Дослідження методів та засобів захисту інформації в корпоративних мережах

Бакалаврська робота

Актуальність дослідження

- Загроза безпеці інформації – сукупність умов та факторів, що створюють потенційну або реально існуючу небезпеку, пов'язану з витоком інформації або несанкціонованими і ненавмисними діями на неї.
- Комп'ютерна революція допомогла інформації стати центром уваги основоположних поглядів. Визнання інформації основою життя навряд чи зводиться до внутрішніх мотивацій. Соціальні, економічні та політичні науки в спробах усвідомлення змін, що відбуваються звертають пильну увагу на комп'ютерну інформацію, як на новий фактор глобального впливу.
- Захист інформації – це діяльність, спрямована на запобігання витоку інформації, що захищається, несанкціонованих і ненавмисних впливів на інформацію, що захищається.
- Враховуючи вищевикладене тема дипломної роботи є актуальною.

Наукова новизна та практична значущість

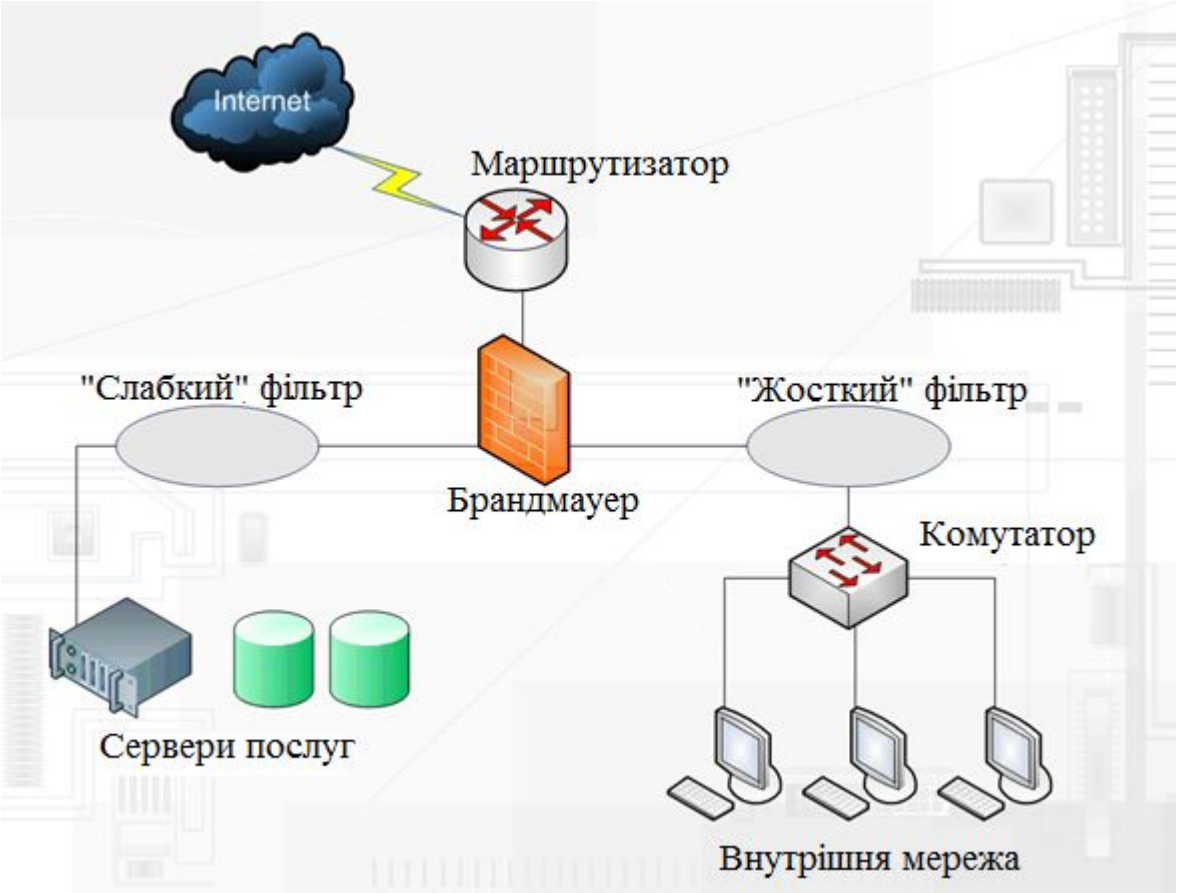
- ***Наукова новизна та практична значущість*** результатів роботи полягає в наступному:
- уперше запропоновано комплексне рішення по всіх рівнях захисту, щодо дійсної корпоративної мережі;
- наведено методи аналізу середовища корпоративної мережі: формування хронологічної послідовності типових впливів базових факторів середовища для їх подальшого аналізу й прогнозу;
- дістало подальшого розвитку вивчення та розробка методів впровадження універсальних засобів інформаційної безпеки у межах діючої корпоративної мережі підприємства.
- Отримані результати можуть бути використані у межах організацій для впровадження засобів інформаційної безпеки по етапах.

Основними результатами роботи є:

- розкриття основних положень теорії захисту інформації;
- проведення класифікації заходів забезпечення безпеки корпоративної мережі;
- дослідження основних методів і засобів захисту інформації в мережах;
- виділення методів і засобів захисту інформації в корпоративній мережі.
- висвітленні загальних аспектів побудови аналітичної системи захисту корпоративної мережі.

ОСНОВНІ ПОЛОЖЕННЯ ТЕОРІЇ ЗАХИСТУ ІНФОРМАЦІЇ

- Найбільш зручний вид обміну інформацією можна уявити і реалізувати на сьогоднішній день у вигляді локальних обчислювальних і розподілених мереж, де кожне автоматизоване робоче місце (АРМ) входить в єдину логічну структуру обміну даними. Локально-обчислювальні мережі, або скорочено ЛОМ, дозволяють максимально прискорити створення великих проектів, які потребують вкладу безлічі співробітників або задіяння різних пристроїв або обчислювальних потужностей різних серверів (СУБД, сховище даних, кластерні блоки для обчислювальних задач, дублювання інформації та ін.).



- Схема контролю зовнішнього периметра мережі

- Засоби активного аудиту

Переведення мережевого адаптера якогось з вузлів мережі в змішаний (*promiscuous*) режим

Підключення до лінії зв'язку спеціального прослуховуючого пристрою

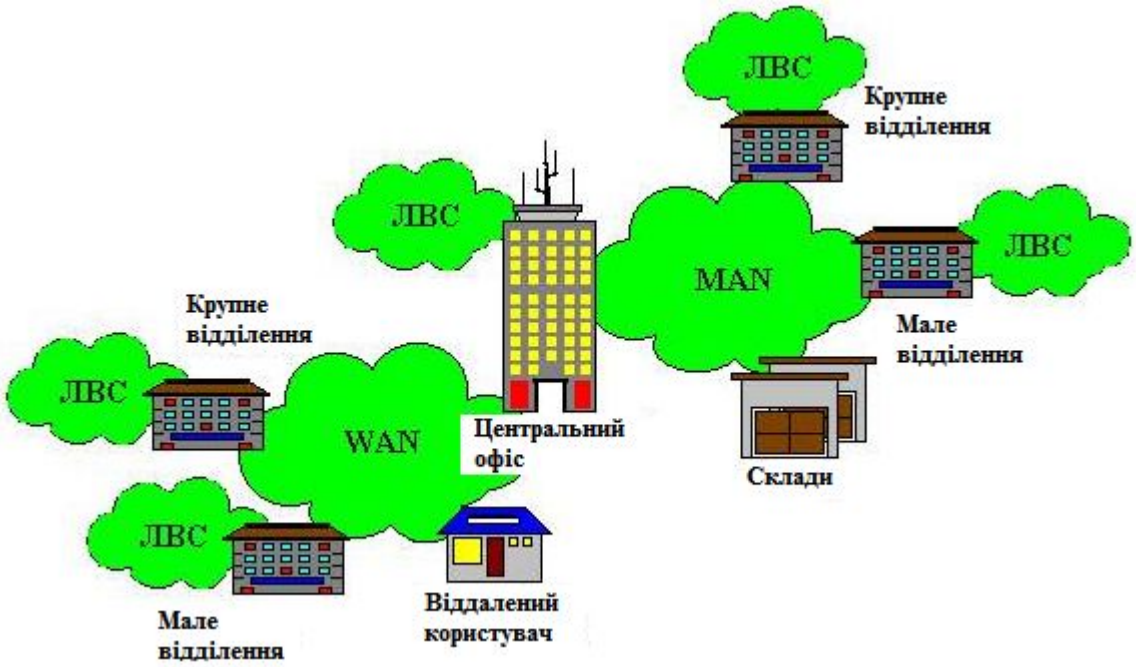
Встановлення контролю над маршрутизатором або іншим пристроєм

Реалізація політик захисту

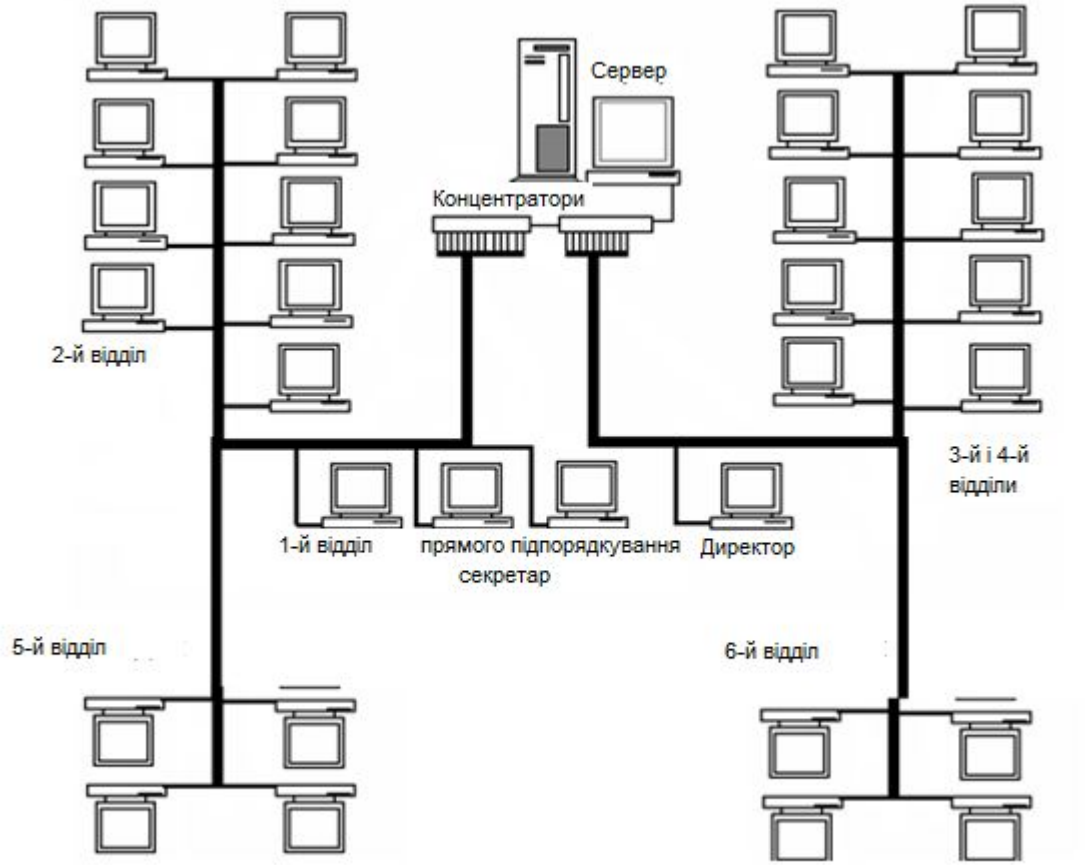
- Типові варіанти реалізації прослуховування інформаційного обміну

МЕХАНІЗМИ ЗАХИСТУ СУЧАСНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ ВІД ЗОВНІШНІХ ВПЛИВІВ

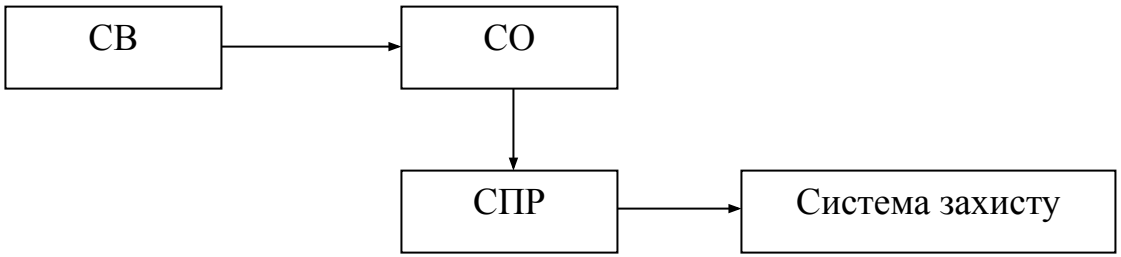
- Успішна діяльність промислової, фінансової або іншої організації багато в чому визначається наявністю єдиного інформаційного простору. Розвинена інформаційна система дозволяє ефективно справлятися з обробкою потоків інформації, що циркулюють між співробітниками підприємства і приймати їм своєчасні та раціональні рішення, що забезпечують виживання підприємства в жорсткій конкурентній боротьбі.



- Узагальнена схема корпоративної мережі



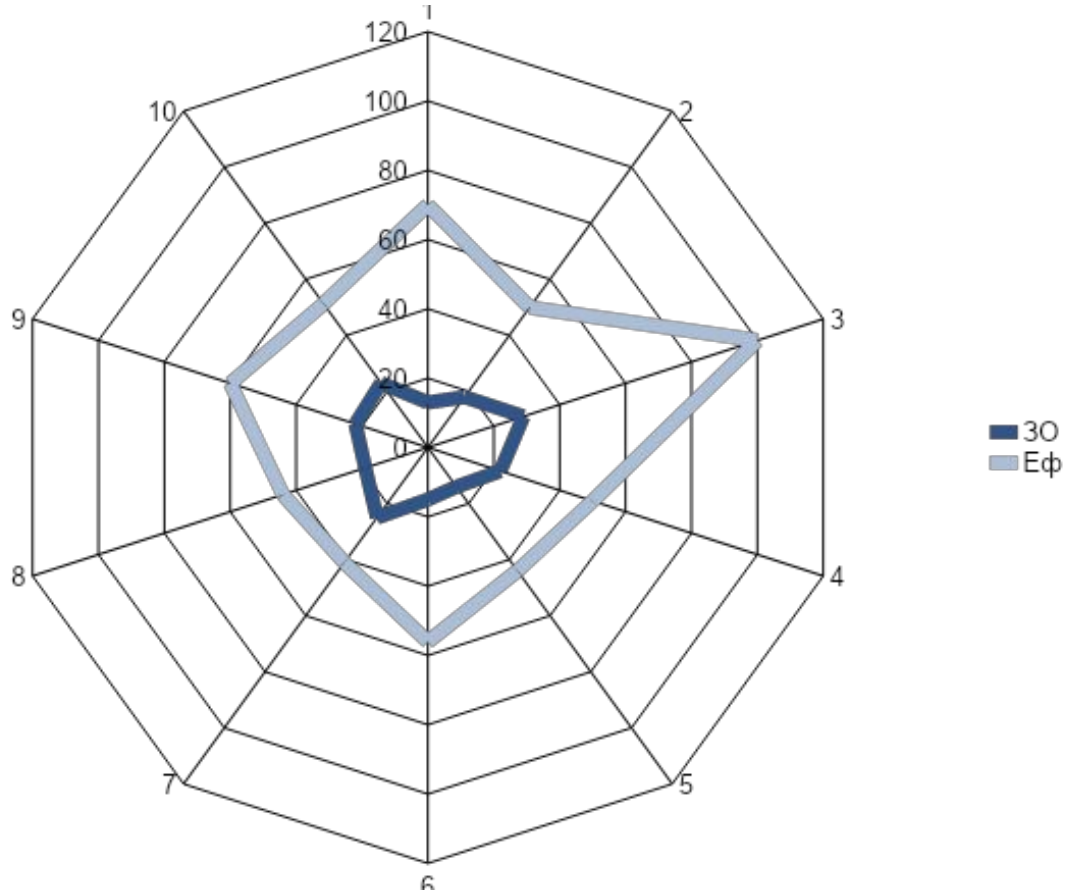
? Топологія мережі підприємства



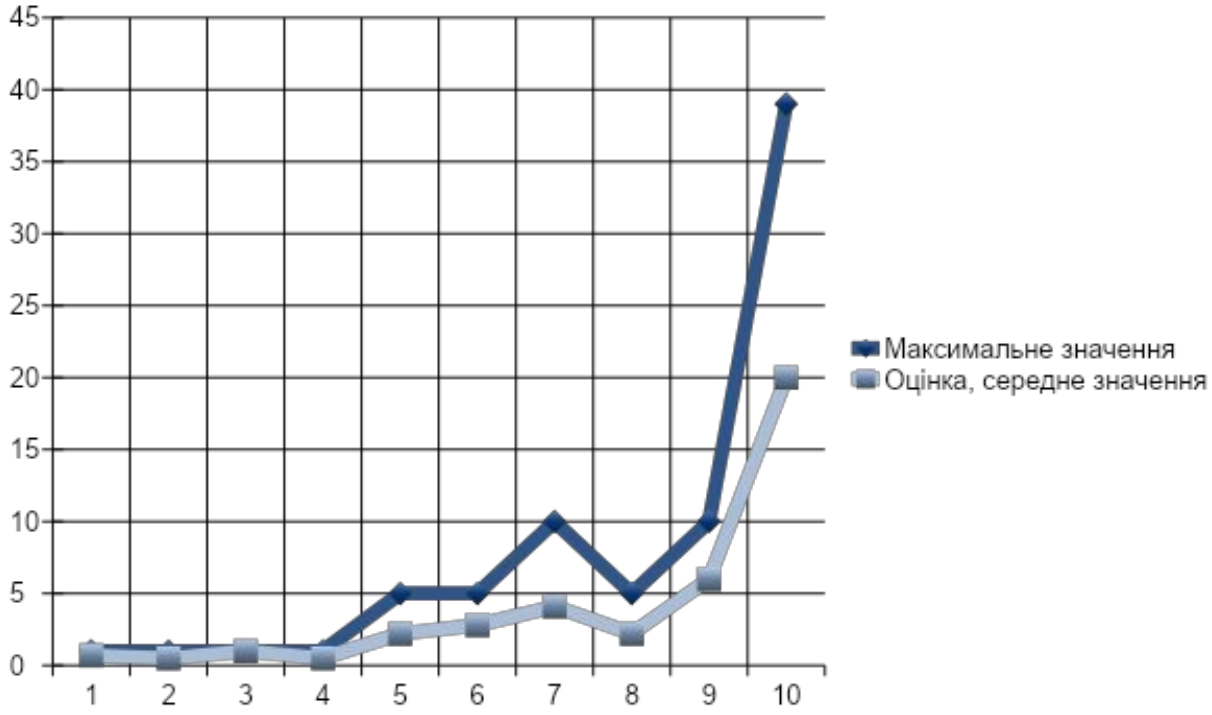
- Загальна архітектура аналітичної системи захисту інформації корпоративної мережі від зовнішніх впливів

РОЗРОБКА АНАЛІТИЧНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ КОРПОРАТИВНОЇ МЕРЕЖІ ВІД ЗОВНІШНІХ ВПЛИВІВ

- На сьогоднішній день, одним з головних напрямків ефективної реалізації будь-якої методики є експериментальне дослідження тобто виявлення якостей досліджуваних об’єктів, перевірка достовірності гіпотез, а також широке та глибоке вивчення досліджуваної наукової тематики. У рамках сучасної науки існує багато різних класифікацій експериментів в залежності від галузі науки, мети дослідження, структури об’єктів та явищ, організаційних заходів, характеру взаємодії об’єкту та засобів дослідження тощо.



- Графік залежності ефективності від Загальної оцінки



- Графік залежності ефективності від середньої оцінки

ВИСНОВКИ

- Аналітична система захисту інформації корпоративної мережі від зовнішніх впливів у своєму складі має базові показники ефективності. Використання описаних показників дасть можливість: швидко приймати управлінські рішення, оцінювати рівень кваліфікації фахівців CERT, підвищити ефективність роботи CERT, зменшити втрати пов'язані з інцидентами, підвищити продуктивність роботи користувачів, ефективно використовувати персонал, підвищити точність інформації в конфігураційний.
- У роботі розроблено аналітичну систему захисту інформації корпоративної мережі від зовнішніх впливів, яка за рахунок визначення показників функціонування CSIRT, виділення серед них ключових показників ефективності, використовуючи багаточинниковий кореляційно-регресійний аналіз, візуалізації залежності KPI та E, дає можливість проводити аудит діяльності управління інцидентами інформаційної безпеки та інших центрів технічного обслуговування інформаційно-телекомунікаційних систем

Дякую за увагу.