Автоматизована система для розробки політики безпеки СУБД

Розробила:
Костельна А.А.

Науковий керівник:
Войтко В.В.

МЕТА РОБОТИ, ОБ'ЄКТ ТА ПРЕДМЕТ ДОСЛІДЖЕННЯ, ЗАДАЧІ ДОСЛІДЖЕННЯ

- Метою роботи є підвищення надійності та захищеності СУБД за рахунок розробки системи створення політик безпеки, що базується на методах оцінювання загроз та ризиків для ідентифікації критеріїв оцінювання можливих загроз.
- Об'єкт дослідження – технології створення політик безпеки для інформаційних систем.
- Предмет дослідження – засоби формування політик безпеки СУБД.

НАУКОВА НОВИЗНА

- Подальшого розвитку отримала система виявлення та протидії мережевим атакам на СУБД, що, на відміну від існуючих, являє собою більш комплексну систему, сформовану за визначеним набором критеріїв оцінювання ризиків, що дозволяє аналізувати значно більшу кількість можливих загроз інформаційній системі та формує відповідний набір політик безпеки та збільшує надійність та захищеність СУБД.
- Дістав подальшого розвитку метод аналізу і обробки критеріїв ризику з метою формування правил політики безпеки інформаційної системи, який на відміну від існуючих формує більш чіткий алгоритм створення політики безпеки, шляхом систематизації розроблених критеріїв оцінювання загроз, що дозволяє формалізувати процес боротьби з атаками та підвищує ступінь захищеності інформаційної системи.

ПРОБЛЕМАТИКА

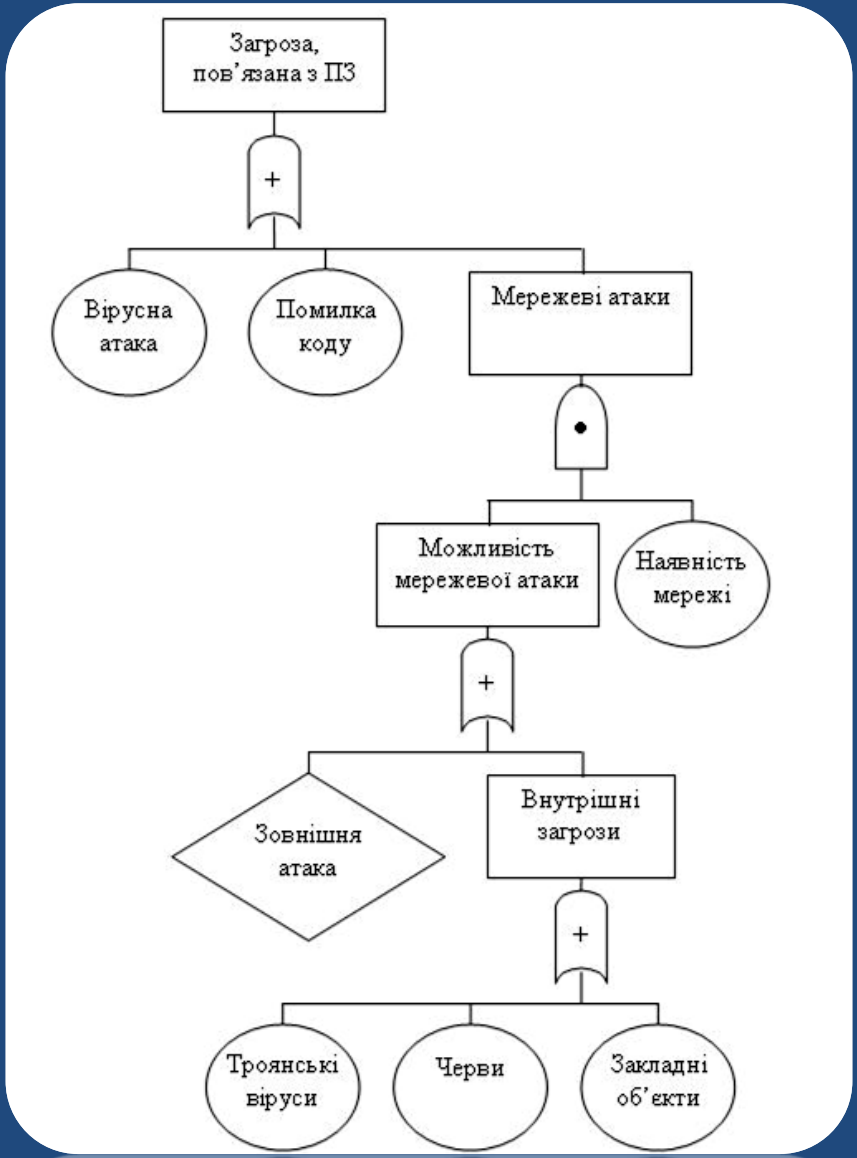
- Атаки на БД

- Викрадення особистих даних
- Пошкодження інформації

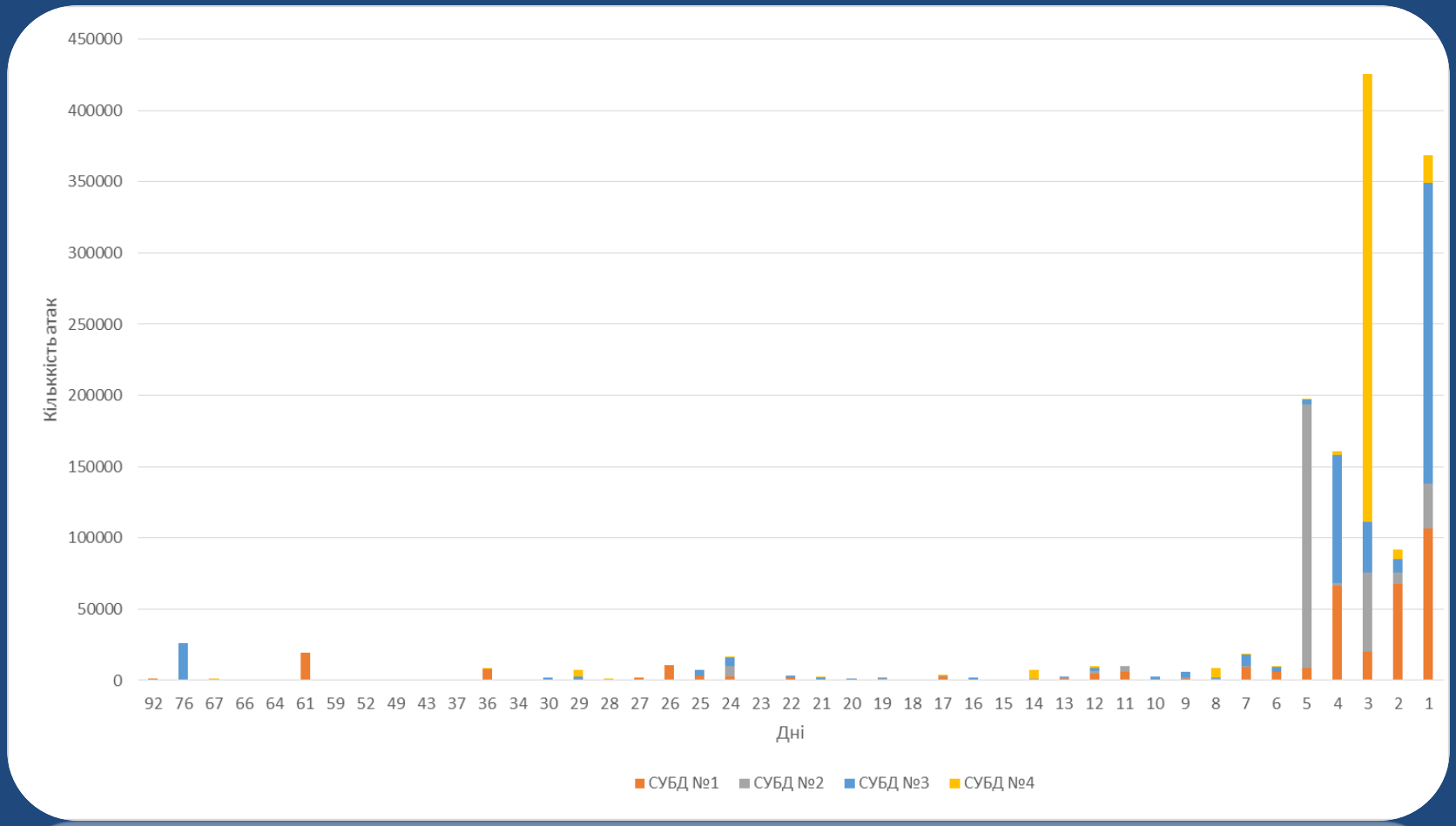
ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА МОДЕЛЕЙ РОЗРОБКИ ПРАВИЛ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Ознаки методів	Метод на основі аналізу всіх відомих загроз	Метод на основі повного аналізу організації
Час реалізації	Швидко (залежить від часу, але слід враховуючи автоматизацію процесу)	Досить довго (від одного місяця до шести, в залежності від розміру компанії)
Вартість	Дешево	Дорого
Можливість автоматизації	Так	Дуже важко
Легкість впровадження	Важко (все описується загальними фразами)	Легко (оскільки розроблюються індивідуально для кожного підрозділу організації)
Ефективність	Середня (не враховує виникнення нових методів атак)	Велика (можливість передбачення різних видів атак)
Математичний апарат	Досить простий (жорстка логіка, не передбачає вдосконалення)	Дуже складний (потребує налаштування під конкретну систему)
Матеріали на вході	Потребує загальну структуру фірми	Повний аналіз організації
Матеріали на виході	Дуже багата кількість документів, інколи не узгоджених	Не велика але чітка політика безпеки

МОДЕЛЬ ДЕРЕВА РИЗИКІВ



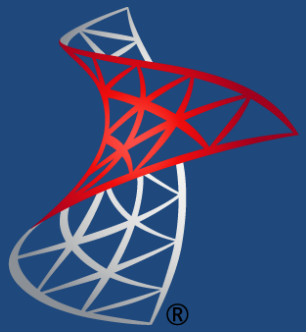
АНАЛІЗ ТРИВАЛОСТІ АТАК ДО ІСНУЮЧИХ СЕРВЕРІВ БАЗ ДАНИХ



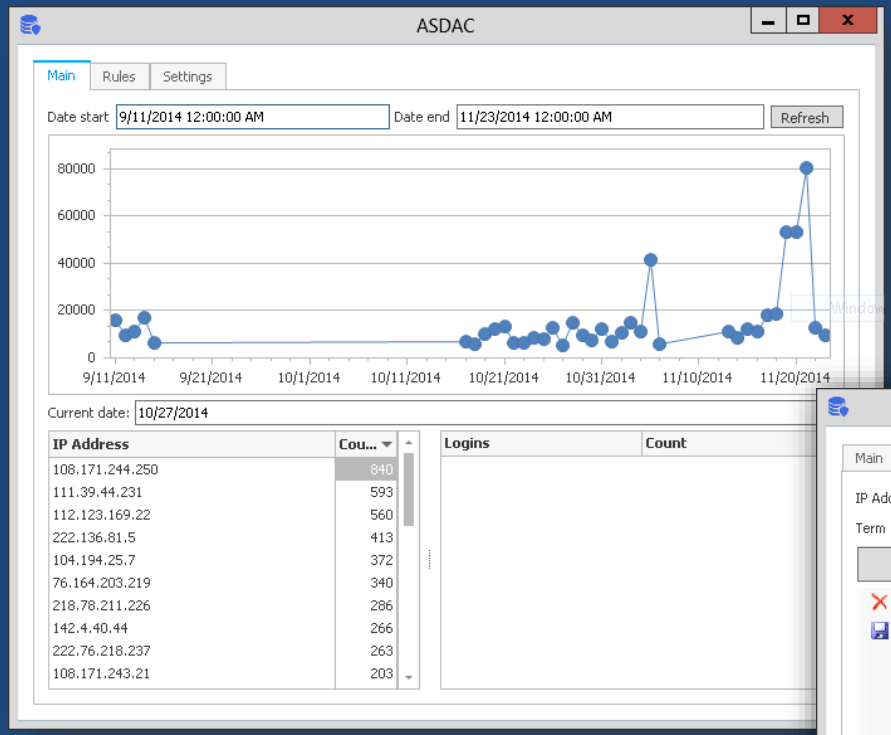
ТЕХНОЛОГІЇ

Для магістерської кваліфікаційної роботи було використано наступні технології:

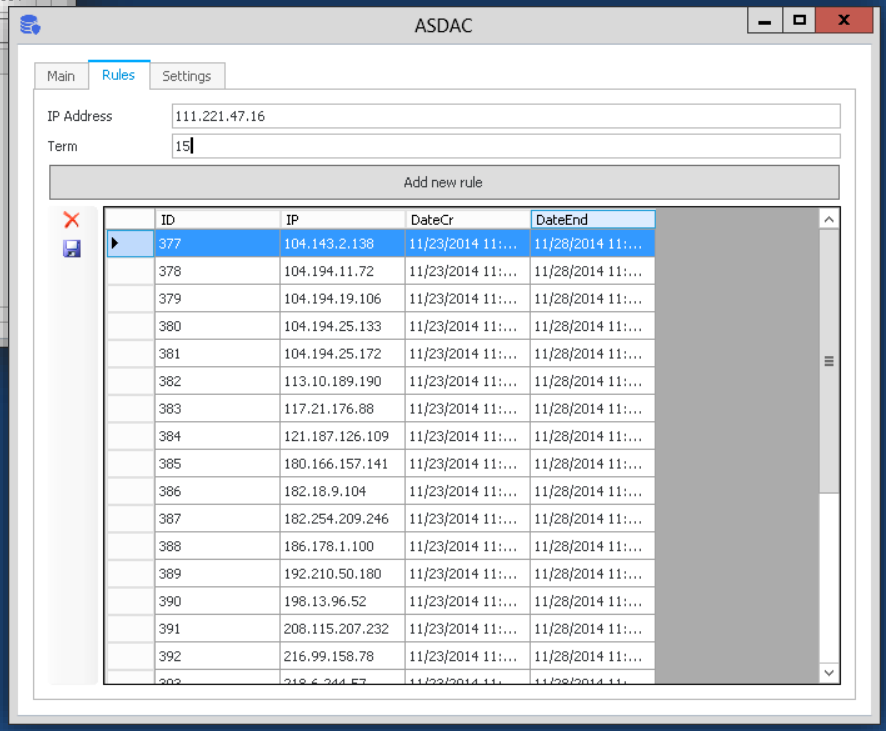
- .NET Framework 4.0

- 

ПРИКЛАД ВИГЛЯДУ ПРОГРАМИ

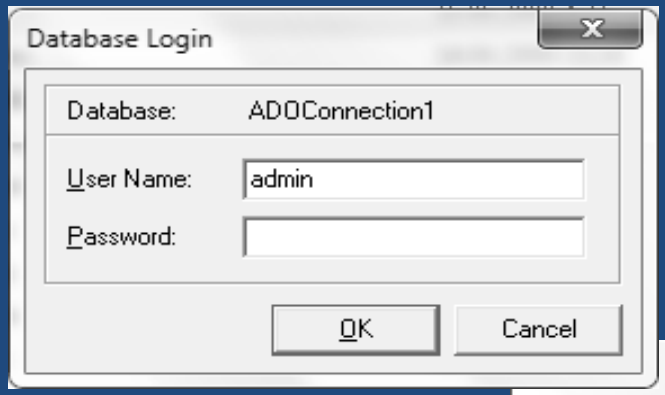


Головна форма з логами, статистикою та часовою діаграмою.

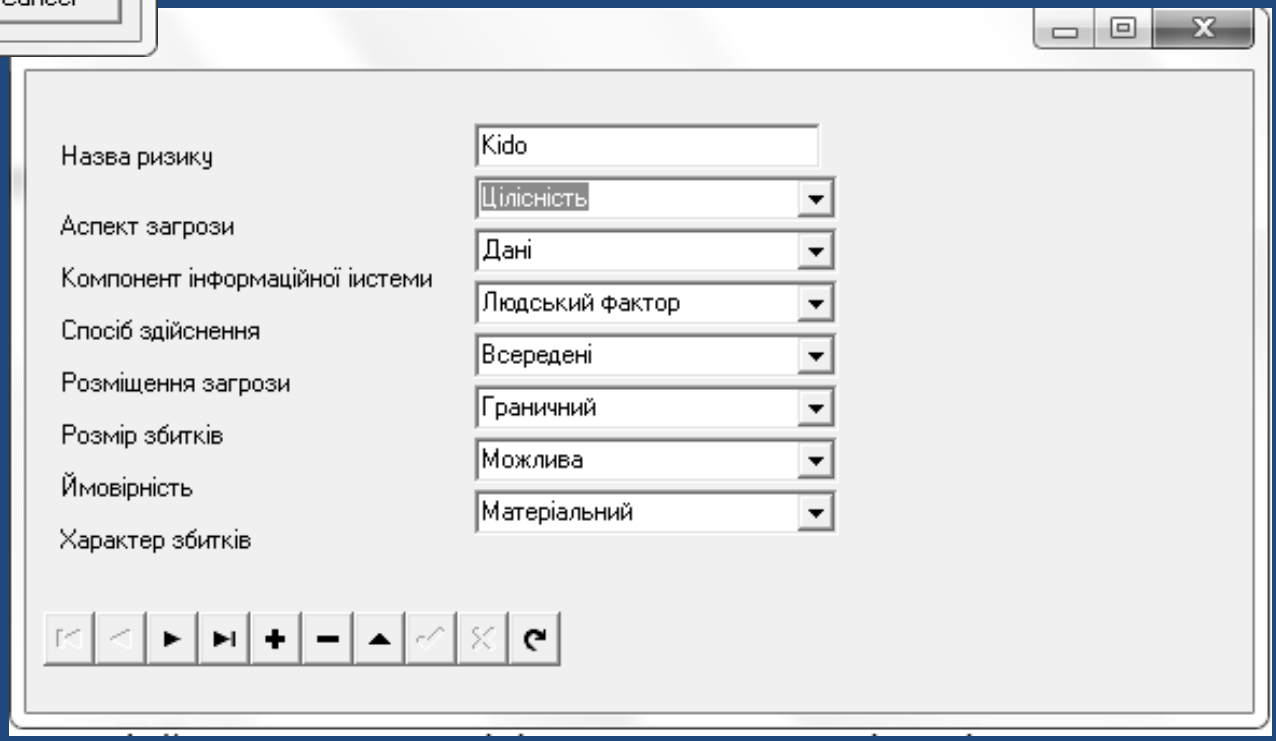


Автоматичне додавання нового правила

ПРИКЛАД ВИГЛЯДУ ПРОГРАМИ



Діалогове вікно входу в програму



Форма додавання ризику

ВИСНОВКИ

- Було проаналізовано цільовий ринок для системи захисту баз даних. Проведено пошук програм-аналогів, та розглянуто їх основні переваги та недоліки. Вибрано основного конкурента та проведено порівняльний аналіз якості та конкурентоспроможності власної розробки та вибраного конкурента. Отримані результати вказують на те, що власний продукт має високу якість та значно нижчу ціну і тому є конкурентоспроможним.
- Проаналізовано існуючі методи розробки правил політик безпеки, методи оцінювання ризиків, проведено порівняльну характеристику методів розробки політик інформаційної безпеки
- Розглянуто методи та системи оцінювання загроз, етапи створення політики інформаційної безпеки, створено математичну модель політики інформаційної безпеки, визначено спосіб ідентифікації розділів політики безпеки. Також було розглянуто способи авторизації до MS SQL Server, розроблено механізм виявлення та блокування атак до СУБД, визначено структурні елементи майбутньої автоматизованої системи захисту та розроблено її алгоритм роботи.
- В результаті роботи розроблено базу даних(базу знань), що дозволяє оцінити будь який ризик та програмний продукт, який дозволяє в багатокористувацькому режимі заповнювати базу знань, отримано програмний продукт, що складається з трьох компонентів та реалізує створення політик безпеки для захисту бази даних. Для реалізації проекту було обрано сучасне середовище розробки Visual Studio 2013, та мову C#, основною перевагою якої є використання останніх сучасних методів та засобів розробки.
- Проведено тестування системи.
- Проведено розрахунок кошторису витрат на розробку програмного продукту, ціни реалізації, розрахунок чистого прибутку та експлуатаційних витрат, річного економічного ефекту та терміну окупності витрат розробника.

За темою дослідження

- Робота брала участь у Всеукраїнському конкурсі ІТ-Еврика з членами жюрі з Швеції.
- Результати розробки

  Доповідалися на XLIV

  Науково-технічній конференції

  професорсько-викладацького складу, співробітників та студентів університету з участю працівників науково-дослідних організацій та інженерно-технічних працівників підприємств м. Вінниці та області 2015 року, м. Вінниця, в секціях загальноінженерних та технічних наук.
- Отримано свідоцтво про реєстрацію авторського права на твір (реєстраційний номер 58294 – від 26.01.2015р)

ДЯКУЮ ЗА УВАГУ!