УДК 330.47
JEL Classification D81
DOI https://doi.org/10.33146/2307-9878-2023-4(102)-97-104

Tetiana Kapeliushna[1]
State University of Information and Communication Technologies, Kyiv, Ukraine

Enterprise Data Security in the Cloud Environment: Threat Analysis

Abstract. *Wider use of cloud services leads to increased cyber attacks on data arrays in cloud storage. Ensuring privacy in the cloud comes at a cost, and businesses are willing to bear these costs for data security. However, there is still a high risk of data being tracked and stolen due to existing vulnerabilities in the Internet environment. The purpose of the article is to analyze threats to data in the cloud environment under conditions of uncertainty and to reveal their increase in the virtual IT infrastructure of the enterprise. The advantages and disadvantages of enterprises using cloud services for data storage were revealed. Considering the amount of financial losses and reputational risks, the issue of protecting networks and services in the cloud, especially when hosting confidential or secret information, is a priority for enterprises of all industries. According to Significant Cyber Incidents, cyber incidents against government, defence and high-tech companies in the world were analyzed during 2021-2022. It was found that the attacks were primarily aimed at critical infrastructure enterprises and government organizations. Analysis of data from the Future Risk Report 2022 shows that climate change, geopolitical tensions, cyber security risks, and energy risks will remain the most significant risks over the next decade. It was revealed that since the beginning of the full-scale invasion, the number of attacks on Ukrainian enterprises of critical infrastructure and the telecommunications sphere has increased significantly. This shows that hacker attacks are one of the tools of hybrid warfare, capable of causing significant damage to the country's economy. The revealed trend in Ukraine confirms the predictions of international experts that cyber threats will grow in conditions of uncertainty and geopolitical instability. The article provides a chronology of massive cyberattacks on Ukrainian enterprises and organizations in the IT sphere over the past two years. It was determined that the means of reducing risks in the field of cyber security, which lead to the saving of costs of enterprises for data security, are the tools of artificial intelligence of security and further automation of threat identification. Thus, cyber security becomes an integral component in ensuring the full functioning of the enterprise, and the ways and means of its achievement require further research.*

Keywords: *enterprise security, uncertain conditions, cloud services security, virtual IT infrastructure, cyber incidents.*

Suggested Citation
Kapeliushna, T. (2023). Enterprise Data Security in the Cloud Environment: Threat Analysis. *Oblik i finansi*, 4(102), 97-104. https://doi.org/10.33146/2307-9878-2023-4(102)-97-104

Тетяна Капелюшна
Державний університет інформаційно-комунікаційних технологій, Київ, Україна

Безпека даних підприємства у хмарному середовищі: аналіз загроз

Анотація. *Ширше використання хмарних сервісів веде до посилення кібератак на масиви даних у хмарних сховищах. Забезпечення конфіденційності в хмарі потребує затрат і підприємства готові нести ці витрати задля безпеки даних, проте, все одно існує високий ризик відслідковування та викрадення даних через існуючі вразливості інтернет-середовища. Метою статті є аналіз загроз щодо даних у хмарному середовищі в умовах невизначеності та вияв їх посилення у віртуальній IT-інфраструктурі підприємства. Розкрито переваги і недоліки використання підприємствами хмарних сервісів для збереження даних. Зважаючи на обсяги фінансових втрат та репутаційні ризики, питання захисту мереж та сервісів у хмарі, особливо при розміщені конфіденційної або секретної інформації, є пріоритетним для підприємств всіх галузей. За даними Significant Cyber Incidents проаналізовано кіберінциденти на урядові, оборонні, високотехнологічні компанії у світі впродовж 2021-2022 рр. Виявлено, що атаки були націлені насамперед на критично важливі підприємства та урядові організації. Аналіз даних Future Risk Report 2022 свідчить, що найбільшими ризиками впродовж наступного десятиліття залишатимуться* ***зміни клімату, геополітична напруженість, ризики кібербезпеки, а також енергетичні ризики.*** *Виявлено, що з початку повномасштабного вторгнення суттєво зросла кількість атак на українські підприємства критичної інфраструктури та телекомунікаційної сфери.*

[1] **Tetiana Kapeliushna**, State University of Information and Communication Technologies, Kyiv, Ukraine.
ORCID 0000-0001-7490-6751
E-mail: e-skr@ukr.net

Це свідчить про те, що хакерські атаки є одним із інструментів гібридної війни, що здатен завдавати значної шкоди економіці країни. Виявлена тенденція в Україні підтверджує прогнози міжнародних експертів, що в умовах невизначеності та геополітичної нестабільності будуть зростати кіберзагрози. У статті наведено хронологію масованих кібератак на українські підприємства та організації ІТ-сфери впродовж останніх двох років. Визначено, що засобами зменшення ризиків у сфері кібербезпеки, які ведуть до економії витрат підприємств на безпеку даних, є інструменти штучного інтелекту безпеки та подальшої автоматизації ідентифікації загроз. Таким чином, кібербезпека стає невід'ємним компонентом в забезпеченні повноцінного функціонування підприємства, а шляхи та засоби її досягнення вимагають подальших досліджень.

Ключові слова: *безпека підприємства, невизначені умови, безпека хмарних сервісів, віртуальна ІТ-інфраструктура, кіберінциденти.*

Постановка проблеми. У бізнес-середовищі зростає роль діджиталізації, спостерігається тенденція до переходу роботи підприємств у режим віддаленого доступу, що посилюється невизначеними умовами впродовж останніх років (пандемія, воєнний стан). У цілях безпеки підприємства прагнуть створити належні умови і приділяють значну увагу захисту персоналу та інфраструктури від ризиків, що виникають у процесі операційної діяльності. Проте, через воєнні дії ускладнюється пряма комунікація (фізична), збільшуються ланцюги постачання послуг, адже сторони намагаються якнайшвидше та безпечніше передавати інформацію по перевірених каналах. Задля пришвидшення комунікації та територіального охоплення споживачів, постачальників, посередників підприємства використовують хмари та хмарні сервіси. Таким чином, уможливлюється відкриття інтернет-магазинів, спільне використання баз даних, віддалене управління бізнесом, використання поштових серверів. Хмара слугує віртуальною ІТ-інфраструктурою підприємства, в якій можна розгорнути будь-які системи та програми, а її захист є викликом для фахівців з кібербезпеки.

Аналіз останніх досліджень і публікацій. Низка опрацьованих наукових джерел вказує на високий інтерес до функціонування підприємств у цифровому середовищі. Дослідженню проблемних питань безпеки даних і функціонування підприємств у діджиталізованому середовищі та віртуальній ІТ-інфрастуктурі приділили увагу вчені: І. Шевчук, Б. Депутат, К. Нікітенко, А. Осадчий, С. Михайловина, О. Матрос, О. Поліщук, М. Дауд, Ш. Ту, Ч. Сяо, Х. Аласмарі, М. Вакас, С. Ур Рехман, Д. Марвана. Разом із тим залишається потреба в аналізі загроз, які постають перед підприємствами, що сьогодні в умовах невизначеності функціонують у діджиталізованому середовищі.

Перехід до більш активного використання бізнесом хмарних сервісів в Україні став реакцією на зовнішні та внутрішні виклики. Як зазначають І. Шевчук та Б. Депутат, починаючи з 2014 року через анексію територій Донбасу та Криму, це питання гостро постало для підприємницьких структур. Підприємці були вимушені рятувати власний бізнес та переїжджати на більш безпечні території, ними використовувалися хмарні сервіси для продовження роботи, тому що створення власних сервісів потребувало значних витрат [1].

Використання хмар має ряд переваг: безперешкодний доступ до даних з будь-якої точки за наявності Інтернету; зменшення витрат на утримання (відсутність потреби у купівлі обладнання, програмного забезпечення, а також обслуговування); можливість використання не залежно від місця розташування підприємства; високотехнологічність. Однак, як зауважують К. Нікітенко, А. Осадчий, одночасно із перевагами такі технології не позбавлені недоліків, що пов'язані із безпекою даних, яка забезпечується надавачем хмарних послуг [2].

В своєму дослідженні С. Михайловина, О. Матрос, О. Поліщук розглядають позитивні сторони від використання SaaS (Software as a Service): фіксована абонплата; реалізація потреб у віддаленому доступі та виконанні завдань; низька потреба у технічних засобах та пристроях; ліцензоване програмне забезпечення; постійне оновлення та техпідтримка на безоплатній основі. Водночас наголошено і на потребах, які здебільшого стосуються безпеки даних: побудова власної приватної хмари у разі засекречених даних; резервне копіювання даних з метою збереження цілісності даних та уникнення їх втрати [3].

Зарубіжні дослідники М. Дауд, Ш. Ту, Ч. Сяо, Х. Аласмарі, М. Вакас, С. Ур Рехман вважають, що у світі хмарних обчислень безпека даних і ресурсів є головним пріоритетом. Хмарна безпека непокоїть організації, бізнес, науково-дослідницький сектор, але доволі часто виникає супротив та протиріччя щодо розміщення та повного використання хмарних обчислень із міркувань безпеки даних [4].

На думку Д. Марвана, зловмисники можуть атакувати постачальників онлайн-сховищ, оскільки захищені норми реєстрації дозволяють хакерам залишатися анонімними, що ускладнює їх виявлення. Можливості управління та забезпечення конфіденційності в хмарі потребують затрат, і підприємства готові нести ці витрати задля безпеки даних, проте, все одно існує високий ризик відслідковування та викрадення даних через неналежну безпечність інтернет-середовища [5]. Таким чином, питання безпеки даних підприємства у хмарному середовищі та аналізу кіберзагроз залишаються відкритими і потребують подальших досліджень.

Метою статті є аналіз загроз щодо даних у хмарному середовищі в умовах невизначеності та вияв їх посилення у віртуальній ІТ-інфраструктурі підприємства.

Виклад основного матеріалу. Із активним переходом підприємств в період пандемії у віртуальну ІТ-інфраструктуру, зросли загрози цілісності даних та з'явилася потреба у додаткових засобах їх захисту. Тобто ширше використання хмарних сервісів веде до посилення кібератак на масиви даних у хмарах.

Питання безпеки хмарних послуг окреслено у Законі України «Про хмарні послуги», в якому чітко визначено потребу у дотриманні заходів щодо безпеки, які «…мають забезпечувати рівень безпеки електронної комунікаційної мережі, електронної комунікаційної послуги та інформаційних систем, які використовуються для надання хмарних послуг, що відповідає ризику, який виник, та враховувати такі елементи: безпеку систем та устаткування; врегулювання інцидентів; управління безперервністю бізнесу; моніторинг, аудит та випробування; відповідність міжнародним стандартам» [6].

Із зростанням кібератак постає проблема захисту даних у хмарних сервісах, що потребує негайного вирішення. Проаналізувавши кількість атак за даними Significant Cyber Incidents упродовж останніх двох років, виявлено, що по всьому світу атаки посилюються, зокрема й на урядові, оборонні та високотехнологічні компанії (табл. 1).

Таблиця 1. **Кіберінциденти на урядові, оборонні, високотехнологічні компанії (із збитками понад 1 млрд дол.) у 2021-2022 рр.**

Країна походження кіберінциденту	Країна, у якій відбувався кіберінцидент	Підприємства та організації, що зазнавали атак, опис інциденту
1	2	3
Іран	Нідерланди	У лютому 2021 року злом амстердамських серверів, що використовувалися як командно-контрольний центр для подальших атак на політичних опонентів у Нідерландах, Німеччині, Швеції, Індії.
РФ	Україна	Поширення шкідливих документів, які могли б встановити на комп'ютери шкідливе програмне забезпечення. Атака націлена на знищення інформаційних ресурсів системи електронної взаємодії органів виконавчої влади.
Китай	Індія	Кампанія кібершпигунства (фішинг, використання відомих вразливостей в загальнодоступних програмах як початковий режим входу для компрометації корпоративної мережі) проти індійського транспортного сектору (IRCTC, Tata Motors, Національне управління автомобільних доріг Індії, RITES, Dedicated Freight Corridor Corporation of India, Center for Railway Information Systems (CRIS) і Roads & Building Dept, Андхра-Прадеш).
РФ	Польща	Нетривале захоплення вебсайтів Національного агентства з атомної енергії та Міністерства охорони здоров'я Польщі, щоб поширити неправдиві повідомлення про неіснуючу радіоактивну загрозу.
Китай	Афганістан	Фішингові листи з метою отримання доступу до облікового запису електронної пошти одного із чиновників для надсилання представникам національної безпеки підробленого електронного листа із інструкцією дій щодо майбутньої прес-конференції.
Північна Корея	Південна Корея	Кібератака на південнокорейський державний Науково-дослідний інститут атомної енергії (KAERI), що сталася через вразливість у VPN постачальника (тринадцять несанкціонованих IP-адрес отримали доступ до внутрішньої мережі KAERI).
РФ	Австралія	Атака на австралійську комунальну компанію CS Energy з використанням програмного забезпечення з вимогою викупу.
Іран	США	Атаковано акаунти у Facebook через надсилання зараженого шкідливого програмного забезпечення, файлів або обманом змушували жертв (американських військовослужбовців) вводити конфіденційні облікові дані на фішингових сайтах.
США	Китай	Численні кібератаки на Північно-Західний політехнічний університет Китаю з боку Агентства національної безпеки, викрадання даних користувачів і проникнення в цифрові комунікаційні мережі.
Китай	Фінляндія	DDoS-атака на парламент Фінляндії, яка зробила вебсайт парламенту недоступним.
РФ	Норвегія	Атака на державні установи Норвегії за допомогою DDoS-атак, порушуючи роботу державних вебсайтів.

Продовження табл. 1

1	2	3
Індія	Пакистан	Атака на ВПС Пакистану (PAF) у кампанії підводного полювання з метою розгортання шкідливого програмного забезпечення та отримання конфіденційних файлів.
Китай	Німеччина	Китайська хакерська група зламала кілька німецьких фармацевтичних і технологічних компаній (спроба викрадення інтелектуальної власності).
Іран	Ізраїль	Хакери атакували муніципальні системи оповіщення в Єрусалимі та Еліаті, увімкнувши сирени повітряної тривоги в обох містах. Ізраїльська компанія з промислової кібербезпеки приписала атаку Ірану.

Джерело: складено автором за даними [7].

Аналіз кіберінцидентів свідчить, що атаки були націлені насамперед на підприємства та організації, які відносять до критично важливих або урядових. Найбільше нападів чинилася із боку сусіда країни-агресора, Ірану, Китаю, а нанесені збитки вимірювалися в млн та млрд дол. США. Зважаючи на рівень організацій (урядові, оборонні та високотехнологічні), на які були спрямовані атаки, їх можливості захисту від кіберзагроз, постає питання щодо посилення захисту інформаційного середовища усіма підприємствами задля уникнення фінансових втрат та репутаційних ризиків. Лише стійкі до зовнішніх впливів підприємства, які працюють на упередження, здатні функціонувати в умовах невизначеності, відбивати атаки, в тому числі кібератаки, тим самим посилюючи довіру з боку клієнтів та збільшуючи вартість компанії, що позитивно сприймається інвесторами та акціонерами.

За даними глобального дослідження «Future risk report 2022», яке щороку проводиться компанією AXA спільно з науково-дослідним інститутом IPSOS та за консультування Eurasia Group (напрям дослідження – геополітичний аналіз), в якому прийняли участь 4,5 тис. експертів з понад 50 країн, а також близько 20 тис. респондентів, обраних серед населення, можна виокремити ризики світового масштабу [8] (рис. 1).. Найбільшими ризиками, що загрожуватимуть безпеці впродовж наступного десятиліття, є: зміни клімату, геополітична напруженість, ризики кібербезпеки, а також енергетичні ризики.

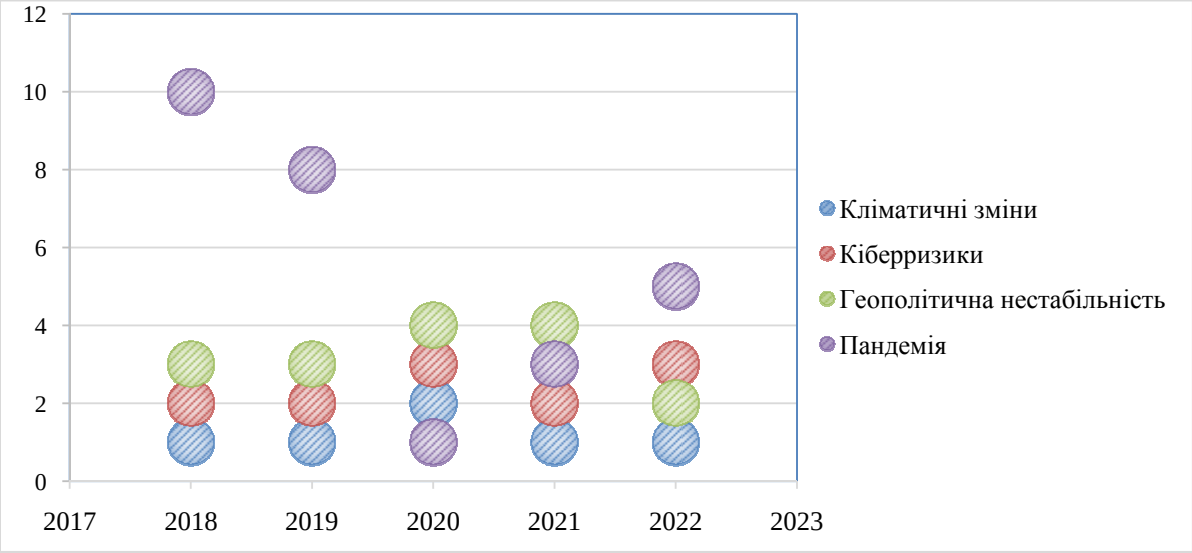

Рис. 1. **Ранги вразливості до ризиків у світі впродовж 2018-2022 рр.**

Джерело: побудовано автором за даними [8].

Неурядова організація Інститут кібермиру (Cyber Peace Institute), що слідкує за кіберстаном у світі, а за її даними також підтверджуються прогнози аналітиків, експертів і громадськості щодо посилення загроз у інформаційному просторі, відзначає стрімке зростання кібератак із початку війни в Україні. Окрім урядових організацій, підвищений інтерес кібернападників становлять підприємства телекомунікаційної сфери, так у грудні 2022 року відбулася триденна атака на сервери української телекомунікаційної компанії. За даними звітів Інституту про безпекову ситуацію в Україні, відзначається активність у фінансовій сфері, торгівлі, енергетиці, медіа, виробництві, ІКТ [9].

За перший квартал 2023 року відбулося 10 інцидентів націлених на сектор інформаційно-комунікаційних технологій [10]. Продовжувалися атаки на фінансовий сектор (приріст на 46%), державне управління (рис. 2).

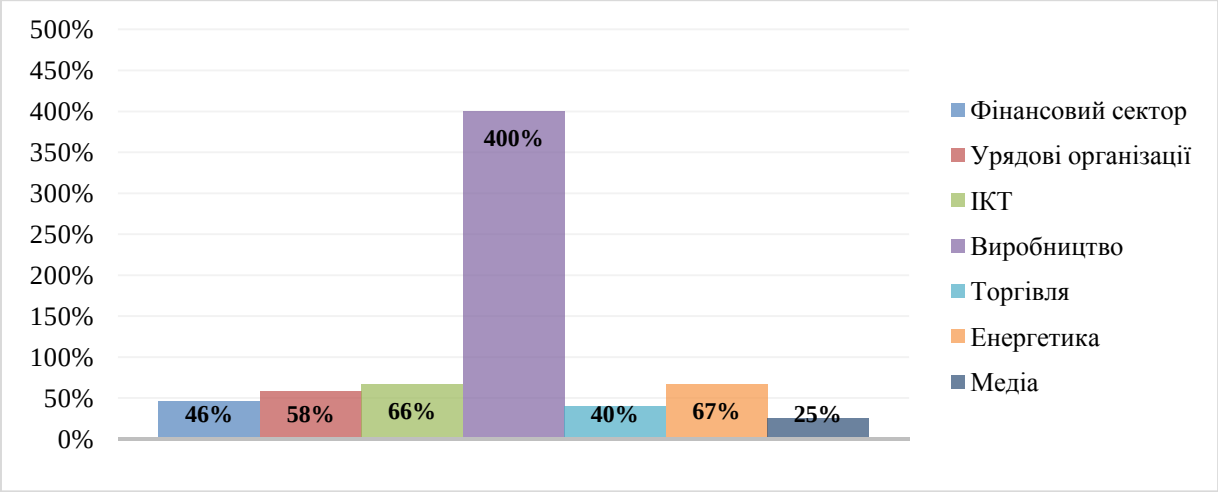

Рис. 2. **Приріст кіберінцидентів за секторами (I кв. 2023 р.)**
Джерело: побудовано автором за даними [10].

Критична інфраструктура залишається у полі зору кібернападників, в тому числі й телекомунікаційні підприємства, які забезпечують комунікацію, зв'язок, включаючи компанії-розробники програмного забезпечення, серверів. Відзначається інтенсивність атак впродовж 2023 року, при чому їх посилення відбулося, починаючи із літа. Здійснена низка DDoS-атак на сайти українських провайдерів, телекомунікаційні компанії, сервери розробників веб-платформ (рис. 3).

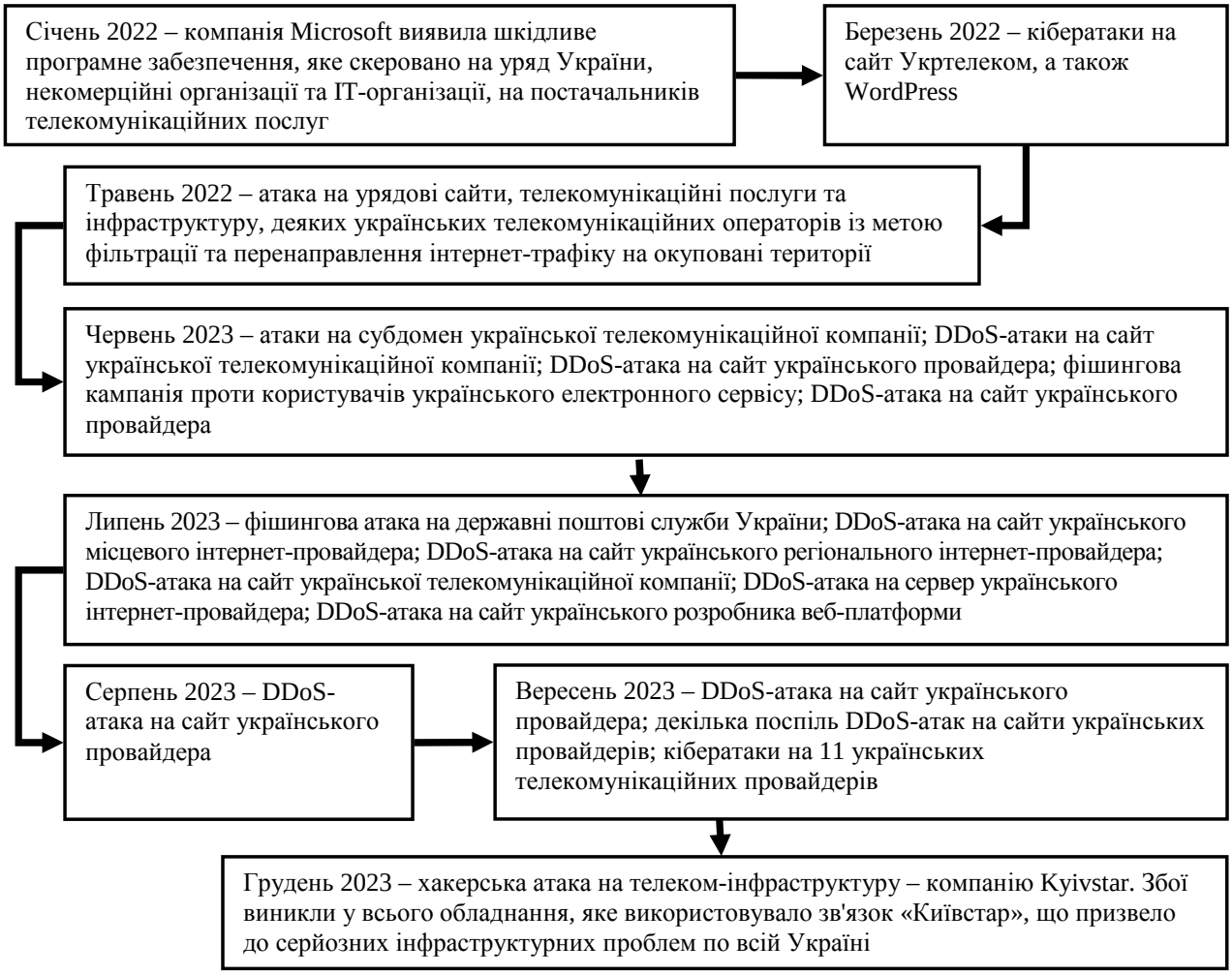

Рис. 3. **Масовані кібератаки на українські підприємства та організації IT-сфери впродовж 2022-2023 рр.**
Джерело: узагальнено автором за даними [13, 14].

За даними спеціалізованого структурного підрозділу CERT-UA (Computer Emergency Response Team of Ukraine) Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України, з травня по вересень 2023 року зафіксовано втручання в роботу 11 українських провайдерів телекомунікацій, а саме в інформаційно-комунікаційні системи, що призвело до збоїв надання послуг.

Використовуючи раніше скомпрометовані системи, зловмисник зміг сканувати мережі на наявність відкритих портів і отримати доступ до дистанційного керування. Потрапивши всередину, зловмисник зміг отримати віддалений доступ та втручатися в роботу інформаційно-комунікаційних систем 11 телекомунікаційних провайдерів України, вивівши з ладу активне мережеве та серверне обладнання, а також системи зберігання даних, що призвело до перебоїв у наданні послуг споживачам.

Враховуючи обсяги атак на IT-інфраструктуру телекомунікаційних підприємств, захист їх інформаційних систем сьогодні є надважливим. Потрібно здійснювати постійний пошук варіантів можливих заходів, засобів, інструментів безпеки, залучаючи при цьому організації, які ефективно борються із загрозами у світовому масштабі. За результатами досліджень компанії IBM нині слабко використовується штучний інтелект безпеки (28% організацій), автоматизованість дій з ідентифікації загроз у мережі теж низька, що сповільнює реакцію підприємств на загрозу та її упередження. Очікується, що штучний інтелект безпеки та автоматизація суттєво скоротять втрати підприємств, оскільки зросте ефективність кібербезпеки підприємств (рис. 4).

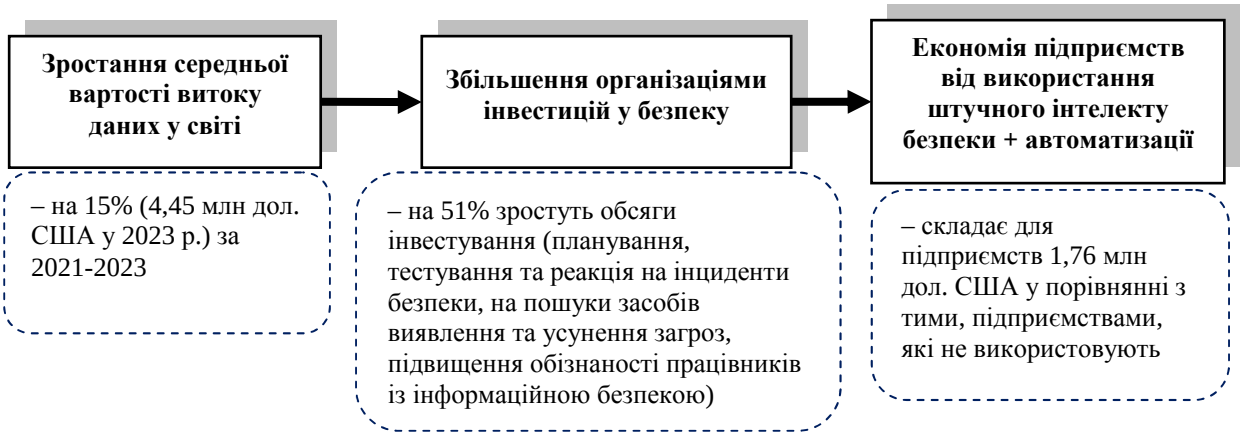

Рис. 4. **Зменшення ризиків та мінімізація втрат від використання штучного інтелекту безпеки та автоматизації**

Джерело: складено автором за даними [15].

До проблем безпеки даних телекомунікаційних підприємств додається використання хмарних сервісів, на них припадає 82% викрадень даних. Інформація важливий ресурс для підприємств, тому надаючи послугу із її передачі, обробки, зберігання телекомунікаційні підприємства мають захищати дані у процесі переміщення у хмарному середовищі (між хмарами, базами даних, програмами, службами).

З метою розвантаження IT-відділу від зростаючої кількості завдань безпеки інформаційної інфраструктури, підприємства користуються послугою SECaaS (Security as a Service) – безпека як послуга. SECaaS включає продукти або послуги безпеки, які надаються як хмарні служби, та відповідають основним характеристикам NIST для хмарних обчислень. Сьогодні в світі спостерігається зростання ринку безпеки як послуги (SECaaS). За оцінками 2022 року розмір такого ринку складав 10,2 млрд дол. США, а в 2033 році, як очікується, він складе понад 81 млрд дол. (прогнозовані дані) [16]. Попит на такі послуги зростатиме через переміщення даних у хмару та підвищення інтересу до масивів даних, що у ній зберігаються.

На думку експертів з різних країн світу, найближчим часом геополітична напруга зростатиме, а інші загрози (зміни клімату, геополітична нестабільність та енергетичні ризики) будуть посилювати одна одну. При цьому, зросла роль високотехнологічних компаній, а також ефективність їх рішень щодо інформаційної та кібербезпеки в порівнянні з діями урядових організацій (наприклад компанія Microsoft відслідкувала російську кіберактивність на початку війни, технології Starlink забезпечили зв'язок на територіях, де велися активні бойові дії). В даному контексті зростає важливість питання безпеки даних підприємств у хмарному середовищі та пошуку інструментів протидії кіберзагрозам.

Висновки. Останнім часом кіберризики все більше привертають увагу аналітиків та експертів, оскільки масштаби використання технологій у всіх сферах (освіта, медицина, фінанси, телекомунікації, енергетика, оборона) невпинно зростають. Нагальним залишається питання захисту підприємств критичної інфраструктури та послуг (вважає 51% експертів), адже кіберризики зростають й стабільно утримуються у трійці найбільших загроз не лише для організацій, підприємств, а й для людства.

Результати дослідження свідчать, що загрози, пов'язані з використання хмарних технологій та сервісів за невизначених умов, є серйозною проблемою, оскільки дані, що в них зберігаються можуть бути викрадені чи знищені. Отже, кібербезпека стає невід'ємним компонентом в забезпеченні повноцінного функціонування підприємства, а шляхи та засоби її досягнення вимагають подальших досліджень.

4 Список використаних джерел

1. Шевчук І., Депутат Б. Економічний аспект використання хмарних технологій у діяльності органів публічної влади та бізнес-структур. *Економіка та суспільство*. 2021. № 31. URL: https://doi.org/10.32782/2524-0072/2021-31-26
2. Нікітенко К. С., Осадчий А. А. Упровадження хмарних технологій у діяльність сучасних підприємств. *Підприємництво і торгівля*. 2020. № 27. С. 53-57. https://doi.org/10.36477/2522-1256-2020-27-09
3. Mykhailovyna S., Matros O., Polishchuk O. Cloud technologies as an important aspect of the development of accounting and taxation. *Efektyvna ekonomika.* 2021. No. 8. URL: https://doi.org/10.32702/2307-2105-2021.8.86
4. Dawood M., Tu S., Xiao C., Alasmary H., Waqas M., Rehman S. Ur. Cyberattacks and Security of Cloud Computing: A Complete Guideline. *Symmetry*. 2023. Vol. 15, no. 11. 1981. https://doi.org/10.3390/sym15111981
5. Darwish M. A., Yafi E., Almasri A. H., Zuhairi M. F. Privacy and security of cloud computing: a comprehensive review of techniques and challenges. *International Journal of Engineering Trends and Technology*. 2018. Vol. 7, no. 4.29. pp. 239-246.
6. Про хмарні послуги: Закон України від 17.02.2022 р. № 2075-IX. URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text
7. Significant Cyber Incidents. URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-09/230911_Significant_Cyber_Events_List.pdf?VersionId=pwkO6dlFR2EhIb5p_WUq5HCiK4Al_6XI
8. Axa Future Risks Report 2022. URL: https://www-axa-com.cdn.axa-contento-118412.eu/www-axa-com/15c65a87-4d11-49a4-b88e-be5953965b37_axa_futurerisksreport_2022_va.pdf
9. Cyber Dimensions of the Armed Conflict in Ukraine. URL: https://cyberpeaceinstitute.org/wp-content/uploads/Cyber%20Dimensions_Ukraine%20Q4%20Report.pdf
10. Cyber Dimensions of the Armed Conflict in Ukraine. URL: https://cyberpeaceinstitute.org/wp-content/uploads/2023/05/Ukraine-Report-Q1_FINAL.pdf
11. World Economic Forum. The Global Risks Report 2022, 17th Edition. URL: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
12. Дослідницька служба Європейського парламенту. Війна Росії проти України: хронологія кібератак. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf
13. Cyberattacks Impact and Harm on the ICT sector | CyberPeace Institute. URL: https://cyberconflicts.cyberpeaceinstitute.org/impact/sectors/ict
14. Група хакерів здійснює деструктивні кібератаки на українських провайдерів – детальний аналіз інциденту від CERT-UA та рекомендації щодо захисту. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/grupa-khakeriv-zdiisnyuye-destruktivni-kiberataki-na-ukrayinskikh-provaideriv-detalnii-analiz-incidentu-vid-cert-ua-ta-rekomendaciyi-shodo-zakhistu
15. Cost of a data breach 2023 | IBM. URL: https://www.ibm.com/reports/data-breach
16. Global Security as a Service market forecast 2022 | Statista. URL: https://www.statista.com/statistics/595164/worldwide-security-as-a-service-market-size

4 References

1. Shevchuk, I. & Deputat, B. (2021). Ekonomichnyi aspekt vykorystannja khmarnykh tekhnologhii u dijaljnosti orghaniv publichnoji vlady ta biznes-struktur [The economic aspect of the use of cloud technologies in the activities of public authorities and business structures]. *Ekonomika ta suspiljstvo*, 31. https://doi.org/10.32782/2524-0072/2021-31-26
2. Nikitenko, K. S., & Osadchyj, A. A. (2020). Uprovadzhennja khmarnykh tekhnologhij u dijaljnistj suchasnykh pidpryjemstv [Implementation of cloud technologies in the activities of modern enterprises]. *Pidpryjemnyctvo i torghivlja*, 27, 53-57. https://doi.org/10.36477/2522-1256-2020-27-09
3. Mykhailovyna, S., Matros, O., & Polishchuk, O. (2021). Cloud technologies as an important aspect of the development of accounting and taxation. *Efektyvna ekonomika*, 8. https://doi.org/10.32702/2307-2105-2021.8.86
4. Dawood, M., Tu, S., Xiao, C., Alasmary, H., Waqas, M., & Rehman, S. U. (2023). Cyberattacks and security of cloud computing: a complete guideline. *Symmetry*, *15*(11), 1981. https://doi.org/10.3390/sym15111981
5. Darwish, M. A., Yafi, E., Almasri, A. H., & Zuhairi, M. F. (2018). Privacy and security of cloud computing: a comprehensive review of techniques and challenges. *International Journal of Engineering Trends and Technology*, *7*(4.29), 239-246.
6. Verkhovna Rada Ukrainy. (2022). Pro khmarni poslughy: Zakon Ukrajiny [About cloud services: Law of Ukraine] Retrieved from https://zakon.rada.gov.ua/laws/show/2075-20#Text

7. Significant Cyber Incidents. Retrieved from https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-09/230911_Significant_Cyber_Events_List.pdf?VersionId=pwkO6dlFR2EhIb5p_WUq5HCiK4Al_6XI
8. Axa Future Risks Report 2022. Retrieved from https://www-axa-com.cdn.axa-contento-118412.eu/www-axa-com/15c65a87-4d11-49a4-b88e-be5953965b37_axa_futurerisksreport_2022_va.pdf
9. Cyber Dimensions of the Armed Conflict in Ukraine. Retrieved from https://cyberpeaceinstitute.org/wp-content/uploads/Cyber%20Dimensions_Ukraine%20Q4%20Report.pdf
10. Cyber Dimensions of the Armed Conflict in Ukraine. Retrieved from https://cyberpeaceinstitute.org/wp-content/uploads/2023/05/Ukraine-Report-Q1_FINAL.pdf
11. World Economic Forum. (2022). The Global Risks Report 2022, 17th Edition. Retrieved from https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
12. Research Service of the European Parliament. (2022). Russia's war against Ukraine: a chronology of cyberattacks. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf
13. Cyberattacks Impact and Harm on the ICT sector | CyberPeace Institute. Retrieved from https://cyberconflicts.cyberpeaceinstitute.org/impact/sectors/ict
14. State Service of Special Communications and Information Protection of Ukraine. (2023). Hrupa khakeriv zdiisniuie destruktyvni kiberataky na ukrainskykh provaideriv – detalnyi analiz intsydentu vid CERT-UA ta rekomendatsii shchodo zakhystu [A group of hackers carries out destructive cyberattacks on Ukrainian providers – a detailed analysis of the incident from CERT-UA and recommendations for protection] Retrieved from https://cip.gov.ua/ua/news/grupa-khakeriv-zdiisnyuye-destruktivni-kiberataki-na-ukrayinskikh-provaideriv-detalnii-analiz-incidentu-vid-cert-ua-ta-rekomendaciyi-shodo-zakhistu
15. Cost of a data breach 2023 | IBM. Retrieved from https://www.ibm.com/reports/data-breach
16. Global Security as a Service market forecast 2022 | Statista. Retrieved from https://www.statista.com/statistics/595164/worldwide-security-as-a-service-market-size