

ФАКТОРИ ВПЛИВУ НА ПРОЦЕС ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАТИВНОЇ ЕКОНОМІКИ

© 2016 ВАЛУЛЛІНА З. В.

УДК 339.9:330.47

Валулліна З. В. Фактори впливу на процес забезпечення інформаційної безпеки корпоративної економіки

Мета статті полягає в дослідженні факторів, що мають найбільш вагомий вплив на процес забезпечення інформаційної безпеки корпоративної економіки. Для визначення цих факторів у статті використано кореляційно-регресійний метод аналізу. Проаналізовано тенденції кіберзлочинів та їх наслідки в сучасних умовах трансформації світової економіки. Наведено результати кореляційно-регресійного аналізу анкетних даних для побудови економіко-математичної моделі. Визначено вплив факторів на показник інформаційної безпеки корпорацій, встановлено взаємозв'язки між обраними факторними величинами, що впливають на якість та ефективність інформаційної безпеки корпоративної економіки. За результатами проведеного дослідження та кореляційного аналізу було побудовано лінійну кореляційно-регресійну модель, яка найбільш точно та якісно відображає процес забезпечення інформаційної безпеки в корпоративній економіці. Практична значущість побудованої кореляційно-регресійної моделі полягає в оцінюванні та можливості попередити та захистити корпорацію від кібератак.

Ключові слова: інформація, безпека, кібератака, фактори впливу, загрози.

Рис.: 1. **Табл.:** 2. **Формул:** 3. **Бібл.:** 10.

Валулліна Зоряна Володимирівна – кандидат економічних наук, доцент кафедри міжнародної економіки, Національний університет водного господарства та природокористування (вул. Соборна, 11, Рівне, 33028, Україна)

E-mail: zoryanka2006@rambler.ru

УДК 339.9:330.47

Валулліна З. В. Факторы влияния на процесс обеспечения информационной безопасности корпоративной экономики

Цель статьи заключается в исследовании факторов, имеющих наиболее существенное влияние на процесс обеспечения информационной безопасности корпоративной экономики. Для определения данных факторов был использован корреляционно-регрессионный метод анализа. Проанализированы тенденции киберпреступлений и их последствия в современных условиях трансформации мировой экономики. Приведены результаты корреляционно-регрессионного анализа личных данных для построения экономико-математической модели. Определено влияние факторов на показатель информационной безопасности корпораций, установлены взаимосвязи между выбранными факторными величинами, влияющие на качество и эффективность информационной безопасности корпоративной экономики. По результатам проведенного исследования и корреляционного анализа была построена линейная корреляционно-регрессионная модель, которая наиболее точно и качественно отражает процесс обеспечения информационной безопасности в корпоративной экономике. Практическая значимость построенной корреляционно-регрессионной модели заключается в оценке и возможности предупредить и защитить корпорацию от кибератак.

Ключевые слова: информация, безопасность, кибератака, факторы влияния, угрозы.

Рис.: 1. **Табл.:** 2. **Формул:** 3. **Библ.:** 10.

Валулліна Зоряна Владимировна – кандидат экономических наук, доцент кафедры международной экономики, Национальный университет водного хозяйства и природопользования (ул. Соборная, 11, Ровно, 33028, Украина)

E-mail: zoryanka2006@rambler.ru

UDC 339.9:330.47

Valiullina Z. V. The Factors of Influence on the Information Security Process in the Corporate Economy

The article is aimed at studying of the factors that have the most significant impact on the process of ensuring the information security in the corporate economy. To determine these factors, the correlative-regression analysis method has been used. Trends in the cyber crime and its consequences in the current conditions of transformation of the global economy have been analyzed. Results of correlative-regression analysis of personal data, used to build an economical-mathematical model, have been presented. Influence of the factors on the rate of information security of corporations has been determined, the relationships between the selected factor values that impact both the quality and the efficiency of the information security in the corporate economy have been identified. On the basis of results of both the study and the correlation analysis, a linear correlative-regression model has been built, which most precisely and accurately reflects the process of ensuring the information security in the corporate economy. The practical significance of the built correlative-regression model consists in evaluation and opportunity to prevent and protect the corporation against cyber attacks.

Keywords: information, security, cyber attack, factors of influence, threats.

Fig.: 1. **Tabl.:** 2. **Formulae:** 3. **Bibl.:** 10.

Valiullina Zoriana V. – PhD (Economics), Associate Professor of the Department of International Economics, National University of Water Management and Natural Resources Use (11 Soborna Str., Rivne, 33028, Ukraine)

E-mail: zoryanka2006@rambler.ru

В умовах корпоративної економіки інформаційна безпека займає значне місце в розвитку економіки та країни в цілому, а питання її якісного забезпечення стають дедалі актуальнішими.

Корпоративна економіка розвивається в унісон з політичними та соціально-економічними умовами, а тому постійно піддається нестабільному розвитку. Пошук шляхів зниження ризиків та загроз своєму функціонуванню приводить до постійного пошуку адекватних управлінських рішень. Для багатьох суб'єктів корпоративної економіки гострою проблемою в останні роки стала інформаційна безпека підприємства.

Процеси всеохоплюючої інформатизації розвитку країни обумовлюють активний вплив інформаційної безпеки на економічну, соціальну, політичну та інші складові її національної безпеки. Такий нерозривний зв'язок інформаційної та національної безпеки пояснюється так: «захищеність інформації та її повнота впливають на стабільність у суспільстві, забезпечення прав і свобод громадян, правопорядок і, навіть, на збереження цілісності держави» [1, с. 221].

Науковому осмисленню питань інформаційної безпеки сприяли праці таких вчених, як М. Гуцалюка [2], І. Парохонського, Г. Яворської, О. Резнікової, К. Ко-

ноненка [3], В. Конаха, Б. Кормича, В. Ліпкана, Ю. Максименко, А. Марущак, Є. Садовської [4], О.Сазонець, В.Світличної, В. Цимбалюка, О. Юдіна, В. Щербина [1], Р. Юсупова, та ін. Українські вчені досліджують інформаційну безпеку з призми державного управління. Значну увагу приділено становленню інформаційного суспільства, визначенню напрямів розвитку та загроз національній безпеці. Поза увагою науковців не залишилися теоретичні аспекти міжнародно-правових норм та питання щодо співробітництва в розрізі регіональних міжнародних організацій.

Динамічний розвиток економічних, політичних, соціальних подій ХХІ століття сформулювали нове уявлення про інформацію як одного з факторів (ресурсів) виробництва. На макрорівні інформація впевнено займає позиції головного фактора могутності держави, адже здатність держави мати у своєму розпорядженні найсучасніші інформаційні технології дозволяє ефективно управляти інформацією. Володіння державою такою здатністю – шлях до подальшого нарощування своєї економічної міцності [2, с. 2].

Протириччя економічних і політичних інтересів глобальних корпорацій і держав-націй створює нові лінії напруги в міжнародній системі. Малі та слабкі країни можуть протиставити могутності глобальних корпорацій лише силу їх внутрішньої консолідації та групової регіональної інтеграції [3, с. 61].

Негативні тенденції ефективного функціонування корпоративної економіки, а саме, забезпечення їх інформаційної безпеки обумовили актуальність дослідження.

Метою даної статті є дослідження факторів, що мають найбільш вагомий вплив на процес забезпечення інформаційної безпеки корпоративної економіки, а також, використовуючи кореляційно-регресійний метод аналізу, обрати фактори впливу на процес забезпечення інформаційної безпеки корпоративної економіки.

В умовах трансформації світової економіки інформація стала визначальною складовою будь-якої корпорації, значення інформаційної безпеки корпоративної економіки зростає з кожним днем. Виробнича та невиробнича сфери діяльності в умовах сьогодення потребують ефективного інформаційного забезпечення.

Враховуючи тенденції в політиці провідних держав світу щодо протидії загрозам у кіберпросторі та зміну внутрішньої інформаційної політики цих держав, а також посилення компоненти кібербезпеки, більшість держав світу активно модернізують власні сектори безпеки відповідно до викликів сучасності [4].

Розглянемо на прикладі США, які галузі народного господарства є найбільш вразливими та привабливими для кіберзлочинців станом на 2015 р. (рис. 1).

Варто зазначити, що цілями кібератак у 2015 р. у США стає фінансовий сектор та банки, на які припадає 28,33 млн дол. Компанії фінансового сектора постійно перебувають під прицілом кіберзлочинців. Банківські організації прикладають максимум зусиль, щоб захистити свій бізнес і зберегти хороші відносини з клієнтами. Друге місце займає енергетика та комунальне господарство. Хакерські атаки були націлені на енергетичні



Рис. 1. Середні річні втрати від кіберзлочинців, млн дол. [5]

об'єкти та завдали втрат на 27,6 млн. дол. Кібератаки спрямовуються через автоматизовані системи управління, які використовуються для ефективного функціонування повсякденних суспільно-економічних відносин, структур економіки чи органів влади.

Варто зауважити, що кібератаки відбуваються по всьому світі щоденно у незначних масштабах. Кібератаки у XXI ст. стали звичайним явищем, як переглянути власну електронну скриньку, і впродовж останніх 12 місяців практично кожна галузь народного господарства по всьому світу була схильна до якогонебудь типу кіберзагроз. Вони можуть бути спрямовані проти інфраструктури урядів, військових організацій, корпорацій та суспільно-економічних відносин.

Слід зазначити, що Будапештська Конвенція, як основоположний документ у сфері боротьби з кіберзлочинністю, надає умовну класифікацію кіберзлочинів, що поділяються на такі категорії [6, с. 8]:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (так звані «СІА-злочини»), зокрема:

- ✦ незаконний доступ, наприклад, шляхом злому, обману та іншими засобами;
- ✦ нелегальне перехоплення комп'ютерних даних;
- ✦ втручання в дані, включаючи навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це;
- ✦ втручання в систему, включаючи навмисне створення серйозних перешкод функціонуванню комп'ютерної системи, наприклад, шляхом розподілених атак на ключову інформаційну інфраструктуру;
- ✦ зловживання пристроями, тобто виготовлення, продаж, придбання для використання, розповсюдження пристроїв, комп'ютерних програм, комп'ютерних паролів або кодів доступу з метою здійснення «СІА-злочинів»;

2) правопорушення, пов'язані з комп'ютерами, включаючи підробку і шахрайство, здійснені з використанням комп'ютерів;

3) правопорушення, пов'язані зі змістом інформації, зокрема дитяча порнографія, расизм та ксенофобія;

4) правопорушення, пов'язані з порушенням авторських і суміжних прав, наприклад, незаконне відтворення і використання комп'ютерних програм, аудіо/відео й інших видів цифрової продукції, а також баз даних і книг.

Оцінювання факторів впливу на процес забезпечення інформаційної безпеки в корпоративній економіці варто проводити за певною розробленою послідовністю:

- ✦ дослідження літературних джерел і статистичних матеріалів з інформаційної безпеки у світі з метою попереднього відбору факторів, що впливають на процес забезпечення інформаційної безпеки корпоративної економіки;
- ✦ вибір факторів, що впливають на процес забезпечення інформаційної безпеки в корпоративній економіці;

- ✦ розробка анкети стандартизованого інтерв'ю для фахівців щодо впливу на процес забезпечення інформаційної безпеки корпоративної економіки;
- ✦ обробка анкети стандартизованого інтерв'ю та оцінка рівня взаємних рекомендацій експертів;
- ✦ визначення тісноти зв'язку між факторами (X) та результативною ознакою – інформаційною безпекою корпоративної економіки (Y) за допомогою коефіцієнта кореляції;
- ✦ виявлення основних факторів впливу на процес забезпечення інформаційної безпеки корпоративної економіки.

Для емпіричного дослідження інструментів регулювання та визначення напрямів забезпечення інформаційної безпеки корпоративної економіки було розроблено спеціальний інструментарій – анкету стандартизованого інтерв'ю. Зауважимо, що результати анкетування залежать від правильності та зручності розроблення анкети. У процесі підготовки анкети стандартизованого інтерв'ю враховувалися: структура та послідовність запитань, використання відкритих і закритих запитань, коректне та логічне формулювання запитань, пропорційність градацій у відповідях, проміжок часу заповнення анкети. Відзначимо, що переважна більшість запитань анкети стандартизованого інтерв'ю розроблена з урахуванням думки респондентів, що дозволяє максимально об'єктивно дати відповідь на поставлене запитання.

Уданому дослідженні вибірку становили співробітники наукових установ, працівники органів державного управління, програмісти, співробітники банківських установ, співробітники корпорацій, працівники робітничих професій та студенти, які безпосередньо є користувачами інформаційних технологій та професійно орієнтовані на аналітичну базу вирішення напрямів забезпечення інформаційної безпеки. Вік досліджуваних – від 16 до 76 років, в анкеті знайшли чільне місце допоміжні відомості про респондентів, які відображають об'єктивну характеристику опитуваних (вид діяльності, освіта, стать та дохід). Усього у дослідженні взяло участь 100 експертів.

Респонденти, що взяли участь в опитуванні, обиралися методом взаємних рекомендацій з оцінкою їх узгодженості. До участі в анкетуванні залучались експерти, рівень взаємних рекомендацій яких перевищував 69%, що є достатнім для формування не випадкової експертної групи та за коефіцієнтом конкордації Кендела.

Проведене анкетування з питань доцільності запровадження інформаційної безпеки в корпоративній економіці та огляд наукової літератури дали можливість виділити такі фактори впливу на процес забезпечення інформаційної безпеки корпоративної економіки:

- ✦ рівень антивірусного забезпечення;
- ✦ навчання користувачів;
- ✦ сканери безпеки;
- ✦ взаємодію керівництва та персоналу;
- ✦ системи виявлення атак;
- ✦ резервне копіювання;
- ✦ нормативне забезпечення;

- ✦ криптографія;
- ✦ моделі безпеки;
- ✦ персонал.

Використовуючи кореляційно-регресійний метод економічного аналізу, можемо визначити основні фактори впливу на процес забезпечення інформаційної безпеки в корпоративній економіці.

Кореляційний та регресійний методи аналізу вирішують три основні завдання:

- ✦ визначення за допомогою рівнянь регресії аналітичну форму зв'язку між варіацією ознак X та Y ;
- ✦ знаходження і статистичне оцінювання рівняння зв'язку між результативною і факторною ознаками на підставі регресивного аналізу;
- ✦ інтерпретація отриманого рівняння та його використання [7].

Для розробки регресійної моделі використаємо стандартний алгоритм її побудови. Результати проведеного анкетування запишемо у вигляді матриці X , розміром $m \times n$, а у вигляді вектора-стовпця Y – результативну ознаку:

$$Y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_h \end{pmatrix}; X = \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1m} \\ x_{21} & x_{22} & \dots & x_{2m} \\ \dots & \dots & \dots & \dots \\ x_{n1} & x_{n2} & \dots & x_{nm} \end{pmatrix}. \quad (1)$$

Зазначимо, що комплексну взаємодію всіх досліджуваних чинників (X_1, X_2, \dots, X_n) з результативним показником (Y) можна описати за допомогою математичної моделі у вигляді рівняння лінійної множинної регресії:

$$Y = a_0 + a_1 X_1 + a_2 X_2 + \dots + a_n X_n, \quad (2)$$

де Y – залежна змінна; X_1, X_2, \dots, X_n – незалежні змінні; a_0, a_1, \dots, a_n – параметри моделі [8, с. 465].

Використовуючи стандартний пакет прикладної програми MS Excel (компонент «Пакет аналізу»), визначимо вплив досліджуваних факторів на інформаційну безпеку корпорації (Y).

За допомогою кореляційних матриць та кореляційних зв'язків здійснюється відсів факторів які найменше впливають на Y . Доцільно виділити тісноту зв'язку між множинами X та Y за допомогою коефіцієнта кореляції r , кількісне значення яких доцільно обмежити відповідними інтервалами оцінки (табл. 1) [9, с. 218].

Таблиця 1

Шкала інтервалу оцінки коефіцієнта кореляції	
Тіснота зв'язку	Інтервал оцінки
Зв'язок відсутній	$r = 0$
Зв'язок слабкий	$0 \leq r < 1/3$
Зв'язок середній	$1/3 \leq r < 2/3$
Зв'язок сильний	$2/3 \leq r < 1$
Зв'язок повний	$ r = 1$

Джерело: складено за даними [10, с. 14].

Для проведення кореляційного аналізу пропонуємо розглянути десять факторів впливу на показник інформаційної безпеки корпорацій. За результатами проведеного кореляційно-регресійного аналізу для інформаційної безпеки корпоративної економіки було виявлено чотири найбільш впливових фактори: рівень антивірусного забезпечення (0,91); нормативне забезпечення (0,51); персонал (0,95); резервне копіювання (0,88).

Побудова багатофакторної регресійної моделі за відібраними чотирма найважливішими факторами впливу на інформаційну безпеку корпоративної економіки дозволяє кількісно відобразити вплив факторів на інформаційну безпеку корпоративної економіки (Y). За результатами регресійного аналізу було побудовано математичну модель у вигляді рівняння лінійної множинної регресії

$$Y = -1,69 - 0,039 \cdot X_1 + 0,348 \cdot X_2 + 0,456 \cdot X_3 + 0,499 \cdot X_4. \quad (3)$$

Згенеровані результати регресійної статистики, що найбільш повно характеризують отриману кореляційно-регресійну модель, яка побудована для визначення найважливіших факторів впливу на інформаційну безпеку корпоративної економіки, представлено в табл. 2.

Коефіцієнт множинної кореляції R для інформаційної безпеки корпоративної економіки дорівнює 0,95, що свідчить про сильний зв'язок між факторами впливу та результативною ознакою даної моделі. Значення коефіцієнта множинної детермінації R^2 дорівнює 0,906. Отриманий результат R^2 вказує, що на 90,6% інформаційна безпека корпорацій обумовлюється відібраними вищезазначеними факторами, а 9,4% відображають інші відібрані фактори даної моделі.

Таблиця 2

Результати моделювання інформаційної безпеки

Показник	Коефіцієнт регресії	Стандартна помилка	t-статистика
Y-перетин	-1,69875	0,279374	-6,08056
Чинник X_1	0,039114	0,036062	1,084651
Чинник X_2	0,348376	0,056076	6,212594
Чинник X_3	0,45682	0,080543	5,671757
Чинник X_4	0,499895	0,086124	5,80438
Множинний R	0,95187		
R^2	0,90605		
Нормований R^2	0,90210		
Стандартна похибка	0,29292		
Спостереження	100		

Джерело: складено та розраховано автором.

ВИСНОВКИ

Таким чином, в умовах корпоративної економіки корпорації пристосовують свою діяльність до ризиків та факторів невизначеності. Однією з основних загроз

сьогодення є кібератака, а відтак, інформаційна безпека корпорації займає одне з першочергових значень та потребує до себе значної уваги. Очевидно, що сучасна соціально-економічна, політична та суспільна складові зумовляють необхідність боротьби з кіберзлочинністю.

Проведений кореляційний аналіз десяти факторів впливу на інформаційну безпеку корпоративної економіки (Y) дав змогу визначити найбільш впливові фактори впливу на процес забезпечення інформаційної безпеки корпоративної економіки. За результатами кореляційного аналізу було побудовано лінійну кореляційно-регресійну модель, яка найбільш точно та якісно відображає процес забезпечення інформаційної безпеки в корпоративній економіці. Практична значущість побудованої кореляційно-регресійної моделі полягає в оцінюванні та можливості попередити та захистити корпорацію від кібератак. ■

ЛІТЕРАТУРА

1. **Щербина В. М.** Інформаційне забезпечення економічної безпеки підприємств та установ / В. М. Щербина // Актуальні проблеми економіки. – 2006. – № 10. – С. 220–225.
2. **Гуцалюк М.** Інформаційна безпека України: нові загрози / М. Гуцалюк // Бизнес и безопасность. – 2003. – № 5. – С. 2–3.
3. **Парахонський Б. О.** Міжнародне безпекове середовище: виклики і загрози національній безпеці України. Аналітична доповідь / Б. О. Парахонський, Г. М. Яворська, О. А. Резнікова; за ред. К. А. Кононенка. – К.: НІСД, 2013. – 64 с.
4. **Садовська Є. В.** Міжнародний досвід у боротьбі із загрозами інформаційній безпеці – уроки для України [Електронний ресурс] / Є. В. Садовська. – Режим доступу: http://www.dsaua.org/index.php?option=com_content&view=article&id=185%3A2013-05-12-18-06-49&catid=66%3A2010-12-13-08-48-53&Itemid=90&lang=uk
5. The Statistics Portal [Electronic resource]. – Mode of access: <http://www.statista.com/>
6. Департамент фінансових розслідувань. Кіберзлочинність та відмивання коштів [Електронний ресурс]. – Режим доступу: <http://minfin.kmu.gov.ua/file/link/396800/file/tipolog2013.pdf>
7. **Лопатюк Р. І.** Прогнозування рівня інвестиційної діяльності підприємств аграрної сфери [Електронний ресурс] / Р. І. Лопатюк // Ефективна економіка. – 2013. – № 4. – Режим доступу: <http://www.economy.nayka.com.ua/?op=1&z=1967>
8. Економіко-математичне моделювання: навчальний посібник / За ред. О. Т. Іващука. – Тернопіль: ТНЕУ «Економічна думка», 2008. – 704 с.
9. **Валіулліна З. В.** Моделювання технологічного оновлення підприємств пасажирського автомобільного транспорту за допомогою кореляційно-регресійного аналізу / З. В. Валіулліна // Вісник Дніпропетровського ун-ту. Серія: Економіка. – Дніпропетровськ, 2014. – № 2. – С. 216–221.
10. **Тимейчук О. Ю.** Математичні методи і моделі в розрахунках на ЕОМ: інтерактивний комплекс навч.-метод. забезпечення / О. Ю. Тимейчук. – Рівне: НУВГП. – 2009. – 58 с.

REFERENCES

"Departament finansovykh rozsliduvan. Kiberzlochynnist ta vidmyvannia koshtiv" [The Department of financial investigations. Cybercrime and money laundering]. <http://minfin.kmu.gov.ua/file/link/396800/file/tipolog2013.pdf>

Ekonomiko-matematychnе modeliuвання [Economic-mathematical modeling]. Ternopil: TNEU; Ekonomichna dumka, 2008.

Hutsaliuk, M. "Informatsiina bezpeka Ukrainy: novi zahrozy" [Information security of Ukraine: new threats]. *Biznes i bezopasnost*, no. 5 (2003): 2-3.

Lopatiuk, R. I. "Prohnozuvannia rinvnia investytsiinoi diialnosti pidpriemstv ahranoi sfery" [Forecasting the level of investment activity of the enterprises of agrarian sphere]. <http://www.economy.nayka.com.ua/?op=1&z=1967>

Parakhonskyi, B. O., Yavorska, H. M., and Reznikova, O. A. *Mizhnarodne bezpekove seredovyshe: vyklyky i zahrozy natsionalnii bezpetsi Ukrainy* [International security environment: challenges and threats to national security of Ukraine]. Kyiv: NISD, 2013.

Shcherbyna, V. M. "Informatsiine zabezpechennia ekonomichnoi bezpeky pidpriemstv ta ustanov" [Information support of economic security of enterprises and institutions]. *Aktualni problemy ekonomiky*, no. 10 (2006): 220-225.

Sadovska, Ye. V. "Mizhnarodnyi dosvid u borotbi iz zahrozamy informatsiinii bezpetsi - uroky dlia Ukrainy" [International experience in combating information security threats - lessons for Ukraine]. http://www.dsaua.org/index.php?option=com_content&view=article&id=185%3A2013-05-12-18-06-49&catid=66%3A2010-12-13-08-48-53&Itemid=90&lang=uk

The Statistics Portal. <http://www.statista.com/>

Tymeichuk, O. Yu. *Matematychni metody i modeli v rozrakhunkakh na EOM: interaktyvni kompleks navchalno-metodychnoho zabezpechennia* [Mathematical methods and models in calculations on computer: interactive complex of teaching-methodological support]. Rivne: NUVHP, 2009.

Valiullina, Z. V. "Modeliuвання tekhnolohichnoho onovlennia pidpriemstv pasazhyrskoho avtomobilnoho transportu za dopomohoiu koreliatsiino-rehesiinoho analizu" [Modeling of technological renovation of passenger automobiles enterprises by using correlation and regression analysis]. *Visnyk Dnipropetrovskoho un-tu. Serija «Ekonomika»*, no. 2 (2014): 216-221.