DOI: https://doi.org/10.32782/2524-0072/2022-38-16

УДК 334.722:005.57:004.056

БЕЗПЕКА ДАНИХ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОМУ СЕРЕДОВИЩІ ТА ЇЇ СКЛАДНІСТЬ ДЛЯ НОВИХ БІЗНЕС-МОДЕЛЕЙ

DATA SECURITY IN THE INFORMATION AND COMMUNICATION ENVIRONMENT AND ITS COMPLEXITY FOR NEW BUSINESS MODELS

Дячек Ольга Юріївна
кандидат економічних наук,
Харківський національний університет імені В.Н. Каразіна
ORCID: https://orcid.org/0000-0002-7285-6401

Рябченко Кристина Миколаївна
кандидат економічних наук,
Харківський національний університет імені В.Н. Каразіна
ORCID: https://orcid.org/0000-0002-6768-4414

Доценко Анна Володимирівна
студентка,
Харківський національний університет імені В.Н. Каразіна
ORCID: https://orcid.org/0000-0002-3920-9528

Dyachek Olga, Ryabchenko Kristina, Dotsenko Anna
V.N. Karazin Kharkiv National University

Данна стаття присвячена дослідженню безпеки даних в інтернеті та її впливу на бізнес середовище, а також визначенню кола проблем, що виникають із розвитком онлайн підприємництва. Використання передових інформаційних технологій і досягнень науково-технічного прогресу дало людям неабиякі можливості для спілкування, тому проблема кібербезпеки є дуже актуальною у наш час. Зростання кількості підключених пристроїв веде до збільшення ризиків безпеки: від заподіяння фізичної шкоди людям і пошкодження обладнання до кібератак в мережі. Однією з основних проблем цифровізації є забезпечення захищеності даних. Захист даних – це набір процесів і практик, призначених для захисту вашої екосистеми критичних інформаційних технологій.

Ключові слова кібербезпека, кібератака, цифровізація, технології, бізнес.

This article is dedicated to the continued safety of data on the Internet and the contribution to the business environment, as well as to the number of problems that are blamed on the development of online business. The adoption of advanced information technologies and the reach of scientific and technical progress gave people an incredible opportunity for communication, so the problem of cybersecurity is even more relevant in our time. Increasing the number of connected buildings in the lead to an increase in security risks: in the form of physical harm to people and the possibility of cyberattacks in the city. One of the main problems of digitalization is the security of data security. Defense of data – a set of processes and practices that are recognized for the defense of your ecosystem of critical information technologies. If information security is ensured, it will help to protect the information and information infrastructure of the enterprise from negative impacts. Such influences may be accidental or deliberate, internal or external. The result of interventions may be the loss of important information, its changing or using by third side in their own interests. Therefore, information security is an important aspect of business protection and business successful operation. For a variety of reasons, data security is crucial for the public and private sectors. First, the company has a legal and moral obligation to protect the data of its users and customers from falling into the wrong hands. For example, a financial company may need to adhere to the Payment Card Industry Data Security Standard (PCI DSS), which forces the company to take all reasonable steps to protect user data. Second, there is a risk of reputation fraud or data fraud. If a company does not take data security seriously, its reputation can be permanently damaged by advertising, high-profile leaks or hacking. Loss of trade secrets or intellectual property (IP) can affect

future innovation and profitability. In addition, reliability is becoming increasingly important for consumers: the protection of personal data and confidence in the reliability of their activities on the Internet are becoming a priority. This is especially important in the current rapid digitization of all aspects of life.

Keywords: cyber security, cyber-attack, digitalization, technology, business.

Постановка проблеми. Швидка цифровізація впливає на всі аспекти життя – включаючи спосіб взаємодії, роботу, покупки та отримання послуг – а також на те, як створюється та змінюється ціна. У цьому процесі дані та транскордонний потік даних стають все більш важливими для розвитку. Хоча традиційний цифровий розрив відображає значні відмінності у готовності використовувати дані між країнами та всередині них, він пов'язаний із комунікаціями. Цей розрив поглиблюється так званим обміном даними. Країни з обмеженою спроможністю перетворювати дані в цифровий інтелект і можливості для бізнесу та використовувати їх для економічного та соціального розвитку явно знаходяться в невигідному становищі.

Однією з основних проблем цифровізації є забезпечення захищеності даних. Захист даних – це набір процесів і практик, призначених для захисту вашої екосистеми критичних інформаційних технологій. Це включає файли, бази даних, облікові записи та мережі. Ефективна безпека даних передбачає набір елементів керування, програм та методів, які визначають важливість різних наборів даних та застосовують найбільш відповідні засоби безпеки. Вона враховує чутливість різних наборів даних та відповідні нормативні вимоги піддатливості. Як і інші позиції з кібербезпеки (приклад: безпека периметру та файлів) – безпека даних не є кінцевою для запобігання хакерським атакам. Отже, безпека даних – один із багатьох критичних методів оцінки загроз та зменшення ризику, пов'язаного із зберіганням та обробкою даних [6].

Аналіз останніх досліджень і публікацій. Питанню кібербезпеки бізнесу та держав приділяють увагу багато наукових діячів. Так, Безуглий Д.С. обґрунтував необхідність інформаційної безпеки як складової частини національної безпеки країни [1]. У вітчизняній юридичній літературі дослідженню окремих питань цієї проблематики в різні часи приділяли увагу такі фахівці, як А. Марущак, В. Брижко, М. Різак, В. Панченко, О. Радкевич та інші. Аналіз останніх досліджень і публікацій свідчить про те, що певні аспекти вітчизняних проблем інформаційної безпеки у той чи інший спосіб досліджувались у наукових працях Арістова І.В., Березовської І.Р., Дзьобаня О.П., Калюжного Р.А., Кормича Б.А., Ліпкана В.А., Марущак А.І., Цимбалюка В.С., Юдіна О.К. та інших. Питанням формування ефективного механізму правового регулювання протидії загрозам у кібернетичній сфері присвятили свої праці такі науковці: Бурячок В.Л., Шеломенцев В.П., Сопілко І.В., Куцаєв В.В., Мінін Д.С., Гнатюк С.О. та інші. Проте ці дослідження здебільшого зосереджені на сфері правового регулювання та формування системи інформаційної безпеки України. Розгляд цього питання здійснюється і зарубіжними вченими – І. Вельдер, А. Міллер, Р. Холлборг та інші (Dr. Christopher Karvetski, Necati Demir PhD, Oliver Holloway, IBM, John Tsitsiklis (professor MIT), Dimitri Bertsekas (professor MIT), Patric Jaillet (professor MIT)).

Виділення невирішених раніше частин загальної проблеми. Сьогодні, в контексті глобальної цифровізації, питання захисту є надзвичайно важливими і порушуються в більшості країн. Навіть інформаційні гіганти не завжди можуть повністю контролювати чи підтримувати узгодженість та конфіденційність своїх даних/програмного забезпечення, що свідчить про важливість цієї теми.

Не менш важливу проблему становить сьогодні торгівля базами даних, мова йде про інформацію як комерційного, так і особистого характеру. У багатьох країнах, незважаючи на різні підходи до цього питання, частина відомостей закрита для публічного розповсюдження, проте досить часто вона продається особами, які мають до неї доступ.

Формування цілей статті (постановка завдання). Організації по всьому світу вкладають значні кошти в інформаційні технології кібербезпеки, щоб захистити свої критично важливі активи. Незалежно від того, чи потрібно компанії захищати свій бренд, інтелектуальний капітал та інформацію про клієнтів, чи контролювати критичну інфраструктуру, інструменти виявлення інцидентів та пропаганди мають три загальні елементи: люди, процеси та технології.

З різних причин безпека даних має вирішальне значення для державного та приватного секторів. По-перше, компанія має юридичні та моральні зобов'язання захищати дані своїх користувачів і клієнтів від потрапляння в чужі руки. Наприклад, фінансовій компанії

може знадобитися дотримуватися стандарту безпеки даних індустрії платіжних карток (PCI DSS), який змушує компанію вживати всіх розумних заходів для захисту даних користувачів.

По-друге, існує ризик шахрайства з репутацією або шахрайством з даними. Якщо компанія не ставиться до безпеки даних серйозно, її репутація може бути назавжди зіпсована рекламою, гучними витоками чи хакерством. Не кажучи вже про фінансові та матеріально-технічні наслідки вторгнення даних. Компанії повинні витрачати час і гроші на оцінку та усунення втрат, а також на визначення того, які бізнес-процеси виявилися невдалими, а які необхідно покращити.

Виклад основного матеріалу дослідження. Цифрова економіка – це система економічних та соціальних відносин, які формуються на навичках інформаційно-комп'ютерних технологій (ІКТ) для ефективного виробництва, продажу та постачання продуктів та здійснення ділових операцій на ринку.

Вона продовжує розвиватися з великою швидкістю, керованою здатністю збирати, використовувати та аналізувати велику кількість інформації. Цифрові дані виникають із потоків особистої, соціальної та ділової діяльності, що відбувається на різних цифрових платформах. Окрім перспектив за рахунок цифровізації, виникає питання надійності в збереженні усіх даних та ступінь їх захищеності.

Дані стають активом. Збирання, опис, зберігання та опрацювання їх надають змогу отримувати цінну інформацію для використання в ділових процесах, суспільному житті, роботі держави. Вміння працювати з великими даними та їх аналізувати – це можливість першим отримувати цінні ринкові «інсайти», тобто бути конкурентоздатнішим. Доступ до даних здійснюється через Інтернет та інші мережі. Велика частина даних у світі стає відкритою [3].

Проаналізувавши цю таблицю, необхідно знайти розумний і прийнятний баланс між особистою участю в інформаційному просторі та повагою до особистої свободи та прав громадян в Інтернеті. Оскільки все більше комп'ютерів підключаються до Інтернету, у публічний інформаційний простір потрапляє все більше особистої інформації.

Цифрові дані фактично не регулюються, оскільки вони не підпадають під жодні правила, які застосовуються до звичайних товарів. Імовірність неправомірного використання інформації дуже висока і збільшується через адміністративні рішення або комерційні операції.

Необхідно вживати заходів, що дозволяють, якщо не повністю виключити, то хоча б мінімізувати цю небезпеку. Багато приватних компаній давно займаються питаннями безпеки власної продукції в цифровому просторі.

У січні 2002 року голова правління Microsoft Білл Гейтс звернувся до 50 тис. співробітників корпорації з листом, в якому поставив завдання створити для клієнтів захищене інформаційне середовище, яке було б вкрай надійне. Програма захищених інформаційних систем охоплює чотири напрямки: безпека, конфіденційність, безвідмовність і бізнес-етику.

На державному рівні також вживаються заходи, направлені на захист цифрового простору. В Україні діє Закон «Про захист інформації в інформаційно-телекомукаційних системах» від 05.07.1994 № 80/94-ВР. Останні зміни до Закону були прийняті 4 червня 2020 року, які були напрацьовані робочою групою Державної служби спеціального зв'язку та захисту інформації України, Міністерством цифрової трансформації України, Державною митною службою та експертів галузі. Ці зміни стосуються підтвердження відповідності інформаційної системи вимогам із захисту інформації ЄС. Впроваджено вимоги стандартів сімейства системи управління інформаційною безпекою (СУІБ) для окремих категорій інформації. Ці вимоги діятимуть для забезпечення інформаційної та кібербезпеки в ЄС і наближатимуть Україну до європейських норм.

За Законом, підтвердження відповідності комплексної системи захисту інформації (КСЗІ) відбуватиметься за результатами держекспертизи. Відтепер державні інформаційні ресурси та інформація з обмеженим доступом, крім державної таємниці, може оброблятися в системі без застосування КСЗІ, у разі виконання умов:

– підтвердження відповідності системи управління інформаційною безпекою національним стандартам України щодо систем управління інформаційною безпекою;

– використання для захисту інформації в системі засобів криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи;

– жоден з елементів системи не може бути розташований на території України, де органи державної влади тимчасово не здійснюють своїх повноважень, на територіях держав, визнаних Верховною Радою України державами-агресорами, на територіях держав, щодо яких застосовані санкції відповідно до

Таблиця 1

Вид економічної діяльності	Кількість підприємств, які мають доступ до мережі Інтернет					
	Одиниць			у % до загальної кількості підприємств		
	2018	2019	2020	2018	2019	2020
Переробна промисловість	10878	11089	11323	90,0	89,5	90,1
Виробництво харчових продуктів, напоїв і тютюнових виробів	2071	2046	2065	90,2	90,3	2071
Текстильне виробництво, виробництво одягу, шкіри, виробів зі шкіри та інших матеріалів	890	927	963	82,7	82,6	890
Виготовлення виробів з деревини, паперу та поліграфічна діяльність	1264	1305	1352	89,3	88,7	1264
Виробництво коксу та продуктів нафтоперероблення	47	39	42	87,0	90,7	47
Виробництво хімічних речовин і хімічної продукції	419	460	458	90,7	93,1	419
Виробництво основних фармацевтичних продуктів і фармацевтичних препаратів	104	103	109	88,9	89,6	104
Виробництво гумових і пластмасових виробів, іншої неметалевої мінеральної продукції	1628	1608	1662	90,7	89,2	1628
Металургійне виробництво, виробництво готових металевих виробів, крім машин і устаткування	1290	1315	1372	91,3	89,7	1290
Машинобудування; виробництво меблів, іншої продукції, ремонт і монтаж машин і устаткування	3165	3286	3300	91,4	91,0	3165
Виробництво комп'ютерів, електронної та оптичної продукції	248	258	260	95,8	94,2	248
Виробництво меблів, іншої продукції, ремонт і монтаж машин і устаткування	1372	1419	1470	88,6	89,2	1372
Постачання електроенергії, газу, пари та кондиційованого повітря	701	709	754	93,2	92,3	701
Будівництво	4783	4883	5141	87,9	83,9	4783
Інформація та телекомунікації	1949	1946	1971	90,0	89,2	1949
Операції з нерухомим майном	2704	2697	2796	87,8	86,3	2704
Діяльність туристичних агентств, туристичних операторів, надання інших послуг із бронювання та пов'язана з цим діяльність	162	166	153	86,0	72,8	162
Інформаційно-комунікаційні технології	1456	1567	1670	89,9	88,5	1456

Джерело: складено авторами згідно даних [2]

Закону України «Про санкції», та на територіях держав, які належать до митних союзів з такими державами;

– виконання особливих вимог, встановлених Урядом до забезпечення захисту інформації в системах залежно від категорії державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом [4].

На сьогодні Інтернет-платформа є потужною, але вона не призначена для справжньої децентралізації. Більшість сучасних обчислень та зберігання в Інтернеті виконується у хмарних сховищах та центрах обробки даних великих корпорацій. Їх продуктивність і надійність виявляються набагато сильнішими, ніж особисті термінали. В результаті більшість прав та цінностей

користувачів Інтернету захоплюються цими корпораціями.

Бар'єри для розвитку тренду в Україні:

– Відсутність системи правил, регламентів, стандартів збирання, класифікації, зберігання та використання даних (національний, регіональний, галузевий та інші рівні).

– Проблеми захисту інтелектуальної власності.

– Проблеми щодо захисту даних, ризики кібербезпеки.

– Відсутність у громадян достатніх компетентностей роботи з даними (цифрових навичок), відповідної освіти, професій тощо.

Можливості, які створює тренд для України

– Розвиток нової галузі економіки, нові робочі місця.

– Створення бази для розвитку всіх галузей та цифрової економіки.

– Поява ефективного інструменту управління.

– Створення середовища, що унеможливлює корупцію як явище [4].

Завдяки послугам на вимогу та масштабованості хмарні обчислення стали новою технологією. Сьогодні вони найчастіше використовуються для зберігання даних і великих програм або обчислювальних програм. Тому безпека та конфіденційність даних стали основними проблемами, особливо для даних бізнес-рівня.

Враховуючи глобальний характер світової економіки, слід зазначити, що питання цифрової безпеки стає наднаціональним. Типовими загрозами національній цифровій безпеці є фінанси, енергетика та інфраструктура.

Потенційна уразливість цифрових систем створює небезпеку цифрового колапсу, подібного до того, який описали в своїй книзі Люсі та Стівен Хокінг. При цьому можливе загострення соціальних проблем: зростання структурного безробіття як наслідок цифрової революції, відчуження працівника від продукту своєї праці в результаті розвитку дистанційної зайнятості, особисте збіднення індивідів.

Інноваційні та інформаційні ресурси мають позанаціональний характер, застосовуються в різних країнах, тому захист даних – проблема не тільки національного, а й наднаціонального рівня.

У хмарному середовищі дані користувачів зберігаються у віддалених екземплярах віртуальних машин, що знаходяться у розпорядженні хмарних провайдерів. Можуть бути різні зовнішні атаки на віртуальні машини, включаючи атаку шкідливих кодів, компрометацію відповідного монітора віртуальної машини тощо. Крім зовнішньої атаки, користувачі не мають фізичного контролю над своїми даними. Інсайдери хмарних провайдерів могли чітко бачити, що зберігається у їхніх екземплярах віртуальних машин. Було б катастрофою, якщо інсайдери хмарних провайдерів змовилися з супротивниками, щоб навмисно змінити або випустити дані клієнтів.

Існують три основні елементи безпеки даних, яких повинні дотримуватися всі організації: конфіденційність, цілісність та доступність. Ці концепції також називаються Тріадою ЦРУ, яка функціонує як модель безпеки та рамка для першокласної безпеки даних. Ось що означає кожен основний елемент з точки зору захисту ваших конфіденційних даних від несанкціонованого доступу та вилучення даних (рис. 1).

Інструменти та технології захисту даних мають вирішувати зростаючі проблеми, властиві безпеці сучасних складних, розподілених, гібридних та/або багатохмарних обчислювальних середовищ. Вони включають розуміння, де знаходяться дані, відстеження того, хто має до них доступ, а також блокування діяльності з високим ризиком та потенційно небезпечних переміщень файлів. Комплексні рішення щодо захисту даних, які дозволяють підприємствам прийняти централізований підхід до моніторингу та застосування політики, можуть спростити завдання.

Конфіденційна інформація може міститися у структурованих та неструктурованих хмарних сховищах. Рішення для виявлення та класифікації даних автоматизують процес виявлення конфіденційної інформації, а також оцінки та усунення вразливих місць.

Інструменти виявлення та класифікації даних:

– Моніторинг активності даних та файлів. Інструменти моніторингу активності аналізують шаблони використання даних, дозволяючи групам безпеки бачити, хто та для чого звертається до даних, виявляти аномалії та визначати ризики.

– Інструменти оцінки вразливості та аналізу ризиків. Ці рішення полегшують процес виявлення та пом'якшення таких вразливих місць, як застаріле програмне забезпечення, неправильна конфігурація або слабкі паролі, а також можуть визначати джерела даних з найбільшим ризиком зараження.

– Автоматизоване звітування про відповідність вимогам. Комплексні рішення для

Рис. 1. Основні елементи захисту даних

Джерело: складено автором на основі даних [6]

захисту даних з можливостями автоматизованої звітності можуть створити централізоване сховище для перевірок відповідності на рівні підприємства.

Дослідження Інституту Понемона щодо вартості даних та щодо порушення даних виявило, що в середньому збиток, завданий внаслідок порушення даних у США, становив 8 мільйонів доларів. 25575 облікових записів користувачів зазнали впливу середнього інциденту з даними, що означає, що крім фінансових втрат більшість інцидентів призводять до втрати довіри клієнтів та шкоди репутації [7].

Великий відсоток «викриття» даних не є результатом зловмисної атаки, а спричинене необережним або випадковим викриттям конфіденційних даних. Співробітники організації часто розповсюджують, надають доступ, втрачають або неправильно поводяться з цінними даними – випадково або тому, що вони не знають про політику безпеки.

Цю велику проблему можна вирішити шляхом навчання співробітників, а також за допомогою інших заходів, таких як технологія запобігання втраті даних (DLP) та покращений контроль доступу. Середня вартість порушень даних є найвищою в США (рис. 2).

Яскравим та актуальним прикладом проблеми захисту даних є тимчасове відключення основного сайту соціальних мереж Facebook Inc, популярної платформи обміну фотографіями Instagram та додатку для обміну повідомленнями WhatsApp, які були заблоковані десяткам тисяч користувачів.

Reuters, одне з найбільших у світі міжнародних агентств новин та фінансової інформації, не змогло підтвердити проблему, яка впливала на платформу. Однак повідомлення про помилку на веб-сторінці Facebook передбачає помилку системи доменних імен (DNS).

DNS дозволяє веб-адресам доставляти користувачів до місця призначення. Подібний збій у хмарній компанії Akamai Technologies Inc знищив кілька веб -сайтів у липні.

Перебої в технологіях це не рідкість, але водночас затьмарити стільки програм від найбільшої у світі компанії з соціальних медіа було надзвичайно незвично. Останнє значне відключення Facebook відбулося в 2019 році, коли технічна помилка вплинула на його сайти протягом 24 годин.

Цього разу винуватцем стали зміни базової інфраструктури Інтернету, яка координує трафік між її центрами обробки даних. Це призвело до переривання зв'язку та каскаду до інших центрів обробки даних, зупинивши сайт.

Через цей інцидент акції Facebook впали на 5,5% у другій половині дня в понеділок, наблизившись до свого найгіршого показника за майже рік.

Захист даних – це захід безпеки, призначений для запобігання несанкціонованому доступу до баз даних, веб-сайтів і комп'ютерів. Цей процес також забезпечує механізм захисту даних від втрати або пошкодження. Кожен бізнес сьогодні, чи то маленька компанія, місцева компанія чи велика компанія, не може забути вжити заходів безпеки. Відсутність належного плану інформаційної безпеки може призвести до серйозних наслідків для бізнесу. Це важливо з основних причин: забезпечити безперервність бізнесу, уникнути

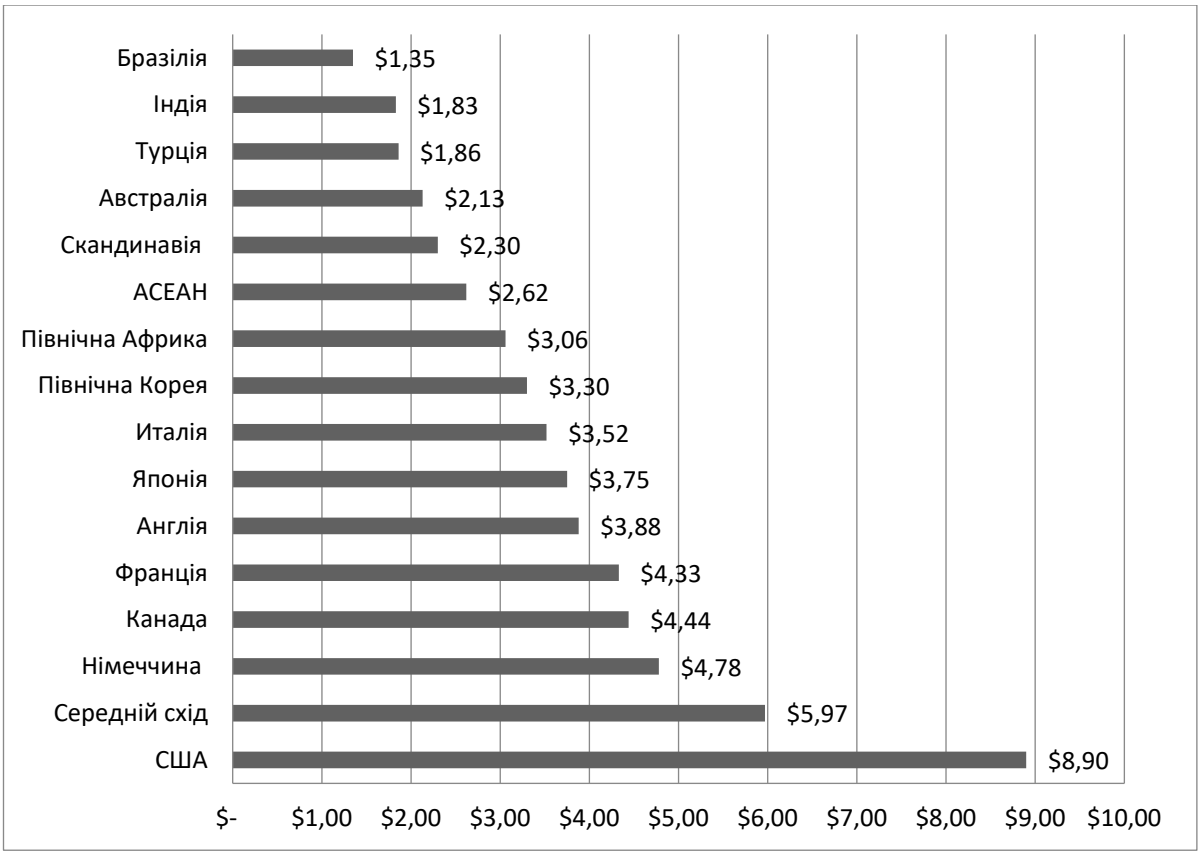

Рис. 2. Вартість вторгнення даних за країною

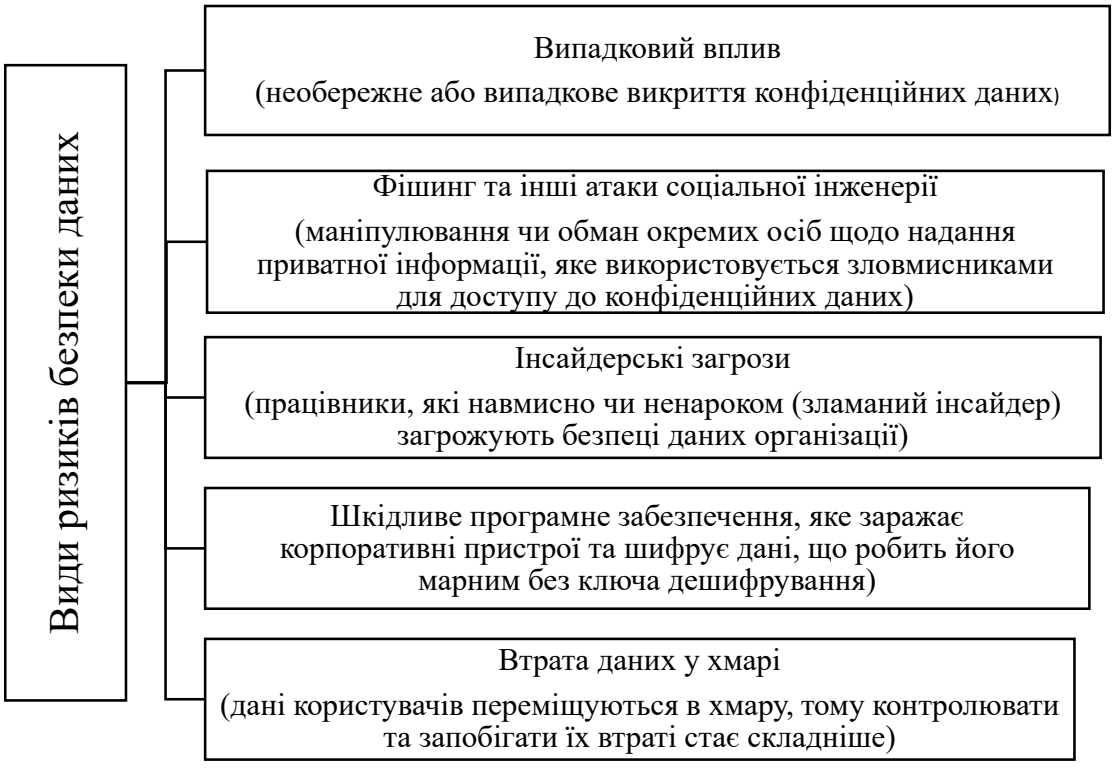

Рис. 3. Види ризиків безпеки даних

витоку даних та запобігти несанкціонованому доступу.

Сьогодні важливість безпеки даних зростає в кожній галузі. Безпека даних у особистому житті потрібна кожному. Кожна компанія має у своїй базі даних великі дані, які необхідно захищати. Якщо цю інформацію будь-яким чином знищити, компанія зазнає величезних збитків. Можна сказати, що «дані – це нова нафта». У будь-якому бізнесі найголовніше – це його дані. Тому, щоб захистити ці дані, компанії також готові використовувати високий рівень безпеки з високою ціною [5].

Використовуючи ці методи для запобігання витоку даних, ви можете мінімізувати ризик і захистити себе від будь-яких кібератак.

Тенденції безпеки даних [7]:

– Штучний інтелект покращує можливості систем безпеки даних, оскільки він може обробляти великі обсяги даних. Когнітивні обчислення – це підмножина штучного інтелекту, який виконує ті ж завдання, що й інші системи штучного інтелекту, але досягається шляхом моделювання процесу мислення людини. У сфері безпеки даних це дозволяє швидко приймати рішення, коли це потрібно терміново.

– Холодна безпека. Зі збільшенням хмарних функцій розширюється і визначення безпеки даних. Зараз організаціям потрібні складніші рішення, оскільки їм потрібно не лише захищати дані, а й додатки та власні бізнес-процеси, які працюють у публічних та приватних хмарах.

– Квантова. Очікується, що революційна технологія Quantum змінить багато традиційних технологій у геометричній прогресії. Алгоритми шифрування стануть різноманітнішими, складнішими та безпечнішими.

Висновок. Цінність бізнесу та захист даних ніколи не були вищими, ніж сьогодні. Втрата комерційної таємниці або інтелектуальної власності (ІВ) може вплинути на майбутні інновації та прибутковість. Крім того, надійність стає все більш важливою для споживачів: захист персональних даних і впевненість у надійності їх діяльності в Інтернеті стають пріоритетними. Це особливо важливо в умовах нинішньої швидкої оцифровки всіх аспектів життя. Додавання додаткового рівня безпеки даних може значно запобігти несанкціонованому доступу до вашої компанії або вашого обладнання та систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Безуглий Д. Інформаційна безпека України: огляд останніх тенденцій. *Фізико-математична освіта.* 2018. Вип. 2(16). С. 13–17.

2. Державна служба статистики України. Київ, 2022. URL: http://www.ukrstat.gov.ua (дата звернення: 20.03.2022).

3. Український інститут майбутнього. Київ, 2022. URL: http://www.uifuture.org (дата звернення: 19.04.2022).

4. Міністерство та Комітет цифрової трансформації України. Київ, 2020. URL: https://thedigital.gov.ua/news/ukhvaleno-zakon-pro-zakhist-informatsii-v-telekomunikatsiynikh-sistemakh (дата звернення 13.10.2021).

5. Ajay Ohri. Importance of Data Security In 2021: Jigso Academy. 20 February, 2021. URL: https://www.jigsawacademy.com/blogs/cyber-security/importance-of-data-security/

6. David Harrington. Data Security: Definition, Explanation and Guide: Varonis / Inside Out Security Blog. July 6, 2021. URL: https://www.varonis.com/blog/data-security/

7. Data Security. Imperva, 2021. URL: https://www.imperva.com/learn/data-security/data-security/ (дата звернення: 12.01.2022).

REFERENCES:

1. Bezugliy D. (2018) Informaciyna bezpeka Ukrainu: oglyad ostannih tendenciy [Information security of Ukraine: an overview of recent trends]. *Fizuko-matematuchna osvita*, vol. 2(16), pp. 13–17.

2. Derjavna slujba statustuku Ukrainu. Kyiv, 2022. Available at: http://www.ukrstat.gov.ua (accessed 20 March 2022).

3. Ukrainskuy instutyt maibutniogo. Kyiv, 2022. Available at: http: //www.uifuture.org (accessed 19 April 2022).

4. Ministerstvo ta komitet cifrovoi transformacii Ukrainu. Kyiv, 2020. Available at: https://thedigital.gov.ua/news/ukhvaleno-zakon-pro-zakhist-informatsii-v-telekomunikatsiynikh-sistemakh (accessed 13 October 2021).

5. Ajay Ohri. Importance of Data Security In 2021: Jigso Academy. 20 February, 2021. Available at: https://www.jigsawacademy.com/blogs/cyber-security/importance-of-data-security/

6. David Harrington. Data Security: Definition, Explanation and Guide: Varonis / Inside Out Security Blog. July 6, 2021. Available at: https://www.varonis.com/blog/data-security/

7. Data Security. Imperva, 2021. Available at: https://www.imperva.com/learn/data-security/data-security/ (accessed 12 January 2022).