Корченко Олександр Григорович, доктор технічних наук, професор, завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: icaocentre@nau.edu.ua
Корченко Александр Григорьевич, доктор технических наук, профессор, заведующий кафедрой безопасности информационных технологий Национального авиационного университета.
Korchenko Alexander, Professor, Doctor of Science in Eng., Head of Academic Department of IT-Security, National Aviation University.

Хорошко Володимир Олексійович, доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: Professor_va@ukr.net
Хорошко Владимир Алексеевич, доктор технических наук, профессор, профессор кафедры безопасности информационных технологий Национального авиационного университета.
Horoshko Volodymyr, Professor, Doctor of Science in Eng., Professor of Academic Department of IT-Security, National Aviation University.

Кудінов Вадим Анатолійович, кандидат фізико-математичних наук, доцент, начальник кафедри інформаційних технологій Національної академії внутрішніх справ України.
E-mail: icaocentre@nau.edu.ua
Кудинов Вадим Анатольевич, кандидат физико-математических наук, доцент, начальник кафедры информационных технологий Национальной академии внутренних дел Украины.
Kudinov Vadym, PhD in physics, associate professor, head of Department of Information technology of the National Academy of Internal Affairs Ukraine.

УДК 004.891:65.012.8(045)

МЕТОДОЛОГІЯ СИНТЕЗУ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ОЦІНЮВАННЯ ШКОДИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ У СФЕРІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ

Олександр Корченко, Максим Луцький, Марія Захарова, Юрій Дрейс

Анотація. *Віднесення відомостей до державної таємниці проводиться державним експертом з питань таємниць шляхом встановлення, обґрунтування та визначення величини можливої шкоди національній безпеці держави у разі їх розголошення для прийняття рішення щодо ступеня їх секретності. Існуючі засоби розрахунку такої шкоди в переважній більшості базуються на отримання умовної (бальної) оцінки її прогнозованої величини. У роботі представлено методологію синтезу системи аналізу і оцінки величини можливої шкоди національній безпеці держави, яка дозволяє на основі моделі інтегрованого представлення параметрів шкоди, отриманих існуючими засоби аналізу у сфері охорони державної таємниці, оцінювати шкоду як в умовних (бальних) одиницях, так і в вартісній (грошовій) величині збитку. Основана вона на розроблених методах: аналізу і оцінки шкоди національній безпеці у сфері охорони державної таємниці, оцінювання важливості відомостей за визначеними сферами державної таємниці, визначення рівня компетентності членів експертної комісії при державних експертах з питань таємниць. Окрім цього, методологія дає можливість відображати результати як в якісній, так і в кількісній формі, наприклад, з використанням лінгвістичних змінних, що часто вживаються для опису складних систем. Програмна реалізація системи з інтегрованою базою даних існуючих засобів дає змогу провести аналіз і оцінку величини можливої шкоди національній безпеці держави з додатковими можливостями автоматизованого формування звіту її результатів.*

Ключові слова: *державна таємниця; оцінка шкоди; методологія системи аналізу і оцінки величини можливої шкоди національній безпеці держави; охорона державної таємниці; параметри шкоди.*

Відомо, що методологічний базис є найважливішим компонентом теорії захисту інформації (ЗІ) [1], який складається з сукупності методів і моделей, необхідних і достатніх для досліджень проблеми ЗІ і вирішення практичних завдань відповідного призначення. В зв'язку з цим на особливу увагу заслуговують завдання аналізу і оцінки величини можливої шкоди (АОШ) національній безпеці держави у сфері охорони державної таємниці (ОДТ) [2]. Проте, при практичному використанні існуючих засобів АОШ [3-5] члени експертної комісії при державних експертах з питань таємниць (далі – ДЕТ) не завжди можуть чітко детермінувати оціночні параметри, оскільки їх часто виражають в якісній формі. Тому особливий інтерес представляють системи [6], які до-

зволяють ефективно проводити АОШ (з врахуванням якісної і кількісної оцінки) в нечіткому слабоформалізованому середовищі. У зв'язку з цим, **метою даної роботи є** розробка відповідної методології синтезу систем АОШ національній безпеці держави у сфері ОДТ.

Використовуючи відомий підхід [1] до побудови методологій (синтезу систем оцінки рівня безпеки інформації в комп'ютерних системах, оцінки систем технічного ЗІ на програмно-керованих автоматичних телефонних станцій (АТС) і вибору найкращого варіанту АТС на базі інтегрованої оцінки рівня гарантій захищеності інформаційних ресурсів), а також логіко-лінгвістичний підхід, пропонується (на підставі розроблених методів [7-9] і моделей засобів АОШ [10] методологія синтезу системи АОШ національній безпеці держави у сфері ОДТ (рис. 1). Вона містить десять етапів: 1) кваліфікація порушення; 2-4) ідентифікація атак, загроз і відомостей, що становлять ДТ; 5) визначення ідентифікуючих та оціночних параметрів; 6) оцінювання важливості відомостей; 7) визначення рівня компетентності; 8) оцінювання основних коефіцієнтів; 9) інтерпретація тяжкого наслідку; 10) оцінка величини сукупної шкоди. Тепер перейдемо до детального опису кожного з етапів.

1. Класифікація порушення. На першому етапі для ідентифікації порушення (подій) у сфері ОДТ необхідно використати звіт про стан забезпечення даної сфери [5] в РСО суб'єкта режимо-секретної діяльності (СРСД). За результатами заповнення розділу 6 "Відомості про виявлені факти втрати МНСІ, розголошення відомостей, що становлять ДТ" *порушення* (***E***) кваліфікуються за наявності у звітному періоді фактів розголошення відомостей, що становлять ДТ (e_1), або втрати її матеріальних носіїв (e_2). Тому множину можливих порушень (подій) $\mathrm{E}=\{\mathrm{e_j}\}, \mathrm{j}=\overline{1,1}$ у сфері ОДТ до інформаційних ресурсів (ІР) держави при j=2 виражено як: $\mathrm{E}=\{\mathrm{e_1},\mathrm{e_2}\}$.

2. Ідентифікація можливих атак. На наступних етапах проводимо ідентифікацію можливих *атак* (***A***) зі визначеного за описом певних способів їх реалізації вкупі з характеристиками ймовірних наслідків реалізації переліку подій-загроз [6], що призводять до появи E у сфері ОДТ, при j=6 як: a_1 = "несанкціоноване отримання СІ зацікавленими особами у результаті порушення правил секретного діловодства і порядку допуску та доступу до МНСІ"; a_2 = "отримання СІ іноземними спецслужбами у результаті агентурного проникнення (шпигунство)"; a_3 = "розголошення відомостей, що становлять ДТ"; a_4 = "втрата МНСІ"; a_5 = "перехоплення СІ, яка передається за допомогою засобів телекомунікації (інформаційно-телекомунікаційних систем (ІТС), автоматизованих систем (АС) тощо), а також через технічні канали витоку інформації, в тому числі канали побічного електромагнітного випромінювання і наводок (ПЕМВН), зокрема в мережах електроживлення технічних засобів обробки і збереження інформації"; a_6 = "знищення або модифікація СІ деструктивними силовими впливами". Узагальнено множина існуючих атак A приймає наступний вигляд: $\mathrm{A}=\{\mathrm{a_j}\}, \mathrm{j}=\overline{1,6}$.

3. Ідентифікація загроз. Далі проводиться ідентифікація основних *загроз* (***T***), направлених на запобігання порушення (П) властивостей захищеності інформації (конфіденційності (К), цілісності (Ц), доступності (Д)), що визначають вимоги до функціонування складу комплексу засобів захисту (КЗЗ) АС для обробки інформації однієї або кількох категорій конфіденційності в РСО СРСД, де організовано та забезпечено режим секретності (РС) з метою ефективного функціонування системи ОДТ (СОДТ). Множина таких загроз T приймає вигляд: $\mathrm{T}=\{\mathrm{t_e}\}, \mathrm{e}=\overline{1,7}$.

4. Ідентифікація відомостей, що становлять ДТ. Даний етап проводиться на основі розділу 6 звіту [5], де конкретизуються у вигляді номера статті ЗВДТ [4] та їх СС (наприклад, 1.11.5 / Таємно) *відомості* (***x***$_i$) відносно яких відбулися порушення (події) e_1 чи e_2. Таку множину відомостей визначимо як $\mathrm{x_i}\in \mathbf{PV}_{\mathrm{N.i.j}}$, де PV – короткий зміст цих відомостей, N – сфера ДТ, що виражена у вигляді символьної змінної як $\mathrm{N}\in\{\mathrm{N_1},\mathrm{N_2},...,\mathrm{N_v}\}$ (v – кількість ідентифікаторів сфер), при v=4 наступні: N_1 = "оборони"; N_2= "економіки, науки і техніки"; N_3= "зовнішніх відносин"; N_4= "державної безпеки і охорони правопорядку", а *i.j* – ідентифікатори статті ЗВДТ за сферою N_v.

5. Визначення ідентифікуючих та оціночних параметрів. На цьому етапі для створення можливості експертній комісії з питань таємниць (далі – ЕКТ) у процесі оцінювання використовувати ширший спектр необхідних величин пропонується використовувати модель інтегрованого представлення параметрів шкоди (ІППШ), яка отримана на основі розробленого методу [7]. Отже, для цього необхідно скористатися повним набором ідентифікуючих та оціночних компонент, які можуть використовуватися при АОШ.

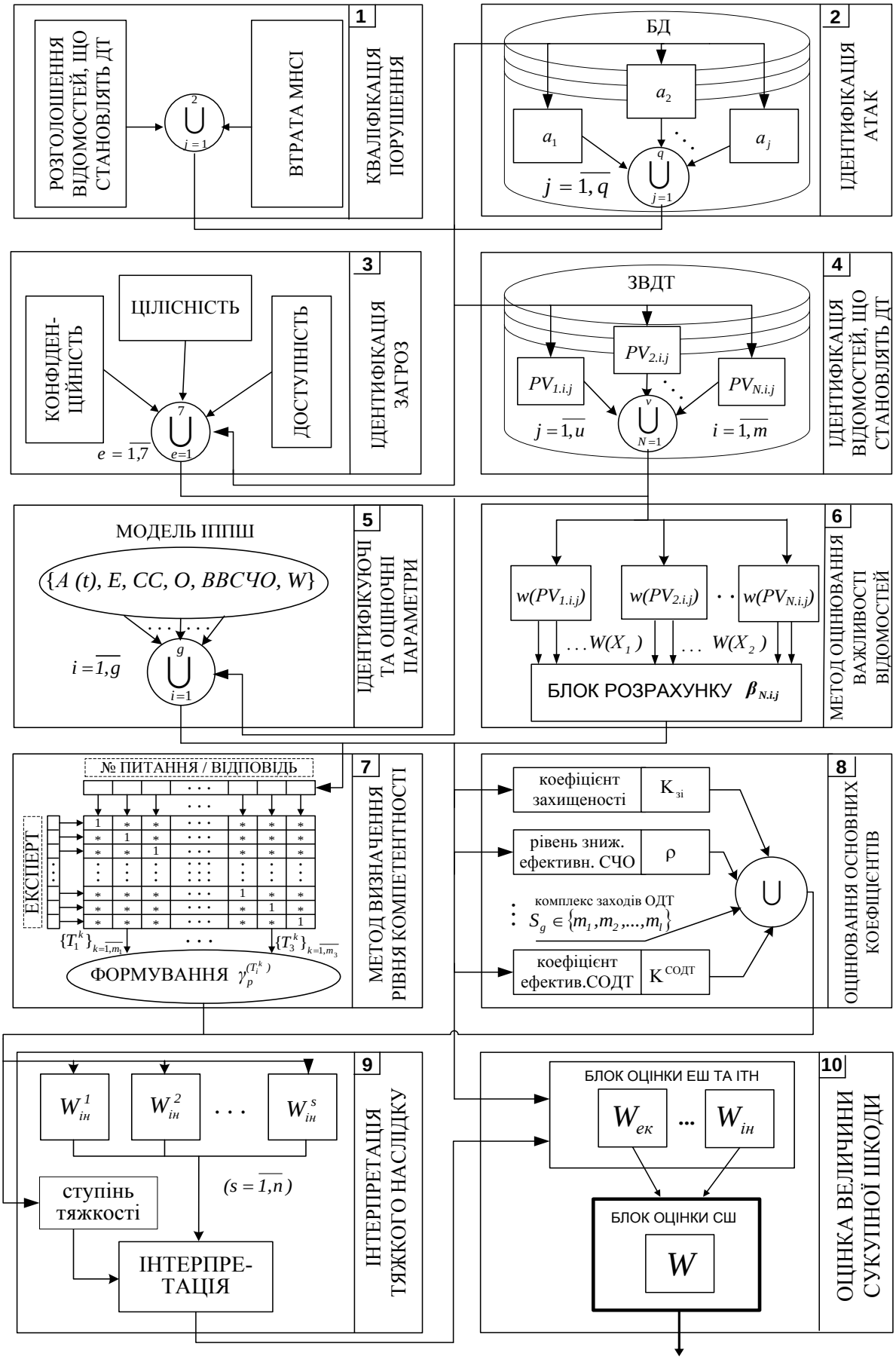


Рис. 1. Схема відображення методології синтезу системи АОШ національній безпеці держави у сфері ОДТ

Пропонується представити параметри можливої шкоди у вигляді десятикомпонентного кортежу: ***<A(t), E,*** $\mathbf{x_i}$***, CC (β), Кзі (Ксодт), S(m), ϱ, ВВСЧО, Кс, W (Wін,Wек)>***, де ***A*** – атака, що характеризує загрозу ***t*** *(конф., ціліс., доступ.);* ***E*** – подія (розголошення ДТ чи втрата МНСІ); $\mathbf{x_i}$ – *і*-ті відомості, що становлять ДТ; ***CC*** – ступінь секретності (Т, ЦТ, ОВ), що визначає їх важливість (***β***) у сферах ДТ; ***Кзі*** – коефіцієнт захищеності інформації, що характеризує ефективність функціонування СОДТ(***Ксодт****);* ***S*** – перелік завдань РСО, що містить комплекс ***m*** заходів та способів ОДТ; ***ϱ*** – рівень зниження ефективності складової частини об'єкта (СЧО); ***ВВСЧО*** – відносна вартість СЧО; ***Кс*** – коефіцієнт морального старіння інформації; ***W*** – показник сукупної шкоди (СШ) (як сума економічної шкоди (***Wек***) та від іншого тяжкого наслідку (***Wін***)). Результатом проходження даного етапу є формування набору оцінних параметрів, які використовуватимуться для АОШ національній безпеці держави у сфері ОДТ на етапах 8-10.

6. Оцінювання важливості відомостей. На даному етапі проводиться оцінювання *важливості* відомостей, що становлять ДТ за існуючими сферами *N* ЗВДТ [8]. Для цього визначається загальний перелік відомостей (***X***), що становлять ДТ у сфері N_v як $X=\{PV_{1.i.j},PV_{2.i,j},...,PV_{N.i.j}\}, i=\overline{1,m},\ j=\overline{1,n},\ N=\overline{1,v},\ i\neq j$ та окремо відомості $x_i \in PV_{N.i.j}$, що оцінюються. Далі, внаслідок механічної заміни СС на середнє інтервальне значення прогнозованої СШ за [3] як величини "питомої ваги" розраховується коефіцієнт важливості відомостей $\boldsymbol{x}_i$ як відношення їх "питомої ваги" $\boldsymbol{w}(PV_{N.i.j})$ до показника сумарної величини прогнозованої СШ переліку відомостей ***X*** (сумарної "питомої ваги" ***W***(*X*)), що становлять ДТ за сферою N_v і виражається як $\beta_{N.i.j}=w(PV_{N.i.j})/W(X_N)$. За результати цього етапу можна провести порівняльний аналіз важливості окремо як статей ЗВДТ за існуючими сферами ДТ.

7. Визначення рівня компетентності. Цим етапом проводиться визначення рівня компетентності членів ЕКТ при ДЕТ за допомогою розробленого інтегрованого методу [9] для сфери ОДТ. В основу методу, на відміну від відомих, покладено застосування набору оціночних параметрів моделі ІПШІ у комбінованих видах суджень експерта відповіді якого формують трикутні матриці і після нормування їх елементів проводиться визначення рівня компетентності за існуючою формулою $\gamma_p=\sum\limits_{\substack{i,j=1\\ i>j\\ (j=p)\vee(i=p)}}^{n} t_{ij}/\sum\limits_{p=1}^{n}\ \sum\limits_{\substack{i,j=1\\ i>j\\ (j=p)\vee(i=p)}}^{n} t_{ij}$, $p=\overline{1,n}$. Даний метод визначення рівня компетентності членів ЕКТ може застосовуватися ДЕТ під час віднесення відомостей до ДТ зі встановленням їх СС шляхом визначення та обґрунтування прогнозованої величини СШ (***W***) як суми економічної шкоди (***Wек***) та шкоди від іншого тяжкого наслідку (***Wін***).

8. Оцінювання основних коефіцієнтів. На даному етапі за допомогою існуючих засобів [3-6] та розробленого методу [7] АОШ проводиться оцінювання основних коефіцієнтів, які характеризують: а) рівень зниження ефективності використання об'єкта (СЧО) відомостей $\rho=1-\left(W(X)-w(PV_{N.i.j})\right)/W(X)$; б) ефективність фукнціонування СОДТ СРСД $K^{содт}=1-\rho$; в) захищеність інформації в РСО $K_{зі\ N}=\Upsilon\cdot P^T$, де Υ – вектор-рядок значень коефіцієнтів захищеності СІ у сфері *N* від атак (загроз), *P* – вектор-рядок значень показників ефективності ($P=\sum\limits_{g=1}^{l}P(a_j/S_g), g=\overline{1,l}$) усунення (нейтралізації) можливих атак a_j, $(.)^T$ – символ операції транспонування; г) ступінь можливого старіння відомостей $K_c=1-T_ф/T_н$, де $T_ф$ – термін дії охоронного документа в розрахунковому році *t* (наприклад, дата виявлення e_1 чи e_2 або дата інформування органу СБУ); $T_н$ – номінальний термін дії охоронного документа ("ОВ" – 30, "ЦТ" – 10, "Т" – 5 років); д) інші стани забезпечення ОДТ тощо. За результатами цього етапу проводиться обґрунтування величини фінансування заходів ОДТ для забезпечення РС та кількісний розрахунок показника ЕШ та ІТН у балах.

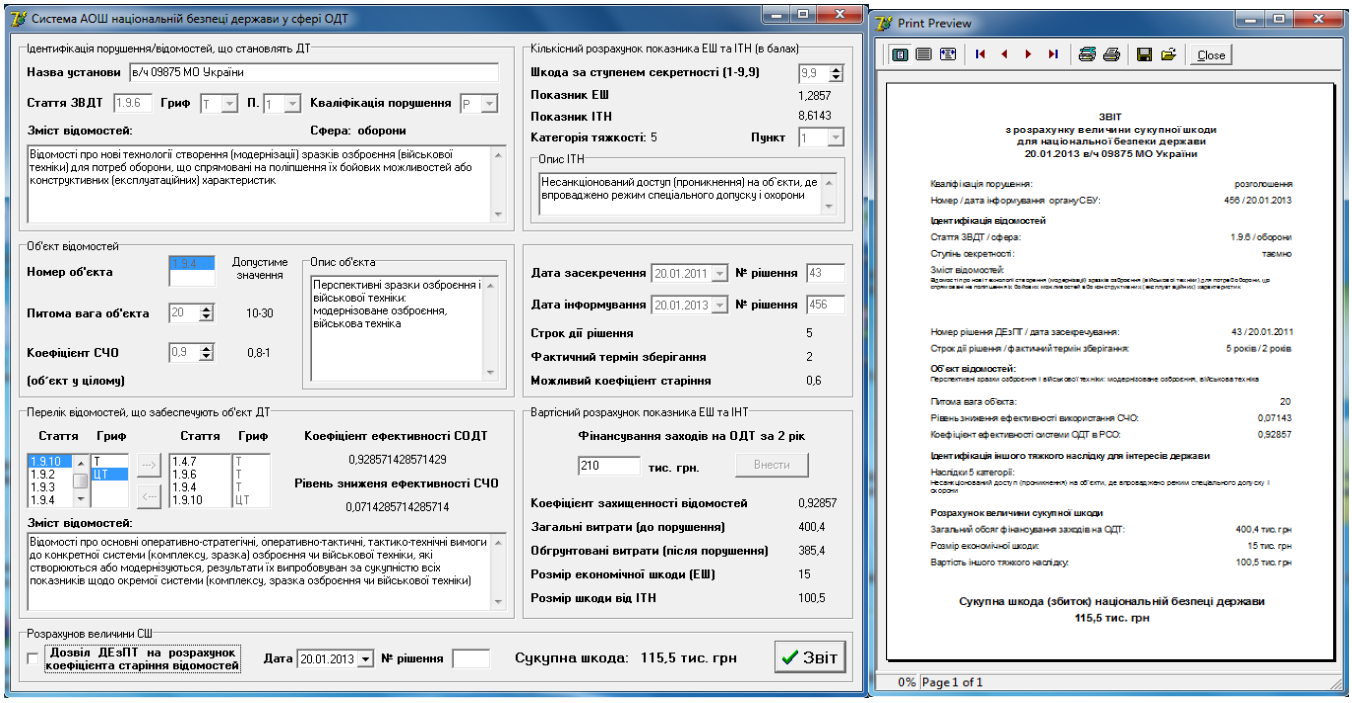
9. Інтерпретація тяжкого наслідку. На передостанньому етапі, використовуючи *перелік ІТН* [3], що містить п'ять сформованих категорій можливих наслідків за ступенем їх тяжкості, проводиться інтерпретація прогнозованої бальної величини шкоди (***Wін***) як $W_{ін}=W-W_{ек}=W_{cc_{max}}-Q\cdot k\cdot\rho$ до опису тяжкого наслідку, що мав місце. Результатами етапу є остаточна кількісна та якісна оцінка величини можливої шкоди від ІТН.

10. Оцінка величини сукупної шкоди. На останньому етапі проводиться остаточний розрахунок величини СШ (***W***), яка складається із суми загальної вартісної величини ЕШ $Ц_{W_{ек}}(t_n)$ та

ІТН $Ц_{W_{ін}}(t_n)$, $t_n = \overline{1, t_к}$ з урахуванням можливого до цих відомостей, за рішенням ДЕТ, існування закону старіння інформації, що виражається наступною узагальненою формулою:

$$Ц_W(t_n) = \sum_{t_n=1}^{t_к} (Ц_{W_{ек}}(t_n) + Ц_{W_{ін}}(t_n)) \cdot K_c,$$ де t_n – початковий рік розрахункового періоду; $t_к$ - кінцевий рік розрахункового періоду. Отримане кінцеве значення показника СШ показує вартісну (грошову) величину можливої шкоди національній безпеці держави у разі настання існуючих подій *E* у сфері ОДТ.

На підставі запропонованої методології можна будувати як програмні (рис. 2, а), так і програмно-апаратні системи, призначені для ефективного АОШ національній безпеці держави у сфері ОДТ, які використовують як вхідні дані різні набори оціночних параметрів, що дозволяє підвищити гнучкість і розширює можливості проектованих засобів АОШ, що функціонують як в детермінованому, так і в нечіткому слабоформалізованому середовищі.



а) б)

Рис. 2. Програмна реалізація системи АОШ національній безпеці держави у сфері ОДТ (а) з інтегрованими можливостями автоматизованого формування звіту (б) її результатів

Результатом програмної реалізації є автоматизоване формування звіту (рис.2, б) з розрахунку величини можливої шкоди національній безпеці держави. Отримані дані у вигляді сформованого документа можуть бути використані при формуванні експертного висновку або розробці ДЕТ критеріїв визначення шкоди, яку може бути завдано національній безпеці України у разі розголошення СІ чи втрати матеріальних носіїв такої інформації.

ВИСНОВОК. Розроблена методологія синтезу системи АОШ національній безпеці держави у сфері ОДТ, яка на основі моделі ІПШ, методу АОШ та існуючих засобів аналізу і оцінки шкоди дозволяє формалізувати процес створення програмної реалізації та інструментальних засобів з гнучкими інтегрованими можливостями використання заданих множин оброблених величин параметрів шкоди у разі розголошення відомостей, що становлять ДТ чи втрати МНСІ.

ЛІТЕРАТУРА

[1] Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / Корченко А.Г. – К. : “МК-Пресс”, 2006. – 320с. (ил. Монография).

[2] Архипов О. Є. Критерії визначення можливої шкоди національній безпеці України у разі розголошення інформації, що охороняється державою: моногр. / О.Є. Архипов, О.Є. Муратов. – К: Наук.-вид. відділ НА СБ України, 2011. – 195 с.

[3] Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня її секретності / Державний комітет України з питань державних секретів та технічного за-

хисту інформації. Наказ №22 від 09.11.1998 р. – К.: Збірка №8, 1998. – С.4–14.

[4] Про затвердження Зводу відомостей, що становлять державну таємницю / Служба безпеки України; Наказ, Звід від 12.08.2005 № 440 {редакція від 21.11.2011} // [Електронний ресурс]. – Режим доступу:http://zakon2.rada.gov.ua/laws/show/z0902-05

[5] Про затвердження форм звіту про стан забезпечення охорони державної таємниці та інструкцій щодо порядку їх заповнення та подання / Служба безпеки України; Наказ, Інструкція, Форма [...] від 28.11.2008 № 841// [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z1163-08

[6] Архипов О.Є. Оцінювання ефективності системи охорони державної таємниці: монографія / О.Є. Архипов, І.Т. Бородавко, В.П. Ворожко. – К.: Наук.-вид. відділ НА СБ України, 2007. – 63с.

[7] Корченко О.Г. Метод аналізу та оцінки величини можливої шкоди національній безпеці держави у сфері охорони державної таємниці / О.Г. Корченко, С.В. Казмірчук, Ю.О. Дрейс // Захист інформації – 2012. –№3 (56). – С.5-18.

[8] Дрейс Ю.О. Розрахунок коефіцієнтів захищеності відомостей, що становлять державну таємницю / Ю.О. Дрейс, Н.С. Вишневська, Ю.Є. Хохлачова // Захист інформації – 2010. – №3 (48). – С.10–14.

[9] Дрейс Ю.О. Визначення рівня компетентності експертів експертної комісії з питань державної таємниці / Ю.О. Дрейс, О.Г. Корченко // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: збірник наукових праць. – Житомир: ЖВІ НАУ, 2011. – Вип. №4. – С.190–196.

[10] Корченко О.Г. Модель складної орієнтованої інформаційної мережі ЗВДТ / О.Г. Корченко, О.Є. Муратов, Ю.О. Дрейс, І.О. Козлюк // Захист інформації – 2011. – №3 (52). – С.87–94.

REFERENCES

[1] Korchenko A.G. Building security systems on fuzzy sets. Theory and practical solutions / A.G. Korchenko - K.: "MK-Press", 2006, 320 P.

[2] Arkhipov O.E. Criteria of determination of possible harm national safety of Ukraine are in the case of disclosure of information which is guarded the state: monograph / O.E. Arkhipov, O.E. Muratov. - K: Research and Publications Division of the National Academy Depart. Security of Ukraine, 2011, 195 P.

[3] Guidelines state expert on secrets about the grounds for attributing information to state secret and its degree of secrecy/ State Committee of Ukraine on State Secrets and Protection of Information. Order № 22 from 09.11.1998 - K.: Collection No. 8, pp.4-14.

[4] On Approval of Summary of information constituting state secrets / Dept. Security of Ukraine Order, Code of 12.08.2005 № 440 from 21.11.2011 // [electronic resource]. Mode of access: http://zakon2.rada.gov.ua /laws/show/z0902-05

[5] On the approval of a report on the state of protection of state secrets and instructions on how to fill them and submit / Dept. Security of Ukraine, orders, instructions, forms [...] from 28.11.2008 № 841 // [electronic resource]. Mode of access: http://zakon2.rada.gov.ua/laws/show/z1163-08

[6] Arkhipov O.E. Evaluation of the effectiveness of the protection of state secrets: monograph / O.E. Arkhipov, K.: Research and Publications Division of the National Academy Depart. Security of Ukraine, 2007, 63 P.

[7] Korchenko O.G., Kazmirchuk S.V., Dreys Y.O. (2012) "The method of analysis and estimation of possible damage to national security in the protection of state secrets", Information Security, Vol. 56, No. 3, pp. 5-18.

[8] Dreys Y.O., Vishnevskaya N.S., Hohlachova Y.E. (2010) "Calculation of the coefficients security information constituting state secrets", Information Security, Vol. 48, No. 3, pp. 10-14.

[9] Dreys Y.O., Korchenko O.G. (2011) "Determining the level of competence of the expert committee of experts on state secrets" / Problems of creating, testing, use and maintenance of complex information systems: a collection of scientific papers, Zhytomyr: ZMI NAU,. Vol. 4, pp.190-196.

[10] Korchenko O.G., Muratov O.E., Dreys Y.O., Kozlyuk I.O. (2011) "Model complex oriented information network LIISS" , Information Security, Vol. 53, No. 3, pp. 87-94.

МЕТОДОЛОГИЯ СИНТЕЗА И ПРОГРАММНАЯ РЕАЛИЗАЦИЯ СИСТЕМЫ ОЦЕНИВАНИЯ УЩЕРБА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В СФЕРЕ ОХРАНЫ ГОСУДАРСТВЕННОЙ ТАЙНЫ

Отнесения сведений к государственной тайне проводится государственным экспертом по вопросам тайн путем установления, обоснование и определение величины возможного ущерба национальной безопасности государства в случае их разглашения для принятия решения о степени их секретности. Существующие средства расчета такого ущерба в подавляющем большинстве основаны на получение условной (балльной) оценки ее прогнозируемой величины. В работе представлены методология синтеза системы анализа и оценки величины возможного ущерба национальной безопасности государства, которая позволяет на основе модели интегрированного представления параметров вреда, полученных существующими средства анализа в сфере охраны государственной тайны, оценивать ущерб как в условных (бальных) единицах, так и в стоимостной (денежной) величине ущерба. Основана она на разработанных методах: анализа и оценки ущерба национальной

безопасности в сфере охраны государственной тайны, оценки важности сведений по определенным сферам государственной тайны, определение уровня компетентности членов экспертной комиссии при государственных экспертов по вопросам тайн. Кроме этого, методология дает возможность отображать результаты как в качественной, так и в количественной форме, например, с использованием лингвистических переменных, часто употребляемые для описания сложных систем. Программная реализация системы с интегрированной базой данных существующих средств позволяет провести анализ и оценку величины возможного ущерба национальной безопасности государства с дополнительными возможностями автоматизированного формирования отчета ее результатов.

Ключевые слова: государственная тайна, оценка ущерба, методология системы анализа и оценки величины возможного ущерба национальной безопасности государства, охрана государственной тайны, параметры вреда.

SYNTHESIS METHODOLOGY AND SOFTWARE IMPLEMENTATION SYSTEM EVALUATION HARM TO NATIONAL SECURITY IN PROTECTION OF STATE SECRETS

Attributing the information to the state secrets held by state expert on secrets by setting, justification and determination of possible damage to national security if such disclosure for a decision on their degree of secrecy. Existing means of calculating such damage is overwhelmingly based on a conditional (scoring) assess its predicted value. The paper presents the methodology for the synthesis of systems analysis and estimation of possible damage to national security that allows model-based integrated presentation of damage parameters obtained by existing analysis tools in the protection of state secrets, to assess the damage as in conventional (ball) units and in value (monetary) value of loss. Founded she developed method: analysis and assessment of damage to national security in the protection of state secrets, assessing the importance of information on certain areas of state secrets, determine the level of competence of the expert committee members at state expert on secrets. In addition, the methodology enables to display the results in both qualitative and quantitative form, for example, using linguistic variables that are often used to describe complex systems. Software implementation of the system with an integrated database of existing tools allows an analysis and estimate of the possible damage to national security with additional automated reporting its results.

Index Terms: state secrets, damage assessment, the methodology of analysis and estimation of possible damage to national security, the protection of state secrets, the parameters of the damage.

Корченко Олександр Григорович, доктор технічних наук, професор, завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: icaocentre@nau.edu.ua
Корченко Александр Григорьевич, доктор технических наук, профессор, заведующий кафедрой безопасности информационных технологий Национального авиационного университета.
Korchenko Alexander, Professor, Doctor of Science in Eng., Head of Academic Department of IT-Security, National Aviation University.

Луцький Максим Георгійович, доктор технічних наук, доцент, професор кафедри безпеки інформаційних технологій Національного авіаційного університету
E-mail: lutskyi.maksym@rada.gov.ua
Луцкий Максим Георгиевич, доктор технических наук, доцент, професор кафедры безопасности информационных технологий Национального авиационного университета
Luttskyy Maksym, Doctor of Science in Eng., Professor of Academic Department of IT-Security, National Aviation University**.**

Захарова Марія В'ячеславівна, кандидат технічних наук, доцент, завідувач кафедри інформатики та інформаційної безпеки, Черкаський державний технологічний університет.
E-mail: zmaria@ya.ru
Захарова Мария Вячеславовна, кандидат технических наук, доцент, заведующий кафедрой информатики и информационной безопасности, Черкасский государственный технологический университет.
Zaharova Mariya, PhD in Eng., Associate Professor, Head of Academic Department of informatics and IT-Security, Cherkasy state technological university

Дрейс Юрій Олександрович, викладач кафедри безпеки інформаційних і комунікаційних систем Житомирського військового інституту ім. С.П. Корольова Національного авіаційного університету.
E-mail: dr_yr_al@mail.ru
Дрейс Юрий Александрович, преподаватель кафедры безопасности информационных и коммуникационных систем Житомирского военного института им. С.П. Королева Национального авиационного университета.
Dreys Yuriy, teacher in information and communication systems department of the Zhytomyr Military Institute named after S.P. Koroleva of the National Aviation University.