

ДОСЛІДЖЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВ УКРАЇНИ ЗА ДОПОМОГОЮ ДИСПЕРСІЙНОГО АНАЛІЗУ

© 2016 САЗОНЕЦЬ О. М., КАЧАН О. І.

УДК 339.9:330.47

Сазонець О. М., Качан О. І. Дослідження загроз інформаційній безпеці підприємств України за допомогою дисперсійного аналізу

Метою статті є проведення дослідження інформаційної безпеки підприємств України за допомогою дисперсійного аналізу. У зв'язку з розширенням видів інформаційної діяльності в корпоративному середовищі зростає і кількість видів захисту від інформаційної небезпеки. Розглянуто поняття й базові категорії економічної безпеки. Виявлено, що інформаційна безпека корпоративної економіки суспільно-економічних відносин полягає в боротьбі з уразливістю корпоративних комп'ютерів, зі зломом смартфонів працівників корпорації, а також у необхідності виявлення й ліквідації шкідливих програм, у запобіганні загрози користувачам WI-FI. Серед загроз інформаційній безпеці виділено уразливість комп'ютерних систем, яку розподілено по видах. Проведено дослідження ставлення українців до загроз інформаційній безпеці. Розглянуто шкоду, яку завдають корпоративним інформаційним системам низький рівень інформатизації фінансово-кредитної системи, промисловості, сільського господарства і т. ін. та використання неліцензійного програмного забезпечення для обробки інформації.

Ключові слова: інформатизація суспільства, інформаційна безпека, експертне опитування, дисперсійний аналіз.

Рис.: 3. **Табл.:** 6. **Формул.:** 16. **Бібл.:** 11.

Сазонець Ольга Миколаївна – доктор економічних наук, професор, академік АЕН України, академік АГН України, завідувачка кафедри міжнародної економіки, Національний університет водного господарства та природокористування (вул. Соборна, 11, Рівне, 33028, Україна)

E-mail: onsaz@mail.ru

Качан Олена Іванівна – асистент, кафедра міжнародної економіки, Національний університет водного господарства та природокористування (вул. Соборна, 11, Рівне, 33028, Україна)

E-mail: olena.kachan@oa.edu.ua

УДК 339.9:330.47

UDC 339.9:330.47

Сазонець О. М., Качан О. І. Исследование угроз информационной безопасности предприятий Украины с помощью дисперсионного анализа

Целью статьи является проведение исследования информационной безопасности предприятий Украины с помощью дисперсионного анализа. В связи с расширением видов информационной деятельности в корпоративной среде растет и количество видов защиты от информационной опасности. Рассмотрены понятие и базовые категории экономической безопасности. Выведено, что информационная безопасность корпоративной экономики общественно-экономических отношений заключается в борьбе с уязвимостью корпоративных компьютеров, со взломом смартфонов работников корпорации, а также с необходимостью выявления и ликвидации вредоносных программ и предотвращения угрозы пользователям WI-FI. Среди угроз информационной безопасности выделена уязвимость компьютерных систем, которая распределена по видам. Проведено исследование отношения украинцев к угрозам информационной безопасности. Рассмотрен вред, который наносят корпоративным информационным системам низкий уровень информатизации финансово-кредитной системы, промышленности, сельского хозяйства и т. д. и использование неліцензійного програмного обеспечения для обработки информации.

Ключевые слова: информатизация общества, информационная безопасность, экспертный опрос, дисперсионный анализ.

Рис.: 3. **Табл.:** 6. **Формул.:** 16. **Библ.:** 11.

Сазонець Ольга Николаевна – доктор экономических наук, профессор, академик АЭН Украины, академик АГН Украины, заведующая кафедрой международной экономики, Национальный университет водного хозяйства и природопользования (ул. Соборная, 11, Ровно, 33028, Украина)

E-mail: onsaz@mail.ru

Качан Елена Ивановна – ассистент, кафедра международной экономики, Национальный университет водного хозяйства и природопользования (ул. Соборная, 11, Ровно, 33028, Украина)

E-mail: olena.kachan@oa.edu.ua

Sazonets O. M., Kachan O. I. Studying the Information Security Threats to Ukrainian Enterprises by Using Variance Analysis

The article is aimed at studying the information security of enterprises of Ukraine by using variance analysis. Along with the expansion of types of information activities in the corporate environment, the number of kinds of protection from the information danger is growing on. Both the concept and the basic categories of economic security have been considered. It has been found that information security of the corporate economy of the socio-economic relations is called to counter the vulnerability of corporate computers, breaking into the smart-phones of employees of corporation, as well as there's a need to identify and eliminate malware and to prevent threats to users of WI-FI. Among the information security threats, vulnerability of computer systems has been allocated, which has been divided by types. A study on attitude of Ukrainians to the information security threats has been carried out. The detriment caused to corporate information systems through the low level of informatization of financial-credit system, industry, agriculture, etc., as well as usage of unlicensed software for information processing have been considered.

Keywords: informatization of society, information security, expert survey, variance analysis.

Fig.: 3. **Tbl.:** 6. **Formulae:** 16. **Bibl.:** 11.

Sazonets Olga M. – D. Sc. (Economics), Professor, Academician of the Academy of Economic Sciences of Ukraine, Academician of the Academy of Mining Sciences of Ukraine, Head of the Department of International Economics, National University of Water Management and Natural Resources Use (11 Soborna Str., Rivne, 33028, Ukraine)

E-mail: onsaz@mail.ru

Kachan Olena I. – Assistant, Department of International Economics, National University of Water Management and Natural Resources Use (11 Soborna Str., Rivne, 33028, Ukraine)

E-mail: olena.kachan@oa.edu.ua

Поняття загрози інформаційної безпеки зародилося майже в той самий час, що й інформаційне середовище. Спочатку це були прояви крадіжки інформації з комп'ютера, незаконне використання,

зпсування інформації на комп'ютерах. Пізніше, з розвитком інформаційних мереж, інформаційна безпека перетворилася в засоби перекачування по мережі неправдивої інформації, вірусів. Але це поки що йшлося

про безпеку корпоративної інформації. Зараз питання безпеки відноситься майже до всіх агентів глобального інформаційного середовища. Україна, як активний учасник процесів циклу життя інформації, не стоїть осторонь. Це відбувається як на загальному міжкраїновому рівні, так і всередині кожного окремого підприємства.

Розглядом інформаційної безпеки займалися багато вітчизняних і зарубіжних учених. У роботі Кормича Б. А. досліджуються організаційно-правові питання цієї тематики [1]. Кавун С. В., А. А. Пилипенко, Д. О. Ріпка представили систему консолідованої інформації щодо підприємницької діяльності. [2]. У книзі подано поняття й базові категорії економічної безпеки. Досліджено ризики як чинники, які загрожують економічній безпеці суб'єкта підприємницької діяльності, та управління ними. Економічну безпеку підприємства структуровано та розроблено поняття індикаторів економічної безпеки. Оцінено безпеку економічного простору функціонування підприємства. Запропоновано теоретичні положення щодо сформованої системи управління економічною безпекою підприємства. Хансен Ф. та Олешчук В. А. висвітили процес розвитку економіки та політики виборчого управління доступом до комп'ютерної системи [3]. Що стосується розгляду питань праці та захисту даних на комп'ютерах підприємства, то тут репрезентовано роботу Борисова М. А. [4]. Щербаковим А. Ю. яскраво представлено стан і розвиток економічної інформаційної безпеки [5].

Аналіз представлених наукових робіт з питань інформаційної безпеки показав недостатність дослідження потенційних загроз для українських корпорацій. Саме тому *метою* статті є проведення дослідження інформаційної безпеки за допомогою дисперсійного аналізу.

У зв'язку з розширенням видів інформаційної діяльності в корпоративному середовищі зростає і кількість видів захисту від інформаційної небезпеки. На *рис. 1* представлено схему інформаційної безпеки корпоративної економіки та суспільно-економічних відносин.

Роздивимось процес боротьби з інформаційною небезпекою на прикладі боротьби з уразливістю корпоративних комп'ютерів. Будь-яка компанія націлена на володіння новими, досконалими програмами, у чому неабияку роль відіграє реклама. Знову поставлена на комп'ютер програма може бути досить уразливою. Наприклад, дослідник з інформаційної безпеки Тавіс Орманді винайшов серйозну уразливість в ПЗ компанії Symantec. Програмне забезпечення надавало дозвіл зловмисникові з легкістю отримати віддалений доступ до комп'ютера, де воно встановлено.

Програми Comodo Firewall та Comodo Internet Security також мають серйозну уразливість. У програмі Geek Buddy була знайдена помилка, яка використовувалася при наданні платної технічної підтримки користувачам, з'єднуючи їх з бюро технічної підтримки. Пізніше було виявлено, що це з'єднання не мало захист паролем. З часом творці програмного забезпечення усунули помилку завдяки Тавісу Орманді [7].

Такі недоліки має й операційна система Linux. За словами кіберекспертів з компанії Perception Point, уразливість присутня у версіях ядра цієї операційної системи, починаючи з версії 3.8. За допомогою функції адміністратора ця вразливість дозволяла користувачам, а також програмам в обхід заборон отримати повний доступ до неї. Як результат – десятки мільйонів комп'ютерів потрапили в небезпеку. В зоні ризику опинилися також володарі мобільних телефонів, які використовують ОС Android, тому що вона заснована на ядрі Linux [8].

Уразливість була виявлена і щодо недешевої комп'ютерної техніки компанії Apple Mac, в якій працівники компанії Legba Core знайшли вразливі місця. Неполадки були усунені до оголошення про інцидент широкому колу користувачів. Завдяки цьому компанія Apple купила Legba Core. Тепер користувачі можуть не боятися використовувати комп'ютери Mac.

Бувають також уразливості, які знаходяться в комп'ютерах впродовж довгого часу і не виявляються. Так, у програмному забезпеченні процесора Intel виявлена вразливість, що існувала там протягом 18 років. Це дозволяло хакерам встановлювати на комп'ютери «вічні» віруси, що життєздатні довгий час. Вони порушували роботу персональних комп'ютерів. Компанія виявила і ліквідувала проблему для останнього покоління



Рис. 1. Схема інформаційної безпеки корпоративної економіки та суспільно-економічних відносин [6]

комп'ютера, також вона випустила патч (*патч* – автоматизований програмний засіб, що окремо постачається і використовується для усунення проблем в ПЗ або для зміни його функціонального призначення) для чіпів попередніх поколінь. Однак не завжди його застосування приводить до «вилікування» комп'ютерів.

Уразливості мають великий набір типів (рис. 2).

Кількість, разів

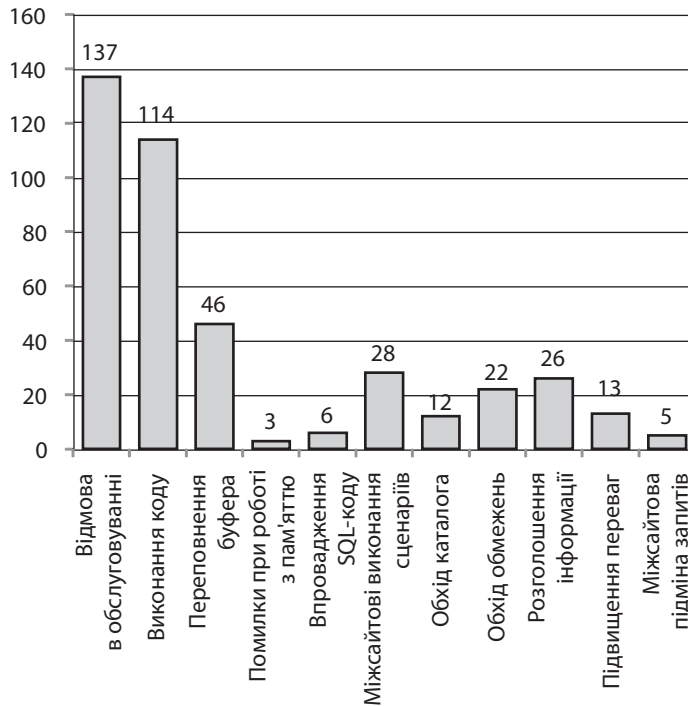


Рис. 2. Розподіл кількості уразливостей за типом [9]

Для проведення дослідження впливу заходів інформаційної безпеки на стан корпоративного середовища було проведено опитування експертів з питань інформаційної безпеки корпоративної економіки в місті Рівне. Метою дослідження було виявлення особливості збирання достовірної інформації та можливих потенційних загроз у сфері інформаційної безпеки в корпорації.

Експертам необхідно було дати оцінку питанням щодо характеристики способів отримання інформації та інформаційної безпеки. Було проведено аналіз цих відповідей і розроблено систему рекомендацій щодо напрямів підвищення безпеки в інформаційній сфері на підприємствах України.

Опитування було проведено серед спеціалістів у галузі економіки, а саме, бухгалтерів, спеціалістів у зовнішньоекономічній діяльності, у менеджменті, маркетингу, а також інших спеціальностей. Питання були пронумеровані залежно від тематики проблеми. Наведемо приклад питань, що були задані респондентам:

1.5. На вашу думку, чи є достовірною інформація, яка міститься в ресурсах Інтернет?

- Абсолютно недостовірною
- Практично недостовірною.
- Частково достовірною.
- Практично достовірною.

Є найголовнішим ресурсом отримання достовірної інформації.

1.6. Як часто Ви користуєтесь ресурсами Інтернету для збору необхідної інформації?

- Використовую майже завжди.
- Використовую досить часто.
- Рідко використовую.

- Практично не використовую.
- Зовсім не використовую.

Також були задані питання щодо можливості реальних інформаційних загроз українській корпорації:

2.4. На Вашу думку, які можливі реальні загрози інформаційній безпеці України для національних корпорацій:

	Абсолютно неможливо	Практично неможливо	Скоріше неможливо	Скоріше можливо	Можливо
2.4.1. Невикористання науково-технічних досягнень					
2.4.2. Низький рівень інформатизації фінансово-кредитної системи, промисловості, сільського господарства і т. ін.					
2.4.3. Використання неліцензійного програмного забезпечення для обробки інформації					
2.4.4. Можливість настання монополізації на ринку інформаційних ресурсів					

Представимо частину дослідження, що використовує інструменти дисперсійного аналізу.

Дисперсійний аналіз – це аналіз мінливості ознаки під впливом будь-яких змінних факторів. В іноземній літературі дисперсійний аналіз часто позначається як ANOVA, що переводиться з англійської як аналіз варіативності. Автором цього методу є Р. А. Фішер [10, с. 224].

Задача дисперсійного аналізу полягає в тому, щоб із загальної варіативності ознаки вичленили варіативність троякого роду:

- 1) варіативність, обумовлену дією кожної з досліджуваних незалежних змінних;
- 2) варіативність, обумовлену взаємодією досліджуваних незалежних змінних;
- 3) випадкову варіативність, обумовлену всіма іншими незалежними змінними.

Варіативність, обумовлена дією досліджуваних змінних та їх взаємодією, співвідноситься з випадковою варіативністю. Показником цього співвідношення є критерій F Фішера (формули (1) – (3)).

$$F_{емпА} = \frac{\text{Варіативність, обумовлена змінною } A}{\text{Випадкова варіативність}}; \quad (1)$$

$$F_{емпВ} = \frac{\text{Варіативність, обумовлена змінною } B}{\text{Випадкова варіативність}}; \quad (2)$$

$$F_{емпА,В} = \frac{\text{Варіативність, обумовлена змінними } A \text{ і } B}{\text{Випадкова варіативність}}. \quad (3)$$

Представимо послідовність операцій в однофакторній моделі дисперсійного аналізу для зв'язаних вибірок.

- 1) Розраховується варіативність ознаки, обумовлена дією досліджуваного фактора:

$$SS_{факт} = \frac{1}{n} \sum T_c^2 - \frac{1}{n} (\sum x_i)^2, \quad (4)$$

де T_c – сума індивідуальних значень по кожній з умов;
 c – кількість умов (градаций фактора);
 n – кількість випробуваних у кожній групі (в кожній з умов);

N – загальна кількість індивідуальних значень;

x_i – кожне індивідуальне значення.

- 2) Визначаємо параметр $SS_{досл}$:

$$SS_{досл} = \frac{1}{c} \sum T_n^2 - \frac{1}{N} (\sum x_i)^2. \quad (5)$$

- 3) Підраховуємо загальну варіативність ознаки:

$$SS_{заг} = \sum x_i^2 - \frac{1}{N} (\sum x_i)^2. \quad (6)$$

- 4) Розраховуємо варіативність, обумовлену неврахованими факторами, випадкову чи остаточну варіативність:

$$SS_{вин} = SS_{заг} - SS_{факт} - SS_{досл}. \quad (7)$$

- 5) Розраховується число ступенів свободи:

$$df_{факт} = c - 1; \quad (8)$$

$$df_{досл} = n - 1; \quad (9)$$

$$df_{заг} = N - 1; \quad (10)$$

$$df_{вин} = df_{заг} - df_{факт} - df_{досл}. \quad (11)$$

- 6) Визначаємо «середній квадрат» – математичне очікування суми квадратів, усереднену величину відповідних SS:

$$MS_{факт} = \frac{SS_{факт}}{df_{факт}}; \quad (12)$$

$$MS_{досл} = \frac{SS_{досл}}{df_{досл}}; \quad (13)$$

$$MS_{вин} = \frac{SS_{вин}}{df_{вин}}. \quad (14)$$

- 7) Підраховуємо значення F і визначимо df_1 за чисельником і df_2 за знаменником:

$$F_{факт} = \frac{MS_{факт}}{MS_{вин}}; \quad (15)$$

$$F_{досл} = \frac{MS_{досл}}{MS_{вин}}. \quad (16)$$

- 8) Визначаємо критичні значення F згідно з таблицями.

- 9) Зіставляємо емпіричні значення F з критичними:

$F_{емп} < F_{кр}$ – гіпотеза H_0 приймається;

$F_{емп} \geq F_{кр}$ – гіпотеза H_0 відкидається [10].

Задомогою модуля дисперсійного аналізу ANOVA у програмі Statistica порівнюємо середні в групах [11, с. 133]. Визначимо внутрішньогрупові описові статистики і кореляції для залежних змінних у кожній з декількох груп, визначених однією чи більшою кількістю незалежних змінних, що групують. Порівнюємо середні та визначимо, в яких саме групах середні відрізняються між собою. Як нульова гіпотеза передбачається, що середні у групах рівні. У *табл. 1* представлені описові статистики для змінних відповідно до пунктів анкети 2.4.2, 2.4.3 (стовпчики таблиці (3) – (8)). Незалежними змінними, що групують, є номер за назвою спеціальності та результати відповіді на пункт анкети 1.6 (стовпчики таблиці (1) – (2)). У стовпцях (3), (6) міститься інформація про значення середніх щодо результатів обробки відповідей на питання згідно з пунктами анкети 2.4.2, 2.4.3 відповідно, у стовпчиках (4), (7) – кількість позитивних відповідей по цих пунктах, у стовпчиках (5), (8) – середньоквадратичне відхилення щодо результатів обробки відповідей на питання згідно з цими пунктами.

Ми бачимо, що найбільше середнє по пункту 2.4.2 для бухгалтерів, які практично не використовують Інтернет. Тобто ці спеціалісти вважають скоріше можливим низький рівень інформатизації фінансово-кредитної системи, промисловості, сільського господарства і т. ін. у корпораціях України. Водночас бухгалтери, що досить часто використовують Інтернет, загрозу використання неліцензійного програмного забезпечення для обробки інформації вважають не цілком реальною. Спеціалісти із зовнішньоекономічної діяльності, що використовують Інтернет майже завжди, розглядають низький рівень інформатизації фінансово-кредитної системи, промисловості, сільського господарства як можливу загрозу не повною мірою. Також треба зауважити, що

Описові статистики для змінних відповідно до пунктів анкети 2.4.2, 2.4.3

Breakdown Table of Descriptive Statistics (Таблиця з даними) N = 150 (Nomissingdata in dep. var. list)							
Спеціальність	1.6	2.4.2 – Means	2.4.2 – N	2.4.2 – Std. Dev.	2.4.3 – Means	2.4.3 – N	2.4.3 – Std. Dev.
1	2	3	4	5	6	7	8
1	1	3,333333	9	1,414214	3,666667	9	0,707107
1	2	3,750000	12	1,138180	3,416667	12	1,311372
1	3		0			0	
1	4	4,000000	1	0,000000	2,000000	1	0,000000
2	1	3,600000	40	0,810191	3,825000	40	0,843907
2	2	3,133333	15	0,990430	3,666667	15	0,723747
2	3		0			0	
2	4	4,000000	1	0,000000	3,000000	1	0,000000
3	1	3,433333	30	1,006302	3,300000	30	1,235956
3	2	3,529412	17	0,943242	3,352941	17	0,996317
3	3	4,000000	1	0,000000	5,000000	1	0,000000
3	4		0			0	
4	1	3,666667	3	1,527525	3,333333	3	1,527525
4	2		0			0	
4	3		0			0	
4	4		0			0	
5	1	3,625000	8	1,060660	4,000000	8	0,755929
5	2	3,500000	12	1,000000	3,333333	12	1,154701
5	3		0			0	
5	4	3,000000	1	0,000000	2,000000	1	0,000000
All Groups		3,506667	150	0,974484	3,546667	150	1,027061

більшою мірою вони вважають за таку використання нелицензійного програмного забезпечення для обробки інформації. Менеджери, які рідко використовують Інтернет, вважають, що низький рівень інформатизації фінансово-кредитної системи, промисловості, сільсько-го господарства загрожує у повній мірі інформаційній безпеці України для національних корпорацій. Щодо використання нелицензійного програмного забезпечення для обробки інформації, то тут вони висловилися досить однозначно в бік її можливості. Середньо можливою загрозою з боку низького рівня інформатизації фінансово-кредитної системи, промисловості, сільсько-го господарства вважають маркетологи, що використовують Інтернет майже завжди. Такою ж вони вважають загрозу, пов'язану з використанням нелицензійного програмного забезпечення для обробки інформації.

Проведемо процедуру апостеріорного порівняння середніх (табл. 2).

Бачимо, що вірогідності на перекресленні усіх стовпчиків і усіх рядків більше, ніж 0,05, що говорить про виконання гіпотези про рівність середніх у групах. Із загального висновку випадають середні по пунктах, де пусті клітинки. Наприклад, для спеціалістів у зовнішньоекономічній діяльності, які рідко використовують Інтернет; для менеджерів, які практично не використовують Інтернет; для маркетологів, що використовують

його досить часто, рідко використовують, практично не використовують Інтернет.

Представимо графічно ці висновки за допомогою діаграми розмаху (рис. 3), що візуалізує ступінь схожості та відмінності середніх у групах, що аналізуються.

Як можна побачити, для спеціалістів-бухгалтерів, спеціалістів із зовнішньоекономічної діяльності, менеджерів середні приблизно однакові для різного ступеня використання Інтернету, тобто відповіді щодо загрози з боку використання нелицензійного програмного забезпечення для обробки інформації не відрізняються. Водночас ставлення до цієї проблеми з боку спеціалістів інших спеціальностей інше.

Проведемо кореляційний аналіз по групах бухгалтерів, що відповіли позитивно на питання, чи завжди вони використовують Інтернет для збору необхідної інформації, відповідно для відповідей на питання анкети 2.4.2 та 2.4.3 (табл. 3).

З табл. 3 видно, що відповіді бухгалтерів, які майже завжди використовують Інтернет, на запитання анкети щодо реальності загрози інформаційній безпеці в корпораціях України відносно низького рівня інформатизації фінансово-кредитної системи, промисловості, сільсько-го господарства і т. ін. та використання нелицензійного програмного забезпечення для обробки інформації сла-

Таблиця 2

Вірогідності щодо виконання гіпотези про рівність середніх у групах

	LSD Test; Variable: 2.4.2 (Таблиця з даними) Marked differences are significant at $p < ,05000$																			
Спец. 1.6	{1} - M = 3,3333	{2} - M = 3,7500	{3} - M = 0,0000	{4} - M = 4,0000	{5} - M = 3,6000	{6} - M = 3,1333	{7} - M = 0,0000	{8} - M = 4,0000	{9} - M = 3,4333	{10} - M = 3,5294	{11} - M = 4,0000	{12} - M = 0,0000	{13} - M = 3,6667	{14} - M = 0,0000	{15} - M = 0,0000	{16} - M = 0,0000	{17} - M = 3,6250	{18} - M = 3,5000	{19} - M = 0,0000	{20} - M = 3,0000
1 1 {1}	0,345			0,527	0,470	0,635		0,527	0,792	0,6347	0,5277		0,6175				0,5489	0,7057		0,7520
1 2 {2}	0,345			0,810	0,648	0,113		0,810	0,355	0,5590	0,8103		0,8973				0,7843	0,5409		0,4719
1 3 {3}																				
1 4 {4}	0,527	0,810			0,693	0,402		1,000	0,577	0,6478	1,0000		0,7730				0,7239	0,6313		0,4802
2 1 {5}	0,470	0,648		0,693		0,125		0,693	0,490	0,8075	0,6930		0,9113				0,9485	0,7614		0,5540
2 2 {6}	0,635	0,113		0,402	0,125			0,402	0,343	0,2650	0,4023		0,4000				0,2629	0,3449		0,8973
2 3 {7}																				
2 4 {8}	0,527	0,810		1,000	0,693	0,401			0,577	0,6478	1,0000		0,7730				0,7239	0,6313		0,4802
3 1 {9}	0,792	0,355		0,577	0,490	0,343		0,577		0,7518	0,5777		0,7003				0,6304	0,8453		0,6702
3 2 {10}	0,634	0,559		0,647	0,807	0,265		0,647	0,751		0,6478		0,8266				0,8237	0,9378		0,6073
3 3 {11}	0,527	0,810		1,000	0,693	0,402		1,000	0,577	0,647			0,7730				0,7239	0,6313		0,4802
3 4 {12}																				
4 1 {13}	0,617	0,897		0,773	0,911	0,400		0,773	0,700	0,8266	0,7730						0,9509	0,7964		0,5642
4 2 {14}																				
4 3 {15}																				
4 4 {16}																				
5 1 {17}	0,548	0,784		0,723	0,948	0,262		0,723	0,630	0,8237	0,7239		0,9509					0,7843		0,5562
5 2 {18}	0,705	0,540		0,631	0,761	0,344		0,631	0,845	0,9378	0,6313		0,7964				0,7843			0,6313
5 3 {19}																				
5 4 {20}	0,752	0,471		0,480	0,554	0,897		0,480	0,670	0,6073	0,4802		0,5642				0,5562	0,6313		

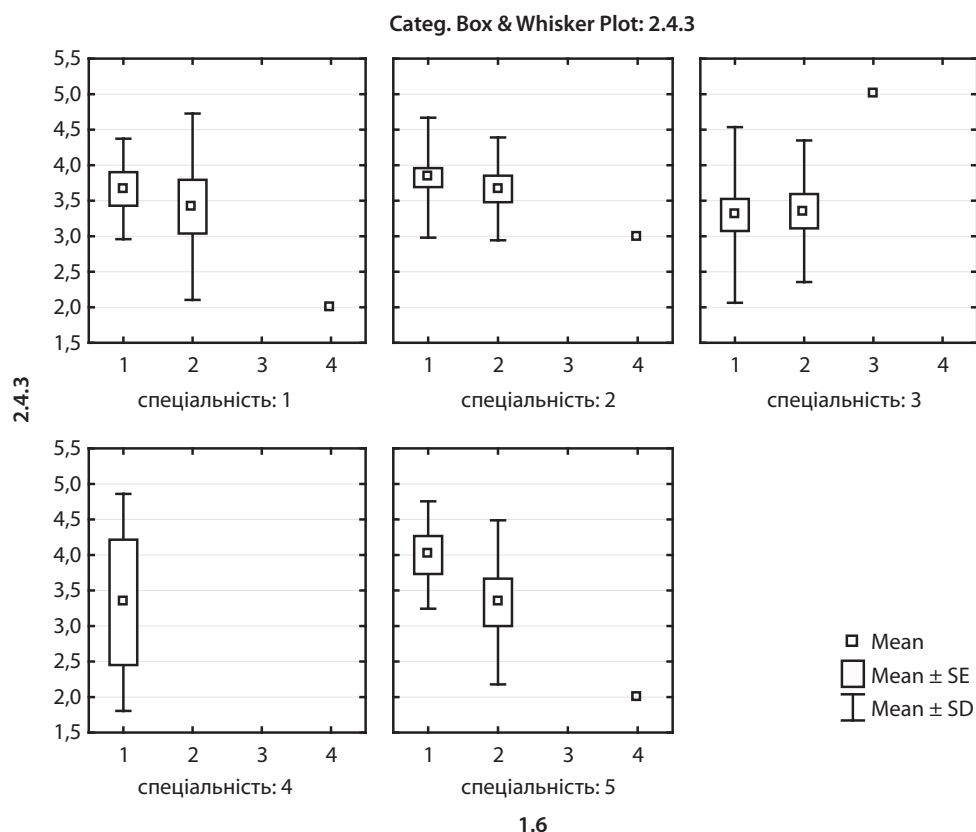


Рис. 3. Діаграма розмаху за пунктом 1.6 анкетування по різних спеціальностях для відповідей на питання 2.4.3 анкети

бо корелюють між собою. Такого ж висновку ми дістаємо для спеціалістів із зовнішньоекономічної діяльності (табл. 4). У цьому випадку зв'язок ще менший.

Для економістів-міжнародників, що використовують досить часто Інтернет, по відповідях на ці запитання кореляція висока (табл. 5).

Таблиця 3

Внутрішньогрупові кореляції та коваріації при дослідженні відповідей на питання запропонованої анкети бухгалтерів (відповідь на запитання анкети 1.6 – 1)

Within-Group Correlations (Таблиця з даними) Group: спеціальність: 1 1.6:1 Marked correlations are significant at $p < ,05000$		
	2.4.2	2.4.3
2.4.2	1,000000	0,500000
2.4.3	0,500000	1,000000

Таблиця 4

Внутрішньогрупові кореляції та коваріації при дослідженні відповідей на питання запропонованої анкети для спеціалістів із зовнішньоекономічної діяльності (відповідь на запитання анкети 1.6 – 1)

Within-Group Correlations (Таблиця з даними) Group: спеціальність: 2 1.6:1 Marked correlations are significant at $p < ,05000$		
	2.4.2	2.4.3
2.4.2	1,000000	0,045002
2.4.3	0,045002	1,000000

Таблиця 5

Внутрішньогрупові кореляції та коваріації при дослідженні відповідей на питання запропонованої анкети для спеціалістів із зовнішньоекономічної діяльності (відповідь на запитання анкети 1.6 – 2)

Within-Group Correlations (Таблиця з даними) Group: спеціальність: 2 1.6:2 Marked correlations are significant at $p < ,05000$		
	2.4.2	2.4.3
2.4.2	1,000000	0,664309
2.4.3	0,664309	1,000000

Найбільшою є кореляція по відповідях маркетологів, які використовують досить часто Інтернет, на запитання анкети щодо реальності загрози інформаційній безпеці в корпораціях України відносно низького рівня інформатизації фінансово-кредитної системи, промисловості, сільського господарства і т. ін. та використання неліцензійного програмного забезпечення для обробки інформації (табл. 6).

Таблиця 6

Внутрішньогрупові кореляції та коваріації при дослідженні відповідей на питання запропонованої анкети для маркетологів (відповідь на запитання анкети 1.6 – 2)

Within-Group Correlations (Таблиця з даними) Group: спеціальність: 3 1.6:2 Marked correlations are significant at $p < ,05000$		
	2.4.2	2.4.3
2.4.2	1,000000	0,786333
2.4.3	0,786333	1,000000

ВИСНОВКИ

Таким чином, проведено дослідження щодо загроз інформаційній безпеці для українських корпорацій. Структуровано типи загроз. Серед загроз інформаційній безпеці виділено таку загрозу, як уразливість комп'ютерних систем. Цю загрозу розподілено по видах. Проведено дослідження ставлення українців до загроз інформаційній безпеці. Розглянуто, якої шкоди корпоративним інформаційним системам завдають низький рівень інформатизації фінансово-кредитної системи, промисловості, сільського господарства і т. ін. та використання нелицензійного програмного забезпечення для обробки інформації. ■

ЛІТЕРАТУРА

- 1. Кормич Б. А.** Організаційно-правові основи політики інформаційної безпеки України: автореф. дис. ... д-ра юрид. наук: 12.00.07. Харків: НУВС України, 2004. 41 с.
- 2. Кавун С. В., Пилипенко А. А., Ріпка Д. О.** Економічна та інформаційна безпека підприємств у системі консолідованої інформації: навч. посіб. Харків: ХНЕУ, 2013. 362 с.
- 3. Hansen F., Oleshchuk V. A.** Conformance Checking of RBAC Policy and Its Implementation // *The First Information Security Practice and Experience Conference*. Singapore: LNCS. 2005. Vol. 3439. P. 144–155.
- 4. Борисов М. А.** Особенности защиты персональных данных в трудовых отношениях. М.: Книжный дом «ЛИБРОКОМ», 2013. 224 с.
- 5. Щербак А. Ю.** Современная компьютерная безопасность. Теоретические основы. Практические аспекты. М.: Книжный мир, 2009. 352 с.
- 6. Sazonets O., Valiullina Z.** Evaluation of information security of corporative economics. LAP LAMBERT Academic Publishing, 2016. 60 p.
- 7.** Уязвимость в Comodo позволяла удаленно захватить компьютер. URL: <http://prostotech.com/internet/95-uyazvimost-v-comodo-pozvoljala-udalennno-zahvatit-kompyuter.html>
- 8.** Уязвимость в Linux поставила под удар десятки миллионов компьютеров. URL: <https://lenta.ru/news/2016/01/20/linuxfail/>
- 9.** Популярное сетевое оборудование и статистика уязвимостей // SecurityLab.ru. URL: <http://www.securitylab.ru/analytics/423523.php>
- 10. Сидоренко Е. В.** Методы математической обработки в психологии. СПб.: Речь, 2006. 350 с.
- 11. Халафян А. А.** Statistica 6. Статистический анализ данных: учебник. 2-е изд., перераб. и доп. М.: ООО «Бином-Пресс», 2010. 528 с.

REFERENCES

- Borisov, M. A. *Osobennosti zashchity personalnykh dannykh v trudovykh otnosheniyakh* [Features of personal data protection in labour relations]. Moscow: LIBROKOM, 2013.
- Hansen, F., and Oleshchuk, V. A. "Conformance Checking of RBAC Policy and Its Implementation". In *The First Information Security Practice and Experience Conference*. Vol. 3439. 144-155. Singapore: LNCS, 2005.
- Kavun, S. V., Pylypenko, A. A., and Ripka, D. O. *Ekonomichna ta informatsiina bezpeka pidpriemstv u systemi konsolidovanoi informatsii* [Economic and information security of enterprises in the system of consolidated information]. Kharkiv: KhNEU, 2013.
- Kormych, B. A. "Orhanizatsiino-pravovi osnovy polityky informatsiinoi bezpeky Ukrainy" [Legal framework the information

security policy of Ukraine]. avtoref. dys. ... d-ra iuryd. nauk: 12.00.07, 2004.

Khalafian, A. A. *Statistica 6. Statisticheskii analiz dannykh* [Statistica 6. Statistical analysis of data]. Moscow: Binom-Press, 2010.

"Populiarnoye setevoye oborudovaniye i statistika uyazvimostey" [Popular network equipment and statistics of vulnerabilities]. SecurityLab.ru. <http://www.securitylab.ru/analytics/423523.php>

Sazonets, O., and Valiullina, Z. *Evaluation of information security of corporative economics*: LAP LAMBERT Academic Publishing, 2016.

Sidorenko, E. V. *Metody matematicheskoy obrabotki v psikhologii* [Methods of mathematical processing in psychology]. St. Petersburg: Rech, 2006.

Shcherbakov, A. Yu. *Sovremennaya kompyuternaya bezopasnost. Teoreticheskiye osnovy. Prakticheskiye aspekty* [Modern computer security. The theoretical foundations. Practical aspects]. Moscow: Knizhnyy mir, 2009.

"Uyazvimost v Linux postavila pod udar desyatki millionov kompyuterov" [Vulnerability in Linux jeopardized tens of millions of computers]. <https://lenta.ru/news/2016/01/20/linuxfail/>

"Uyazvimost v Comodo pozvoljala udalennno zakhvatit kompyuter" [Vulnerability in Comodo was allowed to remotely hijack the computer]. <http://prostotech.com/internet/95-uyazvimost-v-comodo-pozvoljala-udalennno-zahvatit-kompyuter.html>