УДК: 351:007:65.01(477)
DOI: 10.31891/2307-5740-2020-278-1-46

ФЕДОРЕНКО А. Є.
Чернігівський національний технологічний університет

ІНСТРУМЕНТАРІЙ МОДЕЛЮВАННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ

В статті автором сформульовано методологію розробки системи забезпечення інформаційної безпеки національної економіки, в основу якої покладено засади синергетичного управління взаємодією учасників інформаційної сфери, методи (ідентифікації ризиків, побудови профілів інформаційної безпеки учасників інформаційної сфери, прогнозування динаміки поширення контенту цілеорієнтованого змісту, інформаційно-психологічного впливу на учасників), етапи (моніторинг вихідного контенту, виявлення і оцінювання загроз інформаційній безпеці економіки; вироблення заходів з протидії виявленим загрозам та розвитку національної економіки) та прототип програмного забезпечення в основі якого лежать CASE-технології, що дозволяє закласти основи для розробки ефективної стратегії забезпечення розвитку інформаційної сфери економіки та на системному рівні сприяти нейтралізації загроз інформаційній безпеці. Встановлено, що попит учасників на контент деструктивного змісту зменшується практично до 3 разів за рахунок оптимальності побудови системи забезпечення інформаційної безпеки, у свою чергу підвищення рівня розвитку інформаційної сфери досягається на основі скорочення тривалості різних перехідних процесів внаслідок реакції на певний контент до 30%. Отже, розроблені методологічні засади щодо формування і реалізації системи забезпечення інформаційної безпеки національної економіки сприяють досягненню поставленої мети.

Ключові слова: інформаційна сфера, розвиток, забезпечення, національна економіка, інформаційна безпека, моделювання.

FEDORENKO A.
Chernihiv National Technological University

TOOLS FOR MODELING THE INFORMATION SECURITY SYSTEM OF THE NATIONAL ECONOMY

The consequences of the rapid development of information technology in the world and in Ukraine are a significant acceleration of informatization of social activities, strengthening the processes of globalization and internationalization. The intensification of information processes has also affected the system of strategic communications of society, in which the leading role is given to the communicative component. At the current stage of digital transformations for Ukraine as a European state is an extremely important task to mobilize the potential of the information sphere to ensure sustainable development of the national economy, the country's access to such indicators of socio-economic development that will allow equal entry into the modern European economic system. The defining trend for the further development of modern society is the strengthening of the influence of information technology in almost all spheres of activity, marked by fundamental transformations of productive forces, formation of innovative infrastructure of the information sphere, interpreting the content of such transformations, growth of scientific knowledge and its significance business processes, globalization of the economy and the priority of the functioning of network structures.

In the article the author formulates the methodology of development of the information security system of the national economy, which is based on the principles of synergetic management of interaction of information participants, methods (risk identification, construction of information security profiles of information participants, forecasting the dynamics of content-oriented content, information-psychologist participants), stages (monitoring of source content, detection and assessment of threats to information security of the economy; development of measures to counter identified threats and development of the national economy) and a prototype of software based on CASE-technologies, which lays the foundations for developing an effective development strategy information sphere of the economy and at the system level to help neutralize threats to information security. It is established that the demand of participants for destructive content is reduced to almost 3 times due to the optimal construction of information security, in turn, increasing the level of information development is achieved by reducing the duration of various transitions due to response to certain content up to 30%. Thus, the developed methodological principles for the formation and implementation of information security of the national economy contribute to the achievement of this goal.

Keywords: information sphere, development, provision, national economy, information security, modeling.

Постановка проблеми. Наслідками стрімкого розвитку інформаційних технологій у світі та Україні є суттєве прискорення інформатизації суспільної діяльності, посилення процесів глобалізації та інтернаціоналізації. Активізація інформаційних процесів вплинула й на систему стратегічних комунікацій суспільства, у якій провідна роль відводиться комунікативній складовій. На сучасному етапі цифрових трансформацій для України як європейської держави надзвичайно важливим завданням є мобілізація потенціалу інформаційної сфери для забезпечення сталого розвитку національної економіки, виходу країни на такі показники соціально-економічного розвитку, які нададуть можливість на рівних увійти в сучасну європейську економічну систему. Визначальною тенденцією для подальшого розвитку сучасного суспільства є посилення впливу інформаційних технологій практично на всі сфери діяльності, відзначаючись фундаментальними трансформаціями продуктивних сил, формуванням інноваційної інфраструктури інформаційної сфери, які інтерпретують зміст таких перетворень, зростанням наукового знання і його значущості для забезпечення добробуту всього суспільства, інтенсифікацією інформатизації бізнес-процесів, глобалізацією економіки й пріоритетністю функціонування мережевих структур.

Аналіз останніх досліджень і публікацій. Наразі дослідженню проблем, пов'язаних із забезпеченням інформаційної безпеки національної економіки, присвячується значна частина публікацій вітчизняних і зарубіжних вчених як індивідуально, так і в складі наукових колективів. Вагомий внесок у вирішення даної проблеми належить В. Горбуліну, В. Хорошку, О. Додонову, Р. Грищуку, В. Ліпкану, О. Левченку, С. Іванченку, В. Попику, Н. Казаковій, Д. Новікову, О. Чхартішвілі, М. Кастельсу, Дж. Епстейну та іншим.

Незважаючи на широкий спектр напрямів дослідження особливостей забезпечення інформаційної безпеки національної економіки, у працях зазначених учених практично не знайшли відображення питання розробки ефективного інструментарію моделювання системи забезпечення інформаційної безпеки економіки.

Мета статті полягає в обґрунтуванні науково-прикладних засад моделювання системи забезпечення інформаційної безпеки національної економіки України.

Виклад основного матеріалу. Загрози національній безпеці України та відповідні пріоритети державної політики у сферах національної безпеки й оборони визначаються у Стратегії національної безпеки України, Стратегії воєнної безпеки України, Стратегії кібербезпеки України, та інших документах з питань національної безпеки й оборони, які схвалюються Радою національної безпеки і оборони України і затверджуються указами Президента України [1].

Традиційно, усі загрози поділяють на внутрішні та зовнішні [2]. Прикладом зовнішньої інформаційної загрози може бути загроза впливу іншої сторони на інформаційну інфраструктуру країни, інформаційні ресурси, на суспільство, свідомість, підсвідомість особистості з метою нав'язати державі та її громадянам бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєвоважливих сферах суспільної й державної діяльності, керувати їх поведінкою і розвитком у бажаному для іншої сторони напрямку. Власне, це є загрозою суверенітету України в інформаційній сфері, що може бути реалізованою на рівні з військовим збройним протистоянням, а результат, за певних умов, є більш масштабним унаслідок застосування ЗМК для привернення уваги та нав'язування необхідних ідей широкому колу користувачів.

Категорія ризик, будучи семантично тісно пов'язаною з поняттями безпека, небезпека, загроза, в той же час передбачає ймовірність несприятливих наслідків. Ризик виникає лише тоді, коли має місце невизначеність, відсутність вичерпної інформації про умови прийняття рішень. Якщо все відомо — ризик відсутній. Тільки при багатоваріантності майбутнього, наявності елементів непередбаченості можна казати про наявність ризику. Невизначеність є однією з причин виникнення ризику.

Під невизначеністю необхідно розуміти наявність неповної інформації про умови прийняття господарських рішень, а не відсутність будь-якої інформації. Існує думка, що наявність ризику є певною ознакою зрілості економіки, її розвинутості. В економіці з низьким рівнем душового виробництва траєкторія її розвитку практично детермінується стратегією виживання, суворою необхідністю забезпечення мінімальних потреб споживачів, якщо ж відсутні альтернативи рішень, то й відсутній ризик. Отже, ризик необхідна умова регулювання економічних відносин, також необхідно пам'ятати, що джерелами ризику є фактори (явища, предмети, процеси), які спричинюють невизначеність результатів [3]

Оскільки ризики є усвідомленими, то вони носять суб'єктивну природу, відповідно, можуть бути оцінені й ними можна керувати. У цьому і полягає головна відмінність ризику від небезпеки та загрози, оскільки останні зумовлені дією об'єктивних факторів. Традиційно виділяють три підходи, коли говорять про ризик (як елемент системи безпеки): ймовірність настання негативних наслідків; невизначеність; неоднозначний результат. Аналіз зазначених підходів дає змогу виявити головні моменти, характерні для ризикованої ситуації, а саме: випадковий характер події, що визначає, яка з можливих ситуацій реалізується на практиці; наявність альтернативних розв'язків проблеми; ймовірність втілення певних рішень та очікувані результати; очікувані збитки або отримання додаткового прибутку.

У результаті проведених досліджень встановлено, що існуючі засоби і підсистеми інформаційної безпеки національної економіки не відповідають рівню сучасних загроз, тому розроблення дієвого наукового інструментарію для формалізації процесів виявлення і протидії загрозам у інформаційному просторі віртуальних спільнот є актуальним теоретико-прикладним завданням для розвитку національної економіки.

Аналіз останніх досліджень і публікацій за напрямком дослідження показав недостатній рівень теоретичного опрацювання і відсутність практичних рекомендацій щодо розроблення системи забезпечення інформаційної безпеки національної економіки. У цілому така система є компонентом системи забезпечення національної безпеки і може складатися з підсистем для розв'язку окремих завдань. У наукових працях професора А. Ліпкана [4] сформульовано мету і завдання системи забезпечення інформаційної безпеки держави, визначено, що вона розробляється відповідно до положень Конституції України та нормативно-правового забезпечення у досліджуваній сфері. Вказано, що в основу системи забезпечення інформаційної безпеки національної економіки покладено комплекс засобів забезпечення інформаційної безпеки, які застосовують адміністративно-правові, інформаційно-аналітичні, організаційно-управлінські та інші дії для сталого розвитку всього інформаційного середовища країни.

Отже, з метою забезпечення заданого стану функціонування інформаційної сфери необхідно розробити систему підтримки прийняття рішень як компоненту відомчої підсистеми забезпечення безпеки національної економіки на основі розроблених методів виявлення, оцінювання і протидії можливим загрозам. Така система дозволить підвищити загальну ефективність інформаційної сфери економіки України, що додатково актуалізує обраний напрямок наукових досліджень.

Суть ознак інформаційних операцій у національній економіці зводиться до використання інформаційних ресурсів та спеціалізованого програмного забезпечення. Загрози у змісті забезпечення національної безпеки характеризуються наявністю деструктивного інформаційного посилу у економіці. Маніпуляції інструментами державної інформаційної політики у системі забезпечення інформаційної безпеки національної економіки полягають у застосуванні прихованого інформаційного впливу на суб'єктів господарювання для управління їх поведінкою або психологічними характеристиками в інтересах суб'єкта впливу. Особливості організації діяльності суб'єктів господарювання в інформаційній сфері представляю собою набір агрегованих характеристик інформаційної безпеки, які дозволяють визначити рівень її загрози як можливого учасника інформаційної фери, направлених проти безпеки людини, суспільства, держави. Далі проводять обчислення інтегрального показника загроз для формування висновку про рівень виявлених загроз у інформаційній безпеці національної економіки [5-6].

Завершальний етап функціонування системи забезпечення інформаційної безпеки національної економіки полягає у протидії виявленим загрозам. Конкретні рекомендації з протидії визначаються залежно від рівня виявленої загрози на попередньому етапі функціонування системи забезпечення інформаційної безпеки національної економіки. Так, якщо рівень загрози є низьким, то доцільно виконати прогнозування поширення негативних факторів для оперативного коригування прихованих управляючих впливів на інфформаційну безпеку національної економіки. У випадку середнього або існуючого рівня загрози системи забезпечення інформаційної безпеки національної економіки необхідно виконати синтез синергетичного управління взаємодією учасників такої системи. Такі дії забезпечать штучно керований перехід віртуальної спільноти до бажаного стійкого стану національної економіки завдяки підтриманню заданих показників взаємодії учасників інформаційної сфери і запуску процесів самоорганізації. Завершальним компонентом етапу протидії загрозам є формування практичних рекомендацій відповідним державним виконавчими органами з протидії на основі Доктрини інформаційної безпеки України залежно від рівня загрози та сфери суспільної діяльності, на яку вона впливає.

Для побудови системи забезпечення інформаційної безпеки національної економіки для виявлення загроз та оцінювання їх рівня на основі попередніх досліджень запропоновано такий алгоритм функціонування [7-8].

Етап I. Моніторинг стану функціонування інформаційної сфери та її впливу на національну економіку. На початковому етапі проводиться моніторинг інформаційного простору національної економіки з метою виявлення релевантного контенту у даному напрямі. Аналізу підлягають фактори та їх вплив на інформаційну безпеку економіки.

Етап II. Розрахунок частинних проявів загроз у відібраній сукупності факторів. Відібрані на попередньому етапі фактори та особливості функціонування національної економіки досліджуються на наявність ознак застосування для проведення інформаційних операцій у системі забезпечення інформаційної безпеки національної економіки. З цією метою проводиться аналіз наявності загроз інформаційній безпеці.

Етап III. Протидія загрозам системі забезпечення інформаційної безпеки національної економіки. Залежно від отриманого на попередньому етапі значення інтегральної оцінки ознак загроз приймається відповідне рішення для протидії.

У результаті проведеного дослідження встановлено, що діючі в Україні засоби та підсистеми забезпечення розвитку інформаційної сфери економіки не відповідають рівню сучасних загроз інформаційної безпеки національної економіки, тому розроблення дієвого науково-методичного інструментарію для формалізації процесів ідентифікації та протидії загрозам у інформаційній сфері є актуальним теоретико-прикладним завданням. Для забезпечення ефективності реалізації стратегії розвитку інформаційної сфери економіки України запропоновано систему забезпечення інформаційної безпеки національної економіки на засадах протидії внутрішнім та зовнішнім загрозам (рис.1), ефективність використання якої визначається на основі авторського прототипу програмного забезпечення, яке дозволяє формалізовувати процедуру раннього виявлення відповідних інформаційних операцій.

Для проведення проектування прототипу такого програмного забезпечення й оцінювання результативності представленої системи забезпечення інформаційної безпеки національної економіки використано сучасні CASE-технології, насамперед мову UML. Такий відкритий стандарт забезпечує уніфікований процес формування відповідного програмного забезпечення.

Реалізація розробленої автором методології побудови системи забезпечення інформаційної безпеки економіки України, з урахуванням представлених концептуальних основ й методів, дозволяє суттєво підвищити рівень результативності стратегії забезпечення розвитку інформаційної сфери в умовах інтеграції України в загальносвітовий інформаційний простір. У свою чергу, використання такої методології при реалізації стратегії забезпечення розвитку інформаційної сфери дозволяє врахувати різні прояви внутрішніх

й зовнішніх загроз й забезпечує завчасну ідентифікацію їх ознак створюючи цим самим передумови для організації дієвої інформаційної протидії. Встановлено, що попит учасників на контент деструктивного змісту зменшується практично до 3 разів за рахунок оптимальності побудови системи забезпечення інформаційної безпеки, у свою чергу підвищення рівня розвитку інформаційної сфери досягається на основі скорочення тривалості різних перехідних процесів внаслідок реакції на певний контент до 30%. Отже, розроблені методологічні засади щодо формування і реалізації системи забезпечення інформаційної безпеки національної економіки сприяють досягненню поставленої мети.

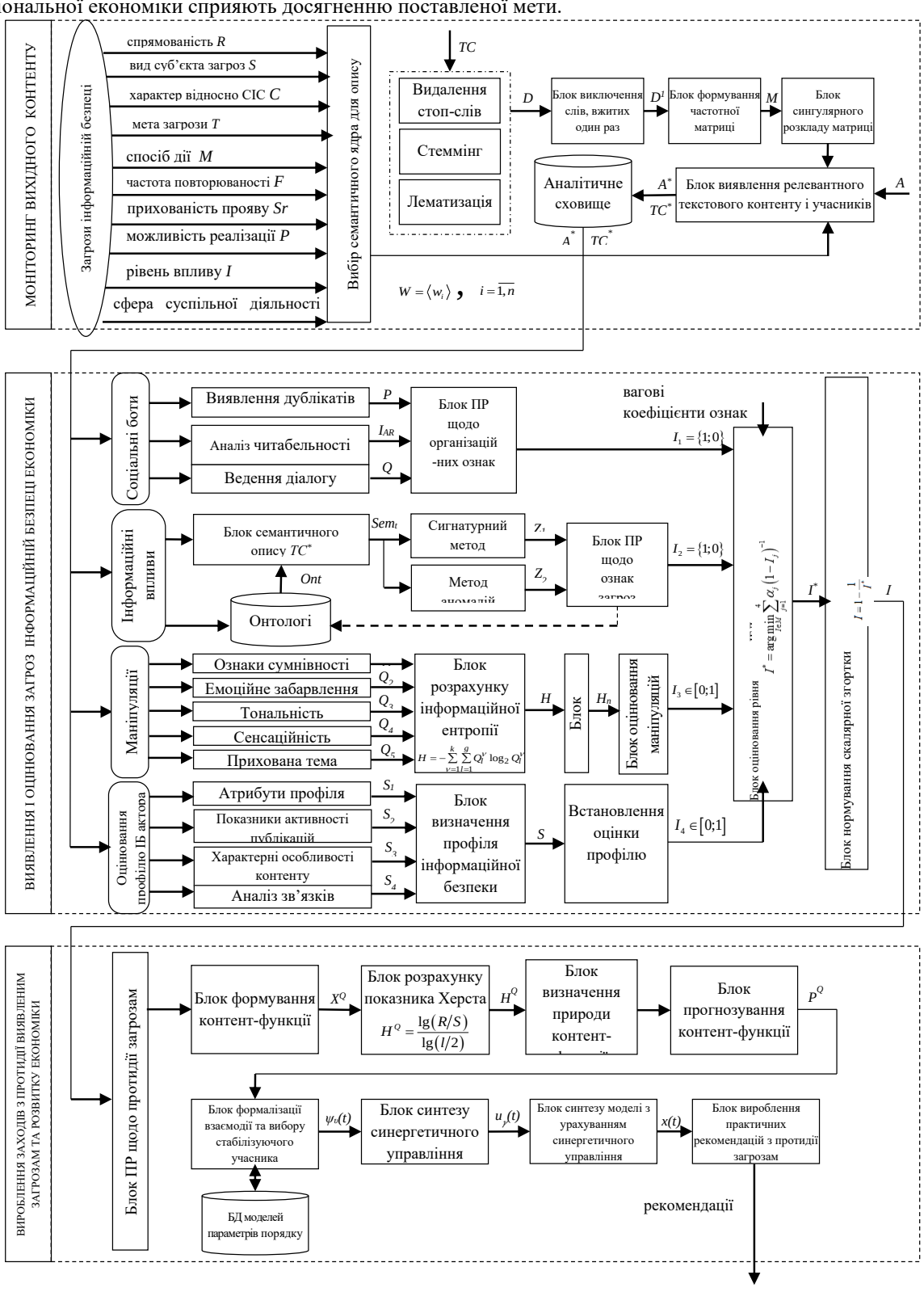

Рис. 1. Архітектура методології формування системи забезпечення інформаційної безпеки національної економіки
Джерело: розроблено автором

Висновки та перспективи подальших досліджень. Розроблено методологію формування системи забезпечення інформаційної безпеки національної економіки, практичне значення якої полягає у використанні дієвого програмного забезпечення, яке, у процесі інтеграції з інноваційними інформаційними технологіями, дозволить забезпечити розвиток інформаційної сфери держави та підвищити рівень інформаційної безпеки національної економіки створивши цим самим передумови для економії ресурсів, які витрачатимуться на її реалізацію. Запропонована методологія передбачає реалізацію трьох етапів (моніторинг вихідного контенту, виявлення і оцінювання загроз інформаційній безпеці економіки; вироблення заходів з протидії виявленим загрозам та розвитку національної економіки), які дозволяють формалізувати процедури раннього попередження, проведення оцінки та протидії внутрішнім і зовнішнім загрозам інформаційній безпеці національної економіки.

Література

1. Закон України «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII. URL: http://zakon.rada.gov.ua/laws/show/2469-19

2. Фінансова безпека машинобудівного підприємства: Методичні засади формування та забезпечення / [Х. О. Мандзіновська, А. М. Штангрет, Я. В. Котляревський, О. В. Мельников]. Львів: Укр. акад. друкарства, 2016. 240 с.

3. Ястремський О. І. Моделювання економічного ризику / О. І. Ястремський. К.: Либідь, 1992. 176 с.

4. Ліпкан В. А. , Максименко Ю. Є. , Желіховський В. М. , Інформаційна безпека України в умовах євроінтеграції, К.: КНТ, 2006.

5. Голубєв В. О. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / В. О. Голубєв, В. Д. Гавловський, В. С. Цимбалюк ; за заг. ред. Р. А. Калюжного. Запоріжжя: Просвіта, 2001. 252 с.

6. Марунич А. В. Захист інформації як основна складова економічної безпеки підприємства. Управління розвитком. 2014. № 14. С. 130-132.

7. Гордієнко С. Б., Микитенко О.С., Данильчук В.Г. Методи та рекомендації забезпечення інформаційної безпеки консалтингової компанії. Вісник ДУІКТ. 2013. № 1. С. 104-107.

8. Ясенев В. Н. Информационная безопасность в экономических системах : учеб. пособ. / В. Н. Ясенев. Н. Новгород: Изд-во ННГУ, 2006. URL: http://ebib.pp.ua/informatsionnaya-bezopasnost-ekonomicheskih88.html.

References

1. Zakon Ukrayini «Pro nacionalnu bezpeku Ukrayini» vid 21.06.2018 r. [Law of Ukraine "On National Security of Ukraine"] № 2469-VIII URL: http://zakon.rada.gov.ua/laws/show/2469-19

2. Mandzinovska H. O., Shtangret A. M., Melnikov O. V. (2016) Finansova bezpeka mashinobudivnogo pidpriyemstva: Metodichni zasadi formuvannya ta zabezpechennya. [Financial security of the machine-building enterprise: Methodical bases of formation and maintenance] 240 s.

3. Yastremskij O. I. (1992) Modelyuvannya ekonomichnogo riziku. [Economic risk modeling] 176 s.

4. Lipkan V. A. , Maksimenko Yu. Ye. , Zhelihovskij V. M. (2006) Informacijna bezpeka Ukrayini v umovah yevrointegraciyi [Information security of Ukraine in the conditions of European integration] K.: KNT, 2006.

5. Golubev, V.O., Havlovskyi, V.D. and Tsymbaliuk, V.S. (2001), Informacijna bezpeka: problemi borotbi zi zlochinami u sferi vikoristannja kompjuternih tehnologij [Information security: challenges to combat crimes in the sphere of computer technologies], zag. red. Kaljuzhnij, R.A., Prosvita, Zaporozhye, Ukraine.

6. Marunich, A.V. (2014), "Information security as a basic component of economic security", Upravlinnja rozvitkom, no. 14, pp. 130-132.

7. Gordiєnko, S.B., Mikitenko, O.S. and Danilchuk, V.G. (2013), "Methods and Recommendations Information security consulting company", Visnik DUIKT, no. 1, pp. 104-107.

8. Jaseniv, V.N. (2006), Informacijna bezpeka v ekonomichnih sistemah [Information security in economic systems], tutorial, NNDU, Novgorod, Russia, available at: http://ebib.pp.ua/informatsionnaya-bezopasnostekonomicheskih88.html.

Рецензія/Peer review : 04.02.2020 Надрукована/Printed : 12.03.2020
Прорецензовано редакційною колегією