УДК 004.056 **Захарова М.В. (ЧДТУ), Корченко А.О. (НАУ), Хропата І.В. (НАУ)**

ПРОГРАМНА МОДЕЛЬ ПРОЦЕСУ ВИБОРУ ЕФЕКТИВНИХ МЕХАНІЗМІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Розроблено програмну модель вибору механізмів захисту інформаційних ресурсів, яка за рахунок використання нечіткої логіки, дозволяє визначити здатність відповідної системи захисту протистояти кібератакам.

При проектуванні ефективної системи захисту необхідно розробити методи визначення цінності або критичності інформаційних ресурсів (ІР) та методи реагування на появу кібератак, застосовувати ефективні механізми захисту (МЗ) для реалізації всіх необхідних функцій, пов'язаних із забезпеченням конфіденційності і цілісності інформації. Застосування традиційних математичних методів для оцінювання ефективності МЗ не завжди можливе, оскільки вони не дозволяють обробляти нечислову і нечітку інформацію, а також встановлювати причинно-наслідкові зв’язки між лінгвістичними параметрами. Тому задача розробки підходу до вибору механізмів захисту та побудова на його основі програмної моделі, яка за рахунок використання нечіткої логіки, дозволить вибрати ефективні механізми захисту ІР, є актуальною.

Для забезпечення захисту інформації в інформаційних системах (ІС) на заданому рівні необхідно застосування ефективних механізмів захисту ІР, що поєднуються в єдину систему захисту інформації (СЗІ). Створення усіх варіантів реальної СЗІ та аналіз їх функціонування є неможливим так як потребує значних временних та фінансових втрат. Моделювання процесів вибору ефективних механізмів, а також систем в цілому дозволяє прискорити вибір оптимального варіанту системи захисту інформації.

У зв‘язку з цим необхідно розробити програмну модель, що дозволить підвищити загальний рівень захищеності всієї системи в цілому та визначити здатність відповідної системи захисту протистояти кібератакам, надати практичні рекомендації для застосування ефективних механізмів захисту ІР.

Підвищити захищеність ІР дозволить вибір ефективних механізмів захисту, де кожному з механізмів захисту ставитися у відповідність деякий набір показників: ресурсоємність, вартість, рівень захисту, що характеризують ступінь впливу даного механізму на ймовірність реалізації кібератаки (рис. 1).

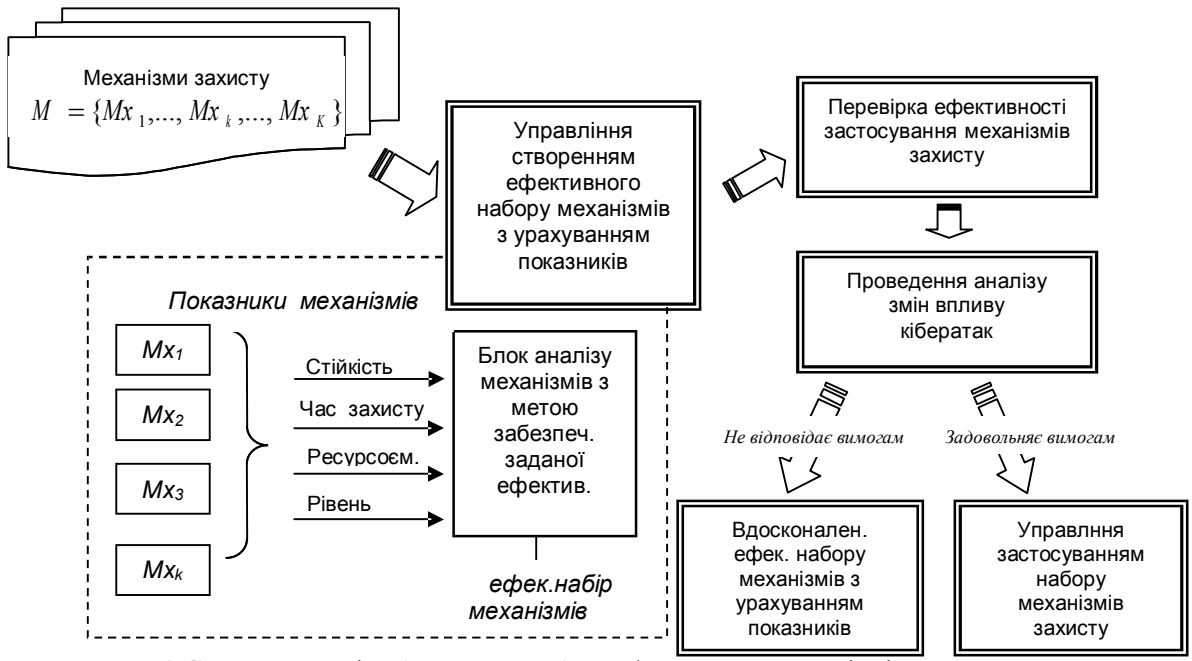


Рис. 1 Схематичне відображення вибору ефективних механізмів захисту ІР

Застосування ефективних механізмів захисту інформації впливає на значення імовірності кібератаки і коефіцієнта її небезпеки. Нехай відомі всі можливі кібератаки безпеці ІС, будь-яка з цих кібератак виявляється і реалізується за період часу з ймовірністю близькою до одиниці. Для кожної кібератаки $R = \{R_1,...,R_n,...,R_N\}$ визначений набір з механізмів захисту $M = \{Mx_1,...,Mx_k,...,Mx_K\}$, де K – кількість механізмів, із заданими значеннями коефіцієнтів ефективності захисту $\varepsilon_{nk}, k = \overline{1,K}$ у вигляді нечітких чисел. Значення ε_{nk} визначатиметься видом кібератаки та рівнем, до якого може бути знижена небезпека кібератаки і ймовірність її реалізації [2].

При виборі ефективних механізмів захисту повинні враховуватися можливості управління ними для забезпечення максимально можливого рівня захищеності ІР. На основі даного підходу розроблено програмну модель (ПМ), що дозволяє змоделювати процес вибору ефективних механізмів захисту та оцінити рівнь захищеності інформаційних ресурсів (рис. 2). ПМ складається з модулів: внутрішнього захисту (процедури ідентифікації та аутентифікації), що використовуються з метою зниження вірогідності роботи з програмою особами без дозволених повноважень, також зменшується можливість припинення роботи програми чи зміни налаштунок особами, що атакують; модулю введення вхідних даних в систему та їх обробки, модулю аналізу ефективності та управління застосуванням механізмів захисту (МЗ), модулю оцінки рівня захищеності, підтримки та прийняття рішень по застосуванню МЗ, модулю моніторінгу рівня захищеності ІР.

В залежності від вибраного класу атаки, ПМ дозволяє змоделювати процеси захисту ІР необхідних об’єктів, які можуть бути атаковані та рекомендує механізми захисту, що можуть протидіяти атаці. Також ПМ реалізує функцію додаткового захисту – примусове встановлення захисту, який за замовчуванням не був рекомендований до встановлення, в залежності від вибраного класу атаки. Не рекомендований до встановлення системою механізм захисту, не приймає участі в розподілені відсотку захисту, але допомагає в роботі системи, і до загального захисту “додає”, приблизно, 2-4%.

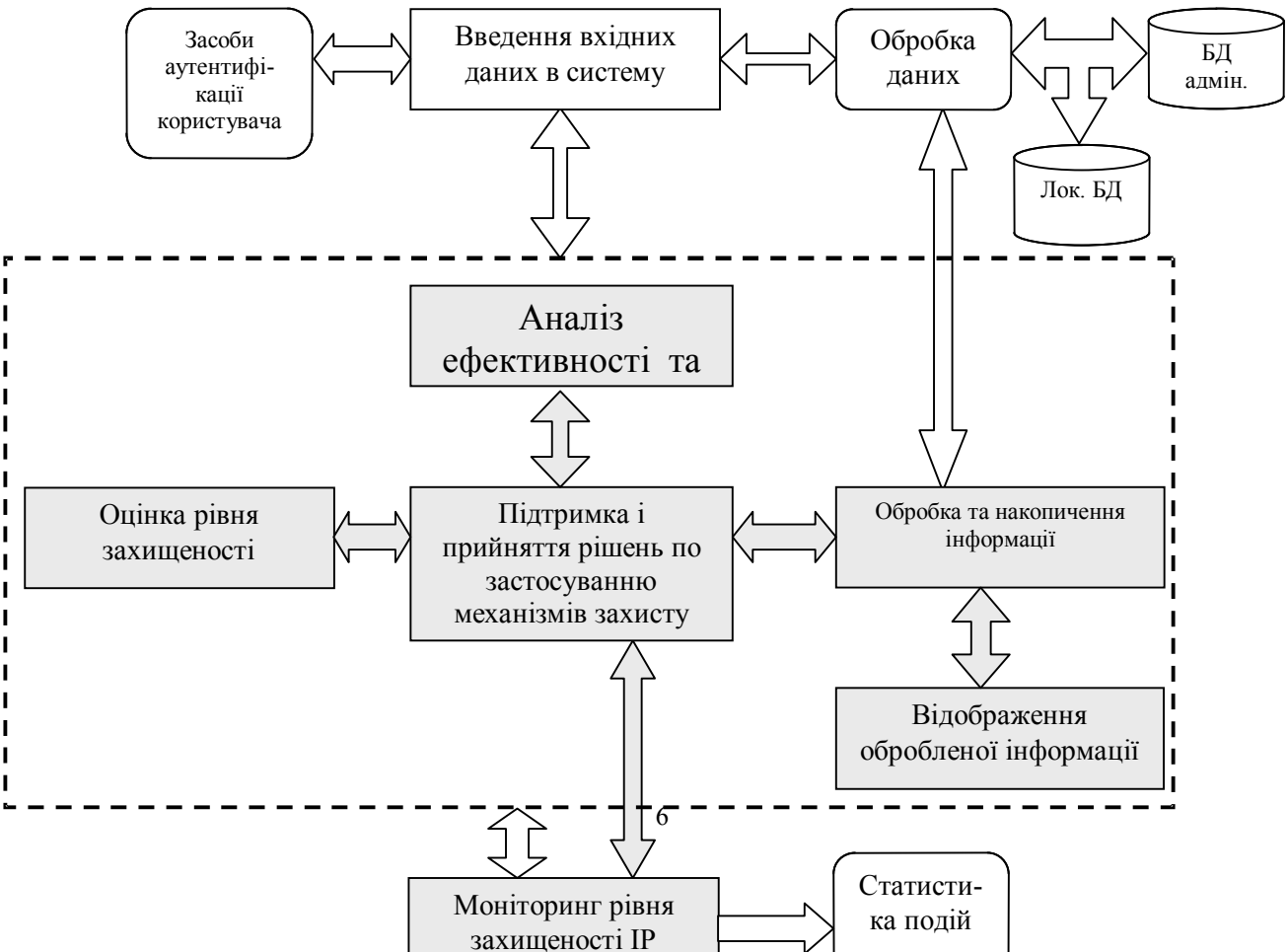


Рис. 2 Схематичне відображення взаємодії модулів ПМ

Головне вікно програми містить елементи керування для забезпечення налаштування, візуалізації, інформування та керування роботою програми (рис. 3). Вхідними даними для ПМ є клас атаки; механізми захисту; об'єкти захисту.

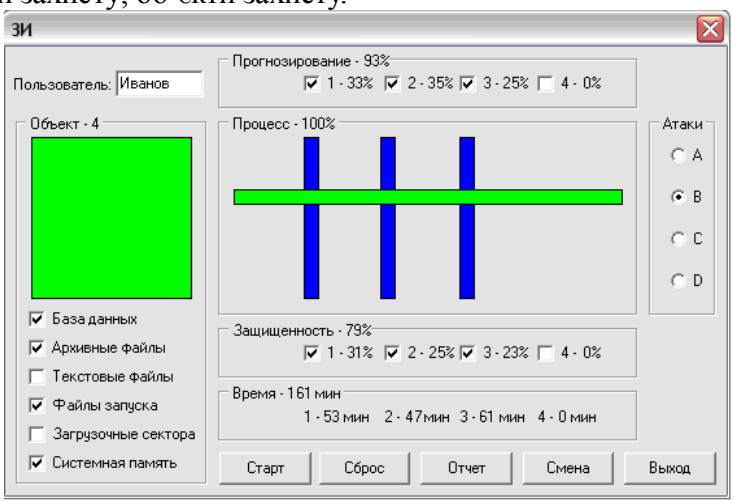


Рис. 3 Вікно інтерфейсу ПМ

Вихідною інформацією є відсоток захищеності; час захищеності; ідомості про поточного користувача, об'єкти захисту, відсотки прогнозування й захищеності та час роботи кожного з механізмів захисту, а також відсоток та час загального захисту від певного класу атаки.

На початку роботи програмної моделі задається кількість механізмів захисту, кількість атак на ресурси, обмеження, та часовий інтервал, за який здіснюються атаки (рис. 4).

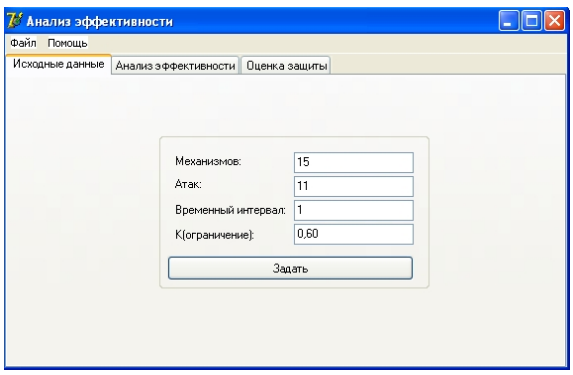


Рис. 4 Фрагмент вікна вводу вихідних даних

В вкладці «Аналіз ефективності» в якості вхідних даних коеффіциети ефективності механізмів захисту, за допомогою програми будується графік та виконується аналіз ефективності механізмів. Коефіцієнт ефективності механізму захисту відповідно коефіцієнта небезпеки кібератаки може бути визначений через значення коефіцієнта небезпеки кібератаки R, тобто наскільки знижується небезпека n-ої кібератаки в результаті застосування κ-ого механізму захисту.

Проводиться оцінка рівня захищеності інформаційних ресурсів (рис. 5) з урахованням зміни інтенсивностей потоків кібератак, що впливають на ІР при застосуванні механізмів безпеки інформації $d\beta = \beta_1 - \beta_2$, де β_1 - інтенсивность потоків кібератак без застосування ефективного набору механізмів, β_2 - інтенсивність порушення безпеки ресурса з використанням ефективного набору механізмів захисту [1].

Наприклад, для R_n=0,3 можна визначити, що найбільш ефективним є набор механізмів Mx_5, Mx_6, оскільки при його застосуванні рівень захищеності ресурсів підвищується на 0,11.

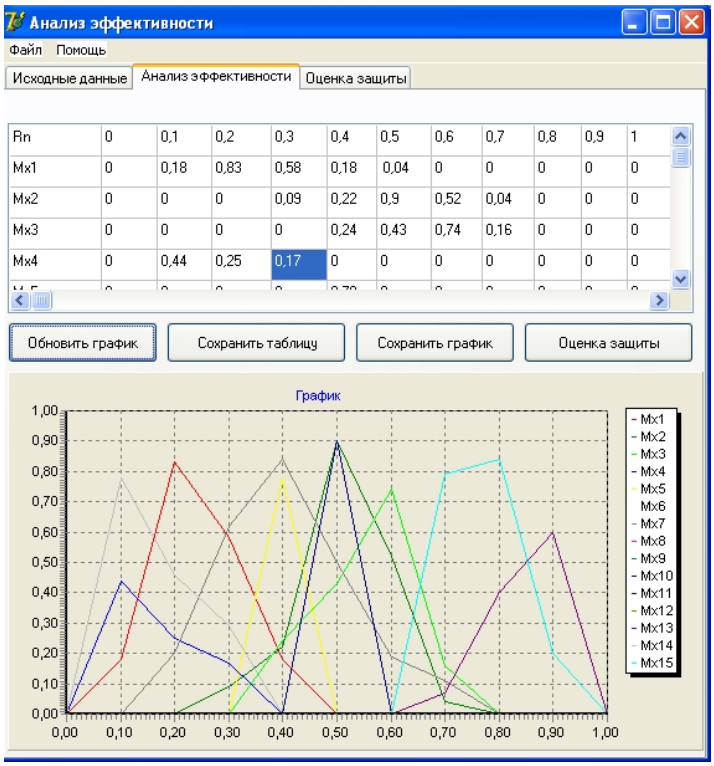
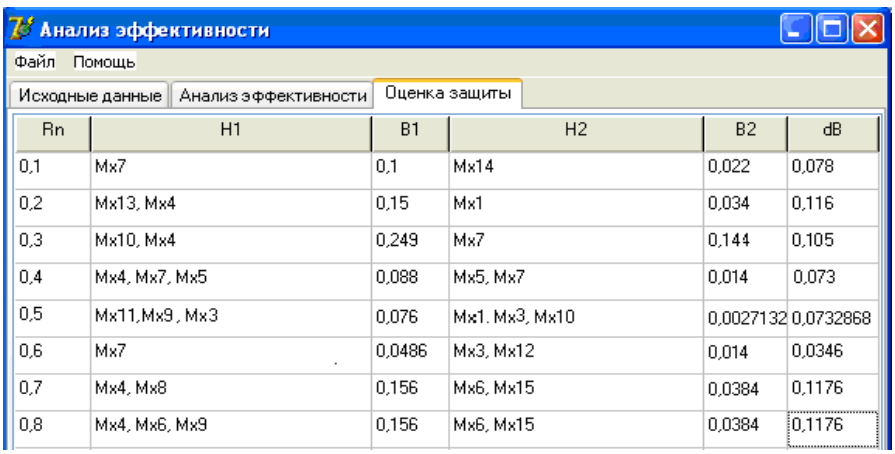


Рис.5 Оцінка ефективності механізмів захисту

За рахунок використання ефективного набору механізмів захисту рівень захищеності інформаційних ресурсів збільшується на 2-11% .



Rn	H1	B1	H2	B2	dB
0,1	Mx7	0,1	Mx14	0,022	0,078
0,2	Mx13, Mx4	0,15	Mx1	0,034	0,116
0,3	Mx10, Mx4	0,249	Mx7	0,144	0,105
0,4	Mx4, Mx7, Mx5	0,088	Mx5, Mx7	0,014	0,073
0,5	Mx11,Mx9 , Mx3	0,076	Mx1. Mx3, Mx10	0,0027132	0,0732868
0,6	Mx7	0,0486	Mx3, Mx12	0,014	0,0346
0,7	Mx4, Mx8	0,156	Mx6, Mx15	0,0384	0,1176
0,8	Mx4, Mx6, Mx9	0,156	Mx6, Mx15	0,0384	0,1176

Рис. 6 Фрагмент вікна оцінки рівня захищеності інфомаційних ресурів

Запропонована програмна модель процесу вибору механізмів захисту інформаційних ресурсів дозволяє оцінити рівень захищеності ІР, прийняти рішення по вибору ефективних механізмів захисту та дозволяє здійснювати поточний контроль і може бути використана на етапах проектування і експлуатації системи захисту ІР. Розроблена програмна модель, за рахунок використання нечіткої логіки, дозволяє визначити здатність відповідної системи захисту протистояти кібератакам та досягти максимізації загального рівня захищеності всієї системи в цілому.

Література

1. Корченко А.О., Паціра Є.В., Захарова М.В..Методологія синтезу механізмів захисту інформаційних ресурсів. Защита информации: сборник научных трудов. – К.: НАУ, 2008.

2. Рындюк В.А., Захарова М.В. Повышение защищенности информационных ресурсов за счет определения коэффициентов эффективности механизмов защиты // Материалы II Международной научно-практической конференции "Информационные технологии в гуманитарном образовании", 22-23 апреля 2009г.,- Пятигорск: ПГЛУ, 2009. – с.398-404.

3. Стасюк О.І., Захарова М.В., Корченко А.О. Побудова ефективних моделей систем захисту інформаці / Защита информации: Сборник научних трудов. – К.: НАУ, 2007.

Надійшла: 03.06.2011 р.

Рецензент: д.т.н., проф. Юдін О.К.