

*І. М. Сисоєва,*

*д. е. н., доцент, професор кафедри економіки обліку та оподаткування, Вінницький навчально-науковий інститут економіки Західноукраїнського національного університету  
ORCID ID: <https://orcid.org/0000-0003-0567-1658>*

*В. В. Роледець,*

*к. е. н., доцент, доцент кафедри фінансів, страхування та банківської справи, Вінницький навчально-науковий інститут економіки Західноукраїнського національного університету  
ORCID ID: <https://orcid.org/0000-0002-6653-6583>*

*О. М. Ціхановська,*

*к. е. н., доцент кафедри економіки, обліку та оподаткування, Вінницький навчально-науковий інститут економіки Західноукраїнського національного університету  
ORCID ID: <https://orcid.org/0000-0002-1276-9891>*

DOI: 10.32702/2306-6814.2023.22.46

# ІНФОРМАЦІЙНИЙ МЕНЕДЖМЕНТ У ЦИРКУЛЯРНІЙ ЕКОНОМІЦІ: НЕБЕЗПЕЧНІ ЗАГРОЗИ Й УРАЗЛИВОСТІ

*I. Sysoeva,*

*Doctor of Economic Sciences, Associate Professor,  
Professor of the Department of Economics, Accounting and Taxation, Vinnytsia Educational  
and Scientific Institute of Economics of the West Ukrainian National University*

*V. Roleders,*

*PhD in Economics, Associate Professor,  
Associate Professor of the Department of Finance, Insurance and Banking, Vinnytsia Educational  
and Scientific Institute of Economics of the West Ukrainian National University*

*O. Tsikhanovska,*

*PhD in Economics, Associate Professor,  
Associate Professor of the of the Department of Economics, Accounting and Taxation,  
Vinnytsia Educational and Scientific Institute of Economics of the West Ukrainian National University*

## INFORMATION MANAGEMENT IN THE CIRCULAR ECONOMY: DANGEROUS THREATS AND VULNERABILITIES

---

***У статті досліджено спрощену модель та принципи циркулярної економіки.***

***Метою статті є виявлення притаманних для циклової економіки загроз та уразливостей для інформаційного менеджменту.***

***Доведено, що використовуючи ІТ-технології під час війни, в управлінні підприємством, велику роль має захист інформації. Інформація сьогодні — цінний ресурс, від якого залежить як функціонування підприємства в цілому, так і його конкурентоспроможність. Загроз безпеки інформаційних ресурсів підприємства багато — це і комп'ютерні віруси, які можуть знищити важливі дані, і промислове шпигунство з боку конкурентів переслідують своєю метою отримання незаконного доступу до інформації є комерційною таємницею, і багато іншого. Тому особливе місце набуває діяльність по захисту інформації, щодо забезпечення інформаційної безпеки***

***Здійснено класифікацію основних видів загроз й уразливостей для інформаційного менеджменту.***

**Introduction.** The key trend in the development of modern world civilization is the use of digital technologies. This is confirmed by the digital transformation of industry, logistics, the sales system, service, etc.

The purpose of the article is to identify the threats and vulnerabilities inherent in the cyclical economy for information management.

The results. Global policies and standards such as extended producer responsibility laws will improve visibility and traceability throughout the value chain and support the development of responsible technology device practices around the world. Using IT technologies during the war, information protection plays an important role in enterprise management. Information today is a valuable resource on which both the functioning of the enterprise as a whole and its competitiveness depend. There are many threats to the security of the company's information resources, including computer viruses that can destroy important data, industrial espionage by competitors pursuing illegal access to information that is a trade secret, and much more. That is why information protection activities, in order to ensure information security, take a special place.

Conclusions. The circular model of the economy is the opposite of the traditional, linear model. While the linear economy implies "take, make and dispose", the circular economy is to "take, make, recycle, restore, reuse, reduce waste, minimize costs, switch to renewable energy sources". The circular economy is inextricably linked to the formation of new business models focused on reducing the amount of resources used, implementing reuse or a closed cycle of production, restoration, redesign, recycling and recycling to ensure a long life cycle. There are many threats to the security of a company's information resources, including computer viruses that can destroy important data, industrial espionage by competitors who pursue illegal access to information that is a trade secret, and much more. Analyzing the importance of information support for the enterprise in making the right management decisions, it is worth noting that the further state, development, and future success of the enterprise depends on what the management decision will be.

*Ключові слова:* циркулярна економіка, інформаційний менеджмент, діджиталізація, загрози, уразливості.  
*Key words:* circular economy, information management, digitalization, threats, vulnerabilities.

## ПОСТАНОВКА ПРОБЛЕМИ

Протягом 2010—2023 рр. ринок був насичений пристроями, що підтримують усі аспекти роботи та повсякденного життя. Результатом є ринок, схильний до падіння цін і коротких циклів інновацій. Поява хмари і великих об'ємів даних призвели до розширення технологічної інфраструктури, а саме великомасштабних центрів обробки даних. Потреби в інфраструктурі зростатимуть по мірі розвитку, наприклад, штучний інтелект (ШІ), буде вимагати більшої обчислювальної потужності, пам'яті та швидкості Інтернету. Паралельно бездротові мережі 5G нового покоління вимагають оновлення апаратного та програмного забезпечення глобальної мережевої інфраструктури.

Крім того, перехід до низьковуглецевої економіки в поєднанні з тенденціями для покращення досвіду користувача сприятиме зростанню обсягу електроніки, наприклад, як у розумних приладах, транспортних засобах, а також у виробництві вітрової та сонячної енергії.

Ключовою тенденцією розвитку сучасної світової цивілізації є застосування цифрових технологій. Підтвердженням цьому слугує цифрова трансформація промисловості, логістики, системи продаж, сервісу тощо. Експерти фінансового ринку прогнозують, що дохід економіки від проявів цифрової трансформації сягне у наступні 5 років до позначки — 30 трлн USD.

Разом з цим експерти стверджують, що такий стан справ вимагатиме суттєвої трансформації, власне, й інформаційно-телекомунікаційної індустрії. Більшою мірою це стосуватиметься автоматизованих систем (АС), включених в контури управління інформаційними та/або технологічними процесами (ІТП), а також інформаційними ресурсами (ІР), які в умовах кібернетичних втручань і загроз забезпечують необхідні послуги та/або сервіси. Негативними наслідками такої трансформації може бути виникнення нових ризиків для безпеки.

Таким чином, визначення цільового спрямування інформаційного менеджменту доцільно розглядати через формування інформаційного суспільства, яке відбувається з використанням інформаційних технологій.

## АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Дослідженню проблем формування та розвитку інформаційного менеджменту присвячені праці багатьох як закордонних так і вітчизняних науковців. О. Матвієнко, М. Цивін [3], Ф. Machlup [4], М. Дворнік [5], О. Повідайчик [6]. Однак, в умовах переходу від традиційної економіки до відновлювальної, формування інформаційного менеджменту потребує теоретико-методичного обґрунтування процесів впливу інформації на відтворення життєдіяльності суспільства.

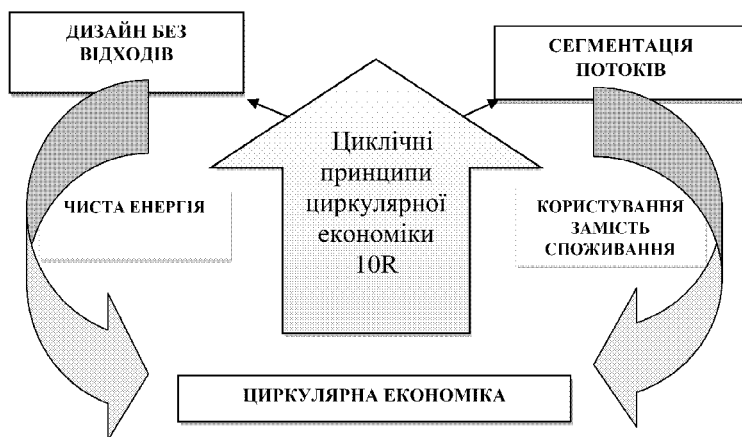


Рис. 1. Спрощена модель циркулярної економіки

Враховуючи мету зазначеного дослідження доцільно навести сутність інформаційного менеджменту. У сучасній науці управління існує безліч підходів до визначення цього поняття. Наведемо один з них. Так поняття "інформаційний менеджмент" визначає широкий спектр видів діяльності, пов'язаних з інформаційними ресурсами, управлінням інформаційними потоками, технологіями і управлінською діяльністю загалом [3, с. 27].

Зазначимо, що власне визначення терміну "інформаційний менеджмент" і досі перебуває у стадії наукових пошуків, хоча виокремилися певні підходи до його розуміння. Поняття "інформаційний менеджмент" вживається у таких значеннях:

1. Управління за допомогою інформації, тобто інформаційне управління (управлінська технологія).
2. Управління власне інформацією (управління інформаційними потоками та інформаційними ресурсами) для оптимізації роботи.
3. Управління процесами інформатизації, тобто управління інформаційною технологією (автоматизована технологія обробки інформації в певній предметній галузі).

Інформаційний менеджмент (ІМ) — це спеціальна область менеджменту, що виділилася як самостійний напрям в кінці 1970-х рр. Сфера інформаційного менеджменту — сукупність всіх видів інформації, необхідної для управління на всіх етапах життєвого циклу підприємства. При цьому визначається не тільки цінність і ефективність використання власне інформації (даних і знань), але і інших ресурсів підприємства, в тій чи іншій мірі входять в контакт з інформацією: технологічних, кадрових, фінансових і т.д. Починаючи з 1992 р. термін "інформаційне суспільство" стали вживати багато західних країн. Відповідно до визначення Єврокомісії, згідно з яким інформаційним називається суспільство, в якому діяльність людей здійснюється на основі послуг, наданих за допомогою інформаційних технологій і технологій зв'язку [6].

В інформаційному суспільстві панування сфери послуг, тобто науки, освіти, охорони здоров'я, культури призводить до створення умов для всебічного розвитку людини, її розумових і фізичних здібностей. Інформаційне суспільство — це вкладення капіталів в людину, оскільки її науковий, освітній і професійний рівень, а також її знання є джерелом суспільного прогресу. Уні-

кальність поняття інформаційного суспільства полягає не лише у тому, що воно носить глобальний характер, а ще й у тому, що воно пов'язане з множиною новітніх категорій: інформація, інформатизація, інформативність, віртуалізація, економіка знань, тощо [6].

### МЕТА СТАТТІ

Метою статті є виявлення притаманних для циклової економіки загроз та уразливостей для інформаційного менеджменту.

### ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Пристрої інформаційних та комунікаційних технологій мають відносно короткий термін служби, оскільки споживачі прагнуть

легкого доступу до новітніх технологій за мінімально можливих витрат. На технологічних підприємствах сервери замінюються в середньому кожні три-п'ять років. Ця тенденція передчасної заміни існуючих продуктів на новіші моделі призводить до двох основних типів відходів.

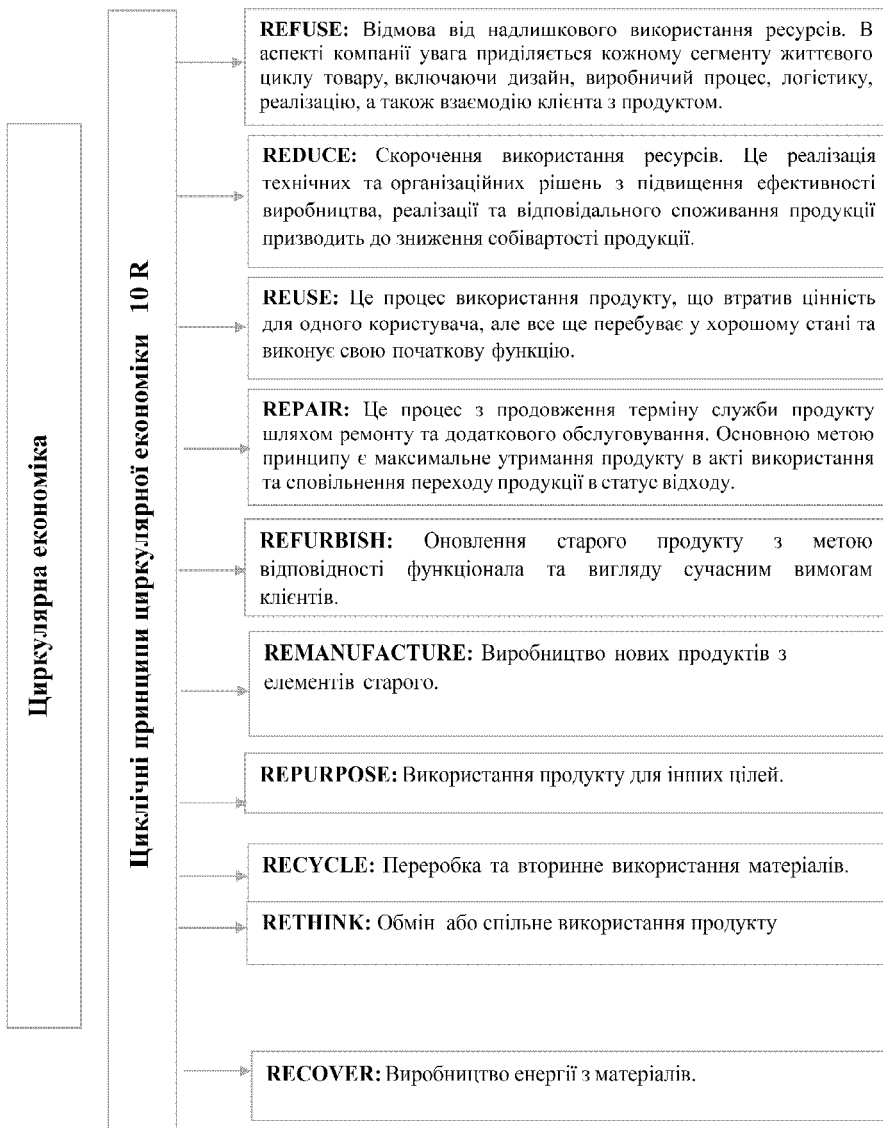
По-перше, це витрачені життєві цикли. Через різке зростання попиту на останні технології, відмінно функціонуючі пристрої та обладнання часто замінюються. Хоча в середньому люди користуються смартфонами лише 22 місяці, потенційне використання цих пристроїв набагато довше (понад 5 років).

Другий тип відходів — це вбудована цінність. Більшість пристроїв інформаційно-комунікаційних технологій, технологічного обладнання підприємства та апаратного забезпечення мережевої інфраструктури містять цінні матеріали, з яких відновлюється максимум 20%. Цьогорічна вартість сировини в глобальних потоках електронних відходів оцінюється в 55 млрд євро.

Індустрія ІКТ має багато сфер можливостей, якими можна скористатися. Відновлення та повторне використання існуючих ІКТ-пристроїв ілюструє першу область можливостей.

Українське інформаційне суспільство та його інфраструктура, хоча і сформовані з урахуванням виділених об'єктів і суб'єктів, що склалися у світовій практиці цього процесу, але відображають соціально — економічні, політичні, культурні, ментальні, побутові та інші риси, притаманні Україні в її нинішньому стані. Ці риси мають зазнати великих змін, щоб перейти до рівня відносин справді інформаційного суспільства, що приводить до специфічних, суто українських шляхів, стратегій та заходів подальшого розвитку інформаційного суспільства.

Отже, циркулярна економіка, яку ще називають економікою замкненого циклу, — це нова модель економічного розвитку, що передбачає відновлення, повторне використання, раціональне споживання ресурсів і дозволяє створити додаткову цінність. Циркулярна економіка спрямована, насамперед, на збереження енергії, економічно чисте виробництво та споживання. Циркулярна модель економіки є протилежною традиційній, лінійній моделі. В той час, як лінійна економіка має на увазі "взяти, зробити і позбутися", економіка циркулярна полягає у тому, щоб "взяти, зробити, переробити, відновити, використати ще раз, знизити рівень відходів,



**Рис. 2. Циклічні принципи циркулярної економіки 10R**

Джерело: сформовано на основі джерела [8].

мінімізувати витрати, перейти до відновлюваних джерел енергії". Тобто економіка замкненого циклу передбачає формування нових підходів до економіки і зосереджується головним чином на тих продуктах і послугах, які дозволяють мінімізувати відходи і інші види забруднень (Рис. 1). Простежується чіткий зв'язок циркулярної економіки з Четвертою промисловою революцією (Революція 4.0, Індустрія 4.0) і, власне, вона має на меті зменшити негативний вплив людини на навколишнє середовище (зміни клімату, накопичення величезних обсягів відходів, виснаження природних ресурсів, деградацію стану довкілля і т. д.) [8; 10].

Що стосується 27 активних членів ЄС, то в контексті досягнення цілей сталого розвитку актуальність циркулярної економіки далі зростає. Від моменту першої згадки про "циркулярність" економіки минуло 30 років, проте лише після впровадження у ЄС її популярність стрімко зросла, а світові лідери поступово усвідомлюють її значущість для досягнення сталого розвитку. 11 березня 2020 р. Європейська Комісія ухвалила План дій щодо "циркулярної" економіки (Circular Economy Action Plan), що є важливою складовою порядку денного стратегії

Європейського "зеленого" курсу (European Green Deal). Метою даного Плану є скорочення споживання в ЄС та подвоєння повторного використання ресурсів у найближчі десятиліття, одночасно сприяючи економічному зростанню [8; 10]. Потрібно зазначити, що в 2018 р. Всесвітнім економічним форумом було значно розширено принципи економіки замкненого циклу і зараз ми маємо не 3R, а 10R — принципів (Рис. 2).

Прогнозовано, що попит на ІКТ-пристрої буде тільки зростати, ще більше скорочуючи ресурси та створюючи більших потоків електронних відходів. У відповідь компанії повинні звернути увагу на два ключові виклики.

По-перше, це збір після закінчення використання. Споживачі часто не віддають на переробку чи правильну утилізацію свої небажані ІКТ-пристрої після покупки новішої моделі. Рішенням будуть нові бізнес-моделі, які дозволять компаніям надавати доступ до продуктів, зберігаючи право власності, таким чином сприяючи контролю над поверненням після закінчення використання. Альтернатива — пропонувати клієнтам стимули для повернення продуктів.

Інша проблема — електронні відходи. Вартість переробки електронних відходів є відносно високою в розвинених країнах, що підвищує ризик

того, що пристрої потрапляють у менш розвинені країни без жодного управління щодо відповідного поводження після завершення використання. Технологія може забезпечити сприятливу економіку в галузі переробки.

Глобальна політика і такі стандарти, як закони про розширену відповідальність виробника, покращать видимість і відстежуваність у всьому ланцюжку створення вартості та підтримають розвиток відповідальних практик використання технологічних пристроїв у всьому світі.

Використовуючи ІТ-технології під час війни, в управлінні підприємством, велику роль має захист інформації. Інформація сьогодні — цінний ресурс, від якого залежить як функціонування підприємства в цілому, так і його конкурентоспроможність.

Загроз безпеки інформаційних ресурсів підприємства багато — це і комп'ютерні віруси, які можуть знищити важливі дані, і промислове шпигунство з боку конкурентів переслідують своєю метою отримання незаконного доступу до інформації є комерційною таємницею, і багато іншого. Тому особливе місце набуває діяльність

**Таблиця 1. Модель загроз автоматизованих систем управління підприємств**

№ з/п	Вид загрози	Джерело загрози	Спосіб реалізації	Наслідки		
				Конфіденційність	Цілісність	Доступність
<b>I. Загрози витоку (технічні канали)</b>						
<i>1. Загрози витоку акустичної (мовної) інформації</i>						
	Загрози застосування закладних передавальних пристроїв ("жучків"), направлених мікрофонів та стетоскопів	Персонал, Користувачі	Недостатній контроль	+		+
<i>2. Загрози витоку видової інформації</i>						
	Загрози порушення технології введення / виведення видової інформації. Копіювання вихідних документів, магнітних та інших носіїв інформації	Персонал, користувачі	Неуважність, недбалість, некомпетентність	+	+	+
<b>II. Загрози витоку інформації, що обробляється на АРМ</b>						
<i>1. Загрози, пов'язані з діями порушників доступу до інформації</i>						
	Тимчасова відсутність персоналу (хвороба, відрядження, відпустка, пандемія)	Персонал, користувачі	Сімейні обставини, епідемії, службова необхідність тощо		+	+
<i>2. Загрози, що виникають при завантаженні операційної системи</i>						
	Загрози, пов'язані з порушенням роботи (випадкове або навмисне) систем зв'язку, електроживлення, водо-/або теплопостачання, кондиціонування	Персонал, користувачі	Неуважність, недбалість, некомпетентність			+
	Загрози, пов'язані з руйнуванням або пошкодженням приміщень ( в. т. військові дії)	Персонал, користувачі, стихійні лиха	Стихійні лиха, кліматичні зміни, військові дії	+	+	+
<i>3. Загрози, що реалізуються після завантаження операційної системи</i>						
	Загрози використання недоліків програм, що реалізують мережеві сервіси (зокрема, відсутність контролю за переповненням буфера) на кшталт «вірусу Морріса»	Хакери	Некомпетентність		+	+
	Загрози віддаленого управління системою, що надаються прихованими компонентами («троянськими» програмами типу Back. Orifice	Хакери	Несанкціоноване підключення	+	+	+
<i>4. Загрози впровадження зловмисних програм</i>						
	Загрози застосування програмних вірусів (включення в ПЗ програмних закладок типу «бомби», «троянського коня» тощо)	Програми, Персонал, Користувачі	Використання неперевіреного ПЗ	+	+	+
<i>5. Загрози інформації із зовнішніх мереж</i>						
	Загрози перехоплення потоку даних, що передаються, якими обмінюються компоненти мережевої ОС	Персонал	Недостатній контроль		+	+
<i>6. Загрози виявлення паролів</i>						
	Загрози здійснення заходів, що можуть призвести до розголошення паролю адміністратора АСУ або до його втрати, тощо	Персонал, користувачі	Неуважність, недбалість, некомпетентність		+	+
<i>7. Загрози віддаленого запуску додатків</i>						
	Загрози віддаленого запуску програми шляхом використання можливостей віддаленого управління системою	Хакери Персонал, користувачі	Отримання доступу інформації та ресурсів АСУ		+	
<i>8. Загрози впровадження зловмисних програм</i>						
	Загрози застосування програм, що використовують не декларовані можливості програмного та програмно-апаратного забезпечення АСУ	Хакери	Пошкодження файлів	+		
	Загрози застосування програм, що генерують комп'ютерні віруси	Хакери	Знищення інформації		+	
	Загрози застосування програм, що виявляють уразливості засобів захисту інформації в АСУ	Хакери, Персонал	Викривлення інформації			

Джерело: створено на основі джерел [2; 9].

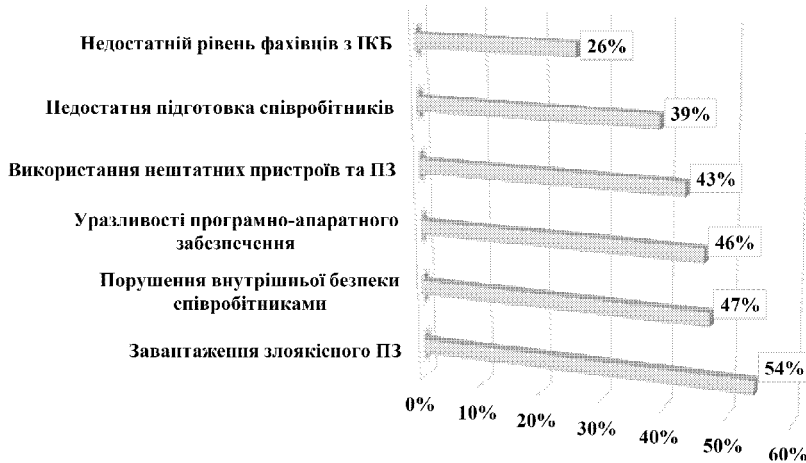
по захисту інформації, щодо забезпечення інформаційної безпеки (Табл. 1).

Мета захисту інформації — мінімізація втрат, викликаних порушенням цілісності або конфіденційності даних, а також їх недоступності для споживачів. Захист інформаційних даних необхідний всім компаніям: від невеликих фірм до великих корпорацій. Захисту підлягають не тільки комп'ютерні пристрої, а й усі технічні засоби, які мають контакт з інформаційними відомостями. Будь-яка інформація, що потрапила в руки злочинців, небезпечна. У зв'язку із цим, потрібно докласти

максимум зусиль для того, щоб забезпечити надійний рівень конфіденційності ІТ-систем. Сьогодні не існує універсальної методики забезпечення захисту, яка надавала б 100% гарантію безпеки. Відповідно, інформаційна система захисту потребує постійного вдосконалення і покращення. Адже, хакери і злочинні елементи безперервно вдосконалюють власні методики злому і несанкціонованого проникнення [7].

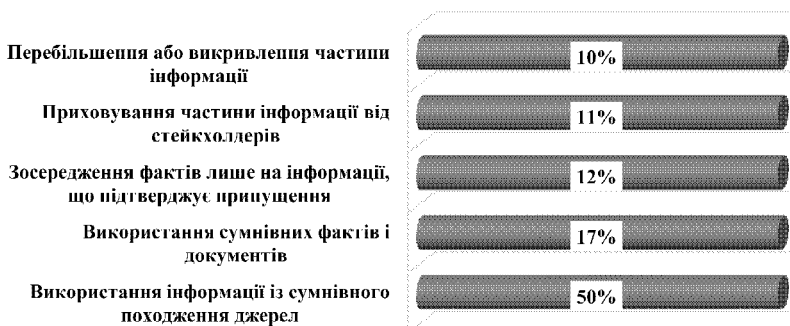
Важливу та ключову роль у процесі функціонування бізнес-структур останнім часом відіграє Всесвітня мережа Internet, що часто сприяє тому, що вони стають об'єктами деструктивних антропогенно-техногенних впливів, серед яких найбільшу шкоду за твердженням фахівців організації CERT (Computer Emergency Response Team) надають наступні: недостатній рівень фахівців з ІКБ; недостатня підготовка співробітників; використання нештатних пристроїв та програмного забезпечення; уразливість програмно-апаратного забезпечення; порушення внутрішньої безпеки співробітниками; завантаження зловмисного програмного забезпечення. Слід зазначити, що загрози, як можливі небезпечні прояви певної дії, яка спрямована проти об'єкта захисту та реалізується через його уразливість. Уразливість — це будь-яка характеристика або властивість, використання якої порушником може привести до порушення безпеки інформації (Рис. 3).

Останнім часом значного поширення набуло таке явище, як фальшива інформація. Наприклад, це — новини, сторінки в соціальних мережах, підроблені під рейтингові сайти, за допомогою яких певні групи людей або окремі особи привертають увагу суспільства до недостовірних подій некоректним шляхом [1]. Подібна інформація, зокрема, недостовірна, розповсюджуються з великою швидкістю, поступово поповнюючись новими подробицями, які є реакцією індивідумів (резонансна інформація може довго висвітлюватись і навіть сприяти створенню нових груп). Можливості інформаційного простору дають змо-



**Рис. 3. Перелік найбільш небезпечних загроз і уразливостей для бізнесу**

Джерело: [9].



**Рис. 4. Недостовірна інформацій в управлінні. Способи потрапляння**

Джерело: [9].

гу створювати псевдореальних осіб, наділяючи їх вигаданою історією, яких індивідууми вважатимуть цілком реальними. Вкидаючи фальшиву інформацію в інформаційний простір, її автори враховують таку особливість мережі Інтернет, як анонімність, можливість множинної дії. Фальшиві матеріали можуть одночасно просуватися через велику кількість сайтів, форумів, блогів, гостьових книг. При цьому у користувачів, які зустрічають одну й ту саму інформацію в різних місцях, складається враження, що вона є достовірною. Розглянемо інші шляхи появи в ресурсах Інтернету недостовірних матеріалів, якими в свою чергу, можуть користуватись менеджери для прийняття неефективних управлінських рішень. Одними з перших на сьогодні, як правило, нову інформацію подають інформаційні агенції. Вона є короткою за змістом, без оцінок і прогнозів. Але ЗМІ, готуючи на її базі свої матеріали, змінюють акценти, подають новини в різному контексті. Тому одне й те саме повідомлення з різних джерел інформації сприйматиметься по-різному. Це можна пояснити тим, що: — ЗМІ працюють з різною аудиторією, тому форма подання матеріалів відрізняється (теоретична версія); — напрями інтерпретації матеріалу визначають власники та спонсори видань (прагматична версія). Зважаючи на те, що достовірність інформації залежить від самих видань, аналітикам слід звертати увагу на першоджерело, уважно вивчати факти, які лежать в основі інформації, ре-

тельно перевіряти сумнівні відомості. Недостовірною (через неможливість її перевірити) дослідник має вважати інформацію, що надходить до інформаційного простору з "конфіденційних", навіть якщо матеріал містить посилання на організацію, яку представляє "джерело".

Наявність новітніх технологій, програмних комплексів, телекомунікаційного та оргтехніки позитивно впливає на якість управлінської роботи, однак варто розуміти, що обсяг коштів, витрачених на автоматизацію розробки управлінського рішення, не повинен перевищувати можливий дохід від впровадження такої системи. Основою інформаційної допомоги є автоматизація процесів прийняття управлінських рішень інформаційні системи. Відсутність в Україні належного нормативно-правового регулювання діяльності як самих інтернет-ресурсів, які поширюють відповідний контент, так і діяльності журналістів /авторів /блогерів, що публікуються на цих сайтах, призводить до численних зловживань з боку недобросовісних користувачів та до порушення особистих прав, немайнові права фізичних та юридичних осіб.

## ВИСНОВКИ

1. Циркулярна економіка, яку ще називають економікою замкнутого циклу, — це нова модель економічного розвитку, що

передбачає відновлення, повторне використання, раціональне споживання ресурсів і дозволяє створити додаткову цінність. Циркулярна економіка спрямована, насамперед, на збереження енергії, економічно чисте виробництво та споживання. Циркулярна модель економіки є протилежною традиційній, лінійній моделі. В той час, як лінійна економіка має на увазі "взяти, зробити і позбутися", економіка циркулярна полягає у тому, щоб "взяти, зробити, переробити, відновити, використати ще раз, знизити рівень відходів, мінімізувати витрати, перейти до відновлюваних джерел енергії".

2. Циркулярна економіка невід'ємно пов'язана з формуванням нових бізнес-моделей, що орієнтовані на зменшення кількості використовуваних ресурсів, впровадження повторного використання або замкнутого циклу виробництва, відновлення, редизайну, рециклінгу та вторинній переробці для забезпечення тривалого життєвого циклу.

3. Визначення "інформаційний менеджмент" вживається в таких значеннях: як управління довідковою інформацією, тобто інформаційне управління (технологія управління); як управлінська актуальна інформація (управління інформаційними потоками та інформаційними ресурсами) для оптимізації робіт; як інформатизація процесів управління, тобто управлінська інформаційна технологія (автоматизована технологія обробки інформації в певній предметній галузі).

4. Існує багато загроз безпеці інформаційних ресурсів компанії, включаючи комп'ютерні віруси, які можуть знищити важливі дані, промислове шпигунство з боку конкурентів, які переслідують незаконний доступ до інформації, яка є комерційною таємницею, і багато іншого. Аналізуючи важливість інформаційної підтримки підприємства в прийнятті правильних управлінських рішень, варто зазначити, що від того, яким буде управлінське рішення, залежить подальший стан, розвиток, успіх у майбутньому підприємства. Важливою умовою прийняття успішного рішення є актуальність і точність використовуваної інформації про стан підприємства. Широка різноманітність продуктів, які з часом продовжують прогресувати у своїх можливостях, створених з метою використання спеціальних завдань або навіть їх модулів, дозволяє звести до мінімуму ймовірність виникнення несприятливого "сценарію", оскільки максимально знизити ризики та підвищити ефективність всього процесу цілепокладання та прийняття рішень.

## Література:

1. Гриник, О., Сисоєва, І. (2022). Економічна безпека України: соціальний аспект. *Економіка та суспільство*, (43). <https://doi.org/10.32782/2524-0072/2022-43-70>
2. Y. Dreis, I. Lozova, A. Biskupskyi, L. Kuzmenko, Ali, T. Al-Khwalde, A. Korchenko. A tuple model for estimating the consequences of personal data leakage in automated systems. VIII International conference of students, PHD-students and young scientists "Engineer of XXI Century" // Processing, transmission and security of information. — Bielsku-Bialej: NATH, 2018. Vol.2. — P. 41—50. ISBN: 978-83-65182-94-4.
3. Matviienko, O. and Tsyvin, M. (2017), "Information management as the basis for the conceptualization of the model of a specialist in information business", *Visnyk Knyzhkovoї palaty*, vol. 4, pp. 27—30.
4. Machlup, F. (2000), "Production and Distribution of Knowledge in the United States", Princeton, 457 p.
5. Dvornik, M. O (2013), "The essence and problems of the development of the information society in Ukraine", *Stalyj rozvytok ekonomiky*, vol 4, available at: [http://basicgroup.com.ua/press\\_centre\\_publications\\_information\\_society\\_development\\_in\\_ukraine](http://basicgroup.com.ua/press_centre_publications_information_society_development_in_ukraine)
6. Povidajchuk, O. (2009), "Information culture of the person: socio-philosophical analysis of the concept", *Naukovyj visnyk Uzhhorods'koho universytetu. Serii: Politolohiia, sotsiologiia, filosofiia*, vol. 11, pp. 189-19.
7. Електронний ресурс: <https://datami.ua/informatsijna-bezpeka-vidi-zagroz-i-metodi-yih-usunennya/>
8. Нова політика ЄС з "циркулярної" економіки: можливості для України. 2020. URL: [https://dixigroup.org/wp-content/uploads/2020/09/dixi\\_pb\\_circular-economy\\_ukr\\_full\\_3.pdf](https://dixigroup.org/wp-content/uploads/2020/09/dixi_pb_circular-economy_ukr_full_3.pdf)
9. Sysoieva I., Pohrishchuk B., Pukas A., Tsikhanovska O., Vatslavskyi O. and Sydorovych O., "Information Management Technology as a Tool for Making Effective Management Decisions," 2023 13th International Conference on Advanced Computer Information Technologies (ACIT), Wroclaw, Poland, 2023, pp. 191—195, doi: 10.1109/ACIT58437.2023.10275328.
10. Сисоєва І.М., Роледерс В.В., Погріщук О.Б. Соціальна відповідальність бізнесу в умовах становлення циркулярної економіки: реалії ведення бізнесу в умовах війни. *Інвестиції: практика та досвід*, № 23 (2022) <https://www.nayka.com.ua/index.php/investplan/issue/view/45>
11. Сисоєва, І. "Особливості аудиту облікової політики підприємств." *Галицький економічний вісник*. — 2007. — Вип 4.15 (2007): 188—192.

## References:

1. Hrynyk, O. and Sysoieva, I. (2022), "Economic security of Ukraine: social aspect", *Ekonomika ta suspil'stvo*, (43). <https://doi.org/10.32782/2524-0072/2022-43-70>
2. Dreis, Y. Lozova, I. Biskupskyi, A. Kuzmenko, L. Al-Khwalde, Ali.T. and Korchenko, A. (2018), "A tuple model for estimating the consequences of personal data leakage in automated systems", VIII International conference of students, PHD-students and young scientists "Engineer of XXI Century". Processing, transmission and security of information, NATH, Bielsku-Bialej, vol. 2, pp. 41—50.
3. Matviienko, O. and Tsyvin, M. (2017), "Information management as the basis for the conceptualization of the model of a specialist in information business", *Visnyk Knyzhkovoї palaty*, vol. 4, pp. 27—30.
4. Machlup, F. (2000), *Production and Distribution of Knowledge in the United States*, Princeton, USA.
5. Dvornik, M.O. (2013), "The essence and problems of the development of the information society in Ukraine", *Stalyj rozvytok ekonomiky*, vol 4, available at: [http://basicgroup.com.ua/press\\_centre\\_publications\\_information\\_society\\_development\\_in\\_ukraine](http://basicgroup.com.ua/press_centre_publications_information_society_development_in_ukraine) (Accessed 25 Oct 2023).
6. Povidajchuk, O. (2009), "Information culture of the person: socio-philosophical analysis of the concept", *Naukovyj visnyk Uzhhorods'koho universytetu. Serii: Politolohiia, sotsiologiia, filosofiia*, vol. 11, pp. 189-19.
7. Datami (2022), "Information security: types of threats and methods of their elimination", available at: <https://datami.ua/informatsijna-bezpeka-vidi-zagroz-i-metodi-yih-usunennya/> (Accessed 25 Oct 2023).
8. DiXi Group (2020), "New EU policy on the "circular" economy: opportunities for Ukraine", available at: [https://dixigroup.org/wp-content/uploads/2020/09/dixi\\_pb\\_circular-economy\\_ukr\\_full\\_3.pdf](https://dixigroup.org/wp-content/uploads/2020/09/dixi_pb_circular-economy_ukr_full_3.pdf) (Accessed 25 Oct 2023).
9. Sysoieva, I. Pohrishchuk, B. Pukas, A. Tsikhanovska, O. Vatslavskyi, O. and Sydorovych, O. (2023), "Information Management Technology as a Tool for Making Effective Management Decisions", 13th International Conference on Advanced Computer Information Technologies (ACIT), Wroclaw, Poland, pp. 191—195, doi: 10.1109/ACIT58437.2023.10275328.
10. Sysoieva, I.M. Roleders, V.V. and Pohrishchuk, O.B. (2022), "Social responsibility of business in the conditions of the formation of a circular economy: the realities of doing business in the conditions of war", *Investytsii: praktyka ta dosvid*, vol. 23, available at: <https://www.nayka.com.ua/index.php/investplan/issue/view/45> (Accessed 25 Oct 2023).
11. Sysoieva, I. (2007), "Peculiarities of auditing the accounting policy of enterprises", *Halyts'kyj ekonomichnyj visnyk*, vol. 4.15, pp. 188—192.

*Стаття надійшла до редакції 08.11.2023 р.*