УДК 004.056.53

М.В. Захарова, к.т.н.

МЕТОДИКА ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ІС НА ОСНОВІ МОДЕЛІ АДАПТИВНОГО ЗАХИСТУ

Черкаський державний технологічний університет, E-mail: zmaria@yandex.ru

Захищеність інформаційного середовища традиційно розглядають як сукупність засобів, що забезпечують захист ресурсів інформаційної системи (ІС), але не враховують можливість адаптації засобів безпеки до зміни загроз, не дають рекомендацій на зміну їх складу. Тому для побудови захищеної ІС необхідно використовувати засоби адаптивного захисту, які не заперечують традиційних методів, а розширюють їх функціональність за рахунок нових технологій. Запропонована методика базується на основних властивостях нечітких систем, пов'язаних з адаптивністю, навчанням, можливістю подання досвіду фахівців інформаційної безпеки у вигляді системи нечітких правил, доступних для аналізу. Запропонована методика дозволяє оцінити або переоцінити рівень захищеності системи, а також надати рекомендації з підвищення безпеки ІС, знизити потенційні ризики.

Ключові слова: *засоби безпеки інформації, дестабілізуючі фактори, адаптивний захист, ризик, інформаційна система*

Постановка проблеми у загальному вигляді. Різноманіття варіантів побудови інформаційних систем породжує необхідність створення різних систем захисту, що враховують індивідуальні особливості кожної з них. Сьогодні існує безліч методів захисту ІС, що знижують ризики втрати інформаційних ресурсів, тому дуже важливим етапом реалізації захисту ІС є вибір ефективного методу захисту конкретної системи.

Аналіз останніх досліджень і публікацій.

В сучасних публікаціях захищеність інформаційних ресурсів та інформаційного середовища традиційно розглядають як сукупність засобів і технологічних прийомів, що забезпечують захист ресурсів інформаційної системи, але не враховують можливість адаптації засобів безпеки (ЗБ) до зміни загроз, не дають рекомендацій на зміну складу ЗБ. Тому для побудови захищеної ІС потрібні засоби, які не лише виявляють і блокують атаки, але і попереджують їх. Розвитком традиційних методів захисту є адаптивний захист [1]. Він не заперечує традиційних методів, а розширює їх функціональність за рахунок нових технологій. В зв‘язку з цим **метою даної роботи** є дослідження адаптивних методів захисту, їх використання для підвищення рівня захищеності ІС та розробка методики побудови системи захисту інформації (СЗІ) на основі моделі адаптивного захисту.

Виклад основного матеріалу дослідження.

Динамічний характер загроз висуває властивість адаптивності ІС в розряд першочергових якостей, необхідної СЗІ. Використання моделі адаптивного захисту (АЗ) дає можливість пристосовуватися до зовнішніх змін середовища функціонування ІС, компенсуючи небажані впливи й дозволяючи системі оптимізувати свою роботу відповідно до встановлених критеріїв, і навіть змінити ціль функціонування, якщо цього вимагають нові умови.

Адаптивні системи захисту орієнтовані на активне протистояння загрозам безпеки. Реалізація такого підходу потребує проведення аналізу ризиків, розробки політики безпеки, використання традиційних засобів захисту, а також впровадження контрзасобів для протистояння загрозам, постійного моніторингу стану системи, що має дозволити оперативно реагувати на ризики безпеки [1]. Адаптивна безпека ІС складається з трьох основних складових: аналізу захищеності ІС, виявлення атак та управління ризиками (див.рис.1).

При розробці сучасних перспективних систем захисту інформації наразі широко використовується теоретичний апарат експертних систем, теорії нечіткої логіки, нейронних мереж. При врахуванні ризиків різних типів зручним представляється використання нечіткої логіки, яка є ефективним засобом моделювання в умовах невизначеності [2]. Крім того, системи нечіткої логіки володіють можливостями до адаптації, можуть навчатися шляхом зміни параметрів функцій належності.

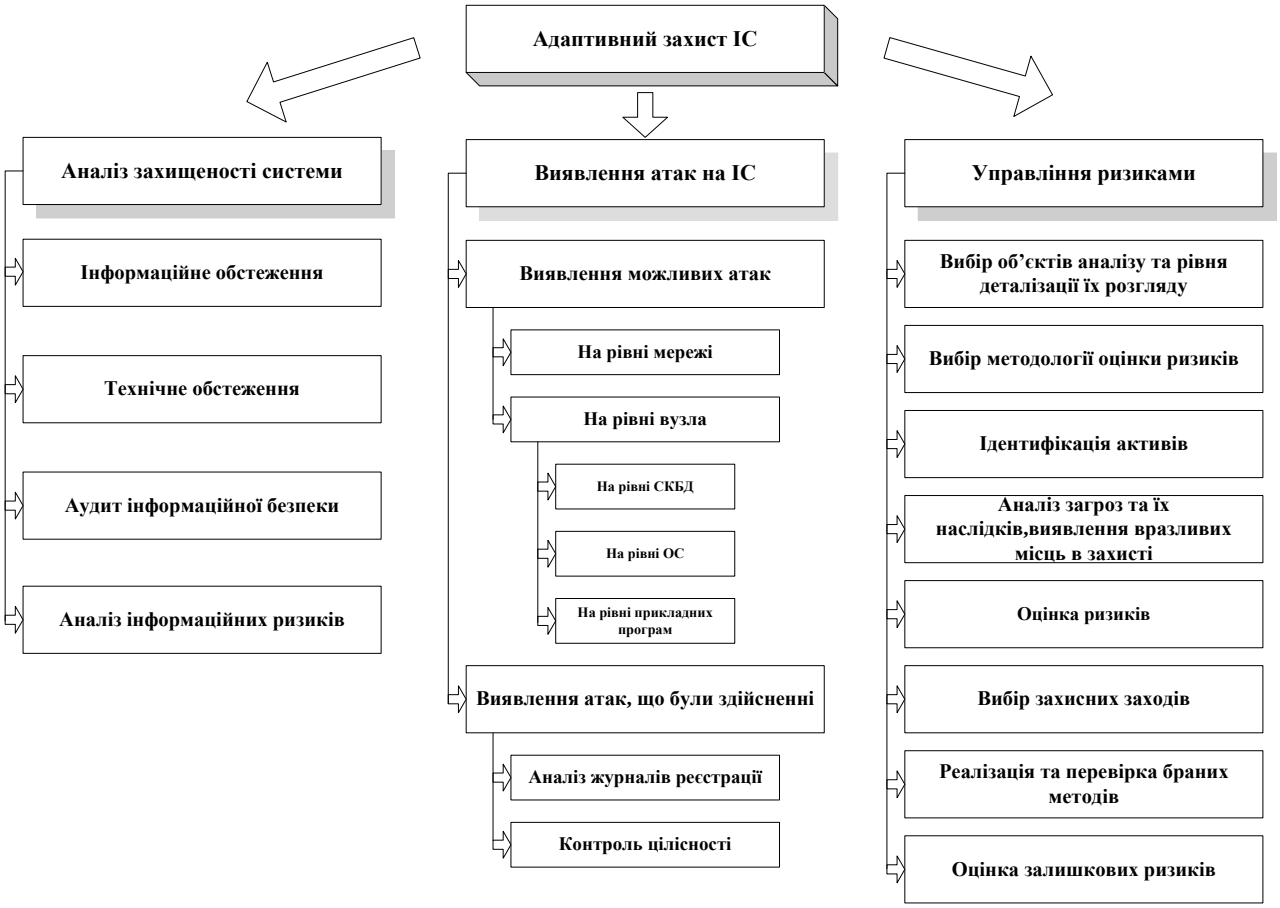

Рис.1 Схема відображення складових АЗ

Розробка методики побудови системи захисту ІС на основі моделі адаптивного захисту включає етапи:

Першим етапом є ідентифікація можливих дестабілізуючих факторів на інформаційну систему, виявлення її уразливих ресурсів (див.рис.2). Наприклад, показниками уразливості ресурсу і його особливо важливих компонентів є ступінь уразливості або ймовірність успішної дії порушників. Ресурсами ІС $X = \{X_1, X_2, X_3, ..., X_M\}$ можуть бути дані, засоби обчислювальної техніки, програмне забезпечення.

Дестабілізуючі фактори (ДФ) - події, наслідком яких можуть бути небажані у змісті захищеності впливи на інформацію, а саме порушення цілісності, приступності та конфіденційності інформації [3]. Аналіз впливу ДФ, у свою чергу, включає складання їх повного переліку і дослідження можливості впливу. При розширенні множини відомих ДФ необхідно провести класифікацію ДФ з наступною адаптацією інформаційних полів шляхом навчання нечітких систем. Зміна множини ДФ буде супроводжуватися корекцією або розширенням системи нечітких правил.

На другому етапі, проаналізувавши всі можливі дестабілізуючі фактори, причини їх виникнення та наслідки їх дії, вибираються засоби безпеки інформації з урахуванням їх спрямованості. Кожному з засобів безпеки (ЗБ) ставитися у відповідність деякий набір критеріїв, що характеризують ступінь впливу даного ЗБ на ймовірність реалізації ДФ.

Оцінка ефективності засобів безпеки виконується на рівні окремого ЗБ, а її результати дозволяють визначити відносну здатність відповідної системи захисту ІС протистояти ДФ [3]. Вимоги до ефективності ЗБ можуть істотно відрізнятися стосовно рішення конкретної задачі захисту. При оцінці ефективності захисту необхідно оцінити рівень адекватних ЗБ по кожному ДФ, враховувати можливі вразливості ІР, для яких необхідно передбачити ефективні ЗБ.

Наприклад, оцінки ЗБ та заходів забезпечення безпеки обираються з діапазону від 1 до 9 (див. табл. 1) [4].

Встановлені та вжиті ЗБ, особливо в початковий період їхньої експлуатації, можуть забезпечувати як надмірний, так і недостатній рівень захисту. Однак недоцільно для захисту ІС використовувати всі можливі ЗБ, необхідно обмежитись комплексом ЗБ, достатнім для відображення ДФ, обумовлених у специфікації на проектування ІС.[5]. Для забезпечення можливості варіювання рівнем захищеності, ЗБ повинні мати певну гнучкість. Особливо важлива ця властивість у тих випадках, коли установку ЗБ необхідно здійснювати на працюючу систему, не порушуючи процесу її нормального функціонування.

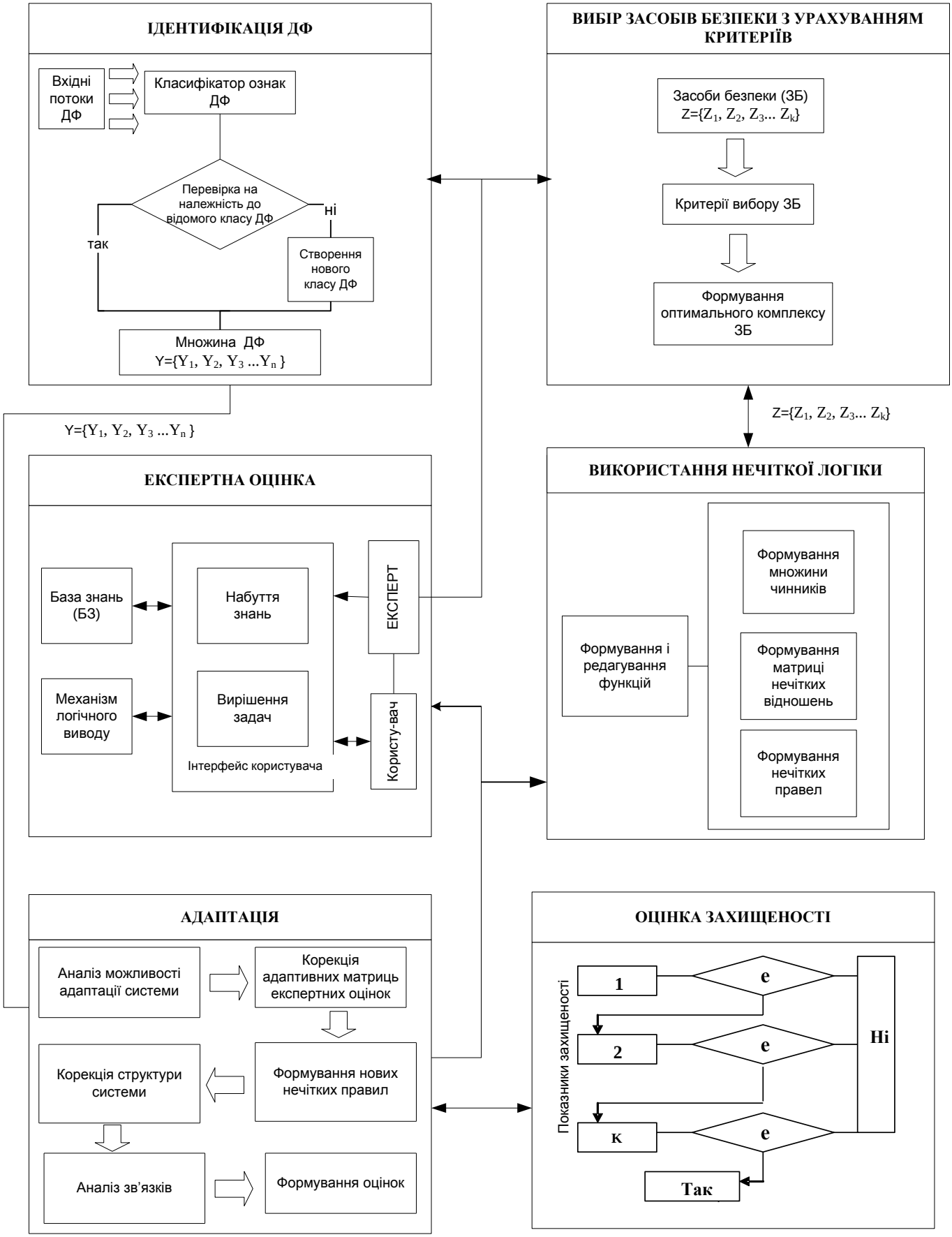

Рис.2 Схема відображення методики побудови системи захисту ІС на основі моделі адаптивного захисту

Таблиця 1

Визначення ефективності ЗБ

Засоби безпеки	Висока ефективність	Середня ефективність	Ефективність нижче середньої	Низька ефективність
Запобігання	Складна атака (8-9)	Контроль за дотриманням секретності (6-7)	Цілісність системи (4-5)	Нагляд за безпекою даних (1-3)
Виявлення	Виявлення за допомогою аналізу (8-9)	Організаційні заходи безпеки (5-7)	Накопичення контрольних параметрів (1-4)	
Розділення прав доступу	За значимістю даних (7-9)	По логічних пристроях (4-6)	По фізичних пристроях (1-3)	
Набір правил для забезпечення безпеки	Адміністративні заходи безпеки (7-9)	Мітки і списки керування доступом (3-6)	Паролі (1-2)	

Тому вчасне реагування на ДФ та доцільний вибір потрібного для даної ситуації ЗБ, дозволить швидко відновити роботу інформаційної системи та зменшити, або взагалі уникнути витрат.

На наступному етапі формуються матриці адаптивних експертних оцінок, на їх основі створюються вихідні системи нечітких правил. Для опису процесів, в яких присутня невизначеність, застосовується система нечіткого виводу. Основними процедурами нечіткого виводу є формування бази правил системи нечіткого виводу, фазифікація вхідних параметрів, агрегування, активізація та дефазифікація [6].

Механізм нечіткого логічного виводу заснований на базі знань, що формується експертами інформаційної безпеки у вигляді системи нечітких предикатних правил виду:

$$\text{П1 : якщо } \delta_1 \text{ існує } \text{À}_{11} \text{ та } \ldots \delta_n \text{ існує } \text{À}_{1n}, \text{ то } y = B_1,$$

$$\text{П2 : якщо } \delta_1 \text{ існує } \text{À}_{21} \text{ та } \ldots \delta_n \text{ існує } \text{À}_{2n}, \text{ то } y = B_2,$$

...

$$\text{Пk : якщо } \delta_1 \text{ існує } \text{À}_{k1} \text{ та } \ldots \delta_n \text{ існує } \text{À}_{kn}, \text{ то } y = B_k,$$

де δ_1 та y - нечіткі вхідні змінні і змінні виведення, відповідно ДФ і ЗБ, а À_{ij} і B_i, $i = \overline{1,k},\ j = \overline{1,n}$ - функції приналежності.

Досвід експертів представляється масивами експертних оцінок, на базі яких формуються системи нечітких предикатних правил для класифікації ДФ $Y = \{Y_1, Y_2, Y_3, ..., Y_n\}$ та ЗБ $Z = \{Z_1, Z_2, Z_3, ..., Z_k\}$. Системи нечітких предикатних правил для подальшої адаптації та аналізу представляються у вигляді нечітких чисел. Таким чином, визначення коефіцієнтів небезпеки ДФ у вигляді чітких значень засноване на аналітичних співвідношеннях, що пов'язують ці коефіцієнти з показниками цінності ресурсів ІС. При визначенні коефіцієнтів небезпеки ДФ у вигляді нечітких величин необхідно проводити експертний аналіз небезпеки ДФ. Такий підхід може виявитися найбільш адекватним реальній небезпеці ДФ, якщо аналіз здійснюється висококваліфікованими фахівцями. Як правило, різні експерти по-різному оцінюють значення параметра і часто важко задати конкретне число, оскільки існує багато чинників, що впливають на оцінювані величини і мають імовірнісну природу. Для подібних випадків коефіцієнти небезпеки [7] задаються у вигляді нечітких чисел, здатних набувати своїх значень з певного заданого інтервалу з різними значеннями функцій приналежності. Знаючи нечіткі значення і функції приналежності коефіцієнтів небезпеки ДФ, можна з врахуванням імовірності реалізації ДФ по правилах теорії нечітких множин розрахувати нечіткі значення міри захищеності ІС від комплексу ДФ.

Рішення про розширення класифікацій атак та механізмів захисту приймається відповідно до системи оцінок достовірності нейтралізації загроз в розрізі окремих ЗБ. Результати експертних оцінок представляють у вигляді матриці

де $Z = \{Z_1, Z_2, Z_3, ..., Z_k\}$ – множина ЗБ, K – кількість засобів, із заданими значеннями коефіцієнтів ефективності захисту $e_{nk}, k = \overline{1,K}$ у вигляді нечітких чисел. У випадку розширення системи нечітких правил формується опис нового відсутнього ЗБ.

$$\begin{array}{c} Z_1 \\ Z_2 \\ \dots \\ Z_k \\ \dots. \\ Z_K \end{array} \begin{pmatrix} \alpha(e_{11}) & \alpha(e_{12}) & \dots & \alpha(e_{1n}) & \dots & \alpha(e_{1N}) \\ \alpha(e_{21}) & \alpha(e_{22}) & \dots & \alpha(e_{1n}) & \dots & \alpha(e_{2N}) \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \alpha(e_{к1}) & \alpha(e_{к1}) & \dots & \alpha(e_{kn}) & \dots & \alpha(e_{kN}) \\ .. & \dots & \dots & \dots & \dots & \dots \\ \alpha(e_{K1}) & \alpha(e_{K1}) & \dots & \alpha(e_{Kn}) & \dots & \alpha(e_{KN}) \end{pmatrix},$$

Далі для вихідних масивів експертних оцінок проводять розрахунок показників захищеності ІС, які використовуються методикою оцінки захищеності ІС для аналізу і корекції, як масивів експертних оцінок та систем нечітких предикатних правил [8].

На п‘ятому етапі вдбувається процес адаптації, пов'язаний з вирішенням завдань класифікації, що призводять до розширення інформаційного поля відомих ДФ. Зміна переліку відомих ДФ у відповідній модифікації інформаційного поля життєвого досвіду, реалізованого у вигляді спеціалізованих структур нечітких НС, які, у свою чергу, описуються системами нечітких предикатних правил [8]. Процес адаптації також пов'язаний з навчанням нечітких НС, що адекватно видозмінює систему нечітких предикатних правил, ставить у відповідність відомим ДФ засоби безпеки ІС.

Наступний етап - оцінка захищеності ІС, яка координує взаємозв'язок ДФ та ЗБ у вигляді систем нечітких предикатних правил, інструментальних засобів розрахунку показників захищеності ІС. Оцінка захищеності ІС - процес встановлення відповідності між результатом захисту і поставленою метою. Формується експертна оцінка достовірності нейтралізації відомих ДФ відомими ЗБ і потенційного збитку, виходячи з досвіду експертів ІБ. Збиток від реалізації ДФ в ІС слід оцінювати у відносних величинах. Розрахунок потенційного збитку проводиться за певний проміжок часу з урахуванням частоти активації ДФ [6]. Оцінка захищеності ІС проводиться на основі порівняння значення показника захищеності з нормативним значенням і на основі порівняння показників захищеності інформації без вживання і в умовах вживання ефективного комплексу ЗБ.

Висновки. Таким чином, використання адаптивного методу захисту ІС дозволяє контролювати практично усі ДФ, класифікувати раніше невідомі ДФ і своєчасно реагувати на них високоефективним способом, що дозволяє не лише усунути вразливості, які можуть привести до реалізації ДФ, але і проаналізувати умови, що призводять до їх появи. Запропонована методика базується на основних властивостях нечітких систем, пов'язаних з адаптивністю, навчанням, можливістю подання досвіду фахівців інформаційної безпеки (ІБ) у вигляді системи нечітких правил, доступних для аналізу. За допомогою методики побудови системи захисту ІС на основі моделі адаптивного захисту зменшується кількість зловживань в ІС, підвищується обізнаність користувачів про події в системі. В цілому запропонована методика дозволяє оцінити або переоцінити рівень захищеності інформаційної системи, а також надати рекомендації з підвищення безпеки ІС, знизити потенційні ризики.

Список літературних джерел:

8. Суханов А.В. Представление знаний в адаптивных средствах мониторинга ИС / *А.В Суханов., А.А. Павлютенков* // Защита информации. Инсайд – №4. – 2008. – С.64 – 68.

9. Корченко А.Г. Построение систем защиты информации на нечетких множествах. / *А.Г. Корченко* – К.:«МК-Пресс», 2006.– 316

10. Корченко А.Г. Методологія синтезу механізмів захисту інформаційних ресурсів / *А.Г. Корченко, Є.В. Паціра, М.В. Захарова* // Защита информации: Сборник научных трудов.- К.: НАУ, 2008. – С.99-102.

11. Столингс В. Криптография и защита сетей. Принципы и практика / *Столингс В.* – М.: Вильямс, 2-е изд., 2001. – 460 с.

12. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. / *В.В. Домарев* — К.: ООО «ТИД «ДС», 2001. — 688 с.

13. Стасюк О.І. Оцінка потенційного збитку КС при впливі загроз / *О.І. Стасюк, М.В. Захарова, А.О. Корченко* // Матеріали ІІ Міжнародної науково-практичної конференції «Проблемы экономики и управления на железнодорожном транспорте». – К .:КУЭТТ, том 2, 2007. – С.135-136.

14. Бабак В.П. Інформаційна безпека та сучасні мережеві технології. Англ.-укр.-рос. слов. термінів / *В.П. Бабак, А.Г. Корченко*. – К.: НАУ, 2003.– 670 с.

15. Нестерук Ф.., Адаптивные средства обеспечения безопасности информационных систем. / *Ф.Г. Нестерук., А.В. Суханов, Л.Г. Нестерук, Г.Ф. Нестерук.* Под ред. Л. Г. Осовецкого. СПб.: Изд-во Политехнического университета, 2008. – 626 с.