Стала економіка

УДК 004.65.056:330.3

DOI https://doi.org/**10.5281/zenodo.15082464**

Кібербезпека бізнесу: загрози для баз даних, фінансові наслідки та інвестиції у захист

Помазун Оксана Миколаївна

кандидат економічних наук, доцент, доцент кафедри інформаційних систем в економіці, Київський національний економічний університет імені Вадима Гетьмана, 03057, Україна, Київ, просп. Берестейський, 54/1,

ORCID: https://orcid.org/0000-0001-9697-1415

Крошко Іван Андрійович

аспірант кафедри інформаційних систем в економіці, Київський національний економічний університет імені Вадима Гетьмана, 03057, Україна, Київ, просп. Берестейський, 54/1,

ORCID: https://orcid.org/0009-0006-3680-4029

Пєтухова Олена Анатоліївна

старший викладач кафедри математичного моделювання та статистики, Київський національний економічний університет імені Вадима Гетьмана, 03057, Україна, Київ, просп. Берестейський, 54/1,

https://orcid.org/0000-0003-2105-7666

Синицький Ростислав Костянтинович

аспірант кафедри інформаційних систем в економіці, асистент кафедри інформаційних систем в економіці, Київський національний економічний університет імені Вадима Гетьмана, 03057, Україна, Київ, просп. Берестейський, 54/1, ORCID : https://orcid.org/0009-0002-6271-3041

Прийнято: 10.03.2025| Опубліковано: 25.03.2025

Анотація. *У сучасних умовах цифровізації бізнесу та зростання залежності компаній від інформаційних технологій витоки даних стали однією з найсерйозніших загроз для корпоративної безпеки. Масштабні інциденти компрометації баз даних призводять до значних фінансових втрат, юридичних санкцій та втрати довіри клієнтів, що вимагає комплексного підходу до управління кіберризиками. Посилення регуляторного контролю та впровадження жорсткіших норм захисту інформації також зумовлюють необхідність перегляду бізнес-стратегій у сфері інформаційної безпеки.* ***Мета.*** *Дослідження спрямоване на аналіз загроз інформаційній безпеці бізнесу, зокрема витоків даних, що впливають на бази даних компаній, а також економічних наслідків таких інцидентів. Визначено основні фактори, що спричиняють компрометацію інформації, та оцінено фінансові ризики, пов'язані із втратою конфіденційних даних. Особливу увагу приділено регуляторним санкціям та інвестиціям компаній у заходи кібербезпеки з метою мінімізації ризиків витоків.* ***Методи.*** *У роботі використано методи аналізу статистичних даних, порівняльного аналізу нормативних вимог у сфері інформаційної безпеки, а також систематизації тенденцій розвитку кіберзагроз. Джерелами інформації стали дані міжнародних аналітичних центрів, звіти компаній із кібербезпеки та матеріали про накладені штрафи за порушення конфіденційності.* ***Результати.*** *Встановлено, що масштаби витоків даних продовжують зростати, при цьому ключовими причинами інцидентів залишаються недостатній рівень контролю доступу до баз даних, людський фактор, атаки через підрядників та експлуатація невиправлених вразливостей. Аналіз фінансових наслідків продемонстрував, що компанії зазнають не лише прямих витрат на ліквідацію наслідків кіберінцидентів, але й значних регуляторних штрафів та судових витрат. Результати дослідження також свідчать про суттєве зростання інвестицій у кібербезпеку, причому основні витрати спрямовані на тестування та*

реагування на інциденти, впровадження технологій виявлення загроз та підвищення рівня обізнаності персоналу. ***Висновки.*** *Поглиблений аналіз проблеми витоків даних у бізнесі підтвердив, що компанії змушені змінювати підходи до інформаційної безпеки, орієнтуючись не лише на мінімізацію наслідків атак, але й на їхнє попередження. Зростаючий рівень фінансових втрат та посилення нормативного регулювання стимулюють організації до перегляду стратегій управління кіберризиками. Виявлено необхідність подальшого дослідження ефективності технологій штучного інтелекту для виявлення та запобігання витокам, оцінки довгострокових економічних збитків від інцидентів, а також вивчення впливу глобальних змін у регуляторній політиці на стратегії кібербезпеки.*

Ключові слова: *бази даних, кібербезпека, витоки даних, інвестиції у кібербезпеку, інформаційна безпека бізнесу, аналітика загроз, статистика кібератак, кіберризики, інциденти інформаційної безпеки, статистичний аналіз витоків даних.*

Business Cybersecurity: Threats to Databases, Financial Consequences, and Investments in Protection

Pomazun Oksana Mykolaivna

Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department of Information Systems in Economics, Kyiv National Economic University named after Vadym Hetman, 03057, Ukraine, Kyiv, 54/1 Beresteiskyi Avenue, ORCID: https://orcid.org/0000-0001-9697-1415

Kroshko Ivan Andriiovych
Postgraduate Student of the Department of Information Systems in Economics, Kyiv National Economic University named after Vadym Hetman, 03057, Ukraine, Kyiv, 54/1 Beresteiskyi Avenue,
ORCID: https://orcid.org/0009-0006-3680-4029

Petukhova Helena Anatoliivna
Senior Lecturer of the Department of Mathematical Modeling and Statistics, Kyiv National Economic University named after Vadym Hetman, 03057, Ukraine, Kyiv, 54/1 Beresteiskyi Avenue,
https://orcid.org/0000-0003-2105-7666

Synytskyi Rostyslav Kostiantynovych
Postgraduate Student of the Department of Information Systems in Economics, Assistant Of Department Of Information Systems In Economics, Kyiv National Economic University named after Vadym Hetman, 03057, Ukraine, Kyiv, 54/1 Beresteiskyi Avenue,
ORCID : https://orcid.org/0009-0002-6271-3041

Abstract. *In the modern era of business digitalization and increasing reliance on information technologies, data breaches have become one of the most serious threats to corporate security. Large-scale incidents of database compromise lead to significant financial losses, legal sanctions, and loss of customer trust, necessitating a comprehensive approach to cybersecurity risk management. The tightening of regulatory control and the implementation of stricter data protection standards further emphasize the need for businesses to revise their information security strategies.* ***Purpose.*** *This study aims to analyze threats to business information security, particularly data breaches affecting corporate databases, and their economic consequences. The key factors leading to data compromise are identified, and financial risks associated with data loss are assessed. Special attention is given*

to regulatory sanctions and corporate investments in cybersecurity measures to minimize breach risks. ***Methods.*** *The study employs statistical data analysis, comparative analysis of regulatory requirements in information security, and systematization of cybersecurity threat trends. The sources of information include reports from international analytical centers, cybersecurity companies and materials on imposed fines for confidentiality violations.* ***Results.*** *The study finds that the scale of data breaches continues to grow, with the primary causes of incidents being insufficient database access control, human factors, supply chain attacks, and the exploitation of unpatched vulnerabilities. An analysis of financial consequences demonstrated that companies incur not only direct costs for mitigating cybersecurity incidents but also significant regulatory fines and legal expenses. The study results also indicate a substantial increase in cybersecurity investments, with primary expenditures directed toward incident response and testing, threat detection technologies, and personnel awareness training.* ***Conclusions.*** *An in-depth analysis of data breaches in business confirms that companies must adapt their approaches to information security, focusing not only on minimizing the consequences of attacks but also on their prevention. The growing financial losses and increased regulatory oversight compel organizations to reassess their cybersecurity risk management strategies. Further research is needed on the effectiveness of artificial intelligence technologies in detecting and preventing data breaches, evaluating the long-term economic impact of incidents, and analyzing the influence of global regulatory changes on cybersecurity strategies.*

Keywords: *Databases, cybersecurity, data breaches, cybersecurity investments, business information security, threat analytics, cyber attack statistics, cyber risks, information security incidents, statistical analysis of data breaches.*

Постановка проблеми у загальному вигляді та її зв'язок з важливими науковими чи практичними завданнями. У сучасних умовах цифровізації бізнесу та глобальної інтеграції інформаційних систем проблема витоків даних набула особливо актуального значення. Збільшення обсягу

цифрових активів, розвиток хмарних технологій та поширення електронної комерції зробили компанії вразливими до цілеспрямованих атак з боку кіберзлочинців. Масштабні інциденти, що спричиняють компрометацію баз даних, не лише ставлять під загрозу конфіденційну інформацію, але й завдають компаніям значних фінансових збитків, підривають довіру клієнтів та призводять до юридичних санкцій.

Згідно з актуальними статистичними даними, значна частка витоків відбувається через людський фактор, недостатній рівень захисту корпоративних баз даних та використання уразливостей у програмному забезпеченні. Крім того, спостерігається зростання загроз, пов’язаних із атаками на постачальників і підрядників, що підкреслює важливість забезпечення комплексного підходу до управління кіберризиками.

Актуальність проблеми також зумовлена посиленням регуляторного контролю. В останні роки було прийнято низку нормативних актів, спрямованих на підвищення стандартів захисту персональних даних та відповідальності компаній за їх збереження. Порушення цих вимог призводить до багатомільйонних штрафів, що стають значним фінансовим навантаженням для бізнесу.

Аналіз останніх досліджень і публікацій. Проблематика захисту інформації та протидії витокам даних у сучасному цифровому середовищі залишається однією з найбільш актуальних і водночас складних завдань, що стоять перед організаціями різних сфер діяльності. Існує значна кількість наукових досліджень та публікацій, присвячених проблемам інформаційної безпеки та захисту від витоків даних, в яких розглядаються різноманітні технології, методи й інструменти для запобігання таким інцидентам.

Актуальність цієї проблеми підтверджується у роботі Ф. Шлакль та ін. [1], автори якої здійснюють міждисциплінарний огляд досліджень щодо причин і наслідків витоків даних, зокрема акцентуючи увагу на управлінських та організаційних аспектах. Автори наголошують на значному зростанні витрат, пов'язаних із витоками даних, та на необхідності всебічного аналізу

цієї проблематики. Вони також визначають перспективні напрямки майбутніх досліджень, підкреслюючи потребу глибшого вивчення впливу витоків на постаждалих та застосування різноманітних теоретичних підходів і методів для комплексного вирішення проблеми.

Ґрунтовне дослідження підходів до захисту від витоків даних та методи протидії внутрішнім загрозам інформаційної безпеки розглянуті в статті І. Еррери Монтано та інших авторів [2]. У роботі основна увага приділяється аналізу систем захисту від витоків даних (DLP), що використовують такі технології, як шифрування, машинне навчання, біометричну автентифікацію, блокчейн, а також керування цифровими правами (DRM). Крім того, у статті розглядаються сучасні тенденції, обмеження та перспективні напрями розвитку зазначених технологій.

Проблеми витоків даних з бази даних підприємств розглядають Лун Чен та інші [3], визначаючи причини таких інцидентів, пов’язані як з внутрішніми, так і зовнішніми загрозами. Автори описують приклади значних витоків інформації, класифікують загрози за походженням і причинами, аналізують сучасні технології та методи виявлення й запобігання втратам даних, а також висвітлюють обмеження цих технологій. Особливий акцент у статті зроблено на складнощах, які виникають у зв’язку зі зростанням обсягів даних.

Шанітамол Грейсі [4] розглядає тенденції та особливості витоків даних за останні 10 років (2004 – 2024 роки), аналізуються галузі, методи кібератак, типи скомпрометованих даних і регіональна специфіка інцидентів. Автори використовують інструмент Power BI для виявлення часових трендів і взаємозв'язків між цими чинниками.

Аналіз витоків даних, їх причини та заходи безпеки також опубліковані в роботі С. Чжана та інш. [5], зокрема, розглядаються типові інциденти витоків даних, їхні причини, наслідки, а також заходи та виклики щодо запобігання таким інцидентам. В статті Р. Патіл та ін. [6] визначені причини, наслідки, сучасні методи виявлення і запобігання витокам корпоративних даних та перспективні напрями розвитку в цій сфері. Ф. Хан та ін. [7] досліджують

ризики, пов'язані з витоками даних (причини, місця виникнення та наслідки), а також способи їх вирішення через профілактику, стримування та відновлення, запропоновані на основі теорії управління ризиками. Подібні питання висвітлені в роботі Рибальченко Л.В. та ін [8], в якій розглядаються особливості застосування методів управління ризиками, аналізу потенційних загроз та здійснення моніторингу рівня кібербезпеки.

С. Алнеяді, Е. Сітхірасенан та В. Мутуккумарасамі [9] розглядають системи запобігання витокам конфіденційних даних, аналізуючи їхні переваги, недоліки, сучасні тенденції та перспективні напрямки розвитку, а також наводять класифікацію методів і технік аналізу, що використовуються в таких системах. Системний підхід до класифікації даних за ступенем конфіденційності та доступності у контексті управління інформаційною безпекою висвітлюється у роботі Лубка Д. В. та Мірошниченка М. Ю. [10], де розглядаються методи запобігання зловмисному впливу через впровадження відповідних політик безпеки, аудитів та криптографічного захисту інформації.

Дослідження О. Гарасимчука та О. Бужович [11] акцентує увагу на стратегіях захисту баз даних у контексті зростаючих кіберзагроз. Автори аналізують інноваційні підходи до кібербезпеки, зокрема застосування багаторівневого шифрування, автентифікації користувачів та механізмів моніторингу, що спрямовані на зменшення ймовірності несанкціонованого доступу та витоків даних. Дослідження підкреслює необхідність впровадження комплексних заходів безпеки, що поєднують технічні та організаційні методи захисту інформації. А. М. Аль-Хавамле [12] досліджує типи кібератак, основні інструменти зловмисників та заходи безпеки, спрямовані на захист інформації від витоків, а також наголошує на необхідності впровадження передових технологій, зокрема двофакторної автентифікації та штучного інтелекту, для запобігання таким загрозам. Цзяньцін У та Пін Чжа [13] визначають основні причини масових витоків даних і також пропонують нову модель захисту інформації, що базується на мінімізації довіри й самостійному шифруванні даних користувачами.

Проте, у даних публікаціях недостатньо дослідженими залишаються економічні наслідки витоків даних та ефективність інвестицій у кібербезпеку, зокрема зв'язок між витратами на інформаційну безпеку та зменшенням фінансових ризиків.

Деякі дослідження акцентують увагу на факторах, що впливають на ймовірність витоків даних, проте не розглядають їх економічних наслідків. У роботі М. Еттреджа, Ф. Го та Ї. Лі [14] аналізується вплив публічного розкриття інформації про комерційні таємниці на ймовірність кібератак. Автори доводять, що компанії, які у своїх звітах зазначають про наявність торгових секретів, частіше зазнають витоків даних, проте дослідження не розглядає фінансових наслідків таких інцидентів, а також не аналізує, наскільки інвестиції у кібербезпеку можуть знизити ці ризики. Схожий підхід простежується у дослідженні К. Абукарі та ін.[15], в якому аналізується вплив тону корпоративної комунікації на вразливість компаній до витоків даних. Дослідження показує, що позитивний тон звітності може підвищувати ймовірність кібератак, проте не містить аналізу того, як такі витоки впливають на фінансові показники організацій та які економічні наслідки вони спричиняють у довгостроковій перспективі.

Проблему забезпечення безпеки персональних даних з позиції правового захисту розглянуто в роботі Чернявської Б. В. та Ковальчука А. Ю.[16]. За результатами досліджень автори зазначають, що кібератаки, витоки персональних даних, розвиток розвідки з відкритих джерел, цифрова ідентифікація та поширення Інтернету речей створюють реальні загрози для приватності особи та безпеки її ідентифікаційної інформації. Проте, автори не аналізують причини витоків персональної інформації та не пропонують шляхів вирішення цієї проблеми.

Дані роботи роблять значний внесок у розуміння факторів, що впливають на ймовірність витоків даних, однак не охоплюють аспекти їхнього економічного впливу. Відсутність детального аналізу фінансових втрат від

витоків даних та ефективності заходів інформаційної безпеки вказує на необхідність подальших досліджень у цьому напрямі.

Виділення невирішених раніше частин загальної проблеми. Попри активний розвиток методів кіберзахисту, проблема витоків даних залишається однією з найактуальніших загроз для бізнесу. Значна кількість досліджень зосереджується на технічних аспектах інформаційної безпеки, розглядаючи методи шифрування, багатофакторну автентифікацію та виявлення загроз. Водночас недостатньо вивченими залишаються економічні наслідки витоків даних, їхній вплив на конкурентоспроможність компаній, а також ефективність інвестицій у заходи кібербезпеки.

Особливої уваги потребує питання взаємозв'язку між витратами на інформаційну безпеку та зменшенням фінансових ризиків, спричинених витоками даних. Попри те, що існують глобальні тенденції щодо зростання інвестицій у кібербезпеку, залишається відкритим питання, які саме заходи забезпечують найбільшу ефективність для різних категорій бізнесу та які фактори впливають на ухвалення рішень щодо фінансування кіберзахисту.

Основний внесок даного дослідження полягає у комплексному підході до вивчення проблеми через поєднання аналізу масштабів витоків даних, оцінки фінансових наслідків та тенденцій інвестицій у кібербезпеку. Дослідження дозволяє визначити ключові фактори ризику, які найбільшою мірою впливають на безпеку корпоративних баз даних, а також сформувати основу для подальших досліджень у сфері оптимізації витрат на інформаційну безпеку. Таким чином, дослідження заповнює наявні прогалини в розумінні економічного впливу витоків даних, що є важливим для ухвалення ефективних управлінських рішень у сфері кіберзахисту.

Формулювання цілей статті (постановка завдання). Зростання кількості витоків даних та їхній значний вплив на фінансовий стан компаній вимагають глибокого аналізу не лише самих інцидентів, а й економічних наслідків та ефективності заходів кібербезпеки. Відсутність комплексного підходу до оцінки фінансових ризиків, спричинених порушеннями

конфіденційності, створює потребу у детальному дослідженні взаємозв'язку між загрозами інформаційній безпеці, регуляторними санкціями та інвестиціями у захист даних.

Мета статті – проаналізувати основні загрози інформаційній безпеці бізнесу, визначити ключові фактори, що призводять до витоків даних, та оцінити їхні економічні наслідки. Окрему увагу приділено фінансовим втратам компаній, регуляторним санкціям та тенденціям інвестування у кібербезпеку.

Для досягнення цієї мети у статті розглянуто такі завдання:

– дослідити основні причини витоків даних, визначивши ключові вразливості, що стають джерелами загроз;
– оцінити економічні наслідки витоків, зокрема фінансові втрати компаній, юридичні санкції та зниження ринкової вартості;
– вивчити регуляторний вплив на кібербезпеку, розглянувши штрафи та нормативні зміни у сфері захисту даних;
– проаналізувати тенденції інвестування у кібербезпеку та визначити основні напрями витрат на захисні заходи.

Дослідження дозволяє оцінити взаємозв'язок між загрозами кібербезпеці, їхніми наслідками та заходами мінімізації ризиків. Отримані результати можуть бути корисними для наукової спільноти, керівників бізнесу та фахівців у сфері кібербезпеки.

Виклад основного матеріалу дослідження. Кібератаки, спрямовані на бази даних компаній, стали масштабною загрозою для бізнесу, державних установ та користувачів. З кожним роком зловмисники застосовують дедалі витонченіші методи, компрометуючи конфіденційну інформацію, що зберігається в цифрових системах. Масові витоки даних не лише ставлять під загрозу особисту інформацію мільйонів людей, але й завдають значних збитків організаціям, які стикаються з фінансовими втратами, репутаційними ризиками та санкціями з боку регуляторних органів.

За останні роки було зафіксовано низку масштабних витоків, які торкнулися мільярдів користувачів по всьому світу. Втрата конфіденційної інформації може бути наслідком як цілеспрямованих атак, так і внутрішніх помилок або недостатнього рівня захисту. Ці інциденти підкреслюють вразливість навіть найбільших корпорацій перед кіберзагрозами, що спричиняють фінансові, репутаційні та регуляторні ризики.

За даними аналітичних оглядів найбільших витоків даних у світі станом на січень 2024 року [17; 18; 19], за останнє десятиліття відбулося кілька масових витоків інформації з баз даних, що суттєво вплинули на інформаційну безпеку бізнесу та користувачів. Серед них найбільш масштабні інциденти включали розкриття мільярдів записів із платформ електронної пошти, соціальних мереж, державних реєстрів та комерційних сервісів. Особливу увагу привертають випадки витоків персональних ідентифікаційних даних, фінансової інформації та біометричних записів, що ставлять під загрозу конфіденційність і викликають довгострокові наслідки для компаній і громадян.

У таблиці 1 наведено перелік найбільших витоків даних, які спричинили значні ризики для компаній, державних установ і користувачів, підкреслюючи вразливість навіть найбільших компаній до атак, що спричиняють фінансові, репутаційні та регуляторні ризики.

Таблиця 1

Найбільші витоки даних у світі (станом на 2024 рік)

Рік	Компанія/ Інцидент	Кількість скомпроме-тованих записів	База даних	Тип даних, що витекли
2022	Реєстрація SIM-карт в Індонезії	1,3 млрд	База даних реєстрації SIM-карт	Національні ідентифікаційні номери, номери телефонів, імена операторів зв'язку [18]
2020	Cam4	10,88 млрд	База користувачів відеочату «для дорослих»	Логіни, IP-адреси, листування [16;17; 20]

2017	Yahoo (розкрито у 2019)	3 млрд	База облікових записів Yahoo Mail та пов'язаних сервісів	Облікові записи, паролі [16; 17; 20]
2024	National Public Data Breach	2,9 млрд	База персональних ідентифікаційних даних громадян	Імена, дати народження, номери соціального страхування [17;21]
2018	Aadhaar (Індія)	1,1 млрд	База даних національної ідентифікаційної системи Індії	Біометричні дані, ідентифікаційні номери [17; 22; 23]
2022	Alibaba	1,1 млрд	База замовлень та даних користувачів онлайн-магазину Taobao	Дані користувачів, історія покупок [17; 24]

Джерело: створено авторами на основі [16 - 24]

Серед інших значних інцидентів варто відзначити витік з даних бази даних компанії із страхування прав власності на нерухоме майно в США First American Financial Corporation (2019 рік), який призвів до розголошення 885 мільйонів записів фінансових транзакцій [17; 25; 26], та інцидент із сервісом перевірки електронної пошти Verifications.io (2019 рік), що скомпрометував 763 мільйони користувачів, включаючи адреси електронної пошти та контактну інформацію [17; 27]. Після витоку даних компанія фактично припинила свою діяльність [17]. У 2021 році витік даних у LinkedIn вплинув на 700 мільйонів користувачів, а у Facebook (2019 і 2021 рік) – загалом було скомпрометовано дані близько 533 мільйонів акаунтів, що містили номери телефонів, електронні адреси та інші ідентифікаційні дані [17; 28].

Аналізуючи статистику найбільших витоків даних за останні роки, можна виділити кілька основних причин, які призвели до великих втрат персональних ідентифікаційних даних, фінансових записів та іншої конфіденційної інформації, а саме [16-24]:

1. Неналежний захист баз даних та їхня відкрита доступність. Найбільший витік даних у світі – Cam4 Data Breach, що скомпрометував 10,88 млрд записів, стався через незахищену базу даних, яка була залишена у відкритому доступі без автентифікації. Подібний сценарій спостерігався і у

випадку Exactis Data Breach (2018), коли понад 340 мільйонів записів були виявлені у відкритій базі, доступній для всіх.

2. Соціальна інженерія та витік облікових записів. У випадку Verifications.io, витік 763 мільйонів записів став можливим через компрометацію email-баз, що вказує на використання фішингових атак або експлуатацію вразливостей у сторонніх сервісах. У 2018 році витік з бази даних Dubsmash скомпрометував 162 мільйони акаунтів, ймовірно, через зламані облікові дані, які використовувалися повторно в інших системах.

3. Атаки на великі технологічні компанії та сервіси. Масштабний витік даних Yahoo зачепив 3 мільярди акаунтів і став наслідком вразливості у внутрішніх системах безпеки компанії, що дозволило зловмисникам отримати доступ до паролів та персональних даних користувачів. Подібна ситуація спостерігалася у LinkedIn (2021, 2012) та Facebook (2019, 2021), де витоки пов'язані з недостатньо захищеними API та зловживанням механізмами доступу до даних.

4. Вразливість державних баз даних та національних реєстрів. Основна причина витоку даних в системі Aadhaar – уразливість в інфраструктурі урядової бази даних та несанкціонований доступ. Витік даних з бази даних National Public Data Breach, в результаті чого персональні ідентифікаційні дані стали доступними на чорному ринку, за оцінками фахівців, спричинений через можливу атаку на державні реєстри або витік через підрядників.

5. Недостатній рівень захисту захищених веб-застосунків та неналежний контроль доступу до конфіденційних даних, що зберігаються в інформаційних системах компаній. Витік даних First American Financial Corporation спричинив розголошення 885 мільйонів фінансових записів через недостатній рівень безпеки у веб-додатках, що дозволяло зловмисникам отримати доступ до документів про банківські перекази. Подібним чином Alibaba у 2022 році втратила 1,1 мільярда записів про своїх клієнтів через

вразливості у внутрішніх механізмах доступу до замовлень та фінансової інформації.

За даними звіту Verizon «Data Breach Investigations Report» за 2024 рік [29], основними причинами витоків даних є викрадення облікових даних, атаки програм-вимагачів, соціальна інженерія та використання вразливості програмного забезпечення. Особливо помітне зростання за останній рік (на 180%) зафіксовано саме у сфері експлуатації вразливості програмних продуктів, що активно використовувались кіберзлочинцями. Значущою причиною також залишається людський фактор, який складає 68% усіх витоків. У порівнянні з попередніми роками спостерігається тенденція до зростання кількості інцидентів, спричинених саме помилками користувачів, що свідчить про необхідність перегляду підходів до контролю та управління інформаційною безпекою в організаціях. Зокрема, 73% випадків витоку даних, пов'язаних із внутрішніми загрозами, спричинені ненавмисними помилками співробітників.

Щорічно також спостерігається тенденція зростання кількості витоків даних, пов'язаних із недостатнім контролем безпеки контрагентів. Зокрема, 15% випадків компрометації даних були спричинені сторонніми постачальниками або партнерами, включаючи ланцюги постачання програмного забезпечення, інфраструктури хостинг-партнерів та організації, що займаються зберіганням даних [29]. Основним фактором ризику є слабкий рівень захисту інформації у таких контрагентів, що створює сприятливі умови для зловмисників, які прагнуть отримати несанкціонований доступ до корпоративних систем. Такі інциденти не лише ставлять під загрозу конфіденційність даних, але й мають значний фінансовий вплив на організації.

Витоки конфіденційної інформації завдають значних фінансових збитків компаніям та державним установам. Окрім безпосередніх втрат, пов'язаних із ліквідацією наслідків інциденту, бізнес стикається з регуляторними штрафами, зниженням ринкової вартості, судовими позовами та репутаційними ризиками. За даними одного із найбільших у світі порталів

статистичних даних Statista, Inc (2024)[30], у 2023 році понад 56,6% випадків витоку даних спричинили порушення бізнес-процесів та прямі фінансові втрати, а близько 40% компаній зазнали репутаційних збитків (рис.1). Ослаблення конкурентних позицій через витоки даних демонструє довгострокові ризики для компаній, адже відновлення довіри споживачів та бізнес-партнерів є складним і дороговартісним процесом. Це свідчить про те, що інформаційна безпека є не лише технічною, але й стратегічною проблемою, оскільки фінансові втрати від кіберінцидентів можуть перевищувати початкові витрати на впровадження систем захисту.

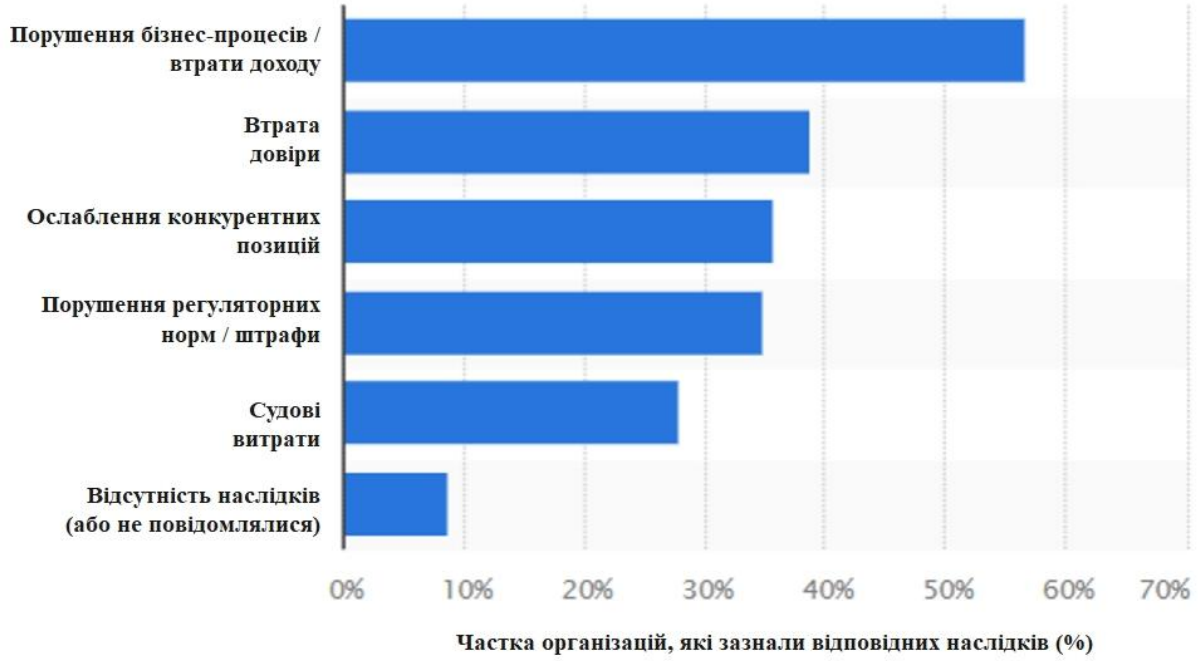

Рисунок 1. Найпоширеніші наслідки витоку даних в організаціях світу у 2023 році

Джерело: Statista, Inc [30]

Представлені на рис.1 дані отримані за результатами дослідження компанії Proofpoint та CyberEdge Group, яке охопило 600 респондентів із 12 країн та 17 галузей. Опитування проводилося серед спеціалістів з кібербезпеки в організаціях із чисельністю понад 1 000 співробітників, а його глобальна похибка становить 4%. Отримані результати дозволяють оцінити масштаби загроз та їхній вплив на бізнес-середовище в умовах цифровізації [30].

Зростаючий тиск з боку регуляторних органів змушує компанії приділяти особливу увагу захисту даних. За останні роки низка корпорацій зазнала багатомільйонних штрафів за недотримання вимог конфіденційності, що свідчить про посилення нормативного контролю у сфері кібербезпеки. Такі санкції не лише компенсують наслідки інцидентів, а й слугують сигналом для бізнесу про необхідність впровадження сучасних систем захисту. Жорсткі регуляторні заходи спрямовані на мінімізацію ризиків витоків даних та формування відповідального ставлення до управління інформаційною безпекою.

За даними Statista, Inc (2025)[31], суми штрафів за порушення конфіденційності продовжують зростати, що підкреслює важливість дотримання стандартів безпеки. У таблиці 1 наведено найбільші штрафи, накладені на компанії за витоки даних, які демонструють масштаб фінансових наслідків для організацій, що не забезпечили належний рівень захисту інформації.

Таблиця 2

Найбільші штрафи за витоки даних (станом на 2025 рік)

Компанія	Рік	Штраф (млн $)	Причина
Meta	2023	1300	Порушення правил GDPR (рішення DPC Ірландії)
Didi Global	2022	1190	Порушення норм конфіденційності у Китаї
Amazon	2021	877	Порушення регуляторних норм Люксембургу
Equifax	2019	575	Вразливості безпеки, що вплинули на 150 млн людей
Meta (Facebook, Instagram)	2023	413	Неправомірне використання даних користувачів
Instagram	2022	403	Порушення конфіденційності даних користувачів
TikTok	2023	370	Збір і обробка даних без згоди користувачів
T-Mobile	2022	350	Витік персональних даних користувачів

LinkedIn	2024	335	Порушення норм безпеки та витік даних
Meta (WhatsApp)	2022	255	Недотримання правил конфіденційності

Джерело: створено авторами на основі [31]

Аналіз найбільших штрафів за витоки даних демонструє посилення відповідальності компаній за недотримання вимог кібербезпеки. Високі штрафи не лише покликані компенсувати завдані збитки, а й служать інструментом стримування подальших порушень, змушуючи бізнес переглядати підходи до безпеки даних. З огляду на зростаючий рівень загроз, компанії змушені не тільки відповідати на кіберінциденти, але й інвестувати у превентивні заходи, що дозволяють мінімізувати ризики порушень безпеки.

Інциденти витоків даних змусили компанії переглянути свої підходи до кібербезпеки та перерозподілити бюджети на захисні заходи. Як показують дані дослідження Statista, Inc (2024) [32], основними напрямками інвестицій у 2024 році стали:

– тестування та реагування на інциденти (55% компаній);

– впровадження технологій виявлення загроз (51%);

– навчання персоналу (46%).

Тобто бізнес приділяє увагу не лише технологічним рішенням, а й зниженню ризиків, пов’язаних із людським фактором, що підкреслює комплексний підхід до кібербезпеки (рис. 2).

Кібербезпека дедалі більше розглядається бізнесом як стратегічний пріоритет, що знаходить відображення у перерозподілі фінансових ресурсів на вдосконалення системи захисту даних та оперативне реагування на загрози. Збільшення інвестицій у тестування та планування заходів реагування підкреслює важливість готовності до потенційних атак.

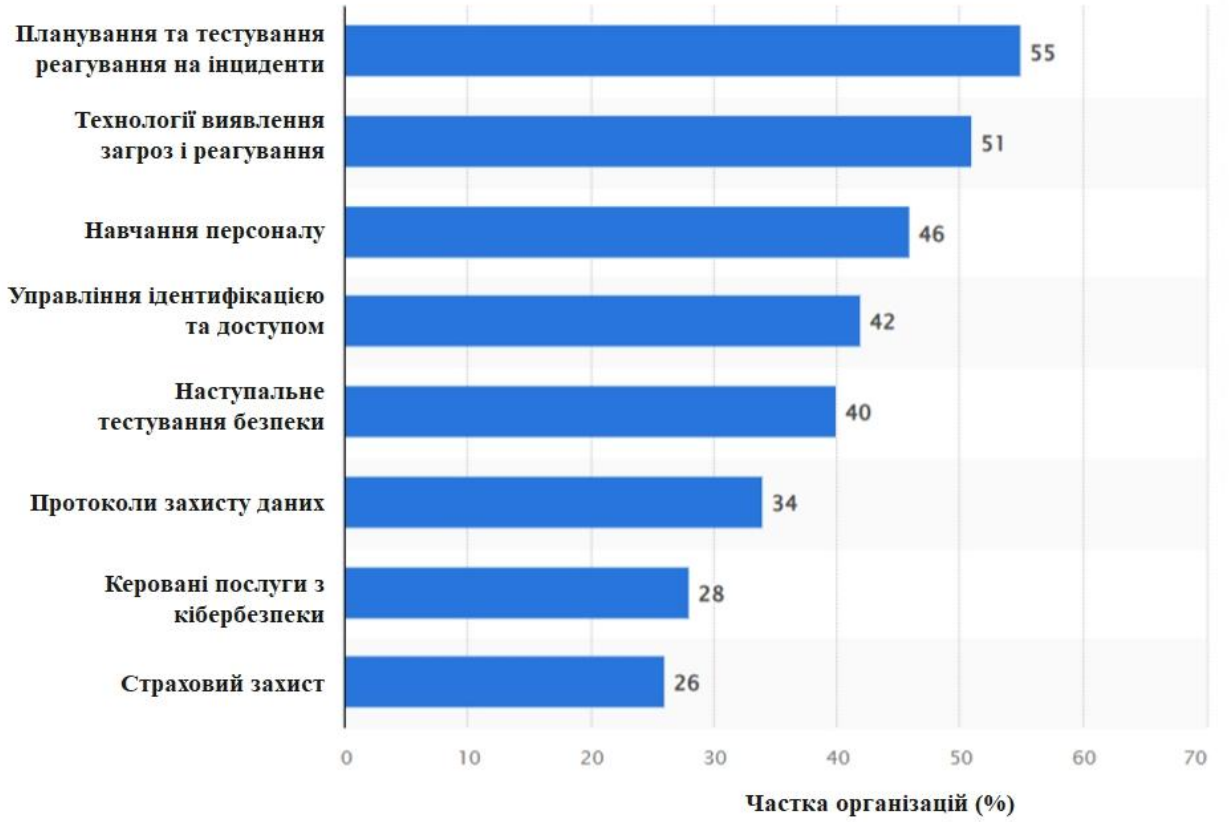

Рисунок 1. Основні напрями інвестицій у кібербезпеку після витоку даних у компаніях світу у 2024 році

Джерело: Statista, Inc [32]

Одним із ключових напрямів кібербезпеки є використання хмарних баз даних, що дозволяє компаніям підвищити масштабованість, ефективність управління інформацією та знизити витрати на інфраструктуру. Водночас, через відкритий доступ і складну архітектуру, хмарні середовища стають дедалі частішими цілями для кібератак, що зумовлює необхідність значних інвестицій у їхній захист.

За даними Statista Inc. [33], ринок безпеки хмарних баз даних демонструє стабільне зростання: у 2022 році його обсяг становив 10,13 млрд доларів США, а до 2029 року прогнозується зростання майже у п’ять разів — до 49,93 млрд доларів США. Така динаміка свідчить про зростаючий попит на захищені хмарні рішення, обумовлений як поширенням кіберзагроз, так і жорсткішими регуляторними вимогами до збереження конфіденційної інформації.

Розвиток цього сегмента підтверджує глобальну тенденцію до переходу компаній на хмарні технології, що потребує відповідного рівня безпеки. У зв'язку з цим бізнеси змушені впроваджувати сучасні рішення для захисту хмарних баз даних, включаючи багаторівневу аутентифікацію, шифрування, моніторинг активності користувачів та автоматизовані системи виявлення загроз.

Водночас значна частина витрат спрямовується на запобіжні заходи, зокрема навчання персоналу та впровадження технологій виявлення загроз, що демонструє перехід до проактивного підходу у кібербезпеці. Це свідчить про те, що компанії адаптуються до нових викликів у сфері інформаційної безпеки, оптимізуючи бюджети на заходи, спрямовані на мінімізацію ризиків витоків даних та фінансових наслідків.

Таким чином, аналіз тенденцій кіберзагроз, фінансових ризиків та інвестицій у захист інформації свідчить про необхідність комплексного підходу до забезпечення кібербезпеки бізнесу. Поєднання технічних рішень, регуляторного контролю та стратегічного управління ризиками є важливим фактором у мінімізації наслідків кіберінцидентів.

Висновки. За результатами проведеного аналізу можна стверджувати, що витоки даних становлять серйозну загрозу для бізнесу, державних установ та користувачів. Масштабні кіберінциденти демонструють вразливість навіть найбільших компаній перед сучасними атаками, що призводить до значних фінансових втрат, репутаційних ризиків та регуляторних санкцій.

Дослідження показують, що ключовими причинами витоків даних є недостатній контроль безпеки баз даних, компрометація облікових записів, соціальна інженерія та атаки через третіх осіб (контрагентів та постачальників).

Аналіз економічних наслідків витоків даних демонструє, що прямі фінансові втрати компаній включають не лише витрати на ліквідацію наслідків, а й штрафи, судові позови та зниження ринкової вартості. Жорсткі регуляторні заходи, зокрема значні штрафи, спрямовані на підвищення рівня

відповідальності бізнесу та стимулюють компанії до впровадження сучасних систем кібербезпеки.

Зростаючі фінансові ризики змушують підприємства активно інвестувати у кібербезпеку, спрямовуючи кошти на тестування та реагування на інциденти, впровадження технологій виявлення загроз та навчання персоналу. Стратегічний підхід до інформаційної безпеки, що поєднує технічні, організаційні та освітні заходи, дозволяє бізнесу мінімізувати ризики та забезпечувати стійкість до кібератак у сучасних умовах цифрової економіки.

Таким чином, підприємства для ефективного управління інформаційною безпекою повинні поєднувати дотримання регуляторних вимог із використанням сучасних технологій кіберзахисту. Комплексний підхід передбачає інвестування у превентивні заходи, зокрема виявлення загроз, тестування стратегії реагування, навчання персоналу та контроль безпеки контрагентів. Лише поєднання технічних, організаційних та освітніх заходів дозволяє мінімізувати ризики витоків даних та їхні фінансові наслідки, забезпечуючи стійкість компаній до зростаючих кіберзагроз у цифрову епоху.

Попри значний прогрес у сфері кібербезпеки, існує низка напрямів, що потребують подальшого дослідження. Зокрема, важливим є вивчення ефективності штучного інтелекту у виявленні та запобіганні витокам даних, зокрема його здатності аналізувати поведінкові аномалії та автоматично реагувати на загрози. Також необхідний аналіз впливу новітніх регуляторних змін на інформаційну безпеку бізнесу та їхнього значення для стратегій захисту даних. Дослідження методів оцінки економічних збитків від витоків інформації дозволить точніше прогнозувати фінансові втрати, включаючи репутаційні ризики та довгострокові наслідки. Окремої уваги потребує безпека хмарних баз даних, оцінка загроз, пов’язаних із використанням хмарних технологій, а також ефективність механізмів захисту в цьому середовищі. Крім того, актуальним залишається вивчення соціально-

інженерних атак та розробка заходів підвищення обізнаності працівників щодо фішингових загроз і методів маніпуляції.

Список використаних джерел

1. Frederic Schlackl, Nico Link, Hartmut Hoehle. Antecedents and consequences of data breaches: A systematic review. *Information & Management.* Volume 59, Issue 4. 2022. 103638. URL : https://doi.org/10.1016/j.im.2022.103638
2. Isabel Herrera Montano, Jose J. García Aranda, J. R. Ramos Díaz, Sergio Molina Cardín, Isabel de la Torre Díez, Joel Rodrigues. Herrera Montano, Isabel et al. Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat. *Cluster Computing* 25. 2022. P. 4289-4302. URL : https://doi.org/10.1007/s10586-022-03668-2
3. Cheng, L., Liu, F., & Yao, D.D. Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7.* 2017. URL : https://doi.org/10.1002/widm.1211
4. Gracy, Shanitamol. A global analysis of data breaches from 2004 to 2024. 2025. URL : 10.48550/arXiv.2502.05205.
5. Xichen Zhang, Mohammad Mehdi Yadollahi, Sajjad Dadkhah, Haruna Isah, Duc-Phong Le, and Ali A. Ghorbani. Data breach: analysis, countermeasures and challenges. *International Journal of Information and Computer Security*. 2022. 19:3-4. P. 402-442. URL : https://doi.org/10.1504/IJICS.2022.127169
6. Patil R., Pise G., Bhosale Y. Root causes, ongoing difficulties, proactive prevention techniques, and emerging trends of enterprise data breaches. *CoRR*. 2023. Vol. abs/2311.16303. URL: https://doi.org/10.48550/arXiv.2311.16303
7. Khan, Freeha S.; Kim, Jung Hwan; Moore, Robin L.; and Mathiassen, Lars. Data Breach Risks and Resolutions: A Literature Synthesis. 2019. *AMCIS 2019 Proceedings*. 14. URL: https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/14

8. Рибальченко, Л. В., Габорець, О. А., & Прокопович-Ткаченко, Д. І. Кіберстійкість: глобальні загрози та національні стратегії кіберзахисту. *Системи та технології*. 2024. № 68(2). С. 95-101. URL : https://doi.org/10.32782/2521-6643-2024-2-68.11

9. Alneyadi S., Sithirasenan E., Muthukkumarasamy V. A survey on data leakage prevention systems. *Journal of Network and Computer Applications*. 2016. Vol. 62. P. 137–152. URL : https://doi.org/10.1016/j.jnca.2016.01.008.

10. Лубко Д. В., Мірошниченко М. Ю. Аналіз сучасних підходів та методик в області захисту інформації та даних. *Вісник Херсонського національного технічного університету*. 2024. № 1(88). С. 232–236. URL : https://doi.org/10.35546/kntu2078-4481.2024.1.32.

11. Гарасимчук О. І., Бужович О. С. Стратегії та інноваційні підходи до захисту баз даних в епоху зростаючих кіберзагроз. *Безпека інформації*, 2024. Том 30. № 1. URL : https://doi.org/10.18372/2225-5036.30.18618.

12. Wu Jianqing, and Ping Zha. A Data Security Model for Altering Data Ecosystem and Affirmatively Prevent Mass Data Breaches. *Feb*. 2022. URL : https://doi.org/10.31219/osf.io/d479z

13. Ahmad Mtair AL-Hawamleh. Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures. *International Journal of Advanced Computer Science and Applications(IJACSA)*. 2023. Vol. 14(2). URL: http://dx.doi.org/10.14569/IJACSA.2023.0140292

14. Michael Ettredge, Feng Guo, Yijun Li. Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*. Volume 37. Issue 6. 2018. Pages 564-585. URL : https://doi.org/10.1016/j.jaccpubpol.2018.10.006

15. Kobana Abukari, Shantanu Dutta, Chen Li, Songlian Tang, Pengcheng Zhu. Corporate communication and likelihood of data breaches. *International Review of Economics & Finance*, 94**.** 2024, 103433. URL: https://doi.org/10.1016/j.iref.2024.103433.

16. Чернявська Б. В., Ковальчук А. Ю. Міжнародно-правовий аспект протидії доксингу в цифрову епоху. *Науковий вісник Ужгородського*

національного університету. Серія: Право. 2024. Том 4 № 85. С. 257-263. URL: https://doi.org/10.24144/2307-3322.2024.85.4.37

17. Statista. Наймасштабніші витоки даних у світі станом на січень 2024 року. URL: https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/

18. Sick of data leaks, Indonesians are siding with a hacker who exposed 1.3 billion SIM card details. 2022. URL : https://restofworld.org/2022/indonesia-hacked-sim-bjorka/

19. World's Biggest Data Breaches & Hacks. 2025. URL : https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

20. 10 найпотужніших кібератак та витоків даних за всю історію. 2024. URL : https://gigatrans.ua/ua/news/10-naypotuzhn-shih-k-beratak-ta-vitok-v-danih-za-vsyu-stor-yu

21. Ariel Zilber. National Public Data admits hackers stole Social Security numbers in massive breach reportedly affecting nearly all Americans. *New York Post*. Aug. 19. 2024. URL : https://nypost.com/2024/08/19/business/national-public-data-admits-hackers-stole-social-security-numbers/?utm_source

22. India's database with biometric details of its billion citizens ignites privacy debate. 2017. URL : https://mashable.com/article/india-aadhaar-uidai-privacy-security-debate

23. В урядовій хмарі Індії роками відбувався витік персональних даних. URL : https://digvel.com.ua/blog/bagatorichnyj-vytik-danyh-v-uryadovij-hmari-indiyi-vidbuvavsya-vytik-personalnyh-danyh-gromadyan/

24. Oiwan Lam. China: Possible police database breach exposes at least 1 billion citizens' personal data. It could be the biggest data leak in history. *Global Voices*. 2022.. URL : https://globalvoices.org/2022/07/06/china-possible-police-database-breach-exposes-at-least-1-billion-citizens-personal-data/

25. Zack Whittaker. First American site bug exposed 885 million sensitive title insurance records. *TechCrunch. May 24*. 2019. URL : https://techcrunch.com/2019/05/24/first-american-millions-sensitive-records/

26. Brian Krebs. First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records. 2019. URL : https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/

27. Verifications.io Data Breach: What & How It Happened? 2024. URL : https://www.twingate.com/blog/tips/verifications-io-data-breach

28. Надія Баловсяк. Доступний мільярд: чим загрожує публікація даних 500 млн користувачів Facebook і LinkedIn. 2021. URL : https://thepage.ua/ua/it/chim-zagrozhuye-vitok-danih-koristuvachiv-facebook-ta-linkedin

29. 2024 Data Breach Investigations Report. 2024. URL : https://www.verizon.com/business/resources/reports/dbir/

30. Statista. Most common consequences of sensitive information loss incidents in worldwide organizations in 2023. 2024. URL : https://www.statista.com/statistics/1387438/loss-sensitive-information-organizations-result-worldwide/

31. Statista. Largest data privacy violation fines, penalties, settlements worldwide as of January 2025(in million U.S. dollars). 2025. URL : https://www.statista.com/statistics/1170520/worldwide-data-breach-fines-settlements/

32. Statista. Main security investment types following a data breach in companies worldwide in 2024. 2024. URL : https://www.statista.com/statistics/1484625/top-cybersecurity-investment-types-after-a-breach-worldwide/

33. Statista. Cloud database security market size worldwide in 2020 and 2029(in billion U.S. dollars). 2024. URL : https://www.statista.com/statistics/1246584/cloud-database-security-market/