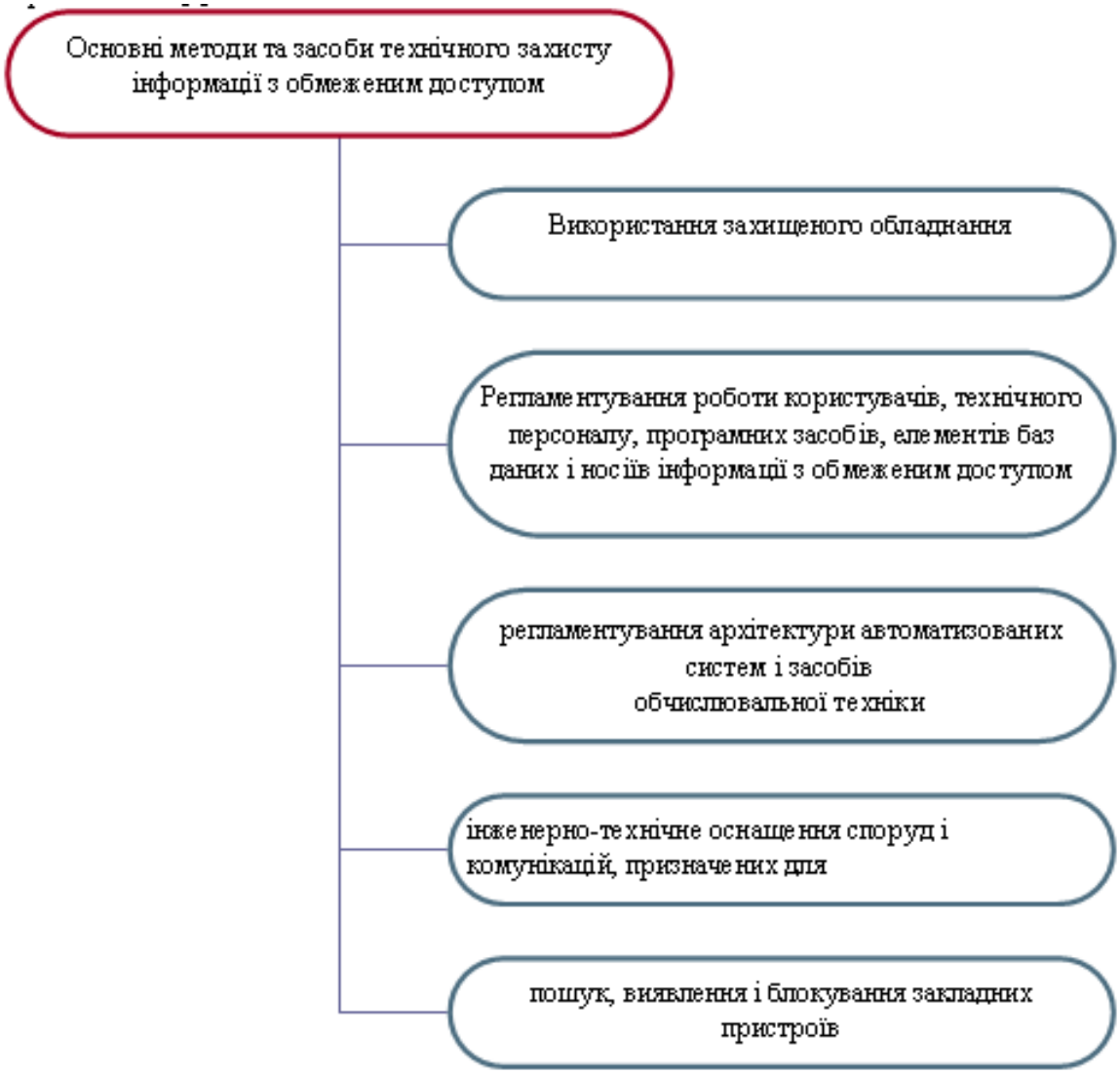

Рис.2 Методи та засоби технічного захисту інформації

Для підтримки та забезпечення робото стійкості системи можливо розглянути на прикладі схема ієрархічної декомпозиції: Такий спосіб дозволяє проводити детальний аналіз та атестацію захищеності інформаційних систем. Також розподіляти захист від можливих загроз на рівні де з’являється важлива інформація, що може зашкодити інформаційній цілісності системи [4].

Надійним засобом підвищення ефективності заходів інформаційної безпеки є навчання та інструктаж працюючого персоналу щодо організаційно-технічних заходів захисту, які застосовуються в конкретній організації. Крім цього, обов'язково мають бути реалізовані наступні організаційні заходи:

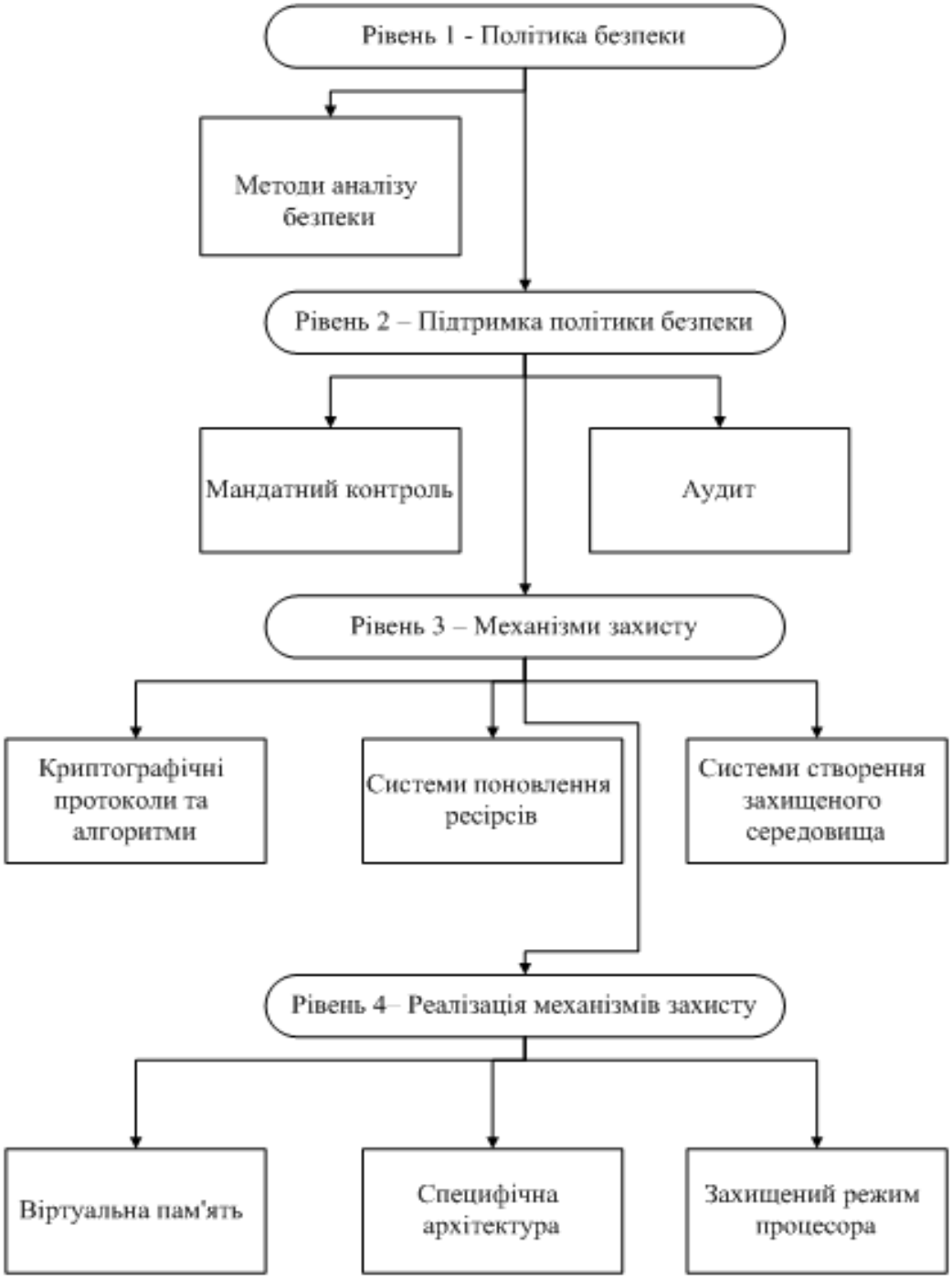

Рис.3 Ієрархічна декомпозиція

Для всіх осіб, що мають право доступу до засобів комп 'ютерної техніки, потрібно визначити категорії допуску, тобто коло службових інтересів коленої особи, види інформації, до яких вона має право доступу, а також: вид такого дозволу, правомочність особи, яка уповноважується для здійснення тих або інших маніпуляцій з засобами комп'ютерної техніки

Слід визначити адміністративну відповідальність за збереження і санкціонування доступу до інформаційних ресурсів. При цьому, за кожний вид ресурсів відповідальність повинна нести одна конкретна особа;

Висновки. Підводячи підсумки, хотілося б відзначити, що проблемам комп'ютерної безпеки в комп'ютерних і корпоративних мережах в повинне надаватися особливе значення. Правильно ієрархічно побудована система доступу до даних, сучасне обладнання, штат

кваліфікованих працівників, відповідальних за комп'ютерну безпеку - це гарант безпеки інформації, а разом з тим і корпорації. Так само хотілося б підкреслити, що ніякі апаратні, програмні та інші засоби, і організаторські роботи різних видів не зможуть гарантувати абсолютну надійність і безпеку даних, але в той же час звести ризик втрат до мінімуму можливо лише при усвідомленому, комплексному підході до питань комп'ютерної безпеки.

ЛІТЕРАТУРА

1. А.В.Олійник, В.М.Шацька - Навчальний посібник - Львів: "Новий Світ-2000", 2006 - 436 с.
2. Митні інформаційні технології: Навч. посіб. Рекомендовано МОН / За ред. П.В. Пашка. — К., 2011. — 391 с.
3. Матієга В. Створення ефективної системи аналізу та управління ризиками / В. Матієга // Митниця. —-2006. — № 5
4. Інформаційні технології та моделювання бізнес-процесів : навч. посіб. / О. М. Томашевський, Г. Г. Цигелик, М. Б. Вітер, В. І. Дудук. – К. : Центр учбової літератури, 2012. – 296 с.

Надійшла: 10.05.2012

Рецензент: д.т.н., проф. Юдін О.К.