ІНСТРУМЕНТАЛЬНІ ЗАСОБИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ НА ПРИКЛАДІ ЛОКАЛЬНОЇ МЕРЕЖІ ВИЩОГО НАВЧАЛЬНОГО ЗАКЛАДУ

Олег Богданович Зачко, доцент Львівського державного університету безпеки життєдіяльності, к.т.н.,
Катерина Василівна Мілян, студентка Львівського державного університету безпеки життєдіяльності

Актуальність. Інформаційні технології набувають все більшого впливу в кожній сфері людської життєдіяльності. На сучасному етапі розвитку інформаційного суспільства для задоволення потреб користувачів поряд з проблемами інформаційного забезпечення виникають проблеми забезпечення обмеженого доступу до ресурсів комп'ютерних систем у всіх сферах діяльності людини. Одна із найгостріших проблем - забезпечення надійного захисту інформації. Особливої гостроти вона набуває у зв'язку з масовою інформатизацією всіх видів діяльності людини та об'єднанні ЕОМ у комп'ютерні мережі чи підключенні до Internet.

Постановка задачі. Метою даної статті є розробка концептуальної моделі організації системи забезпечення комп'ютерної системи на прикладі локальної мережі вищого навчального закладу. До цієї моделі повинні входити вбудовані засоби операційної системи та додаткові скрипти shell, написані системними програмістами.

Основна частина. Організація більшості мереж у навчальних закладах є досить простою, а саме: мережа навчальних комп'ютерних класів представляє собою кілька робочих станцій(15-30 робочих станцій),об'єднаних певним способом у мережу (рис.1).

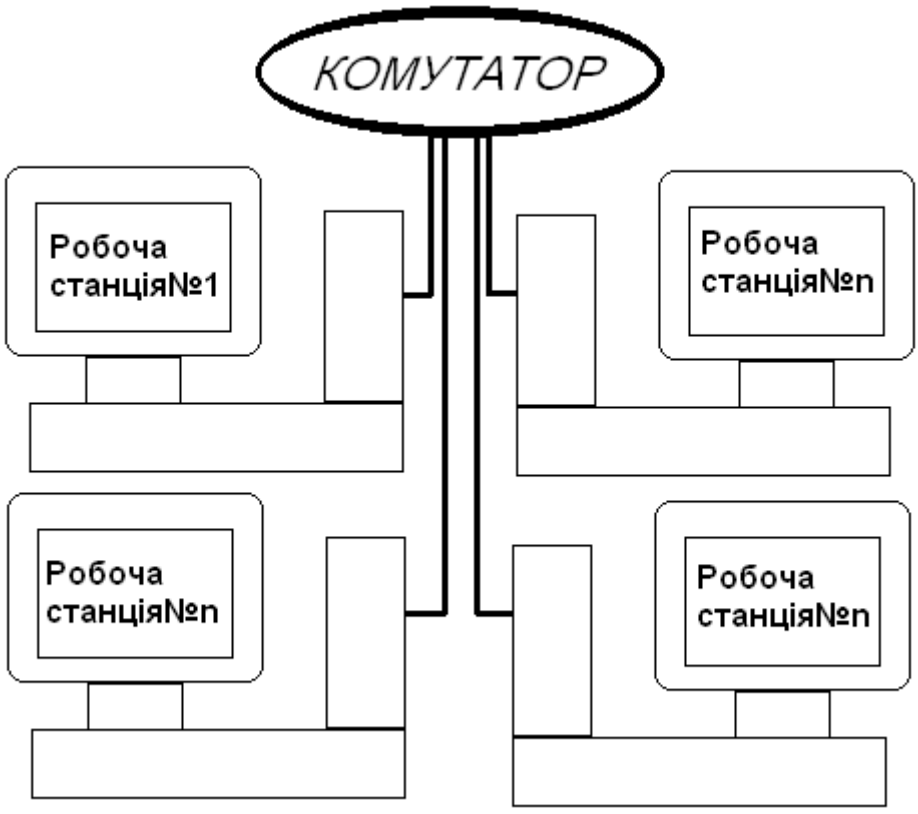

Рис. 1. Найпростіша структурна схема комп'ютерної мережі

З вище сказаного виникає необхідність розподілення прав доступу студентів та викладачів у локальній мережі вищого навчального закладу. У зв'язку з таким розподілом студенти повинні мати доступ тільки до потрібних та дозволених їм ресурсів, і ні в якому разі не взаємодіяти з ресурсами викладача без його дозволу. Тому у більшості навчальних закладів є потреба налаштування системи забезпечення комп'ютерної безпеки як цілісної політики локальної мережі, так і кожної робочої станції зокрема. Отже розглянемо найбільш оптимальні варіанти забезпечення безпеки та обмеження прав доступу до комп'ютерної системи, які можна використати при налагоджені роботи користувача (рис. 2).

У середньому у кожному комп'ютерному класі знаходиться 15-30 робочих станцій, а кількість

службових комп’ютерів на кафедрах може становити до 10 комп‘ютерів. Усі ці комп’ютери зв’язані з сервером, який відповідає за функціонування та роботу всієї локальної мережі. При такій кількості робочих станцій виникає потреба організації ефективного керування мережевими сервісами та забезпечення належного зв'язку між комп‘ютерами.

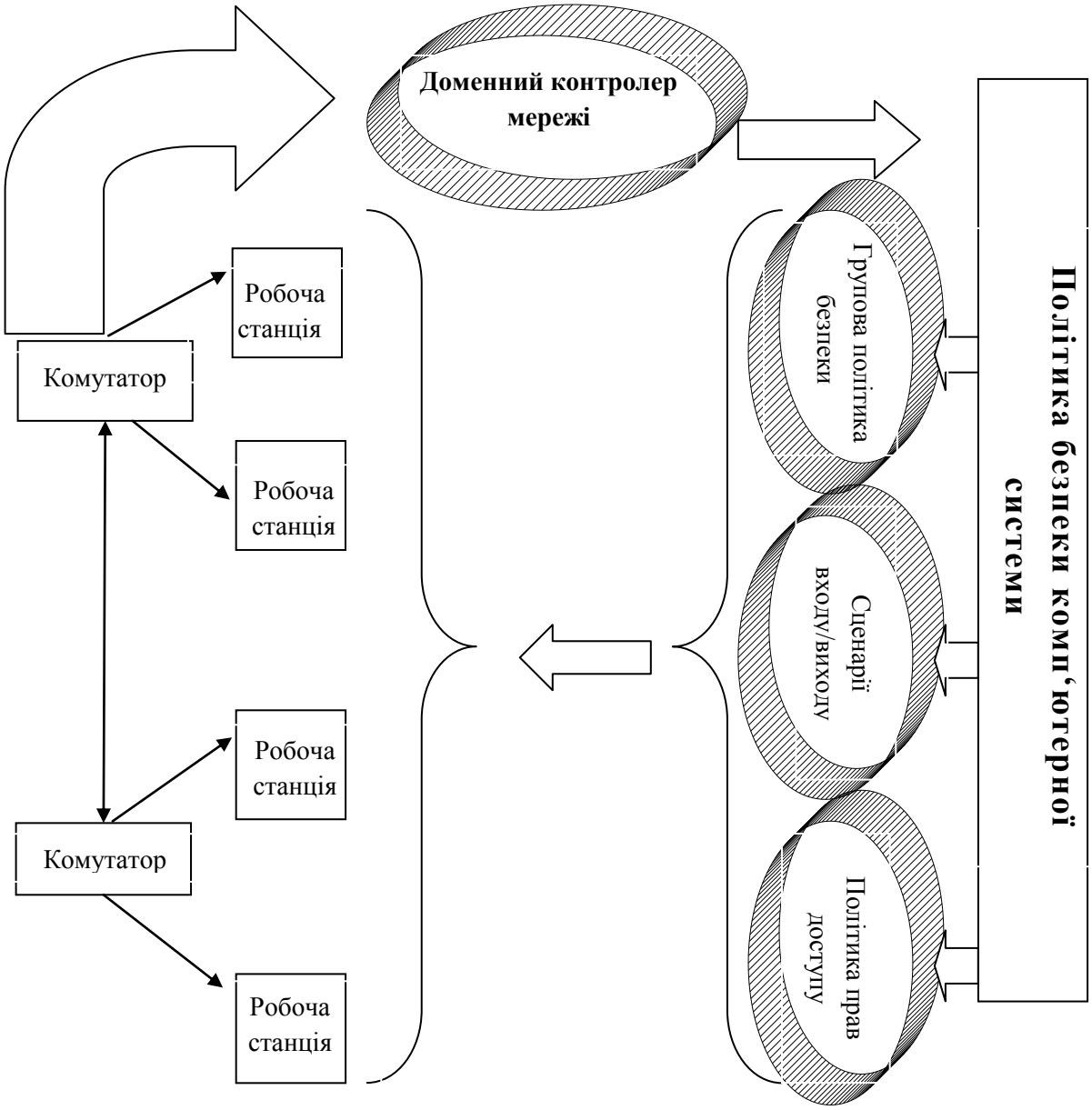

Рис. 2. Структурна схема організації політики безпеки комп‘ютерної системи

Для вирішення проблеми із зв’язком та роботою локальної мережі можна збільшити кількість серверів, кожен з яких буде відповідати за певну функціональну частину служби мережі. Наприклад один сервер може відповідати за локальну мережу, інший за зовнішній зв'язок. Також можна створити окремо сервер баз даних чи поштовий сервер.

Для полегшення та покращення роботи, забезпечення безпеки інформації кожного користувача, у операційній системі Windows є можливість оптимального налаштування робочої станції. Для цього можна використати командні файли, групову політику безпеки, можливості політики обов‘язкових профілів користувача, політики прав доступу та можливості BIOS. Розглянемо детальніше їх можливості.

Командні файли призначені для спрощення задання і виконання часто використовуваних послідовностей команд системи. За допомогою цих файлів користувач може без особливих зусиль створити свій інтерфейс. Командні файли корисні при використанні команд, що вимагають багатьох аргументів і перемикачів. Це дозволяє щоразу не вводити з клавіатури довгий командний рядок, а, наприклад, створити такий командний файл (на основі скриптів shell), який при кожному запуску

системи видалятиме тимчасові файли чи синхронізуватиме час робочої станції з системним часом на сервері.

Засоби групової політики операційної системи Windows використовуються для визначення параметрів політики функціонування комп‘ютерної системи, яка буде застосована до комп’ютерів чи користувачів. За допомогою цієї політики можна змінювати вид робочого столу, параметри автозапуску, вміст меню «пуск», спростити структуру панелі управління, управляти параметрами роботи програм, мережних ресурсів, операційної системи тощо, що спрощує роботу користувача.

Для оптимізації роботи системного програміста у багатокористувацьких системах використовують політику обов‘язкових профілів користувачів. Ця політика дозволяє визначити налаштування робочого середовища користувача, включаючи настройки дисплею, мережевих з’єднань тощо.

Для розмежування доступу до певних ресурсів комп‘ютерної системи використовують політику прав доступу. Ця політика дозволяє забезпечувати розмежування прав доступу та використання певних рівнів доступу до ресурсів мережі.

Висновки. В статті розглянуто прикладну задачу забезпечення безпеки комп‘ютерних систем, зокрема отримано такі результати:

1. Проаналізовані вбудовані засоби операційної системи для забезпечення безпеки комп‘ютерних систем, що дозволяє на їх основі створити політику безпеки локальної мережі.
2. На прикладі локальної мережі вищого навчального закладу запропоновано . структурну схему організації політики безпеки комп‘ютерної системи на основі поєднання групової політики безпеки, командних файлів на основі скриптів shell, політики прав доступу та обов‘язкових профілів користувачів.

Література

1. O'Brien J.A. Management Information Systems: managing information technology in the internetworked enterprise. - Irwin McGraw-Hill, 1999.
2. Raghunathan M., Madey GR. A firm-level framework for planning electronic commerce information systems infrastructure // International journal of electronic commerce. - 1999. - Fabruary. - P. 121-145.