УДК 004.056:32.019.51

Микола Миколайович Биченок *(д-р техн. наук, с.н.с.)*
Олександр Володимирович Войтко *(канд. військ. наук)*
Володимир Миколайович Чернега
Олександр Миколайович Нестеров

Національний університет оборони України імені Івана Черняховського, Київ, Україна

ЕКСПЕРТНА ПРОЦЕДУРА ОЦІНЮВАННЯ РИЗИКІВ НЕГАТИВНИХ ІНФОРМАЦІЙНИХ ВПЛИВІВ

В статті запропонована узагальнена експертна процедура оцінювання ризиків національній безпеці України в умовах негативних інформаційних впливів за результатами аналізу джерел їх надходження. Складність оцінки ризиків негативних інформаційних впливів кількісними методами полягає у необхідності накопичення досить великих обсягів статистичних даних для отримання точних прогнозів щодо рівня ризику. Оцінка ризиків експертними методами має перевагу в умовах відсутності об'єктивних даних про величини ймовірностей виникнення певних негативних інформаційних впливів і відповідних їм наслідкам. Проведена декомпозиція оцінювання ризиків негативних інформаційних впливів на п'ять основних етапів: ідентифікація джерел негативних інформаційних впливів, визначення стану джерел негативних інформаційних впливів, оцінка уразливості об'єктів впливу, визначення ризиків інформаційної безпеці та обґрунтування заходів щодо мінімізації ризиків негативних інформаційних впливів.

Ключові слова: *негативний інформаційний вплив; джерела інформаційного впливу; інформаційний ризик; експертна процедура.*

Вступ

Постановка проблеми. Застосування технологій гібридної війни в сучасних війнах та збройних конфліктах перетворило інформаційну сферу на ключову арену протиборства. Використання найновіших інформаційних технологій впливу на свідомість громадян спрямовано на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності держави [1, 2].

Упереджуючи реагування на небезпеку негативних інформаційних впливів потребує науково-методичного інструментарію для оцінки загроз цих впливів (ризиків інформаційної безпеки) та обґрунтування заходів із запобігання чи мінімізації небажаних наслідків. Застосування такого інструментарію пов'язано, перш за все, з розробкою адекватних математичних моделей ризиків інформаційних впливів.

Аналіз останніх досліджень і публікацій.

Наукове дослідження будь-яких об'єктів чи процесів, у тому числі й інформаційних, починається з вимірювання їхніх параметрів за допомогою формалізованого опису.

Наукові підходи оцінювання інформаційних впливів розглядалися в роботах [3-5]. Так, у роботі [3] розглядається методика виявлення ознак інформаційного впливу на основі аналізу відкритих джерел за визначеними основними етапами. У [4] проведена ідентифікація можливих джерел загроз та факторів, що сприяють їх прояву, із визначенням актуальних загроз інформаційній безпеці. Запропоновано удосконалений підхід щодо аналізу загроз інформаційній безпеці держави у воєнній сфері та визначення заходів протидії їм. У [5] визначені основні показники аналізу інформаційного потоку та наведена методика розрахунку інтенсивності інформаційного впливу, якій здійснюється через повідомлення засобів масової інформації. Зазначені наукові труди в загальній формі дозволяють здійснювати аналіз інформаційних джерел, що є складовою оцінювання ризиків негативних інформаційних впливів.

Аналіз науково-методичного апарату оцінювання ризиків інформаційної безпеки свідчить, що їх основу складають певні методологічні засади, нормативно-правові акти або міжнародні стандарти, які визначають вимоги інформаційної безпеки [6-9]. Найбільш поширеними є: 1) міжнародні стандарти: ISO/IEC 27001:2005, ISO/IEC 27005:2008, ISO/IEC 27000:2009 та ISO/IEC 27001:2013; 2) методики та методології оцінки ризиків інформаційної безпеки: NIST Special Publication 800-30 – управління ризиками на різних стадіях життєвого циклу інформаційної системи, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) – виявлення організацією ризиків інформаційної безпеки у вигляді ризиків конфіденційності, цілісності і доступності активів інформаційних технологій, Control Objectives for Information and Related Technologies (COBIT) – рекомендації щодо оцінки ризиків на етапі планування застосування в організації системи інформаційних технологій та інші. Існуючий

науково-методичний апарат дозволяє робити зважені якісні оцінки, що визначаються експертами. Також набули розвитку і кількісні методи оцінки ризиків інформаційної безпеки [8, 9], але вони потребують накопиченої статистики, яка є основою отримання значень ймовірностей їх виникнення.

Отже, потреба науково-обґрунтованого підходу до безпеки життєдіяльності в інформаційному середовищі зумовлює необхідність формалізації та оцінювання небезпеки негативних інформаційних впливів, тобто ризиків інформаційної безпеки.

Метою статті є дослідження особливостей формалізації та оцінювання ризиків негативних інформаційних впливів методом експертних оцінок.

Виклад основного матеріалу дослідження

Головну трудність для математичного моделювання ризиків інформаційній безпеці становить невизначеність просторово-часових характеристик процесів зародження і прояву джерел негативних інформаційних впливів. У теорії прийняття рішень [10] розрізняються два типи невизначеності: статистичний і нестатистичний. До першого типу відносяться процеси, що можуть спостерігатися достатню кількість разів, зокрема, за допомогою натурних або модельних експериментів. Частота виникнення подій (інформаційних впливів), що характеризують ці процеси, трактується як статистична ймовірність. Якщо досліджувані процеси проявляються недостатню кількість разів, або взагалі припускають реалізацію лише в майбутньому, то вони являють нестатистичний тип невизначеності. У цьому випадку ймовірність трактується не як частота виникнення події, а як ступінь впевненості (міра можливості), що ця подія відбудеться. Нестатистична інтерпретація невизначеності оперує поняттям суб'єктивної ймовірності. Оцінювання суб'єктивних ймовірностей здійснюється за допомогою спеціально організованих експертних процедур на основі декомпозиції складної події на більш прості [10].

Узагальнена експертна процедура оцінювання ризиків інформаційних впливів включає п'ять основних етапів:

1) *Ідентифікація джерел негативних інформаційних впливів* – виконується збір і аналіз усіх доступних відомостей про випадки прояву і негативні наслідки інформаційних впливів у межах оцінюваної території для отримання відповіді на наступні питання:

- які за ґенезою є джерела негативних інформаційних впливів на даній території?
- де, коли і за яких умов вони проявлялися чи можуть проявитися на даній території?

2) *Визначення стану джерел негативних інформаційних впливів* – проводиться аналіз просторово-часових характеристик виявлених джерел для відповіді на такі питання:

- яка була у минулому чи очікується частота виникнення і тривалість негативних інформаційних впливів від цих джерел на даній території при відсутності запобіжних заходів?
- якими будуть зазначені характеристики при різних варіантах запобіжних заходів?

3) *Оцінка уразливості об'єктів впливу* – за результатами аналізу станів джерел негативних інформаційних впливів визначаються відповіді на питання:

- яка чисельність, склад і уразливість об'єктів впливу у межах даної території від можливих інформаційних загроз певного типу?
- яка чисельність, склад і уразливість об'єктів впливу у межах даної території від можливих інформаційних загроз усіх типів?

4) *Визначення ризиків інформаційній безпеці* – на основі проведеного аналізу стану джерел інформаційних загроз і потенційних об'єктів їх впливу формуються відповіді на питання:

- які можливі сценарії зміни стану різних джерел і відповідні негативні наслідки їх прояву?
- якою може бути уразливість об'єктів впливу від усіх і від окремих типів інформаційних загроз?
- якими будуть відповідні частоти прояву різних джерел інформаційних загроз?

5) *Обґрунтування заходів щодо мінімізації ризиків негативних інформаційних впливів* – з урахуванням економічних і соціальних вимог та можливостей заданого регіону розробляються відповіді на заключні питання:

- який припустимий ризик, тобто припустима частота прояву різних джерел?
- якими стануть сценарії зміни стану джерел інформаційних загроз і відповідні негативні наслідки їх прояву після здійснення варіантів запобіжних заходів?
- який варіант цих заходів забезпечує досягнення припустимого ризику при мінімальних витратах на їхню реалізацію?

Для формалізованого представлення ризику інформаційного впливу R можна використати модель [11], що пов'язує між собою ймовірність виникнення певних подій (прояву інформаційних джерел) P і відповідних їм наслідків W:

$$R = P \cdot W \qquad (1)$$

Враховуючи, що $0 \le P \le 1$ та нормовані втрати $0 \le W \le 1$, ці показники можна використовувати для кількісного оцінювання ризику інформаційного впливу в характерних ситуаціях:

при $P = 1$, $W = 0$, $R = 0$ частота прояву інформаційної загрози велика, а величина втрат незначна;

при $P = 0$, $W = 1$, $R = 0$ прояв інформаційної загрози відбувається вкрай рідко, а величина втрат велика;

при $P = 0$, $W = 0$, $R = 0$ незначна частота прояву інформаційної загрози і її наслідків;

при $P \ne 0$, $W \ne 0$, $R \ne 0$ відбуваються різні частоти прояву інформаційних загроз і різні наслідки. Ця ситуація може оцінюватися як

небезпечна і характеризуватися значною величиною ризику інформаційного впливу.

Для обчислення ймовірностей і, відповідно, оцінювання ризиків існують три основні методологічні підходи [12]:

статистичний – за результатами багаторазових спостережень відповідно закону великих чисел розраховують частоту прояву різних джерел негативних інформаційних впливів;

соціологічний – за допомогою цього методу визначається сприйняття населенням і його окремими групами тих чи інших інформаційних впливів. Проводяться соціологічні опитування, під час яких визначаються оцінки інформаційних ризиків, пов'язані з прийняттям тих чи інших рішень щодо запобіжних заходів;

експертний – при використанні першого підходу часто зустрічаються випадки, коли недостатньо статистичних даних щодо прояву різних джерел негативних інформаційних впливів. Тоді залучаються експерти для суб'єктивної оцінки ймовірності прояву того чи іншого джерела.

Висновки

Таким чином, на основі аналізу джерел негативних інформаційних впливів в статті розроблено узагальнену експертну процедуру оцінювання ризиків негативних інформаційних впливів. Оцінка ризиків експертними методами має перевагу в умовах відсутності об'єктивних даних про величини ймовірностей виникнення певних негативних інформаційних впливів і відповідних їм наслідкам.

Напрямком подальших досліджень може бути широке коло питань щодо пошуку механізмів визначення значень інформаційних ризиків у сфері національної безпеки держави.

Література

1. Указ Президента України Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України". [Електронний ресурс]. − Режим доступу: http://zakon2.rada.gov.ua/laws/show/287/2015.

2**. Доктрина** інформаційної безпеки України затверджена указом Президента України № 472017 від 25.02.2017 року. [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/47/2017.

3. Левченко О. В. Методика виявлення заходів негативного інформаційного впливу на основі аналізу відкритих джерел / О.В.Левченко, О.М.Косогов // Системи обробки інформації.– 2016. Вип. 1. – С.100-102.

4. Косогов О. М. Методологічний підхід до аналізу загроз інформаційній безпеці держави у воєнній сфері та визначенню заходів протидії їм. / О.М.Косогов // Наука і техніка Повітряних Сил Збройних Сил України. – 2015. – № 3. – С. 51-53.

5. Марченко-Бабич О. М. Основні показники аналізу інформаційного потоку в інтересах забезпечення інформаційної безпеки / О.М.Марченко-Бабич // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – 2016. – Вип. 53. – С.160-162.

6. Замула О. А. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки / О.А.Замула, В.І.Черниш//Системи обробки інформації. – 2011. – Вип. 2(92). – С. 53-56.

7. Єрмошин В. В. Аналіз і оцінка ризиків інформаційної безпеки для банківських та комерційних систем. / В.В.Єрмошин, Я.В.Невойт // Сучасний захист інформації. – 2014. – № 4. – С. 12-22.

8. Черниш В. І. Методика оцінки інформаційних ризиків з використанням методу аналізу ієрархій. В.І.Черниш // Радіоелектронні і комп'ютерні системи. – 2012. – № 1. С.46-50.

9. Архипов О. Є. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації / О.Є.Архипов, А.В.Скиба // Захист інформації. – 2013. – Т. 15, № 4. – С. 366-375.

10. Биченок М. М. Основи інформатизації управління регіональною безпекою. – К.: РНБОУ, 2005. – 196 с.

11. Мушик Э. Методы принятия технических решений: Пер. с нем. / Э. Мушик., П. Мюллер – М.: Мир, 1990.– 208 с.

12. Саєнко Ю. І. Соціальні ризики та шанси: Соціальні ризики.-Т.2 / Відп. ред. Ю. І. Саєнко, Ю. О. Привалов. – К.: ПЦ "Фоліант", 2004. – 568 с.

ЭКСПЕРТНАЯ ПРОЦЕДУРА ОЦЕНКИ РИСКОВ НЕГАТИВНЫХ ИНФОРМАЦИОННЫХ ВОЗДЕЙСТВИЙ

***Николай Николаевич Быченок** (д-р техн. наук, с.н.с.)*
***Александр Владимирович Войтко** (канд. воен. наук)*
Владимир Николаевич Чернега
Александр Николаевич Нестеров

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В статье предложена обобщенная экспертная процедура оценки рисков национальной безопасности Украины в условиях негативных информационных воздействий за результатами анализа источников их поступления. Сложность оценки рисков негативных информационных воздействий количественными методами заключается в необходимости накопления достаточно больших объемов статистических данных для получения точных прогнозов относительно уровня риска. Оценка рисков экспертными методами имеет преимущество в условиях отсутствия объективных данных о величинах вероятностей возникновения определенных негативных информационных воздействий и соответствующих им последствий. Проведена декомпозиция оценки рисков негативных информационных воздействий на пять основных этапов: идентификация источников негативных информационных воздействий, определения состояния источников негативных информационных воздействий, оценка уязвимости объектов воздействия, определение рисков информационной

безопасности и обоснование мероприятий по минимизации рисков негативных информационных воздействий.

Ключевые слова: *негативное информационное воздействие, источники информационного воздействия, информационный риск, экспертная процедура.*

EXPERT RISK ASSESSMENT PROCEDURE OF NEGATIVE INFORMATION IMPACTS

Mukola M. Bychenok *(Doctor of Technical Sciences, Senior Research Fellow)*
Oleksandr V. Voytko **(***Candidate of Military Sciences)***
Volodymyr M. Cherneha
Oleksandr M. Nesterov

National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

In The article offers a generalized expert procedure for the risks evaluation of negative information impacts. The evaluation is conducted after the results of the source analysis of information impacts. Quantitative methods of evaluation require the accumulation of large volumes of statistical data. Expert methods in such complex process have the advantage. Five stages for the risks evaluation of negative information impacts were proposed: identifying sources of negative information impacts, determining the status of negative information impacts sources, assessing the vulnerability of impact sites, identifying information security risks, and justifying measures to minimize the risks of negative information impacts.

Keywords*: negative information impact; sources of information impact; information risk, expert procedure.*

References

1. Ukaz Prezydenta Ukrajiny Pro rishennja Rady nacionaljnoji bezpeky i oborony Ukrajiny vid 6 travnja 2015 roku "Pro Strateghiju nacionaljnoji bezpeky Ukrajiny". available at: http://zakon2.rada.gov.ua/laws/show/287/2015. 2. **Doktryna** informacijnoji bezpeky Ukrajiny zatverdzhena ukazom Prezydenta Ukrajiny № 472017 vid 25.02.2017 roku. available at: http://zakon2.rada.gov.ua/laws/show/47/2017. **3. Levchenko O.V.,** Kosogov O.M. (2016). The technique of identification of the negative information influence activity that is based on the open sources analysis. [*Metodyka vyjavlennja zahodiv negativnogo informaeijnogo vplyvu na osnovi analizu vidkrytyh dzhcrel*], Sistcmy obrobki informaci'i, Kharkiv, № 1, pp.100-102. **4. Kosogov O.** (2015). Methodological approach to analysis of the national information security threats in the military domain and their countermeasures determination. [*Metodologichnyj pidhid do analizu zagroz informacijnij bezpeci derzhavy u voyennij sferi ta viznachennja zahodiv protydii im*], Kharkiv, Nauka i tehnika Povitrjanyh Syl Zbrojnyh Syl Ukrdiny, № 3, pp.51-53. **5. Marchenko-Babich O.M.** (2016) The basic marks of the information flow analysis for the purpose of The information security [Osnovni pokaznyky analizu informacijnogho potoku v interesakh zabezpechennja informacijnoji bezpeky] // Zbirnyk naukovykh pracj Vijsjkovogho instytutu Kyjivsjkogho nacionaljnogho universytetu imeni Tarasa Shevchenka. Vol. 53, pp.160-162. **6. Zamula O.A.,** Chernysh V.I. (2011) Analysis of international standarts in risk assessment of information security. [Analiz mizhnarodnykh standartiv v ghaluzi ocinjuvannja ryzykiv informacijnoji bezpeky] // Information Processing Systems, № 2(92), pp.53-56. **7. Jermoshyn V.V.,** Nevojt Ja.V., (2014) Analysis and risk assessment for information security and commercial banking system [Analiz i ocinka ryzykiv informacijnoji bezpeky dlja bankivsjkykh ta komercijnykh system] // Modern Information Security, № 4, pp.12-22. **8. Chernysh V.I.** (2012) The methodology of assessing information risks using the analytic hierarchy process. [Metodyka ocinky informacijnykh ryzykiv z vykorystannjam metodu analizu ijerarkhij] // Radioelectronic and computer systems, № 1, pp.46-50. **9. Arkhypov O.E.,** Skyba A.V. (2013) Information risk: research methods and techniques, models and methods of risk identification // Information Security, Vol.4, pp.366-375. **10. Bychenok M.M.** (2009), The Fundamentals of information management regional security. [*Osnovy informatyzatsiyi upravlinnya rehional'noyu bezpekoyu*], Kyiv, RNSD of Ukraine, 196 p. **11. Muschick E.,** Muller P. (1990), Methods Adoption of technical solutions. [*Metody prinyatiya tehnicheskih resheniy*], Moscow "Myr", 208 p. **12. Saenko Y.I.,** Pryvalov Y.O. (2004), Social risks and chances: Social risks – Tom. 2. [*Analiz osnovnykh aspektiv vplyvu DoS-atak na pratsezdatnist kompiuternoi merezhi*], Kyiv, PC "Pholiant", 568 p.