

[Legal Act of Ukraine] (1997). https://zakon.rada.gov.ua/laws/show/994_036#Text
 [Legal Act of Ukraine] (2002). <https://zakon.rada.gov.ua/laws/show/3-2002-n#Text>
 [Legal Act of Ukraine] (2011). <https://zakon.rada.gov.ua/laws/show/2939-17#n107>
 [Legal Act of Ukraine] (2014). https://zakon.rada.gov.ua/laws/show/994_b49#Text
 Lypchuk, M. "Internet-predstavnytstvo orhanu vlady yak mekhanizm dialohovoi vzaiemodii ta kliuchovyi element demokratyzatsii derzhavnoho upravlinnia" [Internet Representation of Public Authorities as a Mechanism for Dialogue Interaction and a Key Element of Democratization of Public Administration]. *Efektivnist derzhavnoho upravlinnia*. 2016. http://www.lvivacademy.com/vidavnitstvo_1/edu_46/fail/ch1/23.pdf

"Otsinka finansovykh pokaznykiv biudzhetyv 806 OTH. Reitynh za 2019 rik" [Estimation of Financial Indicators of Budgets of 806 OTG. Rating for 2019.]. <https://decentralization.gov.ua/news/12192?page=3>
 Piotrowski, S., Grimmeliikhuijsen, S., and Deat, F. "Numbers over Narratives? How Government Message Strategies Affect Citizens' Attitudes". *Public Performance & Management Review*, vol. 42, no. 5 (2019): 1005-1028.
 DOI: 10.1080/15309576.2017.1400992
 Solomko, Yu. "Elektronne uriaduvannia: poniattia, sutnist, pryntsyipy ta napriamy rozvytku" [E-Government: Concept, Essence, Principles and Directions of Development]. *Efektivnist derzhavnoho upravlinnia*. 2018. http://www.lvivacademy.com/vidavnitstvo_1/edu_55/fail/16.pdf

УДК 658

JEL: D21; D89; L25; L86; M15

ВИТІК ІНФОРМАЦІЇ ЯК КЛЮЧОВА ПРОБЛЕМА ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВІЗАЦІЇ ЕКОНОМІКИ

©2020 ПРІТИС В. І., КРИМЧАК Л. А., ГАВЛОВСЬКА Н. І.

УДК 658

JEL: D21; D89; L25; L86; M15

Притис В. І., Кримчак Л. А., Гавловська Н. І. Витік інформації як ключова проблема інформаційно-аналітичного забезпечення економічної безпеки підприємства в умовах цифровізації економіки

Метою статті є дослідження ключової проблеми інформаційно-аналітичного забезпечення діяльності підприємства в умовах цифровізації економіки. В роботі зазначено зростання ролі інформації в здійсненні управлінської діяльності суб'єктом господарювання та загалом її ролі у функціонуванні сучасного підприємства. Розглянуто підходи до трактування понять «інформація» та «інформаційне забезпечення». Визначено, що на сьогоднішній день основною проблемою інформаційно-аналітичного забезпечення господарської діяльності є витік конфіденційної інформації як однієї з форм реалізації загроз інформаційній безпеці підприємства, що полягає в порушенні конфіденційності, цілісності та доступності інформації. Визначено, що до витоку інформації на підприємстві призводять, як правило, такі дії: несанкціонований доступ до конфіденційної інформації; розголошення конфіденційної інформації (у т. ч. ненавмисне); витік інформації по недосконалих технічних каналах. Розглянуто канали можливого витоку інформації. Окрім того, здійснено аналіз статистичних даних витоку інформації в глобальному вимірі. Як показують дослідження, за 2019 р. серед загального обсягу витоку інформації 49,7% обсягу припадає на зовнішніх суб'єктів і 50,3% – на внутрішніх порушників. Загалом, у системі інформаційно-комунікативного забезпечення особливу увагу з боку менеджменту підприємства необхідно приділяти саме внутрішнім комунікаціям, оскільки більше 90% інформації надходить від працівників. Варто зазначити, що причинами витоку інформації підприємства з вини внутрішніх суб'єктів можуть бути: ненавмисні дії з боку співробітників компанії, пов'язані з помилками при обробці, зберіганні чи передачі конфіденційних даних; навмисні, зумовлені певними причинами дії співробітників, що мають доступ до конфіденційної інформації. Сюди можна віднести дії співробітників, які використовують дані підприємства в цілях шахрайства, а також дії колишніх працівників, котрі через бажання помсти за звільнення всіляко «сприяють» витоку конфіденційної інформації, передаючи її конкурентам або ж використовуючи її у власних корисливих цілях.

Ключові слова: інформація, інформаційно-комунікативне забезпечення, витік інформації, канали витоку, підприємство, економічна безпека.

DOI: <https://doi.org/10.32983/2222-4459-2020-10-240-247>

Рис.: 3. **Табл.:** 2. **Бібл.:** 16.

Притис Вадим Ігорович – аспірант кафедри менеджменту, адміністрування та готельно-ресторанної справи, Хмельницький національний університет (вул. Інститутська, 11, Хмельницький, 29016, Україна)

E-mail: boretmagistr@ukr.net

ORCID: <https://orcid.org/0000-0002-6942-2223>

Крымчак Людмила Анатоліївна – кандидат економічних наук, доцент кафедри менеджменту, адміністрування та готельно-ресторанної справи, Хмельницький національний університет (вул. Інститутська, 11, Хмельницький, 29016, Україна)

E-mail: krymchakla@ukr.net

ORCID: <https://orcid.org/0000-0002-2546-9257>

Гавловська Наталія Іванівна – доктор економічних наук, професор, професор кафедри менеджменту, адміністрування та готельно-ресторанної справи, Хмельницький національний університет (вул. Інститутська, 11, Хмельницький, 29016, Україна)

E-mail: nataligavlovsk@gmail.com

ORCID: <https://orcid.org/0000-0003-1084-2853>

Researcher ID: <http://www.researcherid.com/AAE-2507-2020>

UDC 658

JEL: D21; D89; L25; L86; M15

Prytys V. I., Krymchak L. A., Havlovskaya N. I. Leakage of Information as a Key Problem of Information-Analytical Provision of Economic Security of Enterprise in the Context of Digitalization of the Economy

The article is aimed at researching the key problem of information and analytical provision of enterprise in the context of digitalization of the economy. The publication indicates the growth of the role of information in the implementation of management activities by an economic entity and its general role in the operation of the modern enterprise. Approaches to interpretation of the concepts of «information» and «information provision» are examined. It is defined that today the main problem of information-analytical provision of economic activity is the leakage of confidential information as one of the forms of materialization of threats to the information security of enterprise, which consists in violation of confidentiality, integrity and availability of information. It is further defined that the leakage of information at the enterprise is usually caused by the following actions: unauthorized access to confidential information; disclosure of confidential information (including the unintentional disclosure); leakage of information via the imperfect technical channels. The channels of possible information leakage are considered. In addition, the analysis of statistical data on information leakage in the global dimension was carried out. According to the researches, in 2019, among the total volume of information leakage, 49.7% of the volume is accounted for by external actors and 50.3% by internal offenders. In general, in the system of information and communication provision, special attention of the management of enterprise should be directly paid to internal communications, since more than 90% of the information comes in from employees. It should be noted that the reasons for the leakage of the enterprise's information due to the fault of internal actors may be: unintentional actions on the part of the enterprise's employees related to errors in the processing, storage or transmission of confidential data; the caused by certain reasons actions of employees who have access to confidential information. This may include the actions of employees who use the enterprise's data for fraud purposes, as well as the actions of former employees who, motivated by their desire for retaliation for dismissal, «contribute» to the leakage of confidential information, passing it on to competitors or using it for their own mercenary purposes.

Keywords: information, information and communication provision, information leakage, leakage channels, enterprise, economic security.

Fig.: 3. **Tabl.:** 2. **Bibl.:** 16.

Prytys Vadym I. – Postgraduate Student, Department of Management, Administration and Hotel and Restaurant Business, Khmelnytsky National University (11 Instyutyska Str., Khmelnytsky, 29016, Ukraine)

E-mail: boretsmagistr@ukr.net

ORCID: <https://orcid.org/0000-0002-6942-2223>

Krymchak Lyudmyla A. – PhD (Economics), Associate Professor, Department of Management, Administration and Hotel and Restaurant Business, Khmelnytsky National University (11 Instyutyska Str., Khmelnytsky, 29016, Ukraine)

E-mail: krymchakla@ukr.net

ORCID: <https://orcid.org/0000-0002-2546-9257>

Havlovskaya Nataliia I. – D. Sc. (Economics), Professor, Professor, Department of Management, Administration and Hotel and Restaurant Business, Khmelnytsky National University (11 Instyutyska Str., Khmelnytsky, 29016, Ukraine)

E-mail: nataligavlovsk@gmail.com

ORCID: <https://orcid.org/0000-0003-1084-2853>

Researcher ID: <http://www.researcherid.com/AAE-2507-2020>

У сучасних реаліях інформація в бізнес-середовищі є чи не найважливішим ресурсом для будь-якого суб'єкта господарювання. Цілком зрозуміло, що зі зростанням значення інформації підвищується також інтерес у наукових колах до дослідження її як наукової категорії та вивчення ролі інформації в управлінні соціально-економічними системами. Так, серед ряду науковців варто виділити праці Бенька М. [1], Біленської Д.

[2], Гужви В. [3], Демченко С. [5], Івахненкова С. [7], Рудніченка Є. [15; 16] та ін. Однак, незважаючи на значні напрацювання, не можна на даний час виділити єдине універсальне визначення категорії «інформація»; також потребує подальших досліджень проблема витоку інформації та її впливу на економічну безпеку підприємства.

Отже, метою даної статті є аналіз проблеми витоку інформації як ключової в інформаційно-

аналітичному забезпеченні економічної безпеки підприємства в умовах цифровізації економіки.

У цей час більшість поглядів та думок науковців зводиться до того, що інформацію отожнюють з певними відомостями про об'єкти, явища чи стан зовнішнього середовища [3; 6; 12; 14], або ж певними повідомленнями [1; 13]. Усі наявні трактування поняття «інформація» можна віднести до існуючих наукових підходів, наведених у *табл. 1*.

Розглядаючи наукові підходи до трактування поняття «інформація» (див. *табл. 1*), варто звернути увагу на твердження, відповідно до якого інформація являє собою певне повідомлення, яке має цінність, значущість для суб'єкта [13]. Цілковито погоджуємося із думкою авторів, оскільки цінність інформації для будь-якого суб'єкта господарювання визначається її здатністю до реалізації основних цілей діяльності підприємства, оскільки інформація є визна-

чальним фактором, базою прийняття та реалізації управлінських рішень у бізнес-середовищі. Саме тому на сьогоднішній день велика увага науковців та менеджерів прикута саме до інформаційного забезпечення діяльності підприємства, визначення основних його проблемних зон і, що не менш важливо, пошуку шляхів удосконалення. Адже будь-яка прогалина в системі інформаційного забезпечення господарської діяльності може призвести до досить поширеної проблеми в підприємницькому середовищі – витоку інформації, що може мати негативні наслідки для діяльності будь-якого суб'єкта.

Перед тим, як перейти до розгляду проблеми витоку інформації, варто розглянути сутність самого інформаційного забезпечення діяльності підприємства.

У науковій літературі поширеними є два підходи до трактування поняття «інформаційне забезпечення»: як певний процес, що передбачає пошук, використання інформації тощо [14] та як

Таблиця 1

Підходи до визначення поняття «Інформація»

№ з/п	Підхід до визначення поняття «Інформація»	Тлумачення терміна «Інформація»	Автор/Джерело
I	Антропоцентричний	Це відомості, які можуть бути отримані та засвоєні, тобто перетворені на знання	Д. Біленька [2]
	Недетерміністський	Інформація є фундаментальним поняттям	
	Техноцентричний	Це дані, що мають кількісний вимір	
II	Антропоцентричний	Це відомості, які можна отримувати, створювати та передавати	Л. Данильчук [4]
	Атрибутивний	Це дані, відомості, які притаманні будь-якій матерії, а не лише живій	
	Кібернетичний	Дані, які характерні лише для системи, в якій відбуваються процеси керування (клітини організмів, людина, суспільство)	
III	Філософський	Це об'єктивна властивість матерії	С. Демченко [5]
	Кібернетичний	Це сигнали, що можуть бути передані технічним зв'язком; дані, які можна виміряти кількісно	
	Правовий	Це дані, відомості, які можуть бути збережені, використані та передані	
IV	Кількісний (синтаксичний)	Це будь-яке повідомлення, будь-яка послідовність символів	Т. Писаренко, Т. Кваша, Н. Березняк, О. Прудка [13, с. 10]
	Семантичний (значеннєвий)	Зміст повідомлення, отриманий у результаті його інтерпретації	
	Прагматичний	Повідомлення, яке має цінність, значущість для суб'єкта	
	Статистичний	Повідомлення про стан системи, що зменшує невизначеність знань про неї	

Джерело: складено з використанням [11].

сукупність даних, інформаційних ресурсів, заходів і методів їх організації [1, с. 28].

У праці В. В. Іванової [6] зазначена необхідність розрізняти інформаційне забезпечення-ресурс – як сукупність інформації, що формує конкурентні переваги конкретного підприємства, та інформаційне забезпечення-процес – як налагодження системи інформаційної взаємодії всередині організації. Однак, розглядаючи інформаційне забезпечення як процес, варто зазначити таке: обмін інформацією та її змістом, налагодження взаємодії між суб'єктами будь-якої соціально-економічної системи є не чим іншим, як трактуванням категорії «комунікація», про що зазначається в праці [9]. З огляду на це, у контексті дослідження пропонуємо розглядати саме інформаційно-комунікативне забезпечення діяльності підприємств з точки зору аналізу його основних проблем.

Завданням даної роботи є дослідження проблеми витоку інформації на підприємстві та її вплив на систему інформаційно-комунікативного забезпечення господарської діяльності.

Розвиток інформаційних технологій надав суб'єктам господарювання значні можливості для покращення умов управління інформаційними ресурсами (зберігання, швидкості обробки та передачі даних) та оптимізації управлінських процесів загалом. Суб'єкти господарювання отримали доступ до інформаційних мереж з величезними масивами інформації, необхідної для прийняття та реалізації раціональних управлінських рішень у будь-якій сфері господарювання. І сьогодні успішне управління господарською діяльністю напряму залежить від ефективності управління системою інформаційно-комунікативного забезпечення. Однак із появою численних переваг для діяльності підприємств з'являються також значні загрози для інформаційно-комунікативного забезпечення, що також пов'язані із використанням новітніх інформаційних технологій.

Несанкціоноване проникнення в інформаційну систему підприємства спричиняє значні ризики розкриття конфіденційної інформації конкурентам чи іншим особам з різними намірами, а навмисна зміна вмісту інформації, її спотворення уможлиблює репутаційні ризики для підприємства.

Витік інформації – це неконтрольований «вихід» інформаційних даних (головним чином,

конфіденційних) за межі інформаційно-комунікативної системи підприємства.

Витік інформації є однією із форм реалізації загроз інформаційній безпеці підприємства, яка полягає в порушенні конфіденційності, цілісності та доступності інформації. Тобто, у зменшенні або повній втраті інформацією її цінності.

До витоку інформації на підприємстві призводять, як правило, такі дії: несанкціонований доступ до конфіденційної інформації; розголошення конфіденційної інформації (у тому числі ненавмисне); витік інформації по недосконалих технічних каналах.

У праці [10] розглядаються численні канали витоку інформації, які автор поділяє на чотири групи (табл. 2).

Як показують дослідження, за 2019 р. серед загального обсягу витоку інформації 49,7% обсягу припадає на зовнішніх суб'єктів. Найчастіше такими порушниками виступають хакери. На внутрішніх порушників припало 50,3% випадків витоку інформації [8]. Детально структура джерел витоку інформації на підприємстві зображена на рис. 1.

Як видно з рис. 1, на частку зовнішніх порушників витоку інформації (хакерів) припадає 49,7% усіх випадків витоку інформації. Решта 50,3% – це випадки, пов'язані із внутрішніми порушниками.

Так, у 2019 р. 41% випадків від загальної кількості зареєстрованих випадків витоку інформації сталися з вини діючих співробітників (чи їх необережності). 4,6% від загальної кількості – з провини підрядників компанії. 2,3% – з вини керівників компанії та 2,1% – колишніх працівників. І лише 0,3% випадків витоку інформації було спричинено необережними діями системних адміністраторів компанії.

Основними причинами витоку інформації шляхом зовнішніх (хакерських) атак є людський чинник, який полягає в тому, що зловмисники всілякими методами вводять людину в оману та «витагують» з неї конфіденційну інформацію. Такий вид Інтернет-шахрайства отримав сьогодні назву фішинг-атаки. Іншою причиною є використання на підприємстві застарілих технічних пристроїв чи застарілого програмного забезпечення, що є реальною загрозою для економічної безпеки таких суб'єктів.

Загалом, у системі інформаційно-комунікативного забезпечення особливу увагу з боку

Групи каналів витоку інформації на підприємстві

№ з/п	Група каналів	Канали витоку
1	Канали, пов'язані з доступом до елементів системи обробки даних, які не потребують зміни системи	<ul style="list-style-type: none"> – Канали дистанційного прихованого відеоспостереження або фотографування; – застосування підслуховуючих пристроїв; – перехоплення електромагнітних випромінювань і наведень
2	Канали, пов'язані з доступом до елементів системи та зміною структури її компонентів	<ul style="list-style-type: none"> – Спостереження за інформацією з метою її запам'ятовування в процесі обробки; – розкрадання носіїв інформації; – збір виробничих відходів, що містять оброблювану інформацію; – навмисне зчитування даних з файлів інших користувачів; – читання залишкової інформації, тобто даних, що залишаються на магнітних носіях після виконання завдань; – копіювання носіїв інформації; – навмисне використання для доступу до інформації терміналів зареєстрованих користувачів; – маскуванню під зареєстрованого користувача шляхом викрадення паролів та інших реквізитів розмежування доступу до інформації, використовуваної в системах обробки; – використання для доступу до інформації так званих «люків», дір і «лазівок» в автоматизованих системах обробки даних
3	Канали, пов'язані з використанням спеціальних технічних пристроїв чи програм	<ul style="list-style-type: none"> – Незаконне підключення спеціальної реєструючої апаратури до пристроїв системи або ліній зв'язку (перехоплення модемного та факсимільного зв'язку); – зловмисна зміна програм таким чином, щоб ці програми поряд із основними функціями обробки інформації здійснювали також несанкціонований збір і реєстрацію інформації, що захищається; – зловмисне виведення з ладу механізмів захисту
4	Канали, пов'язані з людським фактором	<ul style="list-style-type: none"> – Несанкціоноване отримання інформації шляхом підкупу чи шантажу посадових осіб відповідних служб; – отримання інформації шляхом підкупу чи шантажу співробітників, знайомих, обслуговуючого персоналу або родичів, які знають про рід діяльності

Джерело: складено на основі [10].

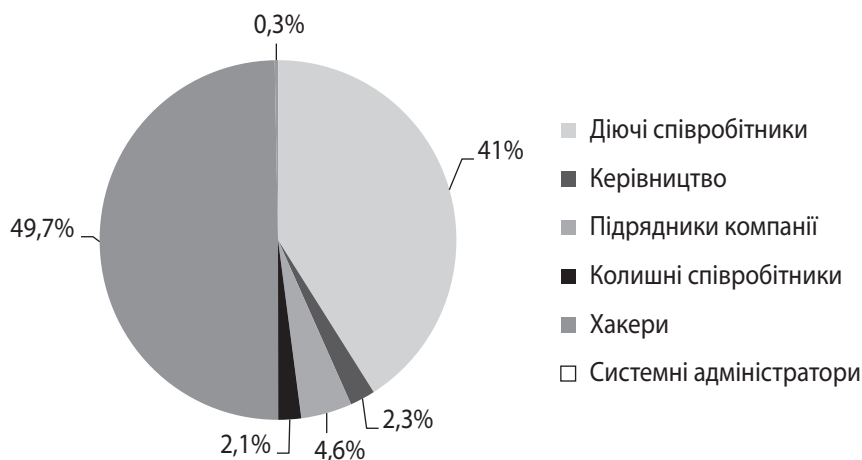


Рис. 1. Джерела витоку інформації

Джерело: побудовано на основі [8].

менеджменту підприємства необхідно приділяти саме внутрішнім комунікаціям. Адже, як показує практика, серед загального обсягу інформації, що циркулює на підприємстві, лише 7–10% її надходить з інформаційного відділу підприємства. Решта – більше 90% – це інформація, яка приходить від самих працівників. Саме тому така велика кількість порушень, пов'язаних із витоком інформації, припадає на співробітників.

Варто зазначити, що причинами витоку інформації підприємства з вини внутрішніх суб'єктів можуть бути:

- ✦ ненавмисні дії з боку співробітників компанії, пов'язані з помилками при обробці, зберіганні чи передачі конфіденційних даних;
- ✦ навмисні, зумовлені певними причинами дії співробітників, що мають доступ до конфіденційної інформації. Сюди можна віднести дії співробітників, які використовують дані підприємства в цілях шахрайства. А також дії колишніх працівників, котрі через бажання помсти за звільнення всіляко «сприяють» витоку конфіденційної інформації, передаючи її конкурентам, або ж використовуючи її у власних корисливих цілях.

Потрібно пам'ятати, що сьогодні без належного захисту інформаційних ресурсів витік корпоративних даних з вини співробітників компанії є значно легшим способом скомпрометувати інформацію, аніж з вини зовнішніх порушників. Оскільки персонал підприємства, як правило, має більші можливості доступу до важливих даних, обізнаний у процесах, які відбуваються на підприємстві та в його інформаційній політиці, а також може знати всі прогалини захисту інформаційно-комунікативного забезпечення діяльності підприємства.

Що ж стосується структури інформації, щодо якої було реалізовано порушення у 2019 р., то 93% такої інформації містили персональні дані, 2,8% – комерційну таємницю (*know how*) та 4,2% – державну таємницю (рис. 2) [8].

Відповідно до джерела [8] дослідження, які були проведені на глобальному рівні, свідчать, що із розвитком сучасних інформаційних технологій система інформаційно-комунікативного забезпечення стала ще більш вразливою. Однією із причин цього стало використання мережі Інтернет в управлінських цілях та в повсякден-



Рис. 2. Структура інформації, щодо якої була порушена конфіденційність

Джерело: побудовано на основі [8].

ному корпоративному житті. Так, через канал мережі за перше півріччя 2019 р. було «злито» майже 90% конфіденційних даних із загального обсягу витоку інформації (рис. 3).

Як видно з рис. 3, більшу частину, а саме 76,6%, склали втрати інформації через використання на підприємствах Інтернет-браузери та «хмарні» служби. Через електронну пошту здійснено 8,4% випадки порушень конфіденційності корпоративної інформації. Такі популярні сьогодні комунікативні служби обміну повідомленнями через мережу Інтернет, як месенджери, стали каналами витоку інформації у 4,3% випадків від загальної кількості зареєстрованих випадків витоку інформації.

Кількість випадків скомпрометованої інформації через втрату паперових документальних носіїв та неполадки в роботі технологічних пристроїв склали 6,3% та 2% відповідно.

Як не дивно, але, за даними джерела [8], через мобільні пристрої зареєстровані витоки інформації склали лише 0,3% від загальної кількості випадків.

Важливо зазначити, що здійснений аналіз випадків витоку інформації базується лише на тих даних, які були зареєстровані. Кількість незареєстрованих випадків витоку інформації може також бути значною.

Отже, з огляду на те, що велика кількість інцидентів, пов'язаних із витоком інформації, була зафіксована через порушення конфіденційності саме суб'єктами внутрішньої комунікації підприємств, важливо велику увагу приділяти сьогодні саме політиці користування корпоративною інформацією.

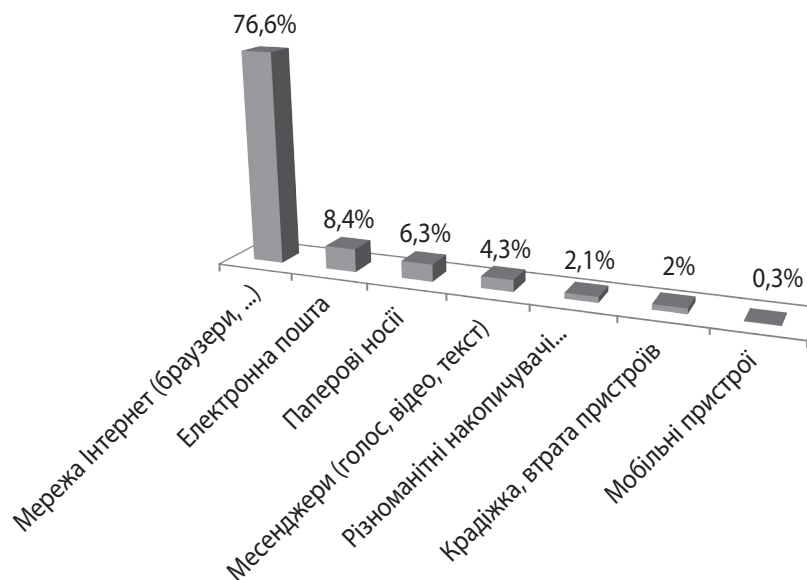


Рис. 3. Розподіл каналів витоку інформації

Джерело: побудовано на основі [8].

Розмежування доступу співробітників до відомостей відповідно до їх повноважень, чітке усвідомлення цінності інформації для діяльності підприємства та відповідальності кожного за втрату чи розповсюдження інформації – важливий елемент захисту інформаційних ресурсів підприємства в системі інформаційно-комунікативного забезпечення.

ВИСНОВКИ

Сьогодні витік інформації є значною загрозою для діяльності будь-якого підприємства в будь-якій країні світу. Втрата репутації чи довіри клієнтів, величезні фінансові збитки, банкрутство підприємства аж до ліквідації суб'єкта господарської діяльності – все це можливі наслідки витоку інформації. Саме тому функціонування системи інформаційно-комунікативного забезпечення діяльності підприємства має бути спрямованим на реалізацію заходів із запобігання витоку інформації, а менеджерів підприємств – на пошук шляхів їх реалізації. ■

ЛІТЕРАТУРА

1. Бенько М. М. Інформаційні системи і технології в бухгалтерському обліку : монографія. Київ : КНТЕУ, 2010. 336 с.
2. Біленська Д. О. Визначення інформації в концепції антропоцентричного підходу. *Теорія і практика правознавства*. 2013. Вип. 2. URL: <http://dspace.nlu.edu.ua/bitstream/123456789/5962/1/Bilenska.pdf>
3. Гужва В. М. Інформаційні системи і технології на підприємствах : навч. посіб. Київ : КНЕУ, 2001. 400 с.
4. Данильчук Л. Сутність дефініції «інформація». *Педагогіка і психологія професійної освіти*. 2012. № 5. С. 18–26. URL: <http://ena.lp.edu.ua:8080/bitstream/ntb/23929/1/4-18-26.pdf>
5. Демченко С. Підходи до змісту поняття «інформація»: кібернетичний, філософський, правовий. *National Law Journal: Theory and Practice*. 2016. No. 1/2. P. 35–38. URL: http://www.jurnaluljuridic.in.ua/archive/2016/1/part_2/7.pdf
6. Іванова В. В. Якісні аспекти інформаційного забезпечення економіки, заснованої на знаннях, інформаційними суб'єктами кластерів. *Економічний часопис-XXI*. 2011. № 9–10. С. 65–68. URL: <http://dspace.nbu.gov.ua/bitstream/handle/123456789/48007/19-Ivanova.pdf?sequence=1>
7. Івахненко С. В. Інформаційні технології аудиту та внутрішньогосподарського контролю в контексті світової інтеграції. Житомир : Рута, 2010. 432 с.
8. Исследования утечек информации ограниченного доступа в 2019 году : аналитический отчет. URL: <https://www.infowatch.ru/analytics/reports/27720>
9. Модель інформаційно-комунікативного впливу суб'єктів забезпечення національної безпеки на джерело загроз / О. Комісаров, Л. Чистоклетов, В. Шишко, О. Хитра, К. Костовська // *Traektori â nauki = Path of Science*. Section «Law». 2019. Vol. 5. No. 1. P. 3001–3011. DOI: 10.22178/pos.42-3
10. Копитко М. І. Менеджмент інформаційних ресурсів та інформаційна безпека підприємств : навч.-метод. посіб. Львів : Ліга-Прес, 2016. 172 с.
11. Лісовський І. В. Інформаційно-аналітичне забезпечення управління витратами промислових підприємств : дис. ... канд. екон. наук : 08.00.04. Хмельницький, 2016. 226 с.

12. Литвак Б. Г. Разработка управленческого решения : учебник. 6-е изд., испр. и доп. М. : Дело, 2006. 440 с.
13. Писаренко Т. В., Кваша Т. К., Березняк Н. В., Прудка О. В. Інформаційне забезпечення інноваційного розвитку: світовий та вітчизняний досвід : монографія. Київ : УкрІНТЕІ, 2015. 239 с. URL: <https://www.pdaa.edu.ua/sites/default/files/node/2731/informzabesp5.pdf>
14. Пуцентейло П. Р. Інформаційне забезпечення аналітичної діяльності в управлінні підприємством. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького*. 2015. Вип. 11. С. 224–232. URL: <https://visnyk.iful.edu.ua/випуск-журналу-№11/інформаційне-забезпечення-аналітичн/>
15. Лісовський І. В., Рудніченко Є. М. Особливості формування системи інформаційно-аналітичного забезпечення управління витратами промислового підприємства. *Науковий вісник Полтавського університету економіки і торгівлі. Серія «Економічні науки»*. 2014. № 4. С. 140–145. URL: http://elar.khnu.km.ua/jspui/bitstream/123456789/4586/1/Nie_2015_1_21.pdf
16. Лісовський І. В., Рудніченко Є. М. Формування моделі оптимізації інформаційно-аналітичного забезпечення управління витратами промислового підприємства. *Бізнес Інформ*. 2015. № 9. С. 129–134. URL: https://www.business-inform.net/export_pdf/business-inform-2015-9_0-pages-129_134.pdf

REFERENCES

- Benko, M. M. *Informatsiini systemy i tekhnologii v bukh-halterskomu obliku* [Information Systems and Technologies in Accounting]. Kyiv: KNTEU, 2010.
- Bilenska, D. O. "Vyznachennia informatsii v kontseptsii antropotsentrychnoho pidkhotu" [Definition of the Concept Use Information in the Anthropocentric Approach]. *Teoriia i praktyka pravoznavstva*. 2013. <http://dspace.nlu.edu.ua/bitstream/123456789/5962/1/Bilenska.pdf>
- Danylchuk, L. "Sutnist definitsii «informatsiia»" [The Essence of the Definition "Information"]. *Pedahohika i psykholohiia profesiinoi osvity*. 2012. <http://ena.lp.edu.ua:8080/bitstream/ntb/23929/1/4-18-26.pdf>
- Demchenko, S. "Pidkhody do zmistu poniattia «informatsiia»: kibernetychnyi, filosofskyi, pravovyi" [Approaches to the Content of the Concept of "Information": Cybernetic, Philosophical, Legal]. *National Law Journal: Theory and Practice*. 2016. http://www.jurnaluljuridic.in.ua/archive/2016/1/part_2/7.pdf
- Huzhva, V. M. *Informatsiini systemy i tekhnologii na pidpriemstvakh* [Information Systems and Technologies in Enterprises]. Kyiv: KNEU, 2001.
- "Issledovaniia utechek informatsii ogranichenogo dostupa v 2019 godu : analiticheskii otchet" [Research of Restricted Information Leaks in 2019: Analytical Report]. <https://www.infowatch.ru/analytics/reports/27720>
- Ivakhnenkov, S. V. *Informatsiini tekhnologii audytu ta vnutrishnyohospodarskoho kontroliu v konteksti svitovoi intehtatsii* [Information Technologies of Audit and Internal Control in the Context of Global Integration]. Zhytomyr: Ruta, 2010.
- Ivanova, V. V. "Yakisni aspekty informatsiinoho zabezpechennia ekonomiky, zasnovanoi na znanniakh, informatsiinyi subiektmy klasteriv" [The Qualitative Aspects of the Information Maintenance of Knowledge Based Economy by the Informational Entities of Clusters]. *Ekonomichni chasopys-XXI*. 2011. <http://dspace.nbuv.gov.ua/bitstream/handle/123456789/48007/19-Ivanova.pdf?sequence=1>
- Komisarov, O. et al. "Model informatsiino-komunikativnoho vplyvu subiektiv zabezpechennia natsionalnoi bezpeky na dzherelo zahroz" [The Model of Informational and Communicative Influence of the Subjects of Ensuring National Security on the Source of Threats]. *Traektoriya nauki = Rath of Science. Section «Law»*, vol. 5, no. 1 (2019): 3001-3011. DOI: 10.22178/pos.42-3
- Kopytko, M. I. *Menedzhment informatsiinykh resursiv ta informatsiina bezpeka pidpriemstv* [Management of Information Resources and Information Security of Enterprises]. Lviv: Liha-Pres, 2016.
- Lisovskyi, I. V. "Informatsiino-analitychne zabezpechennia upravlinnia vytratamy promyslovykh pidpriemstv" [Information and Analytical Support of Cost Management of Industrial Enterprises]: *dys. ... kand. ekon. nauk : 08.00.04*, 2016.
- Lisovskyi, I. V., and Rudnichenko, Ye. M. "Formuvannia modeli optymizatsii informatsiino-analitychnoho zabezpechennia upravlinnia vytratamy promyslovoho pidpriemstva" [Building a Model for Optimization of Information-Analytical Ensuring of Cost Management of Industrial Enterprise]. *Bi-znes Inform*. 2015. https://www.business-inform.net/export_pdf/business-inform-2015-9_0-pages-129_134.pdf
- Lisovskyi, I. V., and Rudnichenko, Ye. M. "Osoblyvosti formuvannia systemy informatsiino-analitychnoho zabezpechennia upravlinnia vytratamy promyslovoho pidpriemstva" [Features of Formation of Information and Analytical Support Industrial Enterprise Cost Management]. *Naukovyi visnyk Poltavskoho universytetu ekonomiky i torhivli. Seriya «Ekonomichni nauky»*. 2014. http://elar.khnu.km.ua/jspui/bitstream/123456789/4586/1/Nie_2015_1_21.pdf
- Litvak, B. G. *Razrabotka upravlencheskogo resheniya* [Development of a Management Solution]. Moscow: Delo, 2006.
- Putsenteilo, P. R. "Informatsiine zabezpechennia analytychnoi diialnosti v upravlinni pidpriemstvom" [Information Support of Analytical in Business Management]. *Naukovo-informatsiinyi visnyk Ivano-Frankivskoho universytetu prava imeni Korolia Danyla Halytskoho*. 2015. <https://visnyk.iful.edu.ua/випуск-журналу-№11/інформаційне-забезпечення-аналітичн/>
- Pysarenko, T. V. et al. "Informatsiine zabezpechennia innovatsiinoho rozvytku: svitovyi ta vitchyzniani dosvid" [Information Support of Innovative Development: World and Domestic Experience]. Kyiv : UkrІNTEI, 2015. <https://www.pdaa.edu.ua/sites/default/files/node/2731/informzabesp5.pdf>