УДК 004.896

Ю.О. Дрейс, викл., аспір.
Л.В. Коваль, студ.
Житомирський військовий інститут ім. С.П. Корольова
Національного авіаційного університету

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ПРОЦЕСУ УПРАВЛІННЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІЙ СИСТЕМІ

(Представлено д.т.н., проф. Корченком О.Г.)

Проведено розробку системи підтримки прийняття рішень процесу управління захисту інформації (ЗІ) в інформаційно-телекомунікаційній системі на основі експертного оцінювання використаних методів та засобів ЗІ відносно деякого часу для надання рекомендацій щодо контролю, управління та підвищення ефективності цього процесу.

Постановка проблеми. Тенденція щодо підвищення кількості атак на інформаційні ресурси залишає актуальним питання захисту інформації (ЗІ), що обробляється в інформаційно-телекомунікаційних системах (ІТС), особливо такої, як інформація з обмеженим доступом (ІзОД). Ефективне забезпечення захисту обробки ІзОД в ІТС можливе лише із застосуванням комплексної системи захисту інформації (КСЗІ), що складає взаємопов'язану сукупність організаційно-правових, інженерно-технічних та програмно-апаратних заходів, засобів та методів ЗІ [1, 2].

Аналіз останніх досліджень та публікацій. У [3–5] розглянуто питання створення і застосування систем підтримки прийняття рішень (СППР) як інформаційних систем нового покоління. Стисло проаналізовано історію їх розвитку, призначення та чинники сприяння поширенню. Подано опис найвідоміших СППР та розгорнутий аналіз їх розвитку і застосування. У [6] описано методи та засоби забезпечення захисту інформації, основні положення, згідно з якими будуються та функціонують ІТС. Але й вони не розкривають питання оцінки рівня захищеності системи в певний час, залежно від рівня, на якому виконуються всі механізми ЗІ.

Метою статті є програмна реалізація системи підтримки прийняття рішень процесу управління захисту інформації в інформаційно-телекомунікаційній системі.

Викладення основного матеріалу. Термін «процес управління» характеризується як перебіг певного явища, послідовної зміни станів, етапів, стадій розвитку й сукупності послідовних дій для досягнення результату. У процесі управління діють і взаємодіють елементи системи управління, тому він означає постійне виникнення якісно нових ознак у системі управління. Отже, *процес управління* – це діяльність об'єднаних у певну структуру суб'єктів та об'єктів управління, спрямована на досягнення поставлених цілей управління шляхом реалізації певних функцій та застосування відповідних методів і принципів управління.

Система підтримки прийняття рішень (СППР) (DSS – Decision Support Systems) – це інформаційні системи, максимально пристосовані до виконання завдань повсякденної управлінської діяльності та є інструментом, що допомагає приймати обґрунтовані та ефективні управлінські рішення особі, що приймає їх (ОПР). Метою СППР є підвищення ефективності прийняття рішень за рахунок автоматичного аналізу великих обсягів інформації, розв'язання неструктурованих і слабкоструктурованих багатокритеріальних задач у режимі реального часу. Процес прийняття рішення складається з декількох основних етапів. За ступенем деталізації розглядають послідовність етапів, їх зміст залежить здебільшого від характеру проблеми, що розв'язується з такою послідовністю дій [2]: виявлення проблемної ситуації та постановка задачі, прийняття рішення; формулювання поняття якості рішення та його структуризація до рівня критеріїв; описання характеристик зовнішнього середовища, прогнозування можливих результатів дій із подальшим виявленням або конструюванням альтернативних варіантів рішень; оцінювання якості варіантів рішень, порівняння їх між собою та вибір одного чи декількох найвідповідніших меті; аналіз рішень, опрацювання плану реалізації та впровадження рішення.

Комплексна система захисту інформації (КСЗІ) – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів ЗІ [1, 6].

Захист інформації (ЗІ) – сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації. *ЗІ в системі* – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі [1, 2].

Існуючі методи та засоби ЗІ в ІТС можна розділити на три основні групи (рис. 1) [6].

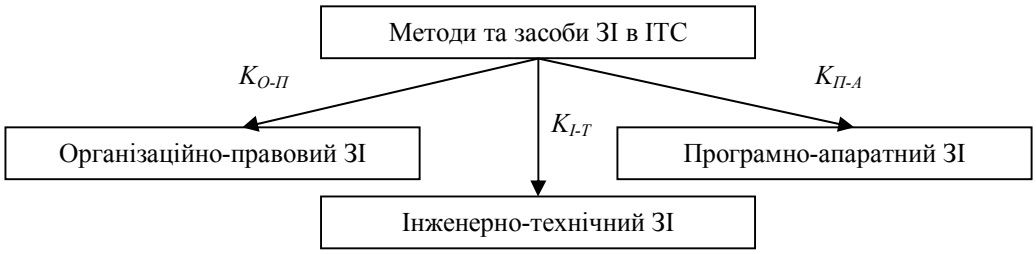

Рис. 1. Методи та засоби ЗІ в ІТС

Коефіцієнти $K_{О-П}$, $K_{І-Т}$, $K_{П-А}$ формуються по кожному з методів ЗІ в ІТС (рис. 2):
– *організаційно-правовий метод ЗІ* ($K_{О-П}$) містить заходи, що проводяться при створенні і експлуатації ІТС, будівництві або ремонті приміщень її розміщення; проектуванні КСЗІ, монтажі та налагодженні технічних і програмних засобів; випробуваннях та перевірці працездатності [3] та ін.: нормативно-правове забезпечення ЗІ (k_1); концепція безпеки ІТС (k_2); служба захисту інформації (k_3); регламентація доступу до ресурсів ІТС (k_4); план модернізації компонентів ІТС (k_5):

$$K_{Î-Ï} = (k_1, k_2, k_3, k_4, k_5); \quad (1)$$

– *інженерно-технічний метод ЗІ* ($K_{І-Т}$) використовує засоби, що передбачають використання технічних пристроїв (або їх комплексу) для реалізації захисної функції фізичних об'єктів, механічних, електричних і електронних пристроїв, елементів конструкцій будівель, засобів пожежогасіння [3] та ін.: охоронні системи ЗІ (k_6); контрольно-пропускний режим доступу (k_7); системи технічного ЗІ (k_8); засоби технічного контролю (k_9); засоби відновлення компонентів ІТС (k_{10}):

$$K_{IIIIIII} = (k_6, k_7, k_8, k_9, k_{10}); \quad (2)$$

– *програмно-апаратний метод ЗІ* ($K_{П-А}$) включає засоби використання електронних та електронно-механічних пристроїв, що входять до складу технічних засобів ІТС і виконують (самостійно або в єдиному комплексі з програмними засобами) деякі функції забезпечення інформаційної безпеки, а саме: резервне копіювання (k_{11}); встановлення міжмережевих екранів (k_{12}); шифрування (розшифрування) інформації (k_{13}); ідентифікація, аутентифікація, авторизація (k_{14}); антивірусний захист інформації (k_{15}):

$$K_{П-А} = (k_{11}, k_{12}, k_{13}, k_{14}, k_{15}). \quad (3)$$

Інформаційно-телекомунікаційна система (ІТС) – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле. Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації [1, 2].

Відповідальність за забезпечення ЗІ в системі покладається на власника системи. Власник системи, в якій обробляється інформація, що є власністю держави, або ІзОД, вимога щодо захисту якої встановлена законом, утворює службу ЗІ або призначає осіб, на яких покладається забезпечення ЗІ та контролю за ним [1].

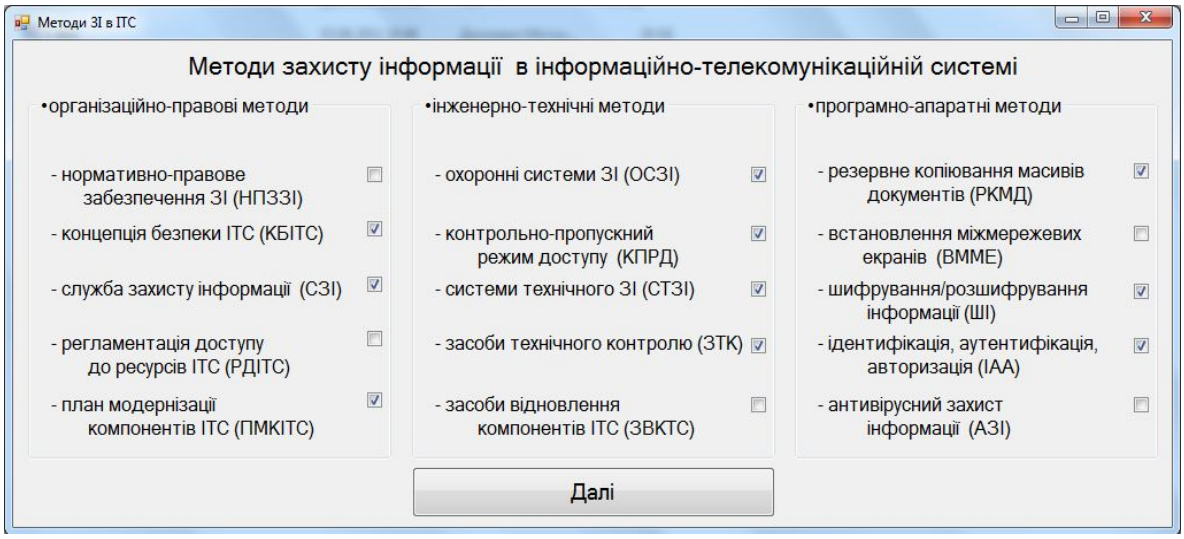

Рис. 2. Інтерфейс програмної реалізації СППР процесу управління засобами ЗІ в ІТС

Компоненти СППР процесу управління ЗІ в ІТС взаємодіють відповідно до моделі (рис. 3).

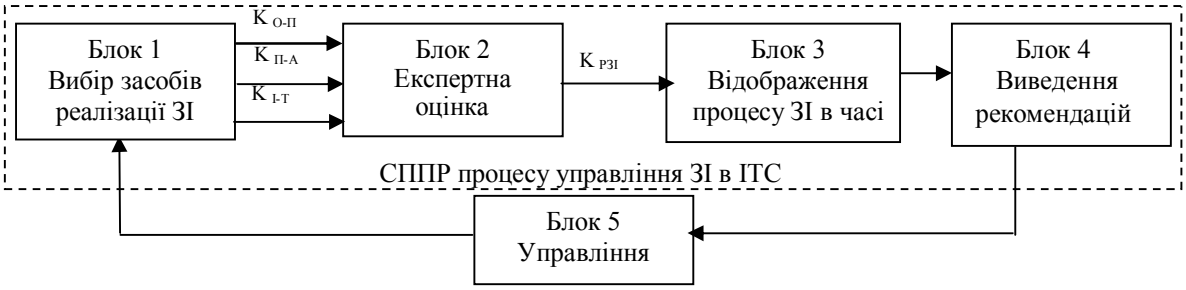

Рис. 3. Модель взаємодії компонентів СППР процесу управління ЗІ в ІТС

Управління ЗІ є складною сукупністю взаємопов'язаних процесів безперервного створення, вдосконалення й контролю над системою механізмів захисту, що використовуються в ІТС (рис. 4).

При цьому важливою є та обставина, що підсистема управління ЗІ є сукупністю однорідних у функціональному відношенні заходів, регулярно здійснюваних в ІТС з метою створення, підтримки й забезпечення умов, об'єктивно необхідних для забезпечення надійного ЗІ необхідного рівня. Узагальнений коефіцієнт рівня ЗІ в ІТС $K_{РЗІ}$ представлятиме масив елементів (4) та за певний місяць розраховується за формулою (5), а за квартал чи рік – за формулою (6) [3–5]:

$$K_{ÐÇ} = \begin{pmatrix} K_{Î\text{-}Ï} \\ . \\ K_{²\text{-}Ò} \\ . \\ K_{Ï\text{-}À} \end{pmatrix} = \begin{pmatrix} \mu(k_1) & . & . & . & \mu(k_{1t}) \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ \mu(k_i) & . & . & . & \mu(k_{it}) \end{pmatrix}, \quad (4)$$

$$K_{РЗІ} = \frac{\sum_{1}^{n} \mu(k_i)}{n}; \quad (5)$$

$$K_{ЗІ} = \sum_{1}^{t} K_{РЗІ}, \quad (6)$$

де $\mu(k)$ – експертна оцінка кожного засобу реалізації ЗІ в ІТС (рис. 5); i – кількість засобів, що використовуються для ЗІ в ІТС; t – кількість місяців, на протязі яких проводиться оцінка ЗІ в ІТС (для кварталу t = 1...4 (рис. 6), року t = 1...12 (рис. 7)); n – кількість експертних оцінок засобів ЗІ в ІТС.

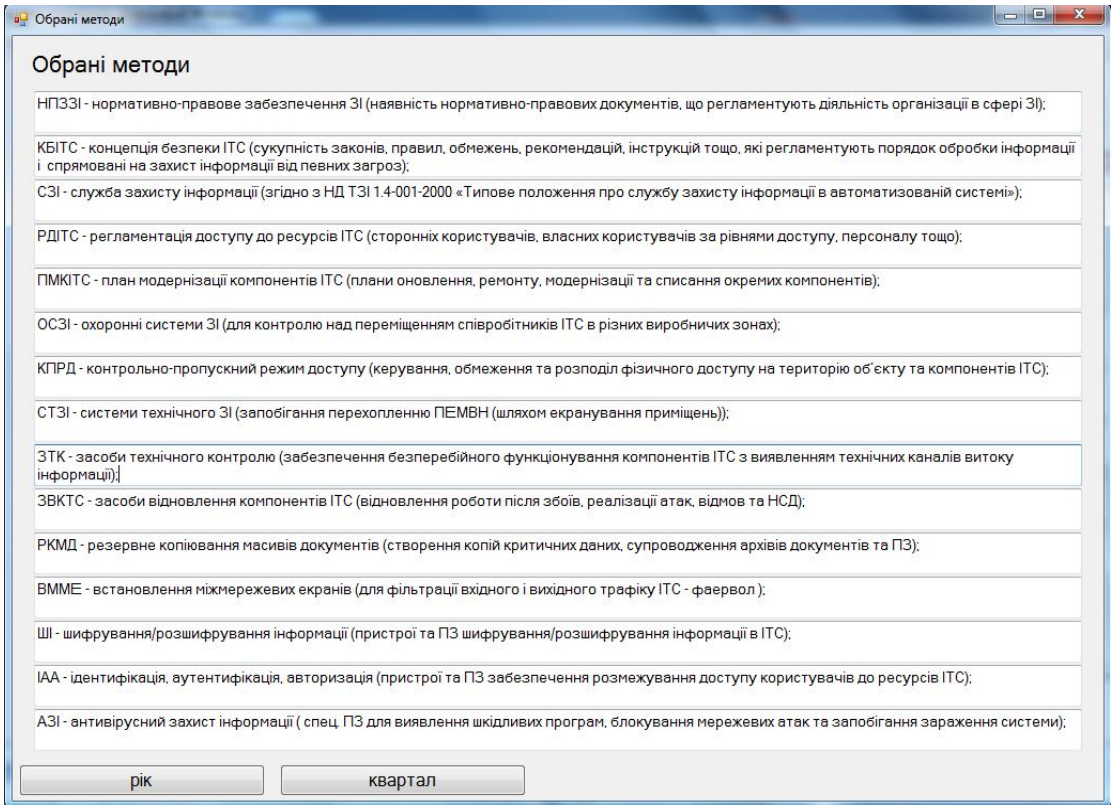

Рис. 4. Коментар та реалізація обраних методів ЗІ в ІТС

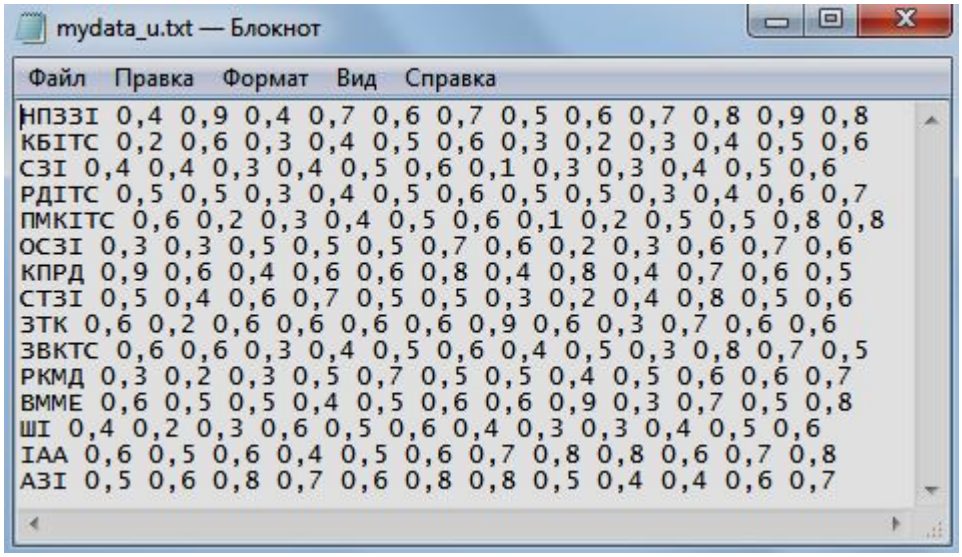

Рис. 5. Експертне оцінювання кожного засобу реалізації ЗІ в ІТС (за рік)

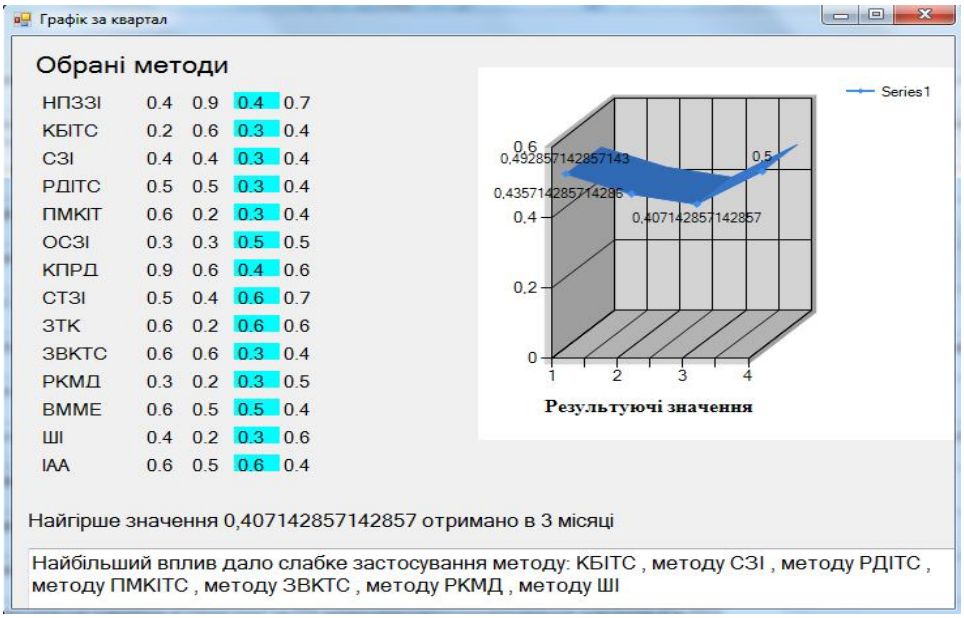

Рис. 6. Експертне оцінювання використаних методів ЗІ в ІТС за квартал

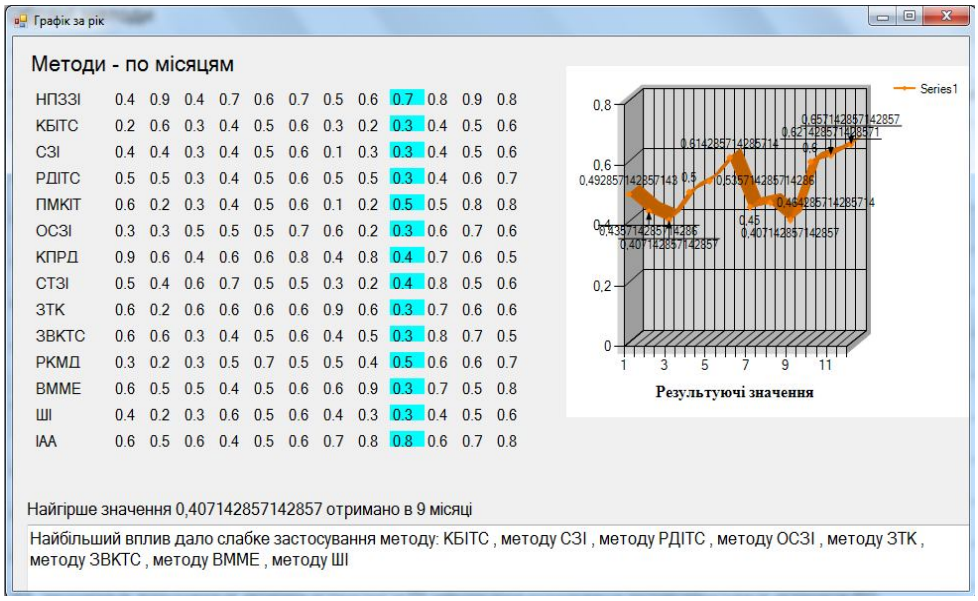

Рис. 7. Експертне оцінювання використаних методів ЗІ в ІТС за рік

Висновок. Розроблена програмна реалізація СППР процесу управління ЗІ в ІТС, що надає рекомендації на основі експертного оцінювання використаних засобів та методів ЗІ за певний період часу з метою постійного контролю, оперативного реагування та прийняття ОПР ефективного рішення як процесу управління ЗІ в системі.

ЛІТЕРАТУРА:

1. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 / Верховна Рада України [Електронний ресурс]. – Режим доступу : www.rada.gov.ua.
2. Нормативно-правове забезпечення інформаційної безпеки : збірник нормативно-правових документів / уклад. *О.Г. Корченко, Ю.О. Дрейс*. – Житомир : ЖВІ НАУ, 2010. – 280 с.
3. *Катренко А.В.* Теорія прийняття рішень / *А.В. Катренко, В.В. Пасічник, В.П. Пасько.* – К. : Видавнича група BHV, 2009. – 448 с.

4. *Гнатієнко Г.М.* Експертні технології прийняття рішень : монографія / *Г.М. Гнатієнко, В.Є. Снитюк*. – К. : Маклаут, 2008. – 444 с.
5. *Ситник В.Ф.* Системи підтримки прийняття рішень : навч. посібник / *В.Ф. Ситник*. – К. : КНЕУ, 2004. – 614 с.
6. *Хорев П.Б.* Методы и средства защиты информации в компьютерных системах / *П.Б. Хорев*. – М. : Академия, 2005. – 256 с.

ДРЕЙС Юрій Олександрович – викладач кафедри безпеки інформаційних і комунікаційних систем Житомирського військового інституту ім. С.П. Корольова Національного авіаційного університету, аспірант кафедри безпеки інформаційних технологій Інституту інформаційно-діагностичних систем Національного авіаційного університету.

Наукові інтереси:

– системи експертного оцінювання інформації з обмеженим доступом.

КОВАЛЬ Любов Володимирівна – студентка кафедри безпеки інформаційних і комунікаційних систем Житомирського військового інституту ім. С.П. Корольова Національного авіаційного університету.

Наукові інтереси:

– системи підтримки прийняття рішень у сфері захисту інформації.

Подано 04.11.2011