Модель оцінювання шкоди національній безпеці в інформаційній сфері

Олександр Корченко[1], Юрій Дрейс[2]

1. Кафедра безпеки інформаційних технологій, Національний авіаційний університет, УКРАЇНА, м.Київ, пр. Космонавта Комарова 1, E-mail: icaocentre@nau.edu.ua

2. Кафедра безпеки інформаційних і комунікаційних систем, Житомирський військовий інститут ім. С.П. Корольова Національного авіаційного університету, УКРАЇНА, м.Житомир, вул. Проспект Миру, 22, E-mail: dr_yr_al@mail.ru

Коротка анотація – Model assessment of damage to national security in the information sector.

Ключові слова – державна таємниця (ДТ) (або секретна інформація (СІ)), службова інформація (СлІ), модель оцінки шкоди, експертиза матеріальних носіїв інформації (МНІ).

I. Вступ

Для запобігання виникнення реальної та потенційної загрози національній безпеці в інформаційній сфері, такої як розголошення інформації з обмеженим доступом, проводяться експертизи МНІ.

Експертиза – організоване державним експертом з питань таємниць (далі – ДЕТ) комплексне вивчення МНІ на предмет наявності чи відсутності у них відомостей, що становлять ДТ, їх достовірності, актуальності та повноти, визначення ступеня обмеження доступу до цих відомостей, встановлення та обґрунтування шкоди, яка може бути завдана державним інтересам внаслідок їх витоку [1]. Проводиться за ініціативою ДЕТ, звернення органів державної влади, підприємств, установ, організацій або громадян (за [2] суб'єктами режимно-секретної діяльності (далі – СРСД)) у випадках [1]: втрати матеріальних носіїв секретної інформації (далі – МНСІ); розголошення відомостей, що становлять ДТ; надання МНІ іноземній державі, міжнародній організації чи її представникам.

За результатами її проведення у експертному висновку окрім даних про ДЕТ, ініціатора, пропозицій експертної комісії, також зазначаються [1]:

1) повні ідентифікаційні ознаки матеріалів експертизи (назва, дата, реєстраційний номер, гриф секретності, номер примірника носія інформації);

2) назви та вид МНІ, їх реєстраційні номери, сторінка, пункт, абзац та інші дані, які містять відомості, що становлять ДТ;

3) до якої сфери забезпечення життєдіяльності належить інформація, яку віднесено до ДТ;

4) стаття Зводу відомостей, що становлять державну таємницю (далі – ЗВДТ), під дію якої підпадає інформація, що становить ДТ;

5) ступінь секретності інформації (Т, ЦТ, ОВ);

6) коротке описання інформації, розголошення якої може завдати шкоди національній безпеці;

7) обставини розголошення інформації, за яких може бути завдано шкоди національній безпеці;

8) *обґрунтування шкоди національній безпеці України*, яку може завдати (чи вже завдав) витік інформації, що міститься у матеріалах експертизи (наслідки витоку цієї інформації).

II. Мета

Проводиться моделювання процесу оцінювання шкоди національній безпеці України при експертизі щодо встановлення наявності чи відсутності у МНІ відомостей, що становлять ДТ чи СлІ, та визначення ступеня обмеження доступу до них.

III. Виклад основного матеріалу

Проведемо аналіз можливості отримання зазначених у п. 1-8) даних для формування експертного висноку. Зокрема, на думку авторів, за п.1-2) наводиться вичерпний перелік відомостей, який слід зазначити і особливих труднощів в їх отриманні не виникає. Отримання необхідної інформації за п.3-6) зводяться до прямого використання закону України "Про державну таємницю" [3] та Зводу відомостей, що становлять державну таємницю (далі – ЗВДТ) [2] як основних нормативно-правових документів, де визначено, що у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку може належати інформація, яку віднесено до ДТ. Також у ЗВДТ [2] наведено перелік та номери статей за якими зареєстровані відомості, що становлять ДТ, їх супені секретності та короткий опис (зміст статей). Що ж стосується обставин за п.7), то вони визначаються за наявністю реальних та потенційних загроз в інформаційній сфері [4], переліком можливих подій-загроз [5], що приводять до порушень у порядку організації та забезпечення режиму секретності СРСД і ефективності діяльності системи охорони ДТ. Уцілому виникають питання [6] до п.8) в обґрунтуванні можливої шкоди національній безпеці, що потребує більш детального аналізу.

Для встановлення та обґрунтування шкоди, яка може бути завдана державним інтересам внаслідок витоку СІ нами присвячено ряд публікацій [7-10]. Всі вони направлені на розробку моделей та методів оцінювання величини можливої шкоди національній безпеці України у разі розголошення відомостей, що становлять ДТ чи втрати МНСІ. У роботах [7, 8] для створення базового набору параметрів, які визначають відомості, що становлять ДТ або СлІ розроблено моделі складної орієнтованої інформаційної мережі (далі – СОІМ) ЗВДТ [7] та ПСлІ Збройних Сил України [8].

З метою узагальнення отриманих ідентифікуючих і оціночних праметрів СОІМ ЗВДТ та СОІМ ПСлІ розроблено базову модель інтегрованого представлення параметрів шкоди та ***модель оцінювання шкоди національній безпеці як складової експертизи МНІ***. Останню приведено на рис.1, де до складу моделі входять: *методики* (МК) оцінювання інформації (***U***): МК 1 – відкритої (**B**) та ІзОД (**A**), МК 2 – конфіденційної ($\mathbf{A_1}$), МК 3 – таємної ($\mathbf{A_3}$), МК 4 – службової ($\mathbf{A_2}$); *лінгвістичні регулятори* (ЛР) (закони

України): ЛР 1 – “Про інформацію”, ЛР 2 – “Про захистперсональних даних”, ЛР 3 – “Про державну таємницю”, ЛР 4 – “Про доступ до публічної інформації” тощо; *лінгвістичний регулятор вибору* (ЛРВ 1) СлІ ($\mathbf{A}_{2.2}$) спеціальної діяльності (оборони країни, контррозвідувальної, оперативно-розшукової) чи ДТ ($\mathbf{A}_{3.1}$) – накази СБ України (наприклад, [1]); *бази знань* (БЗ): БЗ 1 – ЗВДТ (РПВДТ); БЗ 2 – ПСлІ; *моделі* (МЛ) засобів оцінювання: МЛ 1 – СОІМ ЗВДТ [7], МЛ 2 – СОІМ ПСлІ [8]; *бази даних* (БД): БД 1.1 – об’єктів ($\boldsymbol{O}_{N.i.j}$) відомостей ЗВДТ ($\boldsymbol{PV}_{N.i.j}$), БД 1.2 – показників ($\boldsymbol{I}_{N.i.j}$) об’єктів, БД 2.1 – об’єктів ($\boldsymbol{O}_{R.l}$) відомостей ПСлІ ($\boldsymbol{SI}_{R.l}$), БД 2.2 – показників ($\boldsymbol{I}_{R.l}$) об’єктів; *методи* (МД) оцінювання шкоди національній безпеці: МД 1 – у разі розголошення ДТ чи втрати МНСІ ($\boldsymbol{W}_{PV_{N.i.j}}$) [9], МД 2 – у разі розголошення СлІ або втрати матеріальних носіїв СлІ ($\boldsymbol{W}_{SI_{R.l}}$).

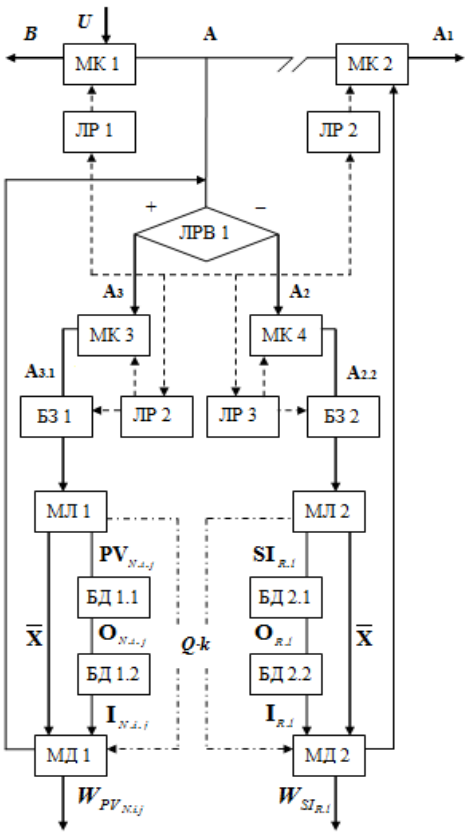

Рис.1 Модель оцінювання шкоди національній безпеці як складова експертизи МНІ

Якщо відомості, щодо яких проводилася експертиза, відповідно до прийнятого ДЕТ рішення не становлять ДТ, вони вивчаються на предмет віднесеності їх до СлІ та доцільності вже прийнятих СРСД заходів (засекречування) чи у необхідності вжиття додаткових (розсекречування або зміну грифа секретності), спрямованих на охорону МНІ.

Висновок

Проведено моделювання процесу оцінювання шкоди національній безпеці як складової експертизи МНІ для підтримки ДЕТ прийняття рішень щодо визначення, у разі можливого витоку наявних на них відомостей, що становлять ДТ, ступеня секретності та присвоєння грифу секретності для цих МНІ або у разі наявності СлІ – грифу обмеження доступу “Для службового користування (ДКС)”.

Література

[1] Щодо порядку організації та проведення експертиз на предмет наявності чи відсутності у матеріальних носіях інформації відомостей, що становлять державну таємницю / Служба безпеки України; Методичні рекомендації, від 28.10.2008 №26/6-7850 // [Електронний ресурс].–Режим доступу: http://www.customs.com.ua/php/document.php?ISN=40688

[2] Про затвердження Зводу відомостей, що становлять державну таємницю / Служба безпеки України; Наказ, Звід від 12.08.2005 № 440 {редакція від 04.01.2013} // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/ show/z0902-05

[3] Про державну таємницю / Верховна Рада України; Закон від 21.01.1994 № 3855-XII {редакція від 18.01.2013} // [Електронний ресурс].–Режим доступу: http://zakon2.rada.gov.ua/laws/ show/3855-12/page

[4] Про основи національної безпеки України / Верховна Рада України; Закон від 19.06.2003 № 964-IV {редакція від 13.10.2012} // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/964-15

[5] 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.

[6] 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.

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

[8] Корченко О.Г. Модель складної орієнтованої інформаційної мережі службової інформації у сфері оборони – Переліку службової інформації Збройних Сил України / О.Г. Корченко, Ю.О. Дрейс // Захист інформації і безпека інформаційних систем: І Міжнар. наук.-техн. конф.: Тези доп. – Львів.: НУ “Львівська політехніка”, 2012. – С.10-11.

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

[10] Дрейс Ю.О. Врахування інтересів держави в методиці оцінювання шкоди у сфері охорони державної таємниці / Інтегровані інтелектуальні робототехнічні комплекси (ІІRTC 2012) : V міжнар. наук.-практ. конф. : Тези доп. – К. : НАУ, 2012. – С.316-318.

Міністерство освіти і науки України

Національна академія наук України

Національний університет "Львівська політехніка"

Інститут прикладних проблем механіки і математики ім. Я.С. Підстригача НАН України

Рада молодих вчених Національного університету "Львівська політехніка"

Головний корпус Львівської політехніки

"ЗАХИСТ ІНФОРМАЦІЇ І БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ"

МАТЕРІАЛИ
ІІ-ої МІЖНАРОДНОЇ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

30 травня - 01 червня 2013 р.

ЗМІСТ

СЕКЦІЯ І

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ