УДК 004.056.5

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ “ТОНКИЙ КЛІЄНТ” ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Башевник А. І.

Кухарська Н. П., ЛДУ БЖД, доцент, канд. фіз.-мат. наук, доцент

Мережеві технології постійно розвиваються. Останнім часом все більшу популярність здобувають рішення на основі використання технології “тонкий клієнт”.

Тонкий (термінальний) клієнт (англ. Thin client) – бездисковий комп’ютер у мережі з клієнт-серверною чи термінальною архітектурою, котрий передає всі завдання з оброблення інформації або велику їх частину серверу. До “тонкого клієнта” через USB-порт можна підключити будь-який периферійний пристрій – клавіатуру, мишу, монітор, принтер тощо, чим забезпечується багатофункціональність робочого місця. “Тонкий клієнт” працює під управлінням компактної версії вбудованої операційної системи (Windows CE, Windows XP Embedded або Linux), до складу якої входять програми необхідні для роботи.

Оброблення інформації відбувається на централізованих комп’ютерах, а на кінцевих робочих станціях вона лише відображається. У зв’язку з цим, використання “тонкого клієнта” має певні переваги, особливо, у комп’ютерних системах, які обробляють інформацію з підвищеними вимогами щодо її захисту. Розглянемо ці переваги.

- Оскільки уся інформація обробляється і фізично зберігається виключно на виділених серверах, то для її захисту доречно використовувати організаційні заходи.
- Адміністрування та оновлення системи виконуються централізовано.
- Відсутність інформації на терміналах користувачів у вимкненому стані не дає змоги зловмиснику скористатися комп’ютером за відсутності персоналу.
- Існує можливість строгого контролю інформаційних потоків в системі.
- Спрощуються процеси аварійного відновлення даних.
- Є можливість організації повного моніторингу дій працівників та управління системою в режимі реального час. Користувачі можуть запускати лише ті програми, котрі встановлені на сервері і виконання котрих дозволено адміністратором. Таким чином легко виключаються ігри на робочому місці і зловживання мережею Internet, що підвищує продуктивність праці.
- Резервне копіювання і захист від вірусів достатньо забезпечити на сервері.

- На робочих місцях встановлюється ”залізо”, яке виробляє мінімум шуму, тепла і електромагнітних завад.
- Надійність системи зумовлена відсутністю механічних компонентів та спрощеною архітектурою “тонкого клієнта”. Термін служби терміналів більший, ніж у звичайних ПК.
- Можливість несанкціонованого перехоплення трафіка виключається програмним шифруванням даних. “Тонкі клієнти” стандартно підтримують перевірку автентифікації на мережевому рівні (Network Level Authentication) і SSL/TLS-шифрування з довжиною ключа до 128 біт.
- Сам по собі “тонкий клієнт”, будучи неприєднаним до сервера, не є повноцінним комп’ютером, через що не представляє особливої цінності для злодіїв.
- Ліцензійне ПЗ, яке доступне всім користувачам, встановлюється тільки на сервері, що виключає витрати на закупівлю дорогого ПЗ для кожного клієнта.
- Немає обмежень в ресурсах, яких слід дотримуватися при використанні персональних комп’ютерів. У розпорядженні “тонких клієнтів” ресурси центрального сервера (оперативна пам’ять, диски та інше).
- Відсутність локальних носіїв інформації не дає можливості персоналу робити копії документів на знімні носії інформації.
- Збої в подачі електроенергії, її вимкнення не призводять до втрати цінної інформації на конкретному робочому місці, оскільки вся інформація зберігається на термінальному сервері. При відключенні електроенергії всі програми, запущені в сеансі користувача, продовжують роботу як ні в чому не бувало. Після того як подача електроенергії буде відновлена, користувачі зможуть продовжити роботу з того моменту, на якому вони її залишили.
- Створення нових робочих місць, введення нових філіалів, не вимагає суттєвої зміни конфігурації системи, встановлення додаткового ПЗ і, що найважливіше, - збільшення витрат на обслуговування.
- Оскільки шкідливе ПЗ не має можливості виконуватися на терміналі, то повністю виключається можливість програмного перехоплення натискань клавіш і даних, що вводяться в різні поля. Таким чином забезпечується захист від атак типу MitB (man-in-the-box).

На основі вище сказаного приходимо до висновку: використання термінальної архітектури дає змогу вирішити багато проблем, що притаманні класичній мережевій архітектурі, і значно підвищити рівень безпеки і надійності інформаційних систем.