УДК 65.012.8

О. О. Йона

ПРОБЛЕМАТИКА СТВОРЕННЯ ІНСТРУМЕНТАРІЮ ДЛЯ ОЦІНКИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ

У статті приводяться чинники, які передують визначенню інструментарію для комплексної оцінки системи захисту інформаційних ресурсів від впливу зовнішніх загроз.

Ключові слова: *інструментарій, захист інформації, безпека.*

1. Вступ

Впровадження у всі сфери управлінської діяльності сучасних інформаційних технологій, які забезпечують автоматизацію документообігу, висуває на перший план задачі захисту інфоресурсів від впливу зовнішніх загроз. Такі загрози обумовлені як внутрішніми, так і зовнішніми чинниками середовища сучасних інформаційно-комунікаційних систем. Їх слабка захищеність при багатьох обставинах може стати причиною економічних втрат. В даний час інформація вже стала товаром та потужним ресурсом впливу. Розвиток інформаційних технологій, під якими розуміються процеси, методи пошуку, збору, зберігання, обробки, надання, поширення інформації та способи здійснення таких процесів та методів, є одними з найважливіших складових інтересів держави в інформаційній сфері. Однак, поряд з перевагами побудови інформаційного суспільства, збільшуються і ризики, пов'язані з існуванням загроз безпеці інформаційних ресурсів. Для забезпечення безпеки необхідно вирішити завдання забезпечення конфіденційності, цілісності та доступності, що потребує створення відповідного інструментарію для їх оцінки.

2. Постановка проблеми

Відповідно до вище викладеного, в умовах розвитку інформаційного суспільства, виникає проблема. *З одного боку* ростуть обсяги інформації, що обробляються. Про це свідчить збільшення частки надання державних послуг в електронному вигляді, розвиток системи ситуаційних центрів, повсюдне введення електронного документообігу та ін. *З іншого боку* — збільшується ймовірність ризиків, пов'язаних з існуванням загроз безпеці інформації. У зв'язку з цим виникає необхідність розробки систем захисту інформації від різних типів загроз. Так як обробка інформації в інформаційних системах виконується засобами обчислювальної техніки, то необхідно розробити такі системи та інструменти для оцінок стану систем захисту, які дозволяли б, не сильно позначаючись на продуктивності, виробляти та вирішувати зазначені *актуальні* завдання.

3. Основна частина

3.1. Аналіз літературних джерел по темі дослідження. Звичайно, що для вирішення проблеми створення інструментарію для оцінки безпеки інформаційних ресурсів, необхідно дослідити загальні принципи побудови інформаційних систем та мереж і, в тому числі, таких, які мають спеціальні засоби захисту. Це питання досить детально розглянуте у [1], що надає можливості встановити ті параметри, які можуть підлягати оцінці щодо захищеності ресурсів. У [2] приведений аналіз тенденцій розвитку захищеності інформаційної безпеки для автоматизованих систем. Базуючись на даних, які є в зазначеній публікації, з'являється можливість передбачити розробку відповідних методик оцінки. Публікація [3] передбачає внесення доповнень до концепції інформаційної безпеки, що також може викликати потребу розробки чи удосконалення оцінок стану захисту інформації. Системний аналіз особливостей впровадження захищених інформаційних мереж в Україні та синтез критерію їх ефективності (*див.* [4]) дозволяє розробити критерії ефективності щодо оцінки ресурсів, які наявні в інформаційних системах. Процедури вибору та застосування програмних засобів для розробки та впровадження систем оцінок, достатньо описані у [5—8]. На основі наявних матеріалів є можливість вибору методів та технологій створення програмного забезпечення для реалізації задачі у вигляді програмного продукту або алгоритму. Опираючись на результати дослідження інформаційних потоків в комплексних системах захисту інформації та метод розрахунку пропускної спроможності, які приведені в [9], є можливість визначення тих складових, що можуть увійти до вимог, які необхідно врахувати при розробці системи оцінок для визначення стану безпеки інформаційних ресурсів. Технології підвищення адаптивності та достовірності імовірнісних моделей оцінки щодо живучості систем захисту шифрування інформації, приведені в [10], дають основу для комп'ютерного моделювання основних елементів

закриття ресурсів від стороннього втручання. У [11] відзначені деякі аспекти щодо створення системи оцінок, які реалізовані в політиці попередження загроз інформаційній безпеці в практичній діяльності Одеської філії ВАТ «Укртелеком».

Вивчення наукових публікацій дозволяє зробити висновок про те, що системи захисту інформації (в деякому ступені наближення) відносяться до систем прийняття рішень. Відповідно, що розробка системи оцінок повинна враховувати точність прийняття рішення і, т. ч., потребує дослідження питань відновлення та оптимізації інформації. Ця проблема розв'язана та приведена у [12].

3.2. Результати досліджень. Проблематику створення інструментарію для оцінки безпеки інформаційних ресурсів, найбільш доцільно розглянути на основі результатів аналізу достатньо великого обсягу. Втім, приведемо лише короткі висновки з цього.

Захищена автоматизована система припускає наявність механізмів захисту її інформаційних ресурсів в середовищі функціонування системи. Ці загрози повинні бути визначені і оцінені з погляду ризиків їх реалізації. *Захищеною* автоматизовану систему можна вважати тоді, коли всі шляхи реалізації виявлених загроз будуть перекриті механізмами захисту, що відповідають як рівню ризиків від їх реалізації, так і вартості витрат на їх реалізацію плюс вартість очікуваних фінансових втрат. Побудова оптимальних систем з погляду їх захищеності припускає врахування великого числа параметрів, які необхідно оцінити. Такий облік вимагає класифікації інформаційних ресурсів по виду, величині збитку, що завдається, і т. д., які мають свої конкретні величини. Враховуючи складність формалізації параметрів інформаційних об'єктів, вплив на процес безлічі чинників, що змінюються, а також складність визначення їх кількісних показників, рішення поставлених задач вимагає застосування апарату теорії нечітких множин і складної системи експертних оцінок. Таким чином, створення інструментарію оцінки загроз, що дають хоча б об'єктивний результат — це проблема, що очікує свого рішення.

Література

1. Казакова Н. Ф. Принципи побудови захищених інтелектуальних мереж [Текст] / **Н. Ф. Казакова** // Вісник ДУІКТ. — К. : ДУІКТ. — 2009. — № 4. — С. 381—388.
2. Казакова Н. Ф. Аналіз розвитку сучасних напрямів інформаційної безпеки автоматизованих систем [Текст] / О. О. Скопа, **Н. Ф. Казакова** // Системи обробки інформації. — Харків : ХУПС ім. І. Кожедуба, 2009. — № 7(79). — С. 48—54.
3. Казакова Н. Ф. Доповнення до концепції інформаційної безпеки [Текст] / **Н. Ф. Казакова** // Сучасна спеціальна техніка. — К. : Державний НДІ МВС України. — 2010. — № 3(22). — С. 74—80.
4. Казакова Н. Ф. Системний аналіз особливостей впровадження захищених інформаційних мереж в Україні та синтез критерію їх ефективності [Текст] / О. О. Скопа, **Н. Ф. Казакова** // Наукові записки Міжнародного гуманітарного університету. — О. : МГУ. — 2009. — № 16. — С. 115—122.
5. Казакова Н. Ф. Аналіз напрямів розвитку інформаційної безпеки у комп'ютерних системах та мережах на основі застосування програмних засобів захисту інформації [Текст] / **Н. Ф. Казакова** // Вісник Львівського національного аграрного університету. — Л. : Львівський нац. агроун-т. — 2010. — № 14. — С. 47—57.
6. Казакова Н. Ф. Організація процесу розробки програмного забезпечення для захищених інформаційних систем [Текст] / **Н. Ф. Казакова** // Сучасний захист інформації. — К. : ДУІКТ. — 2010. — № 2. — С. 48—56.
7. Казакова Н. Ф. Выделение оптимальной совокупности подпрограмм из основной программы работы системы защиты информации [Текст] / В. А. Хорошко, **Н. Ф. Казакова**, Г. А. Сирченко, Е. О. Тискина // Збірник наукових праць Військового інституту КНУ імені Тараса Шевченка. — К. : ВІ КНУ ім. Т. Шевченка. — 2010. — № 26. — С. 138—142.
8. Казакова Н. Ф. Наукові задачі синтезу організаційно-технологічної схеми створення програмного забезпечення для комп'ютерних мереж з обмеженим доступом [Текст] / В. О. Хорошко, **Н. Ф. Казакова** // Захист інформації. — К. : ДУІКТ. — 2009. — № 4(45). — С. 11—18.
9. Казакова Н. Ф. Исследование информационных потоков в комплексных системах защиты информации и метод расчета пропускной способности [Текст] / **Н. Ф. Казакова**, Е. О. Тискина, В. А. Хорошко // Інформаційна безпека. — Луганськ : СНУ ім. В. Даля. — 2009. — № 2(2). — С. 105—115.
10. Казакова Н. Ф. Повышение адаптивности и достоверности вероятностной модели оценки живучести системы защиты шифрования [Текст] / **Н. Ф. Казакова**, Е. О. Тискина, В. А. Хорошко // Інформаційна безпека. — Луганськ : СНУ ім. В. Даля. — 2009. — № 2(2). — С. 69—73.
11. Казакова Н. Ф. Политика предупреждения угроз информационной безопасности в практической деятельности Одесского филиала ОАО «Укртелеком» [Текст] / А. А. Скопа, **Н. Ф. Казакова**, С. Т. Сорока // Вісник Національного технічного університету «ХПІ». — Харків : НТУ «ХПІ». — 2012. — № 17. — С. 42—47.
12. **Казакова Н. Ф.** Відновлення та оптимізація інформації в системах прийняття рішень [Текст] : підручник / Баранов В. Л., Браіловський М. М., Засядько А. А. [та ін.] ; за ред. В. О. Хорошко. — К. : ДУІКТ, 2009. — 134 с. — ISBN 978-966-2970-35-7.

ПРОБЛЕМАТИКА СОЗДАНИЯ ИНСТРУМЕНТАРИЯ ДЛЯ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Е. О. Йона

В статье приводятся факторы, которые предшествуют определению инструментария для комплексной оценки системы защиты информационных ресурсов от воздействия внешних угроз.

Ключевые слова: инструментарий, защита информации, безопасность.

***Елена Олеговна Йона**, аспирант кафедры информационных систем в экономике Одесского национального экономического университета, **тел.: (050) 694-77-44, e-mail: eyona@mail.ru**.*

THE PROBLEM OF THE TOOLS FOR ASSESSING THE SECURITY OF INFORMATION RESOURCES

O. Yona

The article presents the factors that precede the definition of tools for integrated assessment system to protect information resources from external threats.

Keywords: tools, data protection, security.

***Olena Yona**, graduate student at the Department of information systems in economy of Odessa National Economic University, **tel.: (050) 694-77-44, e-mail: eyona@mail.ru**.*