Комплексний захист корпоративних мереж

Актуальність

Актуальність проведення комплексного захисту корпоративних мереж полягає у використанні організаційних та інженерно-технічних заходів, що спрямовані на забезпечення захисту конфеденційної інформації компанії від розголошення, витоку і несанкціонованого доступу.

Проблеми

Проблеми впровадження комплексного захисту корпоративних мереж полягає у створені організаційних та інженерно-технічних заходів що повинні викокористовуватись на підприємстві.

Мета даного проекту – підвищення ефективності комплексного захисту інформації корпоративної комп'ютерної мережі компанії за допомогою використання створеного програмного засобу.

Результатом дипломного проекту є програмний засіб по захисту інформації у корпоративної комп'ютерної мережі що працює у складі існуючої системи управління корпоративними ресурсами підприємства.

Розробка комплексної системи захисту інформації корпоративної мережі повинна передбачати сукупність організаційних та інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу.

До організаційних заходів впровадження корпоративної мережі буде відноситись контроль та моніторинг роботи працівників компанії з серверами, базами даних та робочими станціями у відповідності до матриці доступу:
- терміну використання логінів та паролів користувачів компанії;
- періоду часу доби;
- днів тижня, вихідних та святкових днів;
- робочі дні, відрядження, відпустки;
- локалізація місць (підрозділи) компанії підєднання до провідних та безпровідних точок доступу до корпоративної мережі.

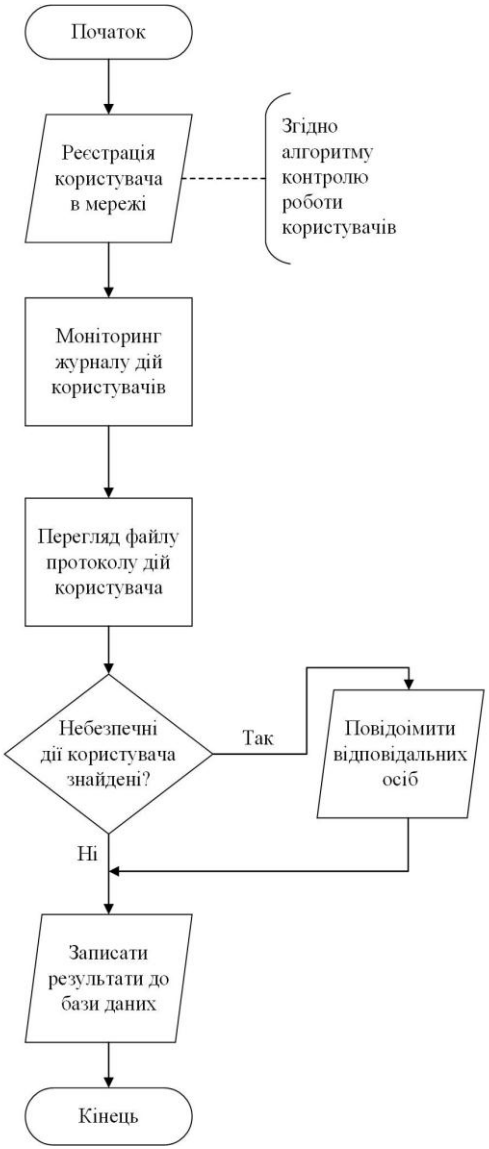
Інженерно-технічні заходи повинні мати багаторівневу структуру і включати наступні рівні:
- рівень захисту автоматизованих робочих місць;
- рівень захисту серверів;
- рівень захисту провідних та безпровідних точок доступу;
- рівень захисту локальних та корпоративної мереж.

На рівні захисту автоматизованих робочих місць повинна здійснюватися ідентифікація та аутентифікація користувачів компанії. До автоматизованих робочих місць персоналу компанії можуть відноситись:
- планшети або смартфони (операційна система Android);
- нетбуки, ноутбуки, стаціонарні персональні комп'ютери (операційна система Unix, Windows).

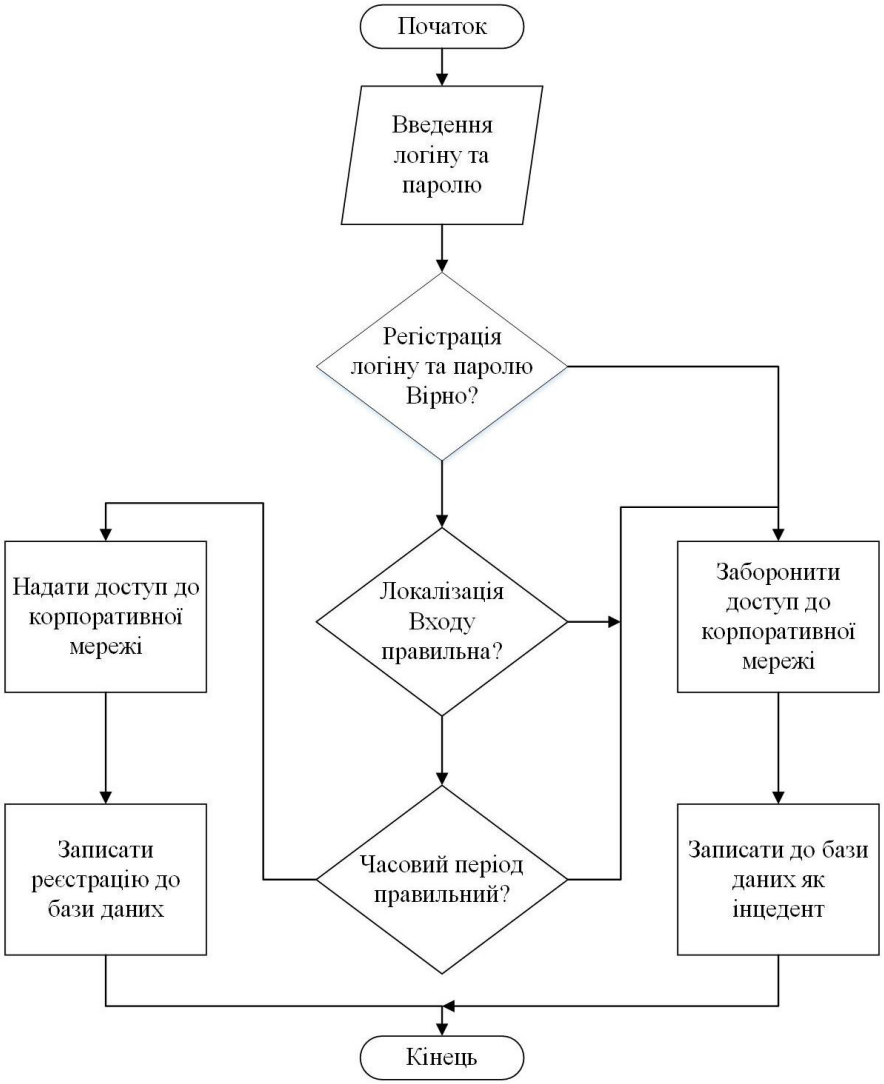
Інженерно-технічний рівень захисту локальних мереж і мережевих серверів повинен забезпечувати:
- ідентифікацію користувачів і встановлення автентичності доступу в систему, до компонентів;
- захист аутентифікаційних даних;
- встановлення аутентичності при доступі до серверів;
- перенаправлення аутентифікаційної інформації від одного компонента до іншого без перевстановлення аутентичності доступу.

Доступ до корпоративної мережі повинен здійснюватися за допомогою реєстрації таких подій:
- використання ідентифікаційних і аутентифікаційних механізмів;
- перевірку часу доступу (дозвіл) на виконання робіт у корпоративній мережі;
- можливість віддаленого доступу до корпоративної мережі;
- перевірку дії користувача з наданими правами відповідності його ролі;
- дії користувачів з критичними об'єктами;
- знищення об'єктів;
- дії, вжиті операторами та адміністраторами системи та/або офіцерами безпеки;
- інші випадки безпеки.

Параметри реєстрації користувачів у корпоративній мережі записуються до бази даних у наступному форматі:
- дата і час події;
- логін користувач;
- роль користувача;
- тип випадку;
- успішна або неуспішна спроба для ідентифікації/аутентифікації додатково;
- походження запиту (наприклад, локальна або віддалена аутентифікації);
- для випадків знищення об'єктів і доставки інформації в місце адреси користувача назва об'єкта.

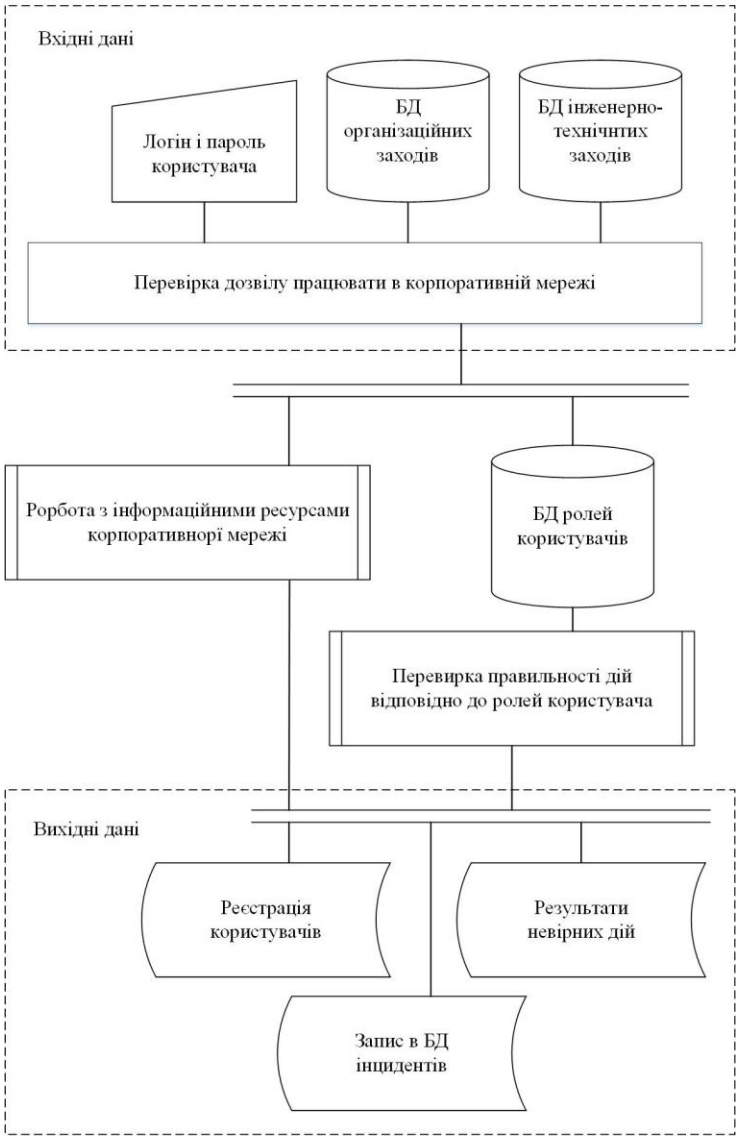


Моніторинг небезпечних дій користувачів.
Схема роботи системи

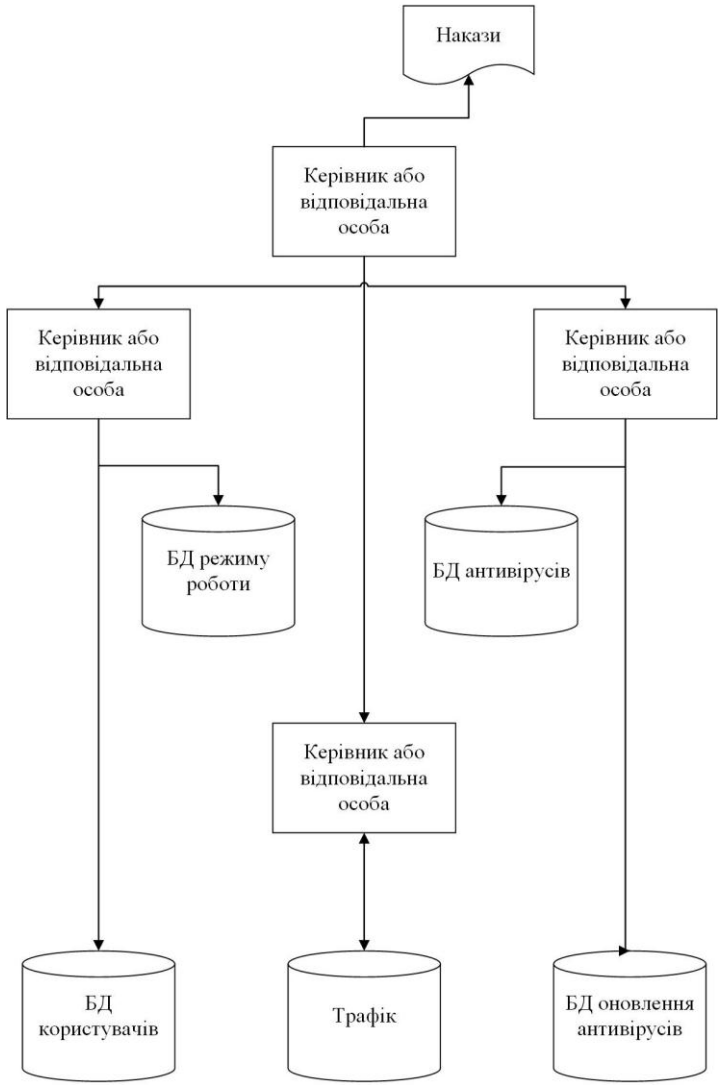


Вхідний інженерно-технічний контроль користувачів.
Схема роботи системи

Моніторинг інженерно-технічних дій користувача.
Схема ресурсів системи



Моніторинг небезпечних дій користувачів.
Схема роботи системи



Організація роботи корпоративної мережі.
Схема ресурсів системи

Організація контролю доступу користувачів до корпоративної мережі.
Схема роботи системи

Таким чином, в роботі було зроблено: програмна розробка комплексного захисту інформації на основі існуючої системи управління корпоративними ресурсами на підприємстві, техніко-економічне обґрунтування розробки, створення розділу з економічної частини.