УДК 330.322.3.001.25 : 004.056

ЕФЕКТИВНІСТЬ ІНВЕСТИЦІЙ В ІНФОРМАЦІЙНУ БЕЗПЕКУ: ПРОБЛЕМИ І РІШЕННЯ.

Верескун Михайло Вікторович, декан факультету інформаційних технологій, д.е.н., доцент, Державний вищий навчальний заклад «Приазовський державний технічний університет», м. Маріуполь.
Mykhaylo Vereskun, The Dean of the Faculty of Information Technology, Doctor of Economics, Associate Professor, State Higher Educational Institution "Priazovsky State Technical University", m. Mariupol.

Vereskun M. V. The effectiveness of investments in information security: problems and solutions.

The article made a comparative analysis of the main advantages and disadvantages of three methods for determining cost effectiveness of information security of industrial enterprises. Two methods based on the use of aggregate indicators: ROI (Return on Investment - return on investment) for a certain period of time, TCO (Total Cost of Ownership - total cost of ownership of assets. Also used the method developed by Gartner Group. The main advantages of ROI is: the ability to predict results and complexity of IP-used indicators. The main disadvantage is the lack of opportunities to determine the value of the confidential information. The main advantages of the indicator of TCO are: better opportunities to account for all possible costs and the ability to justify the expenditure at different levels of readiness of the protection systems. The main disadvantages of the indicator TCO: problem-lichnosti selection of two projects that both reduce costs and the lack of accounting for the impact of risks. The main advantages of the methodology Gartner Group: accounting for the impact of risks and the ability to determine the effectiveness of system security for all levels of the company. The main disadvantage of this method is that it is based only on the analysis of possible risks.

It is proved that the use of any one technique does not give a complete picture of the effectiveness of spending on information security. The conclusion about the necessity of improvement of existing methodologies for assessing efficiency, the main focus of which is their joint use. To do this, the paper proposed an improved methodological approach to assessing the effectiveness of investments in information security, which is based on the procedures of the optimal choice of the protection system, the risk assessment during implementation of the selected alternative and evaluation capabilities of the enterprise regarding making a certain Fig-cov. To facilitate practical implementation of the developed approach in the article the algorithm of its realization.

Верескун М.В. Ефективність інвестицій в інформаційну безпеку: проблеми і рішення.

У статті зроблено порівняльний аналіз основних переваг і недоліків трьох методик визначення ефективності витрат на інформаційну безпеку промислових підприємств. Дві методики базуються на використанні сукупних показників: ROI (Return on Investment - віддача від інвестицій) за певний період часу, TCO (Total Cost of Ownership - сукупної вартості володіння активів. Також використовується методика, розроблена компанією Gartner Group. Основними перевагами ROI є: можливість прогнозування результатів та комплексність використовуваних показників. Основним недоліком є відсутність можливості визначити вартість конфіденційної інформації. Основними перевагами показника TCO є: найкращі можливості для врахування всіх можливих витрат та можливість обґрунтовувати витрати на різних рівнях готовності систем захисту. Основні

недоліки показника ТСО: проблематичність вибору з двох проектів, якщо обидва ведуть до зниження витрат та відсутність обліку впливу ризиків. Основні переваги методики Gartner Group: врахування впливу ризиків та можливість визначити ефективність системи безпеки для всіх рівнів компанії. Основним недоліком вказаної методики є те, що вона побудована лише на аналізі можливих ризиків.

Доведено, що використання якоїсь однієї методики не дає повної картини щодо ефективності витрат на інформаційну безпеку. Зроблено висновок про необхідність удосконалення існуючих методик оцінки ефективності, основним напрямом якого є сумісне їх використання. Для цього в статті запропоновано удосконалений методичний підхід до оцінки ефективності інвестицій в інформаційну безпеку, який ґрунтується на процедурах оптимального вибору варіанту системи захисту, визначення ступеню ризику при впровадженні обраної альтернативи та оцінки можливостей підприємства щодо прийняття на себе визначених ризиків. Для полегшення практичного впровадження розробленого підходу в статті наведено алгоритм його реалізації.

Верескун М.В. Эффективность инвестиций в информационную безопасность: проблемы и решения.

В статье сделан сравнительный анализ основных преимуществ и недостатков трех методик определения эффективности затрат на информационную безопасность промышленных предприятий. Две методики базируются на использовании совокупных показателей: ROI (Return on Investment - отдача от инвестиций) за определенный период времени, ТСО (Total Cost of Ownership - совокупной стоимости владения активов. Также используется методика, разработанная компанией Gartner Group. Основными преимуществами ROI является: возможность прогнозирования результатов и комплексность используемых показателей. Основным недостатком является отсутствие возможности определить стоимость конфиденциальной информации. Основными преимуществами показателя ТСО являются: лучшие возможности для учета всех возможных затрат и возможность обосновать расходы на разных уровнях готовности систем защиты. Основные недостатки показателя ТСО: проблематичность выбора из двух проектов, если оба ведут к снижению расходов и отсутствие учета влияния рисков. Основные преимущества методики Gartner Group: учет влияния рисков и возможность определить эффективность системы безопасности для всех уровней компании. Основным недостатком указанной методики является то, что она построена лишь на анализе возможных рисков.

Доказано, что использование какой-то одной методики не дает полной картины эффективности затрат на информационную безопасность. Сделан вывод о необходимость усовершенствования существующих методик оценки эффективности, основным направлением которого является совместное их использование. Для этого в статье предложен усовершенствованный методический подход к оценке эффективности инвестиций в информационную безопасность, который основывается на процедурах оптимального выбора варианта системы защиты, определении степени риска при внедрении выбранной альтернативы и оценки возможностей предприятия относительно принятия на себя определенных рисков. Для облегчения практического внедрения разработанного подхода в статье приведен алгоритм его реализации.

Постановка проблеми. В даний час інтенсивно розвиваються інформаційні технології що так само, як глобалізація і становлення інформаційної економіки, відноситься до числа макротенденцій сучасного світового господарства.

За період свого існування, і особливо за останнє десятиліття, у сфері застосування інформаційних технологій відбулися докорінні зміни. Вони принесли бізнесу істотну вигоду, але при цьому зажадали більш серйозної уваги до сфери безпеки з боку урядів,

комерційних підприємств, інших організацій та приватних користувачів, які розробляють інформаційні системи, володіють ними, надають їх у користування, управляють ними, обслуговують або використовують їх.

Актуальність теми дослідження визначається і загостренням проблем інформаційної безпеки в умовах інтенсивного вдосконалення технологій та інструментів захисту даних. Про це свідчать зростання порушень інформаційної безпеки і посилюється тяжкість їх наслідків. Так, загальне число порушень у світі щорічно збільшується більш ніж на 100%. Статистика свідчить також, що якщо комерційна організація допускає витік важливої внутрішньої інформації, то вона в 60% випадках стає банкрутом.

Таким чином, існують чинники, що визначають необхідність зваженого підходу до зазначеної проблеми. До них, в першу чергу, необхідно віднести постійно зростаючу кількість інформаційних загроз і ризиків, а також недостатній рівень забезпечення інформаційної безпеки існуючих інформаційних систем. Інформаційні ризики реалізуються через уразливості сучасних інформаційних систем, що підтримують різні види господарської діяльності промислових підприємств. У даній ситуації виникає необхідність забезпечення інформаційної безпеки соціально-економічної системи в цілому.

Тенденції розвитку промислових підприємств України показують, що керівництво вже приймає деякі заходи щодо захисту важливої інформації, проте ці дії не носять системного характеру, оскільки спрямовані на усунення окремих загроз, що залишають за собою безліч вразливих місць. Також однією з основних причин проблем промислових підприємств у сфері забезпечення інформаційної безпеки є відсутність в даній сфері продуманої та затвердженої політики, що базується на організаційних, економічних і технічних рішеннях з подальшим контролем їх реалізації та оцінкою ефективності. Це визначає необхідність розвитку системи забезпечення інформаційної безпеки промислових підприємств.

Таким чином, є актуальними наукові дослідження, спрямовані на підвищення ефективності управління промисловим підприємством на основі формування системи інформаційної безпеки, здатної забезпечити узгодженість дій.

Аналіз останніх досліджень і публікацій. Над проблемами інформаційної безпеки промислових підприємств працює велика кількість вітчизняних та закордонних вчених. Серед вітчизняних вчених слід виділити праці М. В. Грайворонського, О. М. Новікова [1], С. В. Ленкова, Д. А. Перегудова, В. А. Хорошко [2], В. І. Андреєва, В. С. Чередниченко, М. Є. Шелеста [3], А. Г. Корченко, А.Е. Архипова, С.В. Казмирчук [4]. Серед закордонних вчених можна виділити праці М. Витмана [5], В.А. Галатенко [6], В.И. Завгороднего [7], Д.П. Зегжди та А.М. Івашка [8]. Крім того проблемам інформаційної безпеки присвячена велика кількість інтернет ресурсів [9-13]. Проте, в роботах визначених авторів найбільша увага приділяється технічним та організаційним аспектам формування систем інформаційної безпеки промислових підприємств. Розглядаються підходи до створення комплексної системи захисту інформації, надаються характеристики технічних, програмних методів і засобів інформаційного захисту. Проблемам оцінки економічної ефективності витрат на впровадження систем інформаційної безпеки в практику господарювання промислових підприємств приділяється недостатньо уваги.

Ціллю статі є аналіз переваг та недоліків основних методів визначення ефективності витрат на інформаційну безпеку та розробка пропозицій щодо їх удосконалення**.**

Викладення основного матеріалу статті. Економічне обґрунтування витрат на інформаційну безпеку в багатьох методиках наводиться за допомогою використання сукупних показників: показника ROI (Return on Investment - віддача від інвестицій) за певний період часу, показника TCO (Total Cost of Ownership - сукупної вартості володіння активів), Payback (окупність, період часу, необхідний щоб доходи, отримані в результаті інвестицій, покрили витрати на ці інвестиції).

В процесі розгляду сутності та економічного змісту кожної з методик та можливостей

їх використання для оцінки ефективності вкладень в інформаційну безпеку важливе місце займає аналіз основних недоліків та переваг кожної методики. Результати такого аналізу систематизовані в таблиці 1.

Проведений аналіз дозволяє зробити висновок, що для підвищення якості управлінських рішень щодо визначення ефективності витрат на інформаційну безпеку недостатньо користуватися одною з наведених методик. Основною причиною є той факт, що дві перші методики не враховують ризик, а остання – ґрунтується тільки на аналізі можливих ризиків. Тому в статті пропонується удосконалений методичний підхід до оцінки ефективності інвестицій в інформаційну безпеку, який передбачає сумісне комплексне використання цих методик. Такий підхід дозволить підвищити якість оцінки за рахунок використання переваг кожної з наведених методик. Сема запропонованого підходу наведено на рис. 1.

Слід відзначити, що в межах розробленого підходу пропонується проводити оцінку ефективності в два етапи. На першому етапі за допомогою показників ROI, TCO та Payback проводимо ранжування варіантів вкладень в інформаційну безпеку та визначаємо найкращій з них. На другому етапі проводимо оцінку рівня ризику для визначеного варіанту. На третьому етапі проводиться оцінка спроможності підприємства прийняти на себе означений ризик. Для конкретизації практичних дій в межах удосконаленого підходу в роботі розроблено алгоритм оцінки ефективності інвестицій в інформаційну безпеку (рис. 2). Основною відмінною рисою, що є головною в запропонованому алгоритмі, є те що досить трудомістка процедура оцінки ризиків виконується не для всіх альтернатив, а тільки для однієї, яка була визнана найефективнішою.

Таблиця 1. Переваги та недоліки методик оцінки ефективності вкладень в інформаційну безпеку.

Назва методики	**Переваги**	**Недоліки**
ROI	1) дозволяє спрогнозувати перспективи діяльності на осяжний термін вперед; 2) методика сукупних показників (окупність, прибутковість), що дозволяють оцінити ефективність прийнятого рішення;	1) відсутність визначення вартості конфіденційної інформації та визначення витрат на забезпечення її безпеки; 2) ROI - лише розрахункова частина (можлива наявність видаткової, теоретичної частин для більш ефективного обґрунтування);
TCO	1) кращий метод визначення всіх можливих витрат на забезпечення безпеки ІС (причому облік всіх витрат за статтями); 2) обґрунтування витрат для різних рівнів готовності систем захисту від загроз;	1) проблематичність вибору з двох проектів, які обидва ведуть до зниження витрат при інших рівних умовах; 2) TCO - лише видаткова частина при оцінці ефективності; 3) відсутність обліку впливу ризиків;
Gartner Group	1) при обґрунтуванні враховується вплив можливих ризиків; 2) визначення ефективності безпеки ІС для всіх рівнів компаній.	1) наявність теоретичного обґрунтування і відсутність розрахунків; 2) побудова методу в основному тільки на аналізі можливих ризиків.

Якщо в процесі подальшої оцінки спроможності підприємства брати на себе визначений ризик виявиться, що обраний варіант не може бути впроваджений, керівники підприємства можуть або обрати наступну з проранжованих раніше альтернатив, або

розробити заходи, спрямовані на регулювання ступеню ризику.

Запропонований алгоритм реалізується наступним чином.

1. Визначення показника ROI (Return on Investment - віддача від інвестицій) за певний період часу за формулою:

ROI = (ПРИБУТОК – ВИТРАТИ) / ІНВЕСТИЦІІ

ROI дозволяє оцінити наскільки ефективно працюють вкладені в компанію гроші, тобто скільки грошей «виробляє» за рік кожна гривня, вкладена в компанію. Тобто чим вище показник, тим краще.

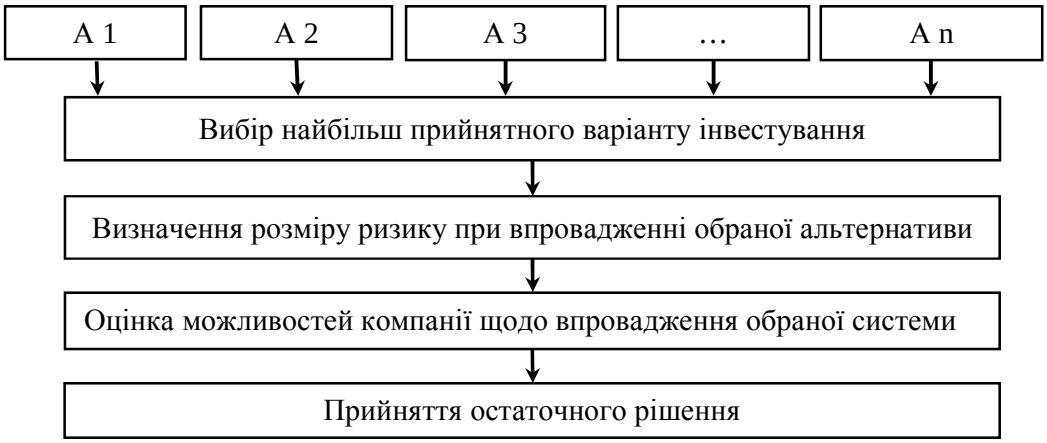

Рисунок 1. Методичний підхід до оцінки ефективності інвестицій в інформаційну безпеку.

2. Розрахунок показника TCO (Total Cost of Ownership - сукупної вартості володіння активів) - це сума прямих і непрямих витрат (за всіма статтями витрат), які несе власник системи протягом усього життєвого циклу експлуатованої системи (завжди вважається для обмеженого періоду часу - і , найчастіше, для 3-х років, адже саме цей час в нормальних умовах функціонує сучасна IT-система).

Тобто це сума витрат:

1) на апаратні засоби і програмне забезпечення;

2) на операції ІС;

3) адміністративні;

4) на операції кінцевих користувачів;

5) на простої.

3. Знаходження показника Payback (окупність) - характеризує період часу, необхідний щоб доходи, отримані в результаті інвестицій, покрили витрати на ці самі інвестиції.

Формула розрахунку терміну окупності інвестицій:

$$PP = \sum_{t=1}^{n} CF \cdot I_0$$

де CF - грошові потоки,

I_o - початкові інвестиції,

n - кількість періодів окупності інвестицій в проект.

Чим менше термін окупності інвестицій, тим привабливіший інвестиційний проект.

4. Застосовується процедура аналіз ризику, що складається з 5 послідовних етапів:

1) Ідентифікація та класифікація об'єктів захисту (ресурсів компанії, які підлягають захисту);

2) Категоріювання ресурсів;

3) Побудова моделі зловмисника;

4) Ідентифікація, класифікація та аналіз загроз і вразливостей;

5) Оцінка ризику.

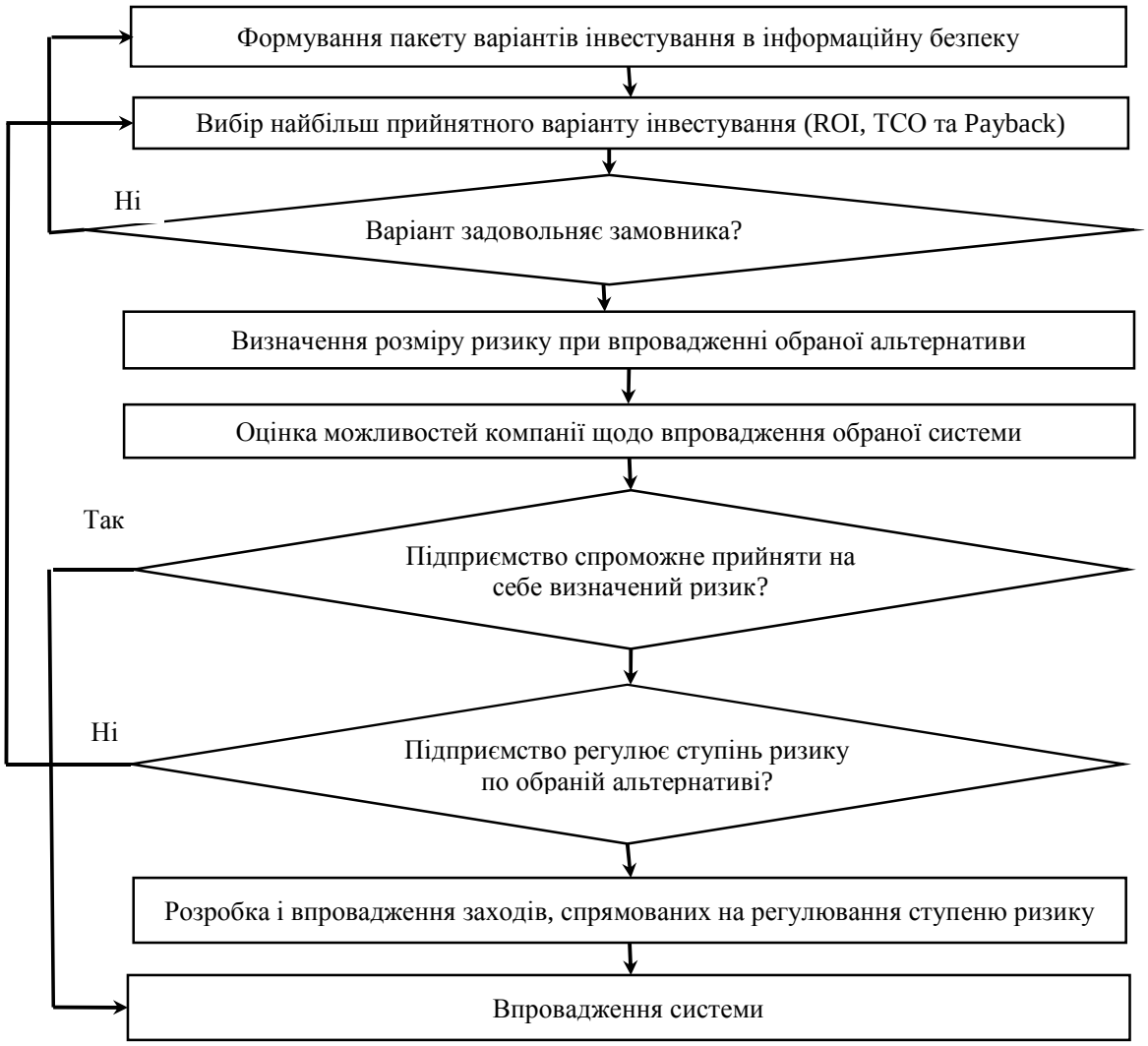

Рисунок 2. Алгоритм реалізації методичного підходу щодо оцінки ефективності інвестицій в інформаційну безпеку.

Після того, як розмір ризику визначено, проводиться оцінка ступеню готовності підприємства прийняти на себе визначений ризик. Взагалі, ця ступінь готовності є показником досить суб'єктивним і залежить, в основному, від схильності ОПР до ризику. Тобто, однакова величина ризику для керівника однієї компанії може бути цілком прийнятною, а для іншого – геть позамежною. Для полегшення прийняття рішення і підвищення рівня його об'єктивності пропонується використовувати відносний показник, який розраховується, як відношення розміру власних коштів підприємства (включаючи амортизацію) до розрахованого рівня ризику. Якщо отримане значення менше, або дорівнює 0,5, то інвестування коштів у обраний варіант є занадто ризикованим. В такому випадку керівництво підприємства має або вжити заходів щодо регулювання ступеню ризику, використовуючи різні інструменти резервування, передачі або зниження ризику, або відмовитися від обраного варіанту інвестицій і повторити процедуру відбору, використовуючи розроблені алгоритми, скоректувавши свої вимоги до системи таким чином, щоб вони співпадали з можливостями підприємства.

Висновки

Результатом проведених досліджень є вирішення важливого наукового завдання щодо удосконалення методики визначення ефективності витрат на інформаційну безпеку промислових підприємств. Основним результатом є удосконалений методичний підхід до оцінки ефективності інвестицій в інформаційну безпеку промислових підприємств, який на відміну від існуючих, передбачає комплексне використання різних методів оцінки ефективності, використання якого дозволить прийняти рішення щодо варіанту здійснення інвестицій з урахуванням рівня ризику та можливостей підприємства щодо його прийняття. Основні висновки по результатам проведеного дослідження зводяться до наступного.

В процесі аналізу економічного змісту існуючих методик оцінки ефективності інвестицій в інформаційну безпеку доведено, що, в залежності від підходу до проведення оцінки, наявні методики спираються або на співвідношення витрат та результатів (ROI, TCO) або на аналіз та оцінку ризиків (Gartner Group).

Виявлено, що кожна з наведених методик окремо є досить ефективним інструментом оцінки, проте основними недоліками існуючих методик є неврахування вартості конфіденційної інформації (ROI), відсутність обліку впливу ризиків (TCO) та побудова лише на результатах аналізу ризиків (Gartner Group).

Запропоновано удосконалений методичний підхід до оцінки ефективності інвестицій в інформаційну безпеку, який на відміну від існуючих, дозволяє оцінити ефективність інвестицій з урахуванням вартості конфіденційної інформації, ступеню ризику та можливостей підприємства щодо його прийняття. В якості інструмента практичної реалізації запропонованого підходу розроблено алгоритм його реалізації, який представляє собою покрокову інструкцію, яка докладно описує послідовність дій в процесі здійснення оцінки з використанням запропонованого підходу.

Список використаних джерел:

1. Грайворонський М. В. Безпека інформаційно-комунікаційних систем : підручник / М. В. Грайворонський, О. М. Новіков ; заг. ред. М. З. Згуровського. – К. : BHV, 2009. – 608 с.
2. Ленков С. В. Методы и средства защиты информации : монография : в 2 т. Т. 2 : Информационная безопасность / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. – К. : Арий, 2008. – 344 с.
3. Основи інформаційної безпеки :підручник / В. І. Андреєв, В. О. Хорошко, В. С. Чередниченко, М. Є. Шелест ; за ред. В. О. Хорошка. – Вид. 2-е, доповн. і переробл. – К. : ДУІКТ, 2009. – 292 с
4. Корченко А.Г. Анализ и оценивание рисков информационной безопасности / А. Г. Корченко, А.Е. Архипов, С.В. Казмирчук. – К.: ООО «Лазурит-Полиграф», 2013. – 275 с.
5. Whitman M. Management of information security /M. Whitman, H. Mattord. – Gengage Learning, 2010. – 592p.
6. Галатенко, В.А. Основы информационной безопасности. - М.: Интуит, 2012.
7. Завгородний, В.И. Комплексная защита информации в компьютерных системах. - М.: Логос, 2013.
8. Зегжда, Д.П., Ивашко, А.М. Основы безопасности информационных систем. - М.: Интуит, 2010.
9. Проект «Информацонная безопаснность бизнеса» [Електроний ресурс]. - Режим доступу: http://www.infosecurity.ru/
10. [Електроний ресурс]. - Режим доступу: http://www.securitylab.ru/.
11. Украинский Информационный Центр Безопасности. [Електроний ресурс]. - Режим доступу: http://www.bezpeka.com/ -
12. Продукты и услуги в области информационной безопасности. [Електроний ресурс]. - Режим доступу: http://www.globaltrust.ru/

References:

1. Grayvoronsky, M.V. and Novikov, O.M. (2009), Security of information and communication systems: the textbook [Bezpeka informatsiyno komunikatsiynih systems: pidruchnik], in Zgurovsky M.Z. (Ed.), Kyiv, 608 p.
2. Lenkov S.V. (2008), Methods and means of information protection: monography:. Vol. 2: Institute of information security, Kyiv, 344 p.
3. Andreev V. I., Khoroshko V.O. and Cherednichenko, V.S .(2009), Fundamentals of Information Security: A Textbook [Basis informatsiynoї bezpeka pidruchnik], in Khoroshki V.O (Ed), Kyiv, 292p.
4. Korchenko A.G. , Arkhipov A.G. and Kazmirchu S.V. (2013), Analysis and evaluation of information security risks, Kyiv,275 p.
5. Whitman M., Mattord H. (2010), Management of information security, Gengage Learning, 592p.
6. Galatenko, V.A. (2013), Fundamentals of Information Security, Intuit, Moscow
7. Zavgorodniy, V.I. (2013), Comprehensive protection of information in computer systems, Logos, Moscow
8. Zegzhda, D.P, Iwashko, A.M. (2010), Fundamentals of Information Systems Security, Intuit, Moscow
9. The "Information security business", available at: http://www.infosecurity.ru/
10. SecurityLab.ru, available at: http://www.securitylab.ru/.
11. Ukrainian Information Security Center, available at: http://www.bezpeka.com/ -
12. Products and services in the field of information security, available at: http://www.globaltrust.ru/
13. Center for Computer Crime Research, available at: http://www.crime-research.ru/.

Ключові слова: інформаційна безпека, інвестиції, ефективність.
Ключевые слова: информационная безопасность, инвестиции, эффективность.
Keywords: information security, investment, efficiency.

Рецензент: В.М. Колосок, д.е.н., доцент, ГВУЗ «Приазовський державний технічний університет».