МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кваліфікаційна наукова праця на правах рукопису

ГЛАЗУНОВ АНДРІЙ СЕРГІЙОВИЧ

УДК 004.056

ДИСЕРТАЦІЯ
КОМП’ЮТЕРНІ БАЄСІВСЬКІ МОДЕЛІ ВИЯВЛЕННЯ ІНСАЙДЕРІВ У ХМАРНИХ СЕРВІСАХ

122 – Комп'ютерні науки

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ А.С. Глазунов

Київ – 2026

АНОТАЦІЯ

Глазунов А. С. **Комп'ютерні баєсівські моделі виявлення інсайдерів у хмарних сервісах.** - Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктор філософії за спеціальністю 122 «Комп'ютерні науки». Національний університет біоресурсів і природокористування України, Київ, 2025.

У дисертаційній роботі представлені результати проведених здобувачем досліджень, які спрямовані на розв'язання актуальної наукової задачі створення моделі інтелектуальної системи виявлення інсайдерських загроз у хмарних сервісах на основі модифікованої байєсівської мережі. Запропоноване рішення має істотне значення для розвитку інформаційних технологій, оскільки забезпечує врахування поведінкових, технічних і організаційних індикаторів, а також сценаріїв шахрайських дій з боку керівного персоналу, а отримані результати реалізовано у вигляді прототипу системи підтримки прийняття рішень, що дозволяє інтегрувати модель у засоби інформаційної безпеки хмарних систем.

Об'єктом дослідження є процес функціонування систем забезпечення інформаційної безпеки у хмарних середовищах інформаційних систем, зокрема для виявлення внутрішніх порушників (інсайдерів) та прогнозування несанкціонованих дій.

Предмет дослідження. Предметом дослідження є математичні моделі, методи та алгоритми формалізації ознак інсайдерських загроз, побудови локальних байєсівських мереж, а також оптимальні процедури багатоальтернативної послідовної перевірки гіпотез для аналізу поведінкових та системних даних, отриманих із засобів кібербезпеки (SIEM, DLP, IDS/IPS тощо).

Стрімке впровадження хмарних сервісів (ХС) у головні галузі економіки та державного управління – фінанси, охорону здоров'я, логістику, енергетику, освіту тощо зумовило необхідність ефективного управління ризиками інформаційної безпеки (ІБ), зокрема тими, що пов'язані з інсайдерськими

загрозами. Хоча хмарні обчислення (ХОб) забезпечують високу гнучкість, масштабованість і швидкість опрацювання даних, вони водночас ускладнюють контроль за поведінкою користувачів і сприяють зростанню ймовірності порушень безпеки з боку внутрішніх суб'єктів доступу. Саме інсайдерські загрози сьогодні визнаються одними з найнебезпечніших і найменш контрольованих форм атак на ІБ хмарних середовищ.

Питання захисту хмарних обчислень та ефективності використання ХС у різних секторах активно досліджувалося вітчизняними фахівцями: Бойком С. В., Довбешком С. В., Ждановим Ю. Д., Зіданом А. М., Мацьком О. Й., Нечипуренком К. О., Савченком В. А., Савченком В. В., Складанним П. М., Шевченком С. М., а також зарубіжними вченими – Agrafiotis I., Agrafiotis J. R., Bart E., Brdiczka O., Buckley P., Cappelli D. M., Chow R., Creese I., d'Ambrosio N., Ducheneaut N., Elmrabit N., Goldsmith M., J. Liu, Legg S., Lewellen T., Moore A. P., Nurse O., Patil A., Perrone G., Price B., R. F. Trzeciak, Romano S. P., Shen J., Spooner D., Wall A., Weiland R. M., Yang L., Yang S. H., Zhou H. та іншими.

Паралельно інтенсивно розвивалися методи аналізу користувацької поведінки з використанням інструментів штучного інтелекту та машинного навчання, серед яких вагоме місце займають байєсівські мережі. Дослідження в цій галузі представлені роботами Бідюка П. І., Головатого Т. І., Згуровського М. З., Опірського І. Р., Просянкіної-Жарової Т. І., Терентьєва О. М., а також Agrafiotis I., Axelrad E. T., Brdiczka O., Darwiche A., Dietz A., Elmrabit N., Gaebel J., Hikal A., Neumuth T., Shen J., Sticha P. J., Stoehr M., Wall A., Yang L., Yang S. H., Zhou H. тощо. Як засвідчив аналіз попередніх досліджень, помітною є тенденція до застосування локальних байєсівських мереж у задачах аналізу ризиків та поведінкової аналітики в інформаційній безпеці.

Втім, аналіз сучасних рішень свідчить про те, що переважна їх більшість зосереджена на виявленні зовнішніх загроз або типових інцидентів інформаційної безпеки без врахування специфіки високорівневих інсайдерських сценаріїв, зокрема з боку керівного складу. Окрім того, у більшості відомих моделей відсутнє належне формалізоване представлення

взаємозв’язку між цифровими слідами, поведінковими індикаторами та ризиками в режимі реального часу.

У зв’язку з цим актуальність теми дисертаційного дослідження зумовлена потребою у створенні вдосконалених імовірнісних моделей та методів для виявлення інсайдерських загроз у хмарних середовищах, які б поєднували аналітичну строгость, адаптивність до сценаріїв поведінки користувачів і можливість впровадження в практичні системи кіберзахисту.

Метою дисертаційного дослідження є підвищення ефективності виявлення та прогнозування інсайдерських загроз у хмарних сервісах інформаційних систем шляхом розробки математично обґрунтованого методу та моделі на основі послідовних байєсівських правил, побудови локальних байєсівських мереж та використання методів інтелектуального аналізу даних.

Для реалізації мети дослідження розроблено модифіковану модель баєсівської мережі для виявлення інсайдерських загроз у хмарних сервісах, яка відрізняється своєю структурою, що включає вузли для оцінювання шахрайських дій керівного персоналу, та здатністю враховувати цифрові сліди, сформовані в процесі взаємодії з хмарною інфраструктурою. Досліджено й реалізовано процедуру побудови оптимальних послідовних баєсівських правил, яка дає змогу оцінювати ймовірність порушення інформаційної безпеки ще до настання інциденту, з урахуванням причинно-наслідкових і нелінійних залежностей між ризиками й обґрунтовано використання технічних, поведінкових та організаційних індикаторів у задачах прогнозування інсайдерської активності. А також програмно реалізовано у вигляді прототипу системи підтримки прийняття рішень для фахівців з інформаційної безпеки, яка забезпечує інтерактивну взаємодію з аналітиком, візуалізацію результатів і підтримку ухвалення обґрунтованих рішень щодо внутрішніх (інсайдерських) загроз.

Вперше розроблено модифіковану модель баєсівської мережі для виявлення інсайдерських загроз у хмарних сервісах інформаційних систем. На відміну від наявних рішень, модель включає спеціалізовані вузли для

врахування дій осіб, які займають керівні посади, і моделює ризики шахрайської поведінки з боку такого персоналу. Модель враховує цифрові сліди, які формуються під час взаємодії користувача з хмарними застосунками, що дозволяє оцінювати ймовірність внутрішніх загроз до моменту фактичного порушення. Структура розробленої моделі включає опис апріорних і апостеріорних ймовірностей для вирішальних технічних, поведінкових та організаційних індикаторів, що забезпечує глибше причинно-наслідкове моделювання ситуацій загрози в умовах неповної інформації.

Удосконалено метод виявлення несанкціонованого доступу до хмарних сервісів шляхом впровадження адаптивної баєсівської мережі з функціональністю прогнозування інсайдерських загроз. Відмінністю даного підходу є врахування не лише поточних індикаторів загрози, але і їхніх взаємозалежностей у часі, що дозволяє виявляти загрозу на ранніх стадіях та своєчасно запобігати порушенням. Запропоновано уточнену процедуру побудови оптимальних послідовних баєсівських правил, які дозволяють адаптувати порогові значення оцінювання ризику залежно від контексту дій. Такий підхід базується на мінімізації апостеріорного ризику і дозволяє приймати виважені рішення щодо безпеки в умовах багатокритеріальної невизначеності.

Дістав подальшого розвитку метод щодо раннього виявлення інсайдерів у хмарному середовищі, який базується на інтеграції технічних, поведінкових і організаційних індикаторів у межах баєсівської моделі. На відміну від наявних моделей, орієнтованих переважно на звичайних користувачів хмарних сервісів, запропонована система дозволяє враховувати специфіку діяльності керівного персоналу, який має підвищений рівень доступу до конфіденційної інформації та ресурсів.

Практичне значення дисертаційного дослідження полягає у розробленні, програмній реалізації та апробації інтелектуальної моделі виявлення інсайдерських загроз у хмарних середовищах з використанням модифікованої баєсівської мережі, що дає змогу здійснювати багатофакторну оцінку ризику,

пов’язаного з поведінкою співробітників, які взаємодіють із хмарними сервісами, зокрема з урахуванням можливих шахрайських дій з боку осіб, які займають керівні посади. У структурі баєсівської мережі враховано цифрові сліди, поведінкові аномалії та організаційні фактори ризику, що дозволяє підвищити точність виявлення внутрішніх порушників на ранніх етапах. У межах роботи програмно на мові Python реалізовано алгоритмічну процедуру побудови оптимальних послідовних баєсівських правил, яка забезпечує гнучку адаптацію порогів прийняття рішень відповідно до накопичених апостеріорних ймовірностей та враховує ймовірнісні витрати помилкових рішень, як хибнопозитивних, так і хибнонегативних, а також змінну етапів ухвалення рішення в системах інформаційної безпеки хмарних сервісів. Це створює основу для впровадження подібної системи підтримки прийняття рішень у різних організаціях з урахуванням специфіки їх політик безпеки, кадрових структур та хмарної архітектури. Програмна реалізація моделі здійснена за допомогою середовища GeNIe/SMILE та мови програмування Python, що дозволяє забезпечити модульність, масштабованість та інтеграцію з типовими інструментами кіберзахисту, такими як SIEM, DLP, IDS/IPS. У моделі реалізовано вузли, які описують як технічні й поведінкові ознаки активності користувачів, так і фактори, пов’язані з організаційним контекстом і управлінськими повноваженнями. Створено прототип системи підтримки прийняття рішень (СППР), адаптований для використання фахівцями підрозділів інформаційної безпеки. СППР забезпечує покроковий інтерфейс введення даних, що дозволяє поступово формувати індивідуальний профіль ризику співробітника, здійснювати автоматичний аналіз на основі заданої моделі та візуалізувати результати у зручному вигляді. В ході експериментальних досліджень продемонстровано ефективність запропонованого рішення, а факт впровадження підтверджується відповідним актом, який додається до дисертації.

Ключові слова: імовірнісне моделювання, хмарні сервіси, інсайдерська загроза, внутрішній порушник, цифрові сліди, система

підтримки прийняття рішень (СППР), машинне навчання, баєсівська мережа, оптимальні послідовні баєсівські правила.

/

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України

1. Глазунов А.С. Розробка байєсівських мереж для системи підтримки прийняття рішень під час аналізу внутрішніх кіберзагроз. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2024. № 1(25), 103–117.

2. Глазунов А.С. Огляд та аналіз досліджень з проблематики інформаційної безпеки хмарних інфраструктур. Інформаційні технології та суспільство. 2024. 1(12), 38–45.

3. Глазунов А.С. Байєсівські правила прогнозування несанкціонованого доступу внутрішнього порушника до публічних сервісів компанії. Наука і техніка сьогодні. 2025. 1(42).

4. Глазунов, А., Гуржій, А. (2025). Метод раннього виявлення інсайдерів у хмарних середовищах. Технічна інженерія, (2(96), 90–94. https://doi.org/10.26642/ten-2025-2(96)-90-94

Тези наукових доповідей

5. Глазунов А. С., Гуржій А. М. Оптимізація навчального порталу Moodle за допомогою Amazon Web Services. Інформаційні технології: економіка, техніка, освіта ‘2023: матеріали Міжнар. наук.-практ. конф. молодих вчених, 26-27 жовтень 2023 року, Київ, 2024. С. 75–77.

6. Глазунов А. С., Матієвський В. В. Порівняльний аналіз управління ідентифікацією та доступом основних хмарних постачальників. Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні '2024 : матеріали XII Міжнар. наук.-практ. конф. (Київ, 21–22 листоп. 2024 р.). Київ, 2024. С. 103–107.

ABSTRACT

Hlazunov A. S. **Computer Bayesian models for detecting insiders in cloud services. -** Qualification for scientific work on the rights of the manuscript.

Dissertation for the degree of Doctor of Philosophy in the speciality 122 "Computer Science". National University of Life and Environmental Sciences of Ukraine, Kyiv, 2025.

The dissertation presents the results of the research, including applications aimed at addressing the current scientific problem of developing an intelligent system for detecting insider threats in cloud services based on a modified Bayesian network. The proposed solution is of significant importance for the development of information technologies, as it takes into account behavioural, technical and organisational indicators, as well as scenarios of fraudulent actions by management personnel. The results are implemented as a decision support system prototype, which allows integrating the model into information security tools for cloud systems.

The object of the study is the functioning of information security systems in cloud environments, in particular for detecting internal violators (insiders) and predicting unauthorised actions.

Subject of the study. The subject of the research is mathematical models, methods, and algorithms for formalising signs of insider threats, building local Bayesian networks, and optimal procedures for multi-alternative sequential hypothesis testing for analysing behavioural and system data obtained from cybersecurity tools (SIEM, DLP, IDS/IPS, etc.).

The rapid introduction of cloud services (CS) into the main sectors of the economy and public administration - finance, healthcare, logistics, energy, education, etc. - has led to the need for effective management of information security (IS) risks, in particular those associated with insider threats. Although cloud computing (CC) provides high flexibility, scalability, and speed of data processing, it also complicates control over user behaviour. It increases the likelihood of security violations by internal access subjects. Insider threats are now recognised as one of the most dangerous and least controlled forms of attacks on cloud IT environments.

The issues of cloud computing protection and the efficiency of using CS across various sectors have been actively studied by domestic specialists: Boyko S. V., Dovbeshko S. V., Zhdanov Yu. D., Zidan A. M., Mats'ky O. Y., Nechypurenko K. O., Savchenko V. A., Savchenko V. V., Skladanny P. M., Shevchenko S. M., as well as foreign scientists - Agrafiotis I., Agrafiotis J. R., Bart E., Brdiczka O., Buckley P., Cappelli D. M., Chow R., Creese I., d'Ambrosio N., Ducheneaut N., Elmrabit N., Goldsmith M., J. Liu, Legg S., Lewellen T., Moore A. P., Nurse O., Patil A., Perrone G., Price B., R. F. Trzeciak, Romano S. P., Shen J., Spooner D., Wall A., Weiland R. M., Yang L., Yang S. H., Zhou H. and others.

In parallel, methods for analysing user behaviour using artificial intelligence and machine learning tools have been intensively developed, among which Bayesian networks play a significant role.. Research in this area is represented by the works of Bidyuk P. I., Golovaty T. I., Zgurovsky M. Z., Opirsky I. R., Prosyankina-Zharova T. I., Terentyev O. M., as well as Agrafiotis I., Axelrad E. T., Brdiczka O., Darwiche A., Dietz A., Elmrabit N., Gaebel J., Hikal A., Neumuth T., Shen J., Sticha P. J., Stoehr M., Wall A., Yang L., Yang S. H., Zhou H., etc. As previous studies have shown, there is a noticeable trend towards the use of local Bayesian networks in risk analysis and behavioural analytics in information security.

However, the analysis of current solutions shows that the vast majority focus on detecting external threats or typical information security incidents, without accounting for the specifics of high-level insider scenarios, particularly those involving the management team. In addition, most known models lack a proper, formalised representation of the relationship between digital traces, behavioural indicators, and risks in real time.

In this regard, the relevance of the dissertation research topic stems from the need to develop improved probabilistic models and methods for detecting insider threats in cloud environments, which would combine analytical rigour, adaptability to user behaviour scenarios, and practical implementation in cybersecurity systems.

The dissertation research aims to increase the efficiency of detecting and predicting insider threats in cloud services of information systems by developing a

mathematically based method and model based on sequential Bayesian rules, building local Bayesian networks and using data mining methods.

To implement the aim of the research, a modified Bayesian network model was developed for detecting insider threats in cloud services, which is distinguished by its structure, which includes nodes for assessing fraudulent actions of management personnel, and the ability to take into account digital traces formed in the process of interaction with cloud infrastructure. The procedure for constructing optimal sequential Bayesian rules has been studied and implemented, which allows assessing the probability of information security violations even before the incident occurs, taking into account cause-and-effect and nonlinear dependencies between risks, and the use of technical, behavioural and organisational indicators in the tasks of predicting insider activity has been substantiated. It has also been implemented programmatically as a prototype decision support system for information security specialists, providing interactive interaction with an analyst, visualisation of results, and support for informed decision-making regarding internal (insider) threats.

A modified Bayesian network model has been developed for the first time to detect insider threats in cloud services of information systems. Unlike existing solutions, the model includes specialised nodes to account for the actions of personnel in management positions and models the risks of fraudulent behaviour by such personnel. The model takes into account digital traces generated during the user's interaction with cloud applications, enabling the assessment of the probability of internal threats before the actual violation. The structure of the developed model includes descriptions of a priori and a posteriori probabilities for crucial technical, behavioural, and organisational indicators, which provide deeper causal modelling of threat situations in conditions of incomplete information.

The method for detecting unauthorised access to cloud services has been improved by implementing an adaptive Bayesian network capable of predicting insider threats. The difference with this approach is that it accounts not only for current threat indicators but also their temporal interdependencies, enabling threats to be detected at early stages and violations to be prevented promptly. A refined

procedure for constructing optimal sequential Bayesian rules has been proposed, allowing adaptation of threshold values for risk assessment based on the context of actions. This approach is based on minimising a posteriori risk and provides for informed security decisions under multi-criteria uncertainty.

The method for early detection of insiders in the cloud environment, which integrates technical, behavioural, and organisational indicators into a Bayesian model, has been further developed. Unlike existing models focused mainly on ordinary users of cloud services, the proposed system accounts for the specific activities of management personnel, who have greater access to confidential information and resources.

The practical significance of the dissertation research lies in the development, software implementation and testing of an intelligent model for detecting insider threats in cloud environments using a modified Bayesian network, which allows for a multifactorial assessment of the risk associated with the behaviour of employees interacting with cloud services, in particular, taking into account possible fraudulent actions by persons occupying management positions. The structure of the Bayesian network takes into account digital traces, behavioural anomalies, and organisational risk factors, which allows for increased accuracy in detecting internal intruders at early stages. As part of the work, an algorithmic procedure for constructing optimal sequential Bayesian rules was implemented in Python, which provides flexible adaptation of decision-making thresholds in accordance with the accumulated posterior probabilities and takes into account the probabilistic costs of erroneous decisions, both false positive and false negative, as well as the variable stages of decision-making in information security systems of cloud services. This provides a basis for implementing a similar decision-making support system across various organisations, while accounting for their specific security policies, personnel structures, and cloud architectures. The software implementation of the model was carried out using the GeNIe/SMILE environment and the Python programming language, which enables modularity, scalability, and integration with typical cybersecurity tools, such as SIEM, DLP, and IDS/IPS. The model implements nodes

that describe both technical and behavioural features of user activity, as well as factors related to the organisational context and managerial powers. A prototype decision support system (DSS) adapted for specialists in information security departments has been developed. The DSS provides a step-by-step data entry interface that allows you to gradually build an individual risk profile for an employee, perform automated analysis based on a given model, and visualise the results in a convenient format. During experimental studies, the effectiveness of the proposed solution was demonstrated, and the implementation is confirmed by the corresponding act attached to the dissertation.

Keywords: probabilistic modelling, cloud services, insider threat, internal violator, digital traces, decision support system (DSS), machine learning, Bayesian network, optimal sequential Bayesian rules.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

БЗ – база знань

БМ – байєсівська мережа

ВП – внутрішній порушник

ІБ – інформаційна безпека

СППР – система підтримки прийняття рішень

ХОб – хмарні обчислення

ХС – хмарні сервіси

ACS – система контролю доступу (Access Control System)

API – програмний інтерфейс прикладного програмування (Application Programming Interface)

AWS – хмарна платформа Amazon Web Services

CPD – умовні розподіли ймовірностей (Conditional Probability Distribution)

DLP – система запобігання витоку даних (Data Loss Prevention)

EM-алгоритм – алгоритм очікування-максимізації (Expectation-Maximization)

IDS – система виявлення вторгнень (Intrusion Detection System)

IPS – система запобігання вторгненням (Intrusion Prevention System)

PCA – метод головних компонент (Principal Component Analysis)

SIEM – система керування подіями інформаційної безпеки (Security Information and Event Management)

ВСТУП

Актуальність теми.

Стрімке впровадження хмарних сервісів (ХС) у найважливіші сфери діяльності як держав, так й окремих компаній (фінанси, охорона здоров'я, логістика, енергетика, освіта та державне управління тощо) обумовлює необхідність ефективного управління ризиками інформаційної безпеки (ІБ), пов'язаних з інсайдерськими загрозами. Хоча хмарні (ХОб) обчислення забезпечують гнучкість, масштабованість та оперативність обробки даних, але одночасно ускладнюють контроль над користувацькою поведінкою, сприяючи зростанню ризику порушень із середини організації. Саме інсайдерські загрози визнані фахівцями одними з найбільш прихованих і складно виявлюваних типів атак на ІБ хмарних середовищ.

Протягом останніх десятиліть низка дослідників активно займалася проблематикою захисту хмарних обчислень та дослідженням ефективності ХС у різних галузях. Це роботи вітчизняних фахівців Бойко С. В., Довбешко С. В., Жданова Ю. Д., Зідан А. М., Мацько О. Й., Нечипуренко К. О., Савченко В. А., Савченко В. В., Складанний П. М., Шевченко С. М. тощо. А також закордонних вчених Agrafiotis I., Agrafiotis J. R., Bart E., Brdiczka O., Buckley P., Cappelli D. M., Chow R., Creese I., d'Ambrosio N., Ducheneaut N., Elmrabit N., Goldsmith M., J. Liu, Legg S., Lewellen T., Moore A. P., Nurse O., Patil A., Perrone G., Price B., R. F. Trzeciak, Romano, S. P., Shen J., Spooner D., Wall A., Weiland R. M., Yang L., Yang S. H., Zhou, H. тощо. Паралельно розвивались підходи до аналізу користувацької поведінки за допомогою методів штучного інтелекту й машинного навчання, серед яких помітне місце займають байєсівські мережі. Праці таких авторів як Бідюк П. І., Головатий Т. І., Згуровський М. З., Опірський І. Р., Просянкіна-Жарова Т. І., Терентьєв О. М., Agrafiotis I., Axelrad E.T., Brdiczka O., Darwiche A., Dietz A., Elmrabit N., Gaebel J., Hikal A., Neumuth T., Shen J., Sticha P. J., Stoehr M., Wall A., Yang L., Yang S.H., Zhou H. тощо, а також дослідження щодо локальних байєсівських мереж для кібербезпеки,

засвідчили зростаючий інтерес до імовірнісних моделей у задачах прогнозування поведінки користувачів.

Попри це, значна частина існуючих рішень фокусується на зовнішніх загрозах або типових сценаріях, що не враховують специфіку високорівневих інсайдерських дій, зокрема з боку керівного персоналу. Крім того, у більшості моделей недостатньо формалізовано зв'язок між цифровими слідами в ХС, поведінковими індикаторами та оцінкою ризику.

Актуальність теми дисертаційного дослідження зумовлена потребою у створенні удосконалених методів та моделей виявлення інсайдерських загроз у хмарних сервісах.

Мета й завдання дослідження.

Метою дисертаційного дослідження є підвищення ефективності виявлення та прогнозування інсайдерських загроз у хмарних сервісах інформаційних систем шляхом розробки математично обґрунтованого методу та моделі на основі послідовних байєсівських правил, побудови локальних байєсівських мереж та використання методів інтелектуального аналізу даних.

Завдання дослідження.

1. Обґрунтувати актуальність забезпечення інформаційної безпеки хмарних сервісів, як важливого компонента цифрової інфраструктури організацій, з урахуванням їх широкого впровадження в бізнес-процеси різних галузей, та виявити обмеження чинних засобів виявлення інсайдерських загроз, орієнтованих переважно на зовнішні атаки.

2. Розробити модифіковану модель байєсівської мережі, яка враховує як технічні та поведінкові індикатори користувачів, так і загрози шахрайських дій осіб, що обіймають керівні посади

3. Удосконалити метод виявлення несанкціонованого доступу до хмарних сервісів шляхом розробки оптимального послідовного байєсівського правила.

4. Провести експериментальні дослідження протопипа системи підтримки прийняття рішень у системах інформаційної безпеки для виявлення інсайдерських загроз.

Робоча гіпотеза дослідження полягає в тому, що підвищення ефективності виявлення інсайдерських загроз у хмарних сервісах інформаційних систем можливе за умови побудови модифікованої байєсівської мережі, яка, на відміну від існуючих рішень, враховує як технічні та поведінкові індикатори користувача, так і загрози шахрайських дій з боку осіб на керівних посадах. У межах цієї гіпотези ефективність виявлення інсайдерів може бути підвищена шляхом формалізації слідів, пов'язаних з активністю в хмарному середовищі, обчисленням апріорних та апостеріорних ймовірностей потенційної загрози, а також реалізацією адаптивної процедури послідовної перевірки гіпотез, що враховує причинно-наслідкові та нелінійні залежності між параметрами ризику.

Об'єктом дослідження є процес функціонування систем забезпечення інформаційної безпеки у хмарних середовищах інформаційних систем для виявлення внутрішніх порушників (інсайдерів) та прогнозування несанкціонованих дій.

Предмет дослідження. Предметом дослідження є математичні моделі, методи та алгоритми формалізації ознак інсайдерських загроз, побудови локальних байєсівських мереж, а також оптимальні процедури багатоальтернативної послідовної перевірки гіпотез для аналізу поведінкових та системних даних, отриманих із засобів кібербезпеки (SIEM, DLP, IDS/IPS тощо).

Методи дослідження. У роботі застосовано міждисциплінарний підхід, що поєднує аналітичні, математичні, статистичні та програмні методи. Аналітичні методи використано для огляду та систематизації наукових підходів до забезпечення інформаційної безпеки хмарних сервісів. Методи теорії ймовірностей та байєсівської статистики – для побудови і навчання байєсівських мереж та визначення апостеріорних ймовірностей гіпотез щодо

наявності інсайдерської загрози. Методи багатоальтернативної послідовної перевірки гіпотез – для формалізації процедури виявлення несанкціонованого доступу на основі накопичення даних, з урахуванням змінних порогових значень і ризику прийняття хибного рішення (хибнопозитивного або хибнонегативного). Методи математичної оптимізації – для мінімізації апостеріорного ризику в процедурі прийняття рішень для забезпечення інформаційної безпеки хмарних сервісів. Програмні методи та інструменти – для створення прототипу байєсівської мережі та візуалізації графової структури моделі та для реалізації функцій обчислення ймовірностей інсайдерської загрози із подальшим відображенням результатів у вигляді гістограм. Методи валідації програмної реалізації для тестування моделі на синтетичних даних, що містять ознаки минулих інцидентів, згенерованих на основі типових сценаріїв поведінки інсайдерів та візуалізація результатів для перевірки якості класифікації співробітників за рівнем ризику.

Наукова новизна одержаних результатів.

Вперше:

розроблено модифіковану модель байєсівської мережі для виявлення інсайдерських загроз у хмарних сервісах інформаційних систем, яка відрізняється від чинних рішень тим, що включає спеціалізовані вузли для моделювання шахрайських дій осіб, які займають керівні посади, та враховує цифрові сліди, сформовані під час взаємодії з хмарними застосунками, і призначена для оцінювання ймовірності внутрішньої загрози з боку керівного персоналу ще до настання безпекового інциденту;

розроблено структуру цієї моделі з описом апріорних і апостеріорних ймовірностей подій, що відповідають ключовим індикаторам інформаційної безпеки, яка відрізняється від аналогів тим, що враховує як технічні параметри, так і поведінкові особливості користувача, для цілей підвищення точності раннього виявлення інсайдерів у хмарному середовищі.

Удосконалено:

метод виявлення несанкціонованого доступу до хмарних сервісів, шляхом впровадження адаптивної байєсівської мережі з можливістю прогнозування інсайдерської загрози, що відрізняється від наявних рішень здатністю враховувати причинно-наслідкові залежності між індикаторами ризику в умовах невизначеності, і дозволяє своєчасно ідентифікувати загрозу до її реалізації, мінімізуючи потенційні збитки.

процедуру побудови оптимальних послідовних байєсівських правил шляхом врахування нелінійних залежностей між ймовірністю реалізації інциденту та оцінками ризику, для забезпечення точної адаптації алгоритму прийняття рішень з інформаційної безпеки хмарних сервісів.

Набув подальшого розвитку:

метод раннього виявлення інсайдерів в організаціях, що використовують хмарні сервіси, який відрізняється від відомих підходів використанням інтегрованої моделі, що враховує одночасно технічні, поведінкові та організаційні характеристики користувача, і призначений для зниження ймовірності несанкціонованого доступу з боку співробітників, зокрема тих, хто має розширені повноваження на керівних посадах.

Практичне значення дисертаційного дослідження полягає у створенні, програмній реалізації та апробації моделі модифікованої байєсівської мережі, що призначена для виявлення інсайдерських загроз у хмарних сервісах організацій.

Програмно реалізовано алгоритмічну процедуру побудови оптимальних послідовних байєсівських правил для прогнозування несанкціонованого доступу, що дозволяє здійснювати поетапну оцінку рівня загрози на основі порівняння апостеріорних ймовірностей гіпотез із гнучкими пороговими значеннями. У цій процедурі враховано вартість помилкових рішень (як хибнопозитивних, так і хибнонегативних) та змінну критичність етапів прийняття рішень, що забезпечує гнучкість налаштування до конкретних організаційних вимог. Розроблено програмну реалізацію байєсівської мережі з використанням середовища GeNIe/SMILE та мови Python, яка підтримує

обробку поведінкових і системних ознак, отриманих із засобів контролю безпеки (SIEM, DLP, IDS/IPS). У програмному застосунку враховано спеціалізовані вузли, що дозволяють моделювати не лише типові сценарії інсайдерської активності, а й шахрайські дії на керівних рівнях управління. Запропонована модель вбудована у прототип системи підтримки прийняття рішень (СППР), орієнтованої на фахівців служб безпеки. СППР має покроковий інтерфейс введення даних, що дозволило поступово формувати профіль користувача й оцінити рівень ризику відповідно до параметрів, заданих у моделі на прикладі підприємства ТОВ “Інфобіт”. Акт впровадження додається.

Особистий внесок здобувача.

Усі результати дисертаційного дослідження, включно з теоретичними положеннями, практичними рекомендаціями та висновками, отримано автором самостійно. Сформульовані в роботі наукові підходи, методи й пропозиції є результатом особистої наукової діяльності здобувача та становлять його внесок у розвиток відповідної галузі знань. Із наукових публікацій, підготовлених у співавторстві, у дисертаційній роботі використано виключно результати, які належать автору особисто.

Апробація результатів дослідження.

Основні наукові положення дослідження обговорювались на науково-практичних конференціях, круглих столах і форумах, серед яких: Міжнародна науково-практична конференція молодих вчених «Інформаційні технології: економіка, техніка, освіта ‘2023», 26-27 жовтня 2023 року, м.Київ, Міжнародна науково-практична конференція «Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні '2024», 21–22 листопада 2024 р., Київ, Міжнародна наукова інтернет-конференція Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення: (м. Тернопіль, Україна, м. Ополе, Польща, 15-16 квітня 2025 р.

Публікація результатів дослідження.

Положення дисертації опубліковано у 4 наукових працях, серед яких 4 статті в наукових виданнях, включених до категорії «Б» Переліку наукових фахових видань України, 2 тези наукових доповідей. Основний внесок за обсягом у матеріалах публікацій належить здобувачу.

Структура та обсяг дисертації.

Дисертаційне дослідження структуровано у вигляді анотації, вступу, трьох основних розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 190 сторінок комп'ютерного тексту. Матеріал ілюстровано 11 таблицями та 37 рисунками. До дисертації також включено 3 додатки. Бібліографічний список містить 153 джерела, з яких 131 – іншомовні (латиницею).

РОЗДІЛ 1.
ОГЛЯД ТА АНАЛІЗ ВИКОРИСТАННЯ ХМАРНИХ ОБЧИСЛЕНЬ І СЕРВІСІВ, ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЇХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Хмарні обчислення (ХОб) надають доступ до мережних ресурсів, таких як сховища даних та обчислювальні потужності, на вимогу, без прямого керування з боку користувачів. На сьогодні хмарні обчислення містять як публічні, так і приватні центри обробки даних, що надають клієнтам єдину платформу через інтернет. Периферійні обчислення (edge computing) – це стратегія досягнення такої мети, як наближення обчислень і збереження інформації кінцевих користувачів, скорочення часу відгуку та оптимізація пропускної спроможності хмарних сервісів. Мобільні хмарні обчислення використовують розподілені обчислення для передачі програм на мобільні пристрої, такі як телефони та планшети.

Перш ніж безпосередньо викладати результати дослідження, необхідно визначитися з термінами, які будуть використовуватися в даному розділі роботи. Інформаційна безпека (далі – ІБ) хмарних сервісів зазвичай охоплює широкий спектр заходів та практик, спрямованих на захист даних і систем хмарних сервісів від загроз, включаючи загрози як ззовні, так і зсередини компанії. Кібербезпека хмарних сервісів, з іншого боку, частіше пов'язана із захистом від кібератак, включаючи захист мереж, систем і даних від кіберзагроз. Коли йдеться про внутрішні загрози, такі як неблагонадійні співробітники або інсайдери, більш доречним та широко застосовуваним терміном є «інформаційна безпека хмарних сервісів». Цей термін відображає більш загальний підхід до захисту інформації та систем у хмарі, включаючи захист від загроз як зсередини, так і ззовні компанії, що надає хмарні послуги.

Термін «інформаційна безпека» (ІБ) наголошує на необхідності комплексного підходу до захисту від різних загроз, в тому числі внутрішніх, і містить широкий спектр заходів і практик, спрямованих на захист інформації та систем хмарних сервісів.

Численні дослідження показують, що хмарні обчислення та мобільні хмарні обчислення стикаються з проблемами ІБ, загрозами та вразливістю для клієнтів, і одним із перспективних шляхів боротьби з цими загрозами є використання методів машинного навчання.

Проте, якщо говорити про використання методів машинного навчання у питаннях безпеки, то ці методи універсальні, і немає можливості розділяти їх на методи машинного навчання для понять «інформаційна безпека хмарних сервісів» та «кібербезпека хмарних сервісів». Методи машинного навчання, такі як алгоритми виявлення аномалій або класифікації, застосовуються в обох випадках для безпеки хмарних сервісів. Вони використовуються для виявлення потенційно ненадійних співробітників або інсайдерів, а також для виявлення аномальної поведінки у хмарі, що допомагає запобігати загрозам безпеці. Отже, використання методів машинного навчання не залежить від того, як термінологічно визначається безпека хмарних сервісів, а є універсальним підходом до безпеки в хмарі. У даному розділі дисертації проведено аналіз загроз та проблем з ІБ, а також виконано огляд запропонованих різними авторами рішень щодо забезпечення ІБ хмарних обчислень і хмарних сервісів. Насамперед розглянуто дослідження, що ґрунтуються на застосуванні алгоритмів машинного навчання для забезпечення безпеки хмарних обчислень та хмарних сервісів.

1.1. Огляд хмарних моделей та сервісів у різних галузях

Модель хмарних обчислень містить три основні типи послуг (див. таблицю 1.1): програмне забезпечення як послуга (SaaS) [1], платформа як послуга (PaaS) [2] та інфраструктура як послуга (IaaS) [3]. У SaaS користувачі отримують доступ до веб-провайдерів SalesForce.com, Google Docs, Gmail і Spreadsheets), що працюють у хмарній інфраструктурі. Завдяки цьому користувачам не потрібно завантажувати, встановлювати і запускати програми на своїх пристроях. PaaS надає можливості для розробки та розгортання програм на платформах і мовах програмування, що підтримуються провайдером. Наприклад, Google App Engine, Microsoft Azure

та платформа Salesforce дають можливість розробникам створювати програми без керування або налаштування хмарної інфраструктури. IaaS надає обчислювальні ресурси (Amazon EC2 для обробки даних, Amazon S3 для зберігання даних) віртуально, у вигляді віртуальних машин, на яких можна розгортати будь-яке програмне забезпечення, зокрема операційні системи (далі – ОС) [4, 5].

Таблиця 1.1 – Моделі хмарних обчислень та приклади їх використання у бізнес-процесах об'єктів інформаційної діяльності (складено автором за матеріалами [1-10])

Модель	Переваги	Недоліки	Компанії, які використовують цю модель
Програмне забезпечення як послуга (SaaS)	1. Доступність 2. Простота використання 3. Масштабованість 4. Економічність	1. Залежність від постачальника 2. Обмежена кастомізація 3. Безпека даних 4. Контроль над даними 5. Доступність 6. Обмежена функціональність 7. Неможливість перенесення даних	Україна Rozetka – використовує SaaS-додаток Salesforce для керування взаємовідносинами з клієнтами. Nova Poshta – використовує SaaS-додаток SAP для керування ресурсами підприємства. PrivatBank – використовує SaaS-додаток Oracle для керування людськими ресурсами. Приклади використання SaaS в інших країнах: Netflix – використовує SaaS-додаток AWS для потокової передачі відео. Airbnb – використовує SaaS-додаток Salesforce для керування взаємовідносинами з клієнтами. Uber – використовує SaaS-додаток Google Maps Platform для визначення розташування та маршрутизації.

Продовження таблиці 1.1

Платформа як послуга (PaaS)	1. Швидке розгортання 2.Масштабованість 3. Економічність 4. Простота використання	1. Залежність від постачальника 2. Обмежена кастомізація 3. Безпека даних 4. Контроль над даними	Україна PrivatBank – використовує PaaS-платформу Google Cloud Platform для розробки та розгортання своїх мобільних додатків. Ukrtelecom – використовує PaaS-платформу Microsoft Azure для створення хмарної інфраструктури. Rozetka – використовує PaaS-платформу Amazon Web Services для розробки та розгортання своїх веб-додатків. Приклади використання PaaS в інших країнах: Netflix – використовує PaaS-платформу Amazon Web Services для потокової передачі відео. Uber – використовує PaaS-платформу Amazon Web Services для обробки даних.
Інфраструктура як послуга (IaaS)	1. Швидке розгортання 2.Масштабованість 3. Економічність 4. Гнучкість	1. Залежність від постачальника 2. Обмежена кастомізація 3. Безпека даних	Україна PrivatBank – використовує IaaS-інфраструктуру Amazon Web Services для створення хмарної інфраструктури. Ukrtelecom – використовує IaaS-інфраструктуру Microsoft Azure для створення хмарної інфраструктури. Rozetka – використовує IaaS-інфраструктуру Google Cloud Platform для створення хмарної інфраструктури Приклади використання IaaS в інших країнах: Netflix – використовує IaaS-інфраструктуру Amazon Web Services для потокової передачі відео. Uber – використовує IaaS-інфраструктуру Amazon Web Services для обробки даних.

Продовження таблиці 1.1

FaaS (Function as a Service) –модель, в якій серверна інфраструктура, runtime-середовище та операційна система повністю керуються провайдером. Користувачі завантажують свій код у вигляді функцій, які викликані на запит	1. Швидке розгортання та масштабування 2. Плата за використаний ресурс 3. Простота використання	1. Обмежений контроль інфраструктури 2. Залежність від провайдера 3. Підходить не для всіх завдань	AWS Lambda, Azure Functions
CaaS (Container as a Service) –модель, в якій контейнери з додатками та їх залежностями розгортаються та керуються на віртуальних машинах	1. Портативність та масштабованість 2. Легко розгортати нові програми 3. Ефективне використання ресурсів	1. Потрібні знання та досвід роботи з контейнерами 2. Обмежений контроль за інфраструктурою	Docker Swarm, Kubernetes, Amazon ECS.
Serverless computing – безсерверна модель обчислень, у якій користувач не керує серверами, а платить лише за час виконання коду	1. Автоматичне масштабування 2. Оплата лише за використані ресурси 3. Швидке розгортання	1. Обмежений контроль за інфраструктурою 2. Підходить не для всіх завдань 3. Залежність від провайдера	AWS Lambda, Azure Functions, Google Cloud Functions.
Hybrid cloud –гібридна хмара поєднує використання локальної інфраструктури і хмарних сервісів	1. Підвищення гнучкості та масштабованості 2. Контроль за конфіденційними даними 3. Оптимізація витрат	1. Складність керування 2. Потрібні знання та досвід роботи з хмарними технологіями	Azure Stack HCI, AWS Outposts, Google Cloud VMware Engine.
Multi-cloud – мультихмарна архітектура використовує кілька хмарних провайдерів для забезпечення redundancia, безпеки та оптимізації витрат	1. Підвищення надійності та доступності 2. Зниження vendor lock-in 3. Доступ до функцій різних провайдерів	1. Складність керування 2. Потрібні знання та досвід роботи з хмарними технологіями	CloudHealth by VMware, Flexera Optima, Apptio Cloudability.

Моделі хмарних обчислень також класифікуються за належністю хмарних центрів даних і типу хмари [6-14] на: приватні, загальнодоступні; гібридні; хмари спільноти.

Приватна хмара цілком належить та контролюється однією компанією чи організацією, що дає змогу їй повністю керувати інфраструктурою і даними. Загальнодоступні хмари керуються третьою стороною та пропонують свої послуги публічно з оплатою за фактом використання. Гібридна хмара поєднує переваги приватних та публічних хмар, даючи можливість запускати певні програми у публічних хмарах, а інші – у приватних. Хмари спільноти об'єднують зусилля організацій (компаній) зі спільними проблемами у загальну хмарну інфраструктуру.

Хмарні обчислення та хмарні сервіси тісно пов'язані один з одним для ведення бізнес-процесів компаній. І якщо хмарні обчислення є модель надання обчислювальних ресурсів на запит через інтернет, то хмарні сервіси, у свою чергу, є додатками та сервісами, доступними через інтернет на основі моделі хмарних обчислень. У роботах [15-20] показано, як із використанням хмарних сервісів (ХС) компанії керують своїми бізнес-процесами, роблячи їх ефективнішими та гнучкішими. У таблиці 1.2 на підставі аналізу літературних джерел узагальнено приклади використання різних хмарних сервісів по галузях.

Приклади, наведені в таблиці 1.2, не охоплюють усі види хмарного програмного забезпечення (далі – ПЗ) і хмарних сервісів, які використовуються в різних галузях, оскільки кожна компанія або організація обирає конкретні види хмарного ПЗ та/або хмарний сервіс залежно від своїх потреб та стратегії розвитку бізнесу.

Таблиця 1.2 – Приклади використання різних хмарних сервісів по галузях (складено автором за матеріалами [10-30])

№	Галузь та джерела, що містять приклади використання	Приклади використання хмарних сервісів
1	Виробництво [19, 20]	Хмарні сервіси використовуються для керування виробничими процесами, запасами та моніторингу обладнання. Різні виробники використовують хмарне ПЗ для керування виробничими лініями та планування виробництва: 1) Siemens Digital Industries Software – компанія надає хмарні рішення для керування виробничими процесами та моніторингу обладнання. Їхнє хмарне ПЗ включає Siemens Opcenter, що забезпечує цифрове керування виробничими операціями і планування виробництва. 2) SAP. Хмарне програмне забезпечення SAP S/4HANA дозволяє компаніям оптимізувати виробничі процеси та ефективно керувати запасами. 3) Oracle Cloud. Хмарне програмне забезпечення Oracle Manufacturing Cloud дозволяє компаніям керувати виробничими операціями та оптимізувати виробничі процеси. 4) Microsoft Azure. Хмарне програмне забезпечення Azure IoT Suite дозволяє компаніям моніторити та керувати обладнанням, що допомагає оптимізувати виробничі процеси.
2	Банківська сфера [21-23]	Банки використовують хмарні сервіси для обробки платежів, керування клієнтськими даними та надання онлайн-банкінгу. Крім того, банки використовують хмарне сховище даних для зберігання та аналізу клієнтської інформації: 1) Capital One – банк використовує хмарні сервіси від Amazon Web Services (AWS) для обробки платежів, аналізу даних та надання онлайн-банкінгу. Як зазначено в [21-23], AWS надає високонадійні та масштабовані хмарні рішення, що дозволяють Capital One забезпечувати своїм клієнтам високоякісне обслуговування. 2) HSBC – банк використовує хмарні сервіси від Microsoft Azure для керування клієнтськими даними та надання онлайн-банкінгу. Azure надає широкий спектр послуг, включаючи зберігання даних, аналітику та безпеку, що дозволяє HSBC ефективно керувати своїми бізнес-процесами. 3) BBVA – банк використовує хмарні сервіси від Google Cloud Platform (GCP) для обробки платежів та керування клієнтськими даними.
3	Охорона здоров'я [24-26]	Хмарні сервіси використовуються для зберігання та обміну медичною інформацією, керування даними пацієнтів, а також для телемедицини: 1) Cerner Corporation – компанія надає хмарні сервіси для керування електронними медичними записами (EMP), планування лікування та керування медичними ресурсами. Їхнє хмарне програмне забезпечення Cerner Millennium дозволяє медичним закладам ефективно керувати медичною інформацією та забезпечувати якісне обслуговування пацієнтів. 2) Epic Systems Corporation – надає хмарні сервіси для керування EMP, планування лікування та спільної роботи медичного персоналу.

Продовження таблиці 1.2

4	Освіта [27, 28]	Хмарні сервіси використовуються для керування навчальними матеріалами, дистанційного навчання та спільної роботи студентів і викладачів. Багато університетів застосовують хмарні програми для керування навчальними планами та онлайн-курсами: 1) Google Workspace for Education – це хмарне рішення від Google, яке надає закладам освіти доступ до хмарних програм для створення документів, презентацій, електронних таблиць та спільної роботи. Google Workspace for Education дозволяє учням і викладачам обмінюватися інформацією та працювати над проєктами в режимі реального часу. 2) Microsoft Education – Microsoft надає хмарні сервіси для освітніх закладів, такі як Office 365 Education, що включає хмарні версії додатків Word, Excel, PowerPoint та інших. Ці ХС дозволяють студентам та викладачам створювати і редагувати документи, презентації та електронні таблиці онлайн. 3) Canvas – це хмарне освітнє ПЗ, яке надає навчальним закладам широкі можливості створювати і керувати онлайн-курсами, оцінювати студентів та взаємодіяти з ними.
5	Торгівля [29, 30]	Хмарні сервіси можна використовувати для керування складом, замовленнями та взаємодії з клієнтами: 1) Amazon Web Services (AWS) – AWS надає хмарні сервіси для роздрібних і оптових компаній, включаючи зберігання даних, аналітику та масштабованість. Компанії використовують AWS для керування онлайн-магазинами, обробки платежів та аналізу продажів. 2) Salesforce Commerce Cloud – це хмарне рішення від Salesforce, яке надає можливості для керування онлайн-торгівлею, клієнтськими відносинами та аналітики продажів. Компанії використовують Salesforce Commerce Cloud для створення персональних клієнтських інтерфейсів та оптимізації продажів. 3) Shopify – це хмарне рішення для створення та керування онлайн-магазинами. 4) Magento Commerce – це хмарне рішення для створення та керування онлайн-магазинами. Magento Commerce надає клієнтам можливості для керування складськими запасами, обробки замовлень та аналітики продажів, що допомагає компаніям оптимізувати свою торгівельну діяльність.
6	Перевезення та логістика [31-33]	Хмарні сервіси використовують для відстеження вантажів, маршрутизації транспорту та керування логістичними процесами: 1) UPS – компанія використовує хмарні сервіси для керування своїми вантажоперевезеннями та логістичними процесами, а хмарне ПЗ для відстеження вантажів, оптимізації маршрутів та керування складськими запасами. 2) Maersk – компанія використовує хмарні сервіси для керування морськими перевезеннями, хмарне ПЗ для відстеження контейнерів, планування маршрутів та керування портовими операціями. 3) FedEx – компанія використовує хмарні сервіси для керування авіаперевезеннями та логістичними процесами, а хмарне ПЗ для відстеження вантажів, оптимізації маршрутів і керування складськими запасами.

Продовження таблиці 1.2

7	Туризм та готельний бізнес [34, 35]	Хмарні сервіси використовуються для керування бронюванням, готельними послугами та відстеження замовлень: 1) Booking.com – одна з найбільших онлайн-платформ для бронювання готелів та житла. Booking.com використовує хмарні сервіси для керування бронюванням, відстеження замовлень та аналізу клієнтських відгуків. 2) Airbnb – платформа для бронювання житла у місцевих жителів. Airbnb використовує хмарні сервіси для керування бронюванням, платежами та забезпечення безпеки клієнтів. 3) Expedia Group – компанія, що володіє декількома онлайн-туристичними агентствами. Expedia Group використовує хмарні сервіси для керування бронюванням, маркетингу та аналітики. 4) Hotelogix – хмарне ПЗ для керування готельним бізнесом. Hotelogix надає можливості для керування бронюванням, обліку клієнтів, маркетингу та аналітики для готелів. 5) Rezdy – хмарне ПЗ для керування туроператорським бізнесом. Rezdy надає інструменти туроператорам і агентствам для керування турами, бронюванням та для звітності.
8	Телекомунікації [36, 37]	Хмарні сервіси допомагають керувати мережевою інфраструктурою, надавати послуги зв'язку та керувати даними: 1) Google Cloud Platform (GCP) – Google надає хмарні сервіси для телекомунікаційних компаній, включаючи зберігання даних, обробку даних та надання послуг зв'язку. 2) Amazon Web Services (AWS) – AWS надає хмарні сервіси для телекомунікаційних компаній, включаючи керування мережевою інфраструктурою, надання послуг зв'язку та аналітику даних. 3) Microsoft Azure – Microsoft надає хмарні сервіси для телекомунікаційних компаній, включаючи керування мережевою інфраструктурою, надання послуг зв'язку та обробку даних. 4) Twilio – хмарні сервіси для розробки та надання послуг зв'язку. Twilio надає API для надсилання повідомлень, дзвінків та інших комунікаційних послуг.
9	Енергетика [38-41]	Хмарні сервіси використовуються для керування енергетичними процесами, моніторингу ресурсів та оптимізації енергоспоживання: 1) General Electric (GE) – використовує хмарні сервіси для керування енергетичними процесами, включаючи моніторинг роботи обладнання, запобігання відмовам та оптимізацію роботи систем. 2) Schneider Electric – компанія використовує хмарні сервіси для керування системами енергозбереження, моніторингу ресурсів та оптимізації енергоспоживання. 3) Тощо.

Продовження таблиці 1.2

10	Дослідження та розробки [42-46]	Хмарні сервіси допомагають вченим та інженерам керувати даними, моделювати процеси і спільно працювати над різними проєктами. Приклади: 1) NASA – використовує хмарні сервіси для обробки та аналізу величезних обсягів даних, отриманих від космічних досліджень, а також для моделювання космічних процесів. 2) Європейська організація з ядерних досліджень (CERN) – використовує хмарні сервіси для обробки даних з великих адронних колайдерів та інших експериментальних установок. 3) IBM Research – використовує хмарні сервіси для розробки і тестування нових технологій, а також для спільної роботи над проєктами із вченими з усього світу. 4) MIT Media Lab – використовує хмарні сервіси для дослідження та розробки нових медіатехнологій, а також для створення прототипів і тестування концепцій. 5) OpenAI – використовує хмарні сервіси для обробки та аналізу даних, створення і навчання штучних інтелектів та проведення досліджень у галузі машинного навчання.

Проте зауважимо, що забезпечення ІБ хмарних сервісів є одним із ключових питань для будь-якої компанії чи організації, що задіяла ці сервіси до своїх бізнес-процесів. Загальні завдання в цій галузі містять [47-50]: 1) захист даних; 2) автентифікацію та керування доступом; 3) моніторинг та виявлення інцидентів; 4) дотримання вимог кібербезпеки (GDPR, HIPAA, PCI DSS та інших стандартів); 5) забезпечення безпеки під час міграції даних.

Проте є й відмінності у підходах до забезпечення ІБ хмарних сервісів, що обумовлено специфікою конкретного бізнесу, використаними технологіями і рівнем чутливості даних. Так, у фінансовій галузі основна увага приділяється захисту фінансових транзакцій, особистих даних клієнтів та дотриманню регуляторних вимог. В охороні здоров'я вимоги до безпеки даних дуже високі через конфіденційність медичної інформації. У сфері торгівлі потрібно забезпечити ІБ платіжних даних клієнтів та захист від шахрайства. В освіті основна увага приділяється захисту особистих даних учнів та забезпеченню доступу до освітніх ресурсів. У сфері туризму і готельного бізнесу необхідно забезпечити захист даних клієнтів та запобігти витоку інформації про бронювання. Кожна галузь має свої унікальні аспекти у

забезпеченні ІБ хмарних сервісів, але загалом завдання пов'язані із захистом даних, керуванням доступом та дотриманням вимог безпеки. У світі, охопленому процесами глобалізації та цифрової трансформації, забезпечення ІБ хмарних сервісів стає стрижневим фактором успіху для компаній. Бізнес-процеси стають все більш інтегрованими та залежними від ІТ, що відкриває нові можливості для зростання та розвитку, але водночас збільшує вразливість до кіберзагроз та кібератак. Використання хмарних сервісів допомагає компаніям поліпшити гнучкість, масштабованість та ефективність своїх бізнес-процесів, але водночас вони стикаються з низкою нових викликів у галузі ІБ. Глобалізація бізнесу вимагає доступу до даних та ресурсів з різних точок світу, що збільшує поверхню атаки і необхідність забезпечення захисту на всіх рівнях. Розширення масштабів інтеграції хмарних сервісів у бізнес-процеси компаній збільшує релевантність завдань забезпечення безпеки даних та додатків. Компанії мають бути готові до загроз як ззовні, так і зсередини, та забезпечити надійний захист своїх інформаційних ресурсів від витоків, крадіжки чи пошкодження. Слід розуміти, що компрометація безпеки хмарних сервісів може мати серйозні наслідки не тільки для компанії, але й для її клієнтів та партнерів. Тому забезпечення ІБ хмарних сервісів є пріоритетним аспектом успішного ведення бізнесу в умовах цифровізації. Тому в наступному параграфі дисертації ми детальніше зупинимося на аналізі попередніх досліджень з проблематики забезпечення ІБ хмарних інфраструктур.

У межах поточного параграфа дисертації отримано такі результати і зроблено такі висновки: показано, що хмарні обчислення відіграють вирішальну роль у бізнесі, надаючи компаніям можливість оперативно реагувати на зміни ринку та ефективно керувати своїми бізнес-процесами; встановлено, що у різних галузях хмарні сервіси знайшли застосування для оптимізації виробничих процесів, керування фінансами, обробки медичних даних, організації освітнього процесу, автоматизації торгівлі, оптимізації логістики тощо; показано, що застосування хмарних обчислень веде до

підвищення ефективності бізнесу за рахунок зменшення витрат на IT-інфраструктуру та поліпшення доступу до даних і додатків. Крім того, хмарні сервіси дають змогу компаніям швидко масштабувати свої операції та впроваджувати нові технології; показано, що ІБ хмарних інфраструктур є вирішальним елементом для успішного ведення бізнесу, забезпечуючи захист даних, безперервність бізнес-процесів, відповідність нормативним вимогам та довіру клієнтів; показано, що проблематика ІБ хмарних сервісів притаманна всім вендорам через загальні вразливості, загрози та специфіки цієї технології і навіть вимоги клієнтів до високого рівня захисту даних.

Аналіз попередніх наукових публікацій є необхідним етапом у проведенні будь-якого дослідження із забезпечення безпеки хмарних обчислень та хмарних сервісів, оскільки він дає змогу оцінити поточний стан проблематики, виявити прогалини і невирішені проблеми, а також використовувати результати попередніх досліджень як основу для розробки нових методологій та підходів. Крім того, аналіз попередніх робіт дасть можливість виявити основні тренди, напрямки та методи, що використовуються в галузі забезпечення безпеки хмарних сервісів.

1.2. Огляд та аналіз досліджень проблематики забезпечення інформаційної безпеки хмарних інфраструктур

Хмарні обчислення з'явилися відносно не так давно як нова структура для спрощення та надання послуг через Інтернет [51]. Організація хмарних обчислень включає в себе розміщення одного або декількох центрів обробки даних (ЦОД), взаємопов'язаних між собою. Ця система спроєктована таким чином, що для користувача немає різниці між фізичними компонентами системи та їх віртуальними уявленнями. Завдяки цьому користувач хмарних обчислень може взаємодіяти з обчислювальними ресурсами, не турбуючись про технічні деталі та організацію процесу, оскільки ці завдання повністю покладаються на оператора хмарного сервісу. Фінансові обмеження, пов'язані з оптимізацією витрат приватних та державних структур (у загальному випадку об'єктів інформаційної діяльності – ОІД), а також зростаючі потреби

в обчислювальних ресурсах вимагали збільшення обсягів сховищ даних із паралельним збільшенням потреб в аналізі. Ці та інші чинники посприяли розширенню попиту на різні хмарні моделі [52, 53].

Однак, як показано в роботах [54, 55], хмарні обчислення та хмарні сервіси мають низку проблем із забезпеченням ІБ. Зауважимо, що з погляду забезпечення ІБ є відмінності між забезпеченням ІБ хмарних обчислень та хмарних сервісів. Ці відмінності можна звести до таких пунктів:

рівень контролю ІБ для хмарних обчислень та хмарних сервісів. У хмарних обчисленнях клієнти мають великий контроль за безпекою своїх даних і додатків, тоді як у хмарних сервісах більше контролю за безпекою має провайдер. У хмарних сервісах клієнт може мати досить обмежені можливості для налаштування та керування політиками безпеки;

поверхневість атак для хмарних обчислень та хмарних сервісів. Клієнтська інфраструктура і програми хмарних обчислень є вразливими перед атаками. Водночас для хмарних сервісів поверхневість атаки, як правило, набагато менша, оскільки провайдер відповідає за ІБ своєї інфраструктури;

відповідність хмарних обчислень та хмарних сервісів. Клієнти хмарних обчислень безпосередньо повинні відповідати вимогам безпеки, однак у хмарних сервісах тільки провайдер несе відповідальність за дотримання вимог ІБ.

Отже, хмарні обчислення та хмарні сервіси мають дещо відмінні моделі безпеки. Вибір конкретної моделі залежатиме від потреб клієнта, його технічної експертизи та вимог безпеки, як це показано в таблиці 1.2. Усе сказане вище і мотивувало виконати аналіз наукових публікацій, присвячених виключно проблематиці забезпечення ІБ хмарних обчислень та хмарних сервісів.

У [56] автори розглянули загальний алгоритм вирішення проблем безпеки підвищення продуктивності хмарної системи. Автори використовували штучні нейронні мережі (ШНМ) для аналізу захищеності хмарного середовища.

У [57] розглядається організація системи безпеки хмарних обчислень, заснована на довірі, у хмарних моделях. Тобто провайдер забезпечує надійність, безпеку та конфіденційність даних у хмарній системі. Авторами запропоновано модель керування доступом на основі довіри як ефективний метод забезпечення ІБ у розподілених обчислювальних інфраструктурах. Як клієнтські, так і хмарні активи клієнтів у хмарній системі в цьому дослідженні оцінюються з урахуванням аналізу їх довіри.

У [58] аналізуються моделі забезпечення ІБ хмарної інфраструктури. Автори розглянули відмітні проблеми ІБ розподілених обчислень, що виникають у результаті використання об'єктами інформаційної діяльності різних моделей хмарних обчислень. Як показано у роботі, приватні хмари зазвичай використовуються організаціями для своїх внутрішніх потреб. Вони вимагають суворого контролю доступу та керування. Публічні хмари надаються сторонніми провайдерами і є менш прозорими щодо безпеки. У публічних хмарах ресурси розділяють між різними клієнтами. Це потребує додаткових заходів безпеки.

У [59] автори проаналізували моделі машинного навчання для підвищення безпеки даних у хмарних системах. Концепція забезпечення ІБ розподілених обчислень обговорюється науковцями в завданні віртуалізації серверних ферм як практичного середовища розгортання бізнес-додатків. На думку авторів, віртуалізація серверних ферм допомагає забезпечити безпеку хмарних обчислень шляхом ізоляції, оскільки віртуальні сервери у фермі ізольовані один від одного, запобігаючи несанкціонованому доступу (НСД). Крім того, ферма може масштабуватись залежно від навантаження, забезпечуючи гнучкість та ефективність. Віртуальні сервери мають різні рівні доступу, що сприяє безпеці.

У [60] автори наводять модель класифікації загроз для хмарних обчислень. Особливість класифікації полягає в тому, що її засновано на можливості алгоритмів машинного навчання для виявлення та вирішення проблем безпеки. Крім того, авторами пропонується модель угруповання

ризиків для хмарних обчислень. Модель ґрунтується на алгоритмах машинного навчання.

Аналогічні дослідження проведені в роботі [61]. Дослідження присвячене аналізу наявних підходів, вкладених у забезпечення ІБ хмарних сервісів. З огляду на те, що хмарні обчислення є однією з найбільш зростаючих галузей у сфері інформаційних технологій, забезпечення безпеки та надійності процесів, що відбуваються у хмарах, а також захист механізмів взаємодії між клієнтами і постачальниками хмарних сервісів становлять релевантне наукове та прикладне завдання. Побоювання щодо втрати даних та їх компрометації стоять біля витоків небажання деяких компаній переміщати свої обчислення до хмар. Автор аналізує різноманітність хмарних сервісів, що надаються різними провайдерами, та порівнює існуючі підходи до забезпечення ІБ у цій сфері. Крім того, пропонується новий підхід, що базується на принципі диверсифікації. На думку автора, застосування диверсифікації необхідне для забезпечення надійності та безпеки компонентів хмарних систем. Цей принцип полягає у використанні унікальної версії кожного ресурсу завдяки окремій комбінації провайдерів хмарних обчислень, географічного розміщення центрів обробки даних, моделей надання хмарних сервісів та моделей розгортання хмарної інфраструктури.

У [62] досліджуються алгоритми машинного навчання, які використовують для усунення загроз ІБ, пов'язаних з поширенням шкідливого ПЗ у хмарних системах. Авторами запропоновано бар'єрну структуру, яка використовує три алгоритми машинного навчання та призначена для виявлення шкідливого ПЗ.

Як показано в [63, 64], хмарні обчислення мають значний потенціал для зростання і стають все більш популярними. Однак, незважаючи на свої унікальні характеристики, хмарні обчислення пов'язані з різними загрозами безпеці. Категоризація загроз виконана багатьма авторами, як-от у роботах [61, 63, 64].

Загрози конфіденційності містять внутрішні загрози для клієнтської інформації, а також ризики зовнішніх атак [65]. У [65] показано, по-перше, що внутрішні ризики для клієнтської інформації пов'язані з несанкціонованим або незаконним доступом до інформації про клієнта з боку інсайдера – постачальника хмарних послуг. Це серйозна проблема безпеки [63]. По-друге, ризик зовнішніх атак стає дедалі актуальнішим для хмарних обчислень. Цей ризик включає віддалені програмні або апаратні атаки, спрямовані на клієнтів та хмарні програми [66]. По-третє, витік інформації –це необмежений ризик для хмарних даних через навмисні та/або ненавмисні людські помилки.

Загрози цілісності інформації з організацією хмарних обчислень розглянуті у роботах [67, 68]. По-перше, це ризик ізолювання інформації, яка неточно поєднує значення параметрів безпеки, необачне проєктування віртуальних машин (ВМ) та зовнішні клієнтські гіпервізори. По-друге, це погане керування доступом клієнтів. Внаслідок неефективного контролю доступу можна зіткнутися з різними проблемами та загрозами ІБ, що дасть можливість потенційним зловмисникам завдати шкоди інформаційним активам, розміщеним у хмарі [69, 70].

Як показано в [71, 72], загрози доступності містять, наприклад, фізичне переривання роботи хмарних обчислень та/або хмарних сервісів, а також пов'язані з неефективними стратегіями відновлення після атак на хмарні системи. У роботах [73, 74, 75, 76, 77, 78] аналізуються різні види атак на хмарні системи. У [73] обговорюються сценарії мережних атак. Як зазначають автори, сканування портів становить для хакерів значний інтерес, оскільки дає інформацію про запуск успішної атаки [73]. У [73] також розглянуті особливості організації атак на основі ВМ. У роботі показано, що різні ВМ, які використовуються на хмарних платформах, викликати різні проблеми з ІБ. Наприклад, у разі, коли шкідливий код, розміщений в середині образу ВМ, буде реплікований під час створення ВМ. Також у [73] аналізуються атаки з урахуванням додатків, які у хмарі. Такі атаки вплинути на продуктивність хмарних додатків та викликати витік інформації зі зловмисною метою.

У [78] розглянуто спуфінг-атаки, у яких хакер чи шкідливе ПЗ діють від імені іншого користувача (чи системи), видаючи себе за дані.

Як самостійний напрямок досліджень із проблематики ІБ хмарних інфраструктур можна вважати роботи, пов'язані із застосуванням методів машинного навчання для забезпечення ІБ хмарних обчислень. Згідно з [79], машинне навчання – це логічна перевірка розрахунків та вимірних моделей, які комп'ютерні системи використовують для реалізації конкретного завдання.

З погляду ІБ методи машинного навчання [80] настільки значущі у хмарі, що в найближчому майбутньому їх використовуватиме кожна хмарна система.

Зі збільшенням попиту на хмарні обчислення та зростанням навантаження на систему, а також обсягу трафіку стає необхідним активне моніторингове втручання в роботу ЦОД. Це дає змогу забезпечити безперебійну роботу інфраструктури, оскільки оперативне реагування на загрози ІБ та несправності сприяє стабільності й безпеці системи. Моніторинг, включаючи відстеження стану компонентів та керування хмарною інфраструктурою, відіграє головну роль у забезпеченні високого рівня послуг, оптимізації розподілу ресурсів і забезпеченні надійності та ІБ. Це однаково необхідно як для клієнтів, так і для провайдерів хмарних послуг. Моніторинг хмарного середовища містить кілька підтипів, кожен з яких виконує свої функції [73]. Зокрема, моніторинг ІБ – виявлення потенційно небезпечних алгоритмів та запобігання порушенням безпеки хмарних систем.

Для ефективної побудови системи моніторингу необхідно розробити математичну модель, що ґрунтується на оцінці параметрів системи в різних станах та часі, а також на основі застосування методів машинного навчання. Такий підхід дасть змогу створити формальний апарат із вхідними, проміжними та вихідними станами, що сприятиме забезпеченню ІБ як хмарним обчисленням загалом, так і хмарним сервісом.

У роботах [81, 82, 83] розглянуто інстанси хмарної інфраструктури у завданні забезпечення ІБ хмарних обчислень. Інстанси є віртуальними або фізичними обчислювальними ресурсами, що надаються хмарним провайдером

для виконання різних завдань і додатків. Ці ресурси включають ВМ, контейнери, сервери, бази даних (БД) та інші обчислювальні ресурси, які масштабовані та налаштовані відповідно до потреб клієнта. На думку авторів [82], інстанси (ВМ або контейнер) хмарної інфраструктури відіграють велику роль у забезпеченні ІБ хмарних послуг (див. рис. 1.1).

По-перше, провайдери часто використовують віртуалізацію для створення та керування інстансами хмарної інфраструктури. Це дає можливість забезпечити ізоляцію та сегментацію ресурсів між різними клієнтами, що допомагає запобігти НСД до даних та додатків. По-друге, інстанси хмарної інфраструктури використовують для виявлення аномалій, потенційних загроз та несанкціонованих дій. Це дає змогу операторам хмарних сервісів оперативно реагувати на можливі інциденти безпеки та запобігати їм. По-третє, використання інстансів хмарної інфраструктури також дає можливість налаштовувати права доступу та політики ІБ для різних користувачів і програм. Це забезпечує контроль за доступом до даних та ресурсів і допомагає запобігти НСД. По-четверте, інстанси налаштовують за допомогою спеціалізованих засобів захисту від DDoS-атак, що допомагає забезпечити безперервність роботи сервісів навіть при масованих мережних атаках.

На рис. 1.1 схематично показано взаємодію хмарної інфраструктури та інстансів у системі виявлення аномалій ІБ на основі застосування методів МН. Така взаємодія може бути реалізована у кілька етапів.

Етап 1. Збір даних.

Хмарна інфраструктура надає середовище для розгортання інстансів, які використовують для виконання різних завдань та програм. У процесі роботи інстанси генерують дані про поведінку, такі як використання ресурсів, мережний трафік, журнали подій тощо.

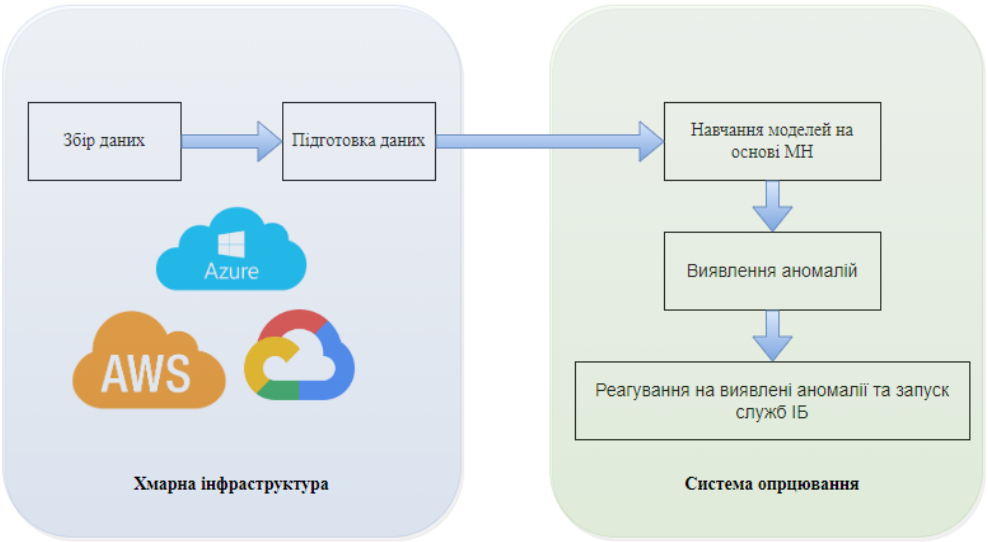


Рис. 1.1 – Схема взаємодії хмарної інфраструктури та інстансів у системі виявлення аномалій ІБ на основі застосування методів МН (Схемка скаладена автором)

Етап 2. Підготовка даних.

Дані, зібрані з інстансів, обробляються та готуються до аналізу. Це може включати очистку даних, масштабування, перетворення форматів і т.д.

Етап 3. Навчання моделей з урахуванням МН.

На основі підготовлених даних будуються моделі МН виявлення аномалій. Ці моделі містять алгоритми класифікації, кластеризації, дерева рішень та інші, здатні виявляти незвичайні або підозрілі патерни в даних.

Етап 4. Виявлення аномалій.

Навчені моделі застосовуються до нових даних, що надходять від інстансів хмарних обчислень, виявлення аномалій. Це може містити аналіз аномальних шаблонів використання ресурсів, незвичайних мережних пакетів, незапланованих подій у журналах та інших незвичайних сценаріїв.

Етап 5. Реагування на виявлені аномалії.

Після виявлення аномалій система ІБ може вживати різних заходів реагування, таких як надсилання повідомлень адміністраторам, блокування доступу до ресурсів, запуск додаткових заходів безпеки тощо.

У даній структурній схемі взаємодію між хмарною інфраструктурою та інстансами в системі виявлення аномалій ІБ засновано на зборі та аналізі даних від інстансів з подальшим навчанням моделей МН для виявлення аномалій та вжиття відповідних заходів щодо забезпечення ІБ. Інстанси хмарної інфраструктури відіграють головну роль в ІБ хмарних сервісів, забезпечуючи ізоляцію, моніторинг, керування доступом та захист від мережних атак. Використання методів МН для виявлення аномалій в інстансах хмарної інфраструктури може бути ефективним способом виявлення незвичайних або шкідливих дій, які загрожують безпеці системи. Однак зазначимо, що для ІБ хмарних сервісів у такій схемі мають деякі відмінності. Це пов'язано з такими чинниками:

Рівень абстракції. Хмарні послуги надають більш абстрактний рівень доступу до обчислювальних ресурсів, ніж просто хмарна інфраструктура. Користувачі хмарних сервісів часто мають справу з більш високорівневими сервісами, такими як платформи як сервіс (PaaS) та програмне забезпечення як сервіс (SaaS). Це може вплинути на способи збирання та аналізу даних для виявлення аномалій, оскільки доступ до низькорівневих деталей інфраструктури може бути обмежений.

Типи даних. У хмарних сервісів генеруються різні типи даних, наприклад, дані про взаємодію користувачів з додатками або обробку транзакцій. Відповідно методи виявлення аномалій спрямовані на аналіз цих специфічних типів даних.

Інтеграція з API. Багато хмарних сервісів надають API для взаємодії з ними. Використання таких API може полегшити збирання даних для виявлення аномалій та інтеграцію із системами ІБ.

Керування доступом та ІБ. Багато хмарних сервісів мають власні механізми керування доступом і заходи безпеки, які впливають на способи виявлення аномалій. Наявність механізмів автентифікації та авторизації сприяє ідентифікації підозрілих активностей.

Відповідно, взаємодія з хмарними сервісами може потребувати врахування специфічних особливостей цих сервісів та адаптації методів виявлення аномалій відповідно до їх характеристик.

Як показано в [83, 84, 85, 86, 87], методи МН, такі як алгоритми кластеризації або методи спостереження без вчителя (метод головних компонентів), використовують для аналізу поведінки інстансів хмарної інфраструктури та виявлення аномалій. Якщо виявляється незвичайна активність у використанні ресурсів або мережному трафіку, це може вказувати на можливу атаку або порушення ІБ.

Відповідно до [84], методи МН використовують для аналізу системних параметрів інстансів хмарної інфраструктури, таких як завантаження процесора, використання пам'яті, дискова активність і т. д. Аномалії в цих параметрах вказують на проблеми з продуктивністю або наявність шкідливого ПЗ.

У [85] наголошується, що методи навчання з учителем застосовують для аналізу журналів подій (логів) інстансів хмарної інфраструктури з метою виявлення аномальних чи підозрілих дій. Можна навчити модель класифікації з урахуванням ретроспективних даних про події визначення, які події є нормальними, які аномальними.

Методи МН застосовують для аналізу мережного трафіку інстансів хмарної інфраструктури з метою виявлення аномалій або атак. Можна використовувати алгоритми виявлення викидів для виявлення незвичайної мережної поведінки, яка може вказувати на атаку або наявність шкідливого ПЗ [86, 87].

Як показав аналіз попередніх досліджень, у зв'язку з міграцією все більшого обсягу даних та додатків у хмарні сервіси ІБ стикається з низкою нових та унікальних викликів. Таблиця 1.3 містить систематизований огляд основних загроз, із якими зіткнулися організації під час використання хмарних сервісів.

Таблиця 1.3 – Систематизований огляд основних загроз, з якими зіткнулися організації під час використання хмарних сервісів (складено автором за результатами аналізу літературних джерел, наведених у цьому дослідженні)

Загроза для ІБ хмарного сервісу	Пріоритетні заходи щодо нівелювання загрози
1	2
Недостатній контроль над обліковими записами, правами, доступом та паролями у хмарних сервісах	Дискретна ізоляція користувачів та додатків. Ефективні інструменти керування правами доступу. Багатофакторна автентифікація (MFA). Керування доступом на основі ролей (RBAC). Авдит доступу та моніторинг з метою виявлення підозрілих активностей та НСД чи спроби вторгнення.
Інтерфейси та API з недостатнім захистом	Проведення регулярного авдиту та оцінки безпеки інтерфейсів і API допоможе виявити потенційні вразливості та недоліки в їх реалізації. Використання стандартів безпеки, таких як OAuth, OpenID Connect, SSL/TLS, а також відповідність принципам RESTful API допомагає забезпечити захист під час роботи з інтерфейсами та API хмарних сервісів. Реалізація суворої системи авторизації для доступу до API допоможе запобігти НСД до хмарного сервісу та захистить дані від витоків.
Некоректна конфігурація та недостатнє керування змінами у хмарному сервісі	Використання засобів автоматизації для налаштування та керування конфігурацією хмарними сервісами допоможе запобігти людським помилкам і забезпечити стандартизацію налаштувань ІБ. Проведення регулярних авдитів конфігурації хмарного сервісу допоможе виявляти та виправляти потенційні вразливості та помилки конфігурації. Впровадження систем моніторингу змін дасть змогу відстежувати й аналізувати всі зміни, які вносяться до хмарного сервісу, що сприятиме оперативному виявленню несанкціонованих дій та запобігатиме загрозам ІБ хмарного сервісу. Розробка та впровадження суворих політик ІБ, включаючи правила конфігурації та процедури керування змінами, допоможе мінімізувати ризики неправильної конфігурації та несанкціонованих змін.
Проблеми безпеки, пов'язані з архітектурою хмарних систем	Об'єктам інформаційної діяльності під час розгляду бізнес-цілей, ризиків, загроз ІБ, а також відповідності законодавству в розріхі хмарних сервісів та особливостям їхньої інфраструктури слід врахувати високу динаміку змін та обмежений централізований контроль у хмарних сховищах. Необхідно акцентувати увагу на розвитку й адаптації інфраструктурної стратегії хмарних сервісів. Під час адаптації рішень необхідно враховувати основні практики оцінки ІБ, що надаються вендором.

Продовження таблиці 1.3

1	2
Загрози та ризики, пов'язані з розробкою додатків для хмарних сервісів	Забезпечення навчання і сертифікації розробників з безпечної розробки додатків для хмарних сервісів допоможе підвищити обізнаність з ІБ та знизити ризик помилок у коді. Під час розробки програм для хмарних сервісів слід використовувати перевірені фреймворки та бібліотеки, які мають вбудовані механізми безпеки та пройшли перевірку на вразливості. Проведення статичного та аналізу коду допоможе виявляти потенційні вразливості та помилки у додатках ще на стадії розробки. Налаштування програм з урахуванням принципів захисту за промовчанням, таких як мінімізація привілеїв та обмеження доступу до ресурсів, допоможе знизити поверхню атаки та зменшити ризик компрометації системи.
Загрози та вразливості, що виникають під час роботи з хмарними сервісами, які надаються зовнішніми компаніями	Перед використанням хмарних сервісів необхідно провести ретельний аналіз безпеки постачальника, включаючи його репутацію, стандарти безпеки, сертифікації та рейтинги надійності. Необхідно укласти SLA (Service Level Agreement), в якому мають бути чітко визначені зобов'язання постачальника в галузі безпеки, включаючи процедури реагування на інциденти, резервне копіювання даних та доступ до авдиту. Здійснення регулярного моніторингу та авдиту ІБ дасть можливість виявляти потенційні вразливості та недоліки у безпеці хмарних сервісів, а також контролювати їхню відповідність стандартам безпеки.
Загрози, пов'язані з системними вразливостями у хмарних сервісах	Необхідно регулярно оновлювати і патчити всі компоненти хмарної інфраструктури, включаючи операційні системи, програми та сервіси, щоб виправити відомі вразливості. Проведення регулярного сканування і моніторингу вразливостей у хмарній інфраструктурі допоможе оперативно виявляти та усувати потенційні загрози ІБ. Обмеження доступу та привілеїв до системних ресурсів і даних у хмарних сервісах допоможе знизити ризик експлуатації вразливостей.
Загрози, пов'язані з ненавмисним витоком даних із хмарного сховища	Необхідно провести перевірку баз даних (БД) PaaS, сховищ та БД, розміщених на хостингу, включаючи ВМ, контейнери (інстанси) та встановлене на них програмне забезпечення. Слід вибирати пошукові машини, які повністю інтегровані у хмарне середовище, для того, щоб своєчасно виявити будь-які кореневі або мережні сервіси, що роблять трафік видимим ззовні.
Загрози, пов'язані з некоректною конфігурацією та застосуванням безсерверних і контейнерних рішень	Використання засобів автоматизації конфігурації та деплойменту, таких як Ansible, Terraform або Kubernetes, допоможе запобігти людським помилкам при налаштуванні та розгортанні контейнерів та безсерверних додатків. Впровадження систем моніторингу та авдиту конфігурації дасть можливість своєчасно виявляти і виправляти місконфігурації в реальному часі, а також відстежувати зміни у конфігурації для виявлення потенційних уразливостей в ІБ хмарних сервісів. Також ефективним може бути застосування принципів least privilege, оскільки налаштування прав доступу та привілеїв для контейнерів і безсерверних функцій згідно з принципом «найменших привілеїв» допоможе знизити ризик експлуатації вразливостей.

Продовження таблиці 1.3

1	2
Загрози, пов'язані з діями організованих злочинних груп та/або хакерських угруповань	Встановлення засобів захисту мережі, firewalls, системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS), а також регулярний моніторинг мережного трафіку для виявлення аномальної активності. Впровадження багаторівневої автентифікації та суворого контролю доступу до хмарних ресурсів, включаючи механізми двофакторної автентифікації, обмеження доступу за ролями та привілеями, а також регулярне оновлення паролів. Застосування шифрування даних у спокої та під час їх передачі між клієнтами та хмарними сервісами допоможе захистити конфіденційну інформацію від НСД. Проведення регулярних авдитів ІБ та моніторингу подій для виявлення і реагування на потенційні загрози та інциденти ІБ. Регулярне створення резервних копій даних та розробка планів відновлення після інцидентів допоможе мінімізувати втрату даних у разі атаки або інциденту ІБ.
Загрози, пов'язані з ексфільтрацією даних хмарних сховищ	Налаштування прав доступу до хмарних сховищ відповідно до принципу «необхідності» (least privilege), коли доступ до даних має надаватися тільки необхідним користувачам та групам. Впровадження систем моніторингу активності та виявлення загроз дасть змогу виявляти у хмарних сховищах даних аномальну активність, таку як незвичайні спроби доступу або завантаження великих обсягів даних. Впровадження систем запобігання витоку даних (DLP), які блокують спроби несанкціонованого експорту або завантаження конфіденційної інформації з хмарних сховищ. Проведення навчання і тренінгів для співробітників за правилами безпечного поводження з даними у хмарних сховищах, а також щодо розпізнавання та запобігання соціальній інженерії та фішинговим атакам.

Зауважимо, що розгляд потенційних порушників внутрішніх та зовнішніх для ІБ хмарних сервісів, таких як Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform та IBM Cloud, є необхідним етапом для забезпечення безпеки даних і ресурсів (інформаційних активів) компаній. Внутрішні порушники, такі як співробітники організації (див. таблицю 1.3), можуть завдати шкоди, маючи доступ до конфіденційної інформації. Водночас зовнішні порушники можуть спробувати отримати НСД до даних через вразливість хмарного сервісу. Особливості технологій захисту ХС різних вендорів відіграють вирішальну роль у запобіганні таким загрозам (див. таблицю 1.4).

AWS пропонує широкий спектр інструментів захисту даних, включаючи механізми керування доступом, шифрування даних та моніторинг безпеки. Azure, у свою чергу, забезпечує можливості керування безпекою віртуальних машин і мереж, а також інтеграцію з інструментами моніторингу та авдиту. Google Cloud Platform пропонує засоби для виявлення та запобігання загрозам, такі як захист від DDoS-атак і механізми автентифікації. IBM Cloud надає можливості керування ключами шифрування, контролю доступу та моніторингу активності у хмарі.

Основний висновок, який можна зробити з таблиць 1.3 і 1.4, полягає в тому, що внутрішні порушники, включаючи потенційних інсайдерів, можуть становити більшу небезпеку для організації, ніж зовнішні порушники. Це пов'язано з тим, що внутрішні порушники мають доступ до внутрішніх систем і даних компанії, що робить їх потенційно більш небезпечними та шкідливими. Для захисту від внутрішніх порушників необхідно використовувати безліч програмних та апаратних засобів захисту. Механізми керування доступом можуть обмежувати дії співробітників доступом лише до необхідної інформації та ресурсів. Моніторинг та авдит дій користувачів дають можливість виявляти підозрілу активність і швидко реагувати на загрози.

Отже, необхідно розв'язати завдання ефективного захисту від внутрішніх порушників, адже вони мають легальний доступ до конфіденційної інформації, ніж зовнішні порушники, і можуть завдати серйозної шкоди організації, якщо це вдасться. Тому захист від внутрішніх загроз є одним із першорядних аспектів інформаційної безпеки будь-якої компанії, включаючи ті, що використовують ХС.

Внутрішні порушники в хмарних сервісах можуть мати доступ до даних та ресурсів компанії через хмарну інфраструктуру. Їх потенційна небезпека полягає у можливості НСД до конфіденційної інформації, зміни даних або порушення цілісності системи. Для захисту від внутрішніх порушників хмарними сервісами використовуються ті самі принципи та заходи, що й для захисту від внутрішніх загроз у звичайних системах. Ці заходи містять

керування доступом, моніторинг дій користувачів, навчання персоналу і розробку суворої політики безпеки.

Таблиця 1.4 – Систематизований огляд і аналіз потенційних порушників для інформаційної безпеки хмарних сервісів та специфіка їх захисту (складено автором за результатами аналізу джерел, наведених у даному дослідженні)

<table>
<tr><td colspan="2">Хмарні сервіси Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, IBM Cloud</td></tr>
<tr><td>Внутрішні порушники</td><td>Зовнішні порушники</td></tr>
<tr><td>Несанкціонований доступ до даних. Співробітники можуть отримати доступ до даних, до яких не мають права доступу, використовуючи свої привілеї.

Витік даних. Внутрішні порушники можуть вкрасти конфіденційні дані та передати їх третім особам.

Видалення або зміна даних. Співробітники можуть видаляти або змінювати дані, що може призвести до втрати інформації або порушення цілісності даних.</td><td>Міжмережні атаки. Нападники можуть намагатися проникнути в мережу хмарного провайдера за допомогою різних методів, таких як атаки, переповнення буфера або фішинг.

Відмова в обслуговуванні (DDoS). Атаки DDoS спрямовані на ХС, що може призвести до недоступності сервісів для законних користувачів.

Загрози безпеки програм. Нападники можуть використовувати вразливість у програмах, розгорнутих у хмарі, щоб отримати доступ до даних або контролю над системою.</td></tr>
<tr><td>Резюме. Співробітник адміністрації, який має доступ до керування хмарним сховищем даних, може скопіювати конфіденційні файли та передати їх конкурентам.</td><td>Резюме. Зловмисники можуть запустити DDoS-атаку на веб-додаток, розміщений у хмарі, щоб тимчасово вивести його з ладу та завдати шкоди бізнесу, який використовує цю програму.</td></tr>
<tr><td colspan="2">Особливості захисту Amazon Web Services (AWS)</td></tr>
<tr><td colspan="2">AWS надає:
багаторівневий захист, включаючи захист на рівні центрів обробки даних, мережний захист і захист на рівні додатків;
механізми ідентифікації та автентифікації користувачів і ресурсів, такі як AWS Identity and Access Management (IAM), для керування доступом;
засоби шифрування даних, такі як AWS Key Management Service (KMS) та SSL/TLS;
інструменти для моніторингу та реєстрації дій користувачів і ресурсів, такі як AWS CloudTrail та Amazon CloudWatch;
захист від DDoS-атак за допомогою AWS Shield та AWS WAF (Web Application Firewall).

Приклад. Компанія використовує AWS CloudTrail для моніторингу всіх дій у своєму обліковому записі AWS, щоб виявляти та запобігати будь-яким несанкціонованим діям або доступам.</td></tr>
<tr><td colspan="2">Особливості захисту Microsoft Azure</td></tr>
</table>

Продовження таблиці 1.4

Azure надає: механізми ідентифікації та автентифікації, такі як Azure Active Directory (Azure AD) для контролю доступу до ресурсів; засоби шифрування даних, включаючи Azure Disk Encryption та Azure Storage Service Encryption; засоби захисту мережі, такі як мережні групи безпеки (Network Security Groups) та служба Azure DDoS Protection; інструменти для моніторингу та авдиту дій користувачів і ресурсів, такі як Azure Monitor та Azure Security Center; засоби для виявлення та запобігання шкідливим програмам і загрозам, такі як Azure Advanced Threat Protection та Azure Security Center. Приклад. Компанія використовує Azure Security Center для безперервного моніторингу своїх ресурсів у хмарі Azure та виявлення будь-яких потенційних загроз чи порушень безпеки.
Особливості захисту Google Cloud Platform
Google Cloud Platform надає: засоби для керування доступом, включаючи Identity and Access Management (IAM), що дає змогу обмежувати доступ до ресурсів на основі ролей та повноважень; інструменти для шифрування даних, включаючи Google Cloud Key Management Service (KMS) для керування ключами шифрування; засоби для налаштування мережної безпеки, включаючи віртуальні приватні хмари (Virtual Private Clouds, VPC), мережні групи безпеки (Security Groups) та службу Cloud Armor для захисту від DDoS-атак; інструменти для моніторингу та авдиту використання ресурсів, таких як Cloud Monitoring та Cloud Audit Logging; інструменти для виявлення та запобігання шкідливим програмам і загрозам, включаючи Cloud Security Scanner та Google Cloud Armor. Приміром. Компанія використовує Google Cloud IAM для суворого контролю доступу до своїх ресурсів у хмарі GCP, що дає змогу запобігти несанкціонованому доступу.
Особливості захисту IBM Cloud
BM Cloud надає: можливості керування доступом та автентифікації, дозволяючи адміністраторам визначати права доступу користувачів до ресурсів хмари; засоби шифрування даних, включаючи IBM Key Protect для керування ключами шифрування; мережні політики та правила безпеки для захисту мережного трафіку, включаючи налаштування віртуальних приватних хмар (VPC) та використання IBM Cloud Internet Services для захисту від DDoS-атак; інструменти для моніторингу та авдиту активності у хмарі, такі як IBM Cloud Monitoring та IBM Cloud Activity Tracker; засоби для виявлення та запобігання шкідливим програмам і загрозам, включаючи IBM Cloud Security Advisor та IBM Cloud Security Groups; До прикладу. Компанія використовує IBM Cloud Key Protect для керування ключами шифрування своїх даних у хмарі IBM Cloud, забезпечуючи захист від несанкціонованого доступу до даних.

У роботах, проаналізованих у даному параграфі, переважно обговорюється коло питань, присвячених проблемі комплексного підходу до забезпечення ІБ хмарних інфраструктур. Як показано в більшості робіт, хмарні обчислення стрімко набирають популярності, витісняючи традиційні моделі ведення бізнес-процесів для об'єктів інформатизації. Проте проаналізовані роботи недостатньо охоплюють питання реалізації системи моніторингу розподілу ресурсів. Також виявлено, що значною мірою розглянуті роботи не торкаються такого аспекту забезпечення інформаційної безпеки хмарних інфраструктур, як застосування методів машинного навчання для створення прогнозної моделі завантаження та методики збору метрик ІБ інстансів. Під інстансами йдеться про віртуальні машини (ВМ) у хмарній інфраструктурі та контейнери. Серед основних питань, які потребують вирішення у межах майбутніх досліджень, слід виділити:

- розробку нових моделей, що описують аномальну поведінку інстансів унаслідок порушення політики ІБ;
- розвиток методів МН з учителем для аналізу журналів подій (логів) інстансів хмарної інфраструктури з метою виявлення аномальних чи підозрілих дій.

У параграфі отримані такі результати:

- показано, що хмарні обчислення забезпечують доступ до мережних ресурсів, таких як сховища даних та обчислювальні потужності, на запит, без прямого керування з боку користувачів. На сьогодні хмарні обчислення містять як публічні, так і приватні центри обробки даних (ЦОД), що надають клієнтам єдину платформу через інтернет. Мобільні хмарні обчислення використовують розподілені обчислення для передачі додатків на мобільні пристрої, такі як телефони та планшети;
- встановлено, що численні дослідження вказують на проблеми інформаційної безпеки, загрози та вразливості для клієнтів, з якими стикаються хмарні обчислення та мобільні хмарні обчислення. Одним із

перспективних методів боротьби з цими загрозами є використання методів машинного навчання;

- проведено аналіз загроз та проблем з ІБ хмарних структур, а також огляд рішень, запропонованих різними авторами, щодо забезпечення безпеки хмарних обчислень та хмарних сервісів. Насамперед, розглянуто дослідження, що ґрунтуються на застосуванні алгоритмів машинного навчання для забезпечення безпеки хмарних обчислень та хмарних сервісів.

У наступному параграфі роботи ми більш детально зупинимося на аналізі методів машинного навчання, які дають можливість створювати ефективні рішення щодо безпеки хмарних сервісів, без прив'язки до особливостей конкретного вендора.

1.3. Аналіз методів машинного навчання, які потенційно можна використовувати для забезпечення безпеки хмарних сервісів

Як зазначено вище, використання методів машинного навчання у забезпеченні ІБ (кібербезпеки) хмарних сервісів дає змогу ефективно захищати дані та інфраструктуру від загроз. Насамперед, машинне навчання дає можливість виявляти нестандартні та підозрілі активності у хмарних середовищах, що вказує на потенційні загрози ІБ. Наприклад, атаки, аномалії в мережному трафіку, незвичайні спроби доступу та інші незвичайні події, які залишаються непоміченими під час використання традиційних методів виявлення загроз. Хмарні послуги генерують безліч даних, які потрібно аналізувати, виявляти загрози та аномалії. Машинне навчання здатне ефективно обробляти й аналізувати великі обсяги даних для виявлення патернів та аномалій, що робить його ефективним інструментом боротьби з кіберзагрозами у хмарних середовищах. Як показав аналіз попередніх досліджень, системи ІБ, що включають в алгоритми своєї роботи методи машинного навчання, здатні адаптуватися до нових загроз і умов середовища, що змінюються. Оскільки моделі МН навчадися на основі нових даних і досвіду, це дає їм можливість швидко адаптуватися до нових загроз та

запобігати їм. Також методи машинного навчання дають змогу автоматизувати процеси виявлення загроз, аналізу даних та реагування на інциденти безпеки, що відповідно підвищує ефективність і швидкість реакції на загрози, знижуючи ризик для організації, яка використовує хмарні послуги у своїх бізнес-процесах. Машинне навчання дає можливість будувати прогнози й моделі для запобігання загрозам та інцидентам безпеки до їх виникнення. Це допоможе організаціям бути проактивнішими у забезпеченні кібербезпеки хмарних сервісів.

Виходячи з вищесказаного, проведено порівняльний аналіз переваг та недоліків різних методів машинного навчання, які потенційно можна використовувати в системах ІБ хмарних сервісів. Результати цього порівняльного аналізу узагальнені в таблиці 1.5.

Розглянемо кожен із методів МН більш детально.

Алгоритми класифікації хмарних сервісів Amazon Web Services (AWS) або інших, використовують для виявлення аномалій у мережному трафіку чи поведінці користувачів. Подібні алгоритми автоматично класифікують мережний трафік на нормальний та потенційно шкідливий, ідентифікують атаки чи незвичайні спроби доступу.

Таблиця 1.5 – Узагальнені результати порівняльного аналізу переваг та недоліків різних методів машинного навчання, які потенційно можна використовувати у системах ІБ хмарних сервісів (Складено автором)

Метод	Переваги	Недоліки
Алгоритми класифікації	1. Бистрота обробки даних. 2. Здатність виявляти шаблони у поведінці користувачів та мережному трафіку.	Необхідність у великому обсязі розмічених даних на навчання моделей.
Алгоритми кластеризації	Здатність виявляти нестандартні групи даних, що корисно для виявлення аномалій в хмарних сервісах.	1. Складність інтерпретації результатів. 2. Вимога високих обчислювальних ресурсів.

Продовження таблиці 1.5

Нейронні мережі	Гнучкість та здатність до навчання на великих обсягах даних.	Складність у налаштуванні параметрів та інтерпретація результатів для ІБ хмарних сервісів.
Алгоритми виявлення викидів	Точність у виявленні аномалій в хмарних сервісах.	Ймовірність помилкових спрацьовувань під час роботи з незбалансованими даними.
Методи аналізу тексту та контенту	Здатність аналізувати текстову інформацію виявлення загроз і аномалій в хмарних сервісах.	Складність у обробці неструктурованих даних та залежність від якості попередньої обробки тексту.
Алгоритми аналізу часових рядів	Здатність виявляти тимчасові залежності та тренди у даних.	Складність у обробці великих обсягів тимчасових даних та чутливість до шумів.
Мережі Байєса	1. Інтерпретованість. Мережі Байєса дають змогу візуалізувати та розуміти залежності між змінними, що робить їх більш інтерпретованими, ніж інші методи машинного навчання. Це необхідно для виявлення внутрішніх порушників, оскільки допомагає зрозуміти, чому модель зробила те чи інше передбачення. 2. Здатність працювати з неповними даними. Мережі Байєса працюють з неповними даними, що часто зустрічається у завданнях кібербезпеки. 3. Вміння обробляти дані із тимчасовою структурою. Мережі Байєса обробляють дані з тимчасовою структурою, що дає змогу враховувати зміни поведінки користувачів у часі. 4. Можливість поєднання інформації з різних джерел. Мережі Байєса об'єднують інформацію з різних джерел, що допомагає робити більш точні прогнози.	1. Складність побудови. Побудова мереж Байєса може бути складним завданням для ХС із великою кількістю змінних. 2. Чутливість до вибору апріорних ймовірностей. Точність мереж Байєса може бути чутливою до вибору апріорних ймовірностей. 3. Обчислювальна складність. 4. Обмежена здатність до узагальнення. Мережі Байєса є менш ефективними, ніж інші методи машинного навчання, у роботі з новими даними, які не були представлені в навчальному наборі.

Як показано в таблиці 1.5, основна перевага таких алгоритмів полягає в їхній здатності швидко аналізувати великі обсяги даних, що доцільно для хмарних сервісів, характерним для яких є великий обсяг обміну інформацією.

Однак для ефективної роботи алгоритмів класифікації знадобиться велика кількість розмічених даних для навчання. Для AWS це може означати, що для навчання моделей класифікації потрібен доступ до даних про мережний трафік та поведінку користувачів, що може бути складно через конфіденційність даних або обмеження ІБ. Для вирішення цих проблем, у свою чергу, можна задіяти такі підходи:

- Створити синтетичні дані [88]. Створення синтетичних даних чи використання симуляцій на навчання моделей класифікації без необхідності використання реальних даних.
- Використовувати техніку навчання з учителем [89]. Використання методів активного навчання, під час якого модель навчається на невеликій підмножині даних, а потім запитує в експертів розмітку для найбільш невизначених прикладів.
- Використовувати трансферне навчання [90]. Використовувати заздалегідь навчені моделі на інших наборах даних і доопрацювати їх для конкретного завдання безпеки в AWS.

Алгоритми кластеризації, також згадані в таблиці 1.5, в розрізі ІБ хмарних сервісів використовують для виявлення груп підозрілої активності або аномалій даних. Вони спроможні автоматично виділяти групи користувачів або події, які незвичайно відрізняються від загальної маси. Це може свідчити про потенційні загрози ІБ. Перевага таких алгоритмів полягає в їхній здатності виявляти неочевидні патерни або угруповання даних, що може бути корисним для виявлення нових типів атак. Алгоритми кластеризації широко використовують для забезпечення ІБ Microsoft Azure, Google Cloud Platform, IBM Cloud та інші хмарні сервіси [6-18].

Однак основним недоліком алгоритмів кластеризації може стати складність інтерпретації результатів у випадках, коли угруповання є неочевидними або потребують додаткового аналізу. Також, як і у випадку з класифікацією, для навчання моделей кластеризації потрібна велика кількість розмічених даних, що може бути складно в реальних умовах забезпечення ІБ

хмарних сервісів через конфіденційність або обмеження доступу до даних. Для усунення цього недоліку можна використовувати згадані вище підходи: синтетичні дані; техніки навчання з учителем і трансферне навчання.

Нейронні мережі у завданнях забезпечення ІБ хмарних сервісів використовують для виявлення складних та нелінійних патернів у даних [91-93]. Це дасть можливість виявляти незвичайні активності або потенційні атаки на хмарні середовища. Перевага використання нейронних мереж полягає в їхній здатності обробляти великі обсяги даних і навчатися на них, а також у гнучкості та здатності адаптуватися до різних типів завдань забезпечення ІБ хмарних сервісів. Нейронні мережі застосовують для виявлення аномального мережного трафіку, аналізу текстових даних для виявлення загроз або навіть аналізу аудіо- та відеопотоків для виявлення підозрілої поведінки. Як показано в таблиці 1.5, основним недоліком нейронних мереж є їхня складність і вимогливість до обчислювальних ресурсів. Це робить дещо проблематичним їх застосування у хмарних сервісах під час роботи з великими обсягами даних. Щоб вирішити цю проблему, можна вдатися до використання: 1) глибокого навчання. У цьому випадку нейронні мережі навчають на великих обсягах даних з використанням глибокого навчання для автоматичного вилучення ознак з даних, що може зменшити залежність від ручної розмітки даних; 2) хмарних обчислень. Для навчання та використання нейронних мереж можна використовувати хмарні обчислювальні ресурси, що дасть змогу масштабувати обчислення та керувати обчислювальними навантаженнями.

Для навчання нейронних мереж на великих обсягах даних, наприклад, для виявлення аномального мережного трафіку або аналізу логів безпеки, можна використовувати хмарні обчислювальні ресурси AWS. AWS надає різні сервіси для обчислень, такі як Amazon EC2 (Elastic Compute Cloud), що допомагають масштабувати обчислення залежно від потреб. Хмарні обчислення дають змогу ефективно використовувати ресурси для навчання нейронних мереж. Можна використовувати кілька екземплярів Amazon EC2 для паралельного навчання моделей на різних частинах даних, що дасть

можливість прискорити процес навчання та знизити навантаження на один екземпляр. Зауважимо, що AWS надає послуги для керування обчислювальними навантаженнями, такі як Auto Scaling. Цей сервіс допомагає автоматично масштабувати кількість екземплярів Amazon EC2 залежно від навантаження. Це дасть можливість оптимізувати використання ресурсів та забезпечить стабільну роботу нейронної мережі. Наведемо невеликий приклад. Припустимо, що компанія використовує AWS для зберігання та обробки даних. З метою забезпечення безпеки даних компанія вирішує використовувати нейронні мережі для виявлення аномалій у мережному трафіку. Вона може розгорнути кілька екземплярів Amazon EC2 для навчання нейронних мереж на історичних даних і використовувати Auto Scaling для масштабування обчислень залежно від навантаження. Тоді компанія зможе ефективно використовувати хмарні обчислювальні ресурси для забезпечення безпеки хмарного сервісу.

Згадані в таблиці 1.5 алгоритми виявлення викидів (аномалій) даних корисні для забезпечення ІБ хмарних сервісів, включаючи Amazon Web Services. Алгоритми виявлення викидів допомогають виявити аномальну чи шкідливу поведінку в мережі або системі, що може свідчити про потенційну загрозу ІБ, а також дають змогу оперативно реагувати на можливі загрози. Наведемо невеликий приклад використання алгоритмів виявлення викидів (аномалій). Припустимо, що компанія використовує AWS для зберігання та обробки своїх даних. Для забезпечення ІБ компанія вирішує використовувати алгоритми виявлення викидів моніторингу мережного трафіку. Алгоритми аналізують трафік щодо аномальних патернів, таких як незвичайно велика кількість запитів з однієї IP-адреси або незвичайно високе навантаження на певний ресурс. Якщо виявляється аномалія, система може спрацьовувати та вживати заходів щодо усунення загрози безпеці. Однак для алгоритмів виявлення викидів (аномалій) є ймовірність помилкового спрацьовування. Що відповідно породжує необхідність виконувати додаткове налаштування під конкретні потреби та характеристики системи. А це потребує часу та ресурсів.

Методи аналізу тексту та контенту також як і всі раніше розглянуті є важливим інструментом для забезпечення ІБ хмарних сервісів, включаючи Amazon Web Services, Microsoft Azure, Google Cloud Platform, IBM Cloud та інші. Відповідно до [94-96] аналіз тексту та контенту може допомогти виявляти підозрілі або шкідливі повідомлення, коментарі або файли, які становлять загрозу ІБ. Аналіз тексту із соціальних медіа та інших публічних джерел може допомогти виявити загрози й тренди, пов'язані з ІБ, а також спроби несанкціонованого доступу до систем і даних. Сервіси хмарної безпеки використовують аналіз контенту для виявлення шкідливих файлів, які завантажуються або передаються через хмарні сервіси. Як показано в [95], алгоритми аналізу тексту здатні аналізувати мережний трафік щодо підозрілих повідомлень або команд, які вказують на атаку або порушення ІБ. За аналогією з попередніми методами наведемо невеликий приклад. Припустимо, що компанія використовує AWS для зберігання та обробки своїх даних. Сервіс виявлення аномалій тексту бере участь у моніторингу текстових даних, що передаються через систему AWS, і дає змогу виявити незвичайні або підозрілі повідомлення, які свідчать про порушення ІБ. Відповідно, якщо виявлено загрозу, то система ІБ спрацьовує та вживає заходів щодо її запобігання.

Алгоритми аналізу часових рядів [97-100] також є ефективними у завданнях забезпечення ІБ хмарних сервісів, включно з Amazon Web Services, Microsoft Azure, Google Cloud Platform, IBM Cloud та іншими. Переваги та недоліки наведені у таблиці 1.5. Зокрема, використання алгоритмів аналізу часових рядів може бути корисним у завданнях прогнозування майбутніх подій чи трендів ІБ, а також для моніторингу продуктивності хмарних сервісів та виявлення аномалій чи проблем. Крім того, алгоритми аналізу часових рядів дозволяють аналізувати дані про мережний трафік та виявляти аномальні патерни, які вказують на мережні атаки або незвичайну активність. Приміром, якась компанія використовує AWS для зберігання та обробки своїх даних. Сервіс аналізу часових рядів може моніторити дані про навантаження та виявляти аномальні патерни, які вкажуть на можливі атаки чи проблеми з

продуктивністю хмарного сервісу. Якщо виявлена аномалія, система ІБ спрацює та задіє заходи щодо усунення аномалії.

Як показав аналіз публікацій, присвячених проблематиці ІБ хмарних сервісів, внутрішні загрози становлять серйозну небезпеку для організацій, оскільки співробітники з доступом до систем та знанням політик безпеки можуть уникнути виявлення. Організації недостатньо готові до виявлення та запобігання таким атакам через орієнтацію традиційних методів ІБ на зовнішні загрози. Більшість моделей виявлення аномалій, розглянутих у даному розділі дисертації, сфокусовані на мережних даних, незважаючи на поведінкові аспекти. Саме тому в наступному параграфі першого розділу роботи ми детальніше зупинимося на особливостях виявлення внутрішніх порушників ІБ хмарних сервісів.

1.4. Особливості виявлення внутрішніх порушників інформаційної безпеки хмарних сервісів на основі методів машинного навчання

Як показано у роботах [101-103], методи машинного навчання, включаючи мережі Байєса, використовують для виявлення потенційно ненадійних співробітників, у тому числі інсайдерів. У роботі [101] автори спочатку визначили набір ознак, які вказують на ризиковану поведінку співробітника, такі як незвичайні спроби доступу до даних, несанкціоноване використання привілеїв, зміни робочого розкладу та інші. Далі дані про ці ознаки були використані для навчання моделі машинного навчання (мережа Байєса). У цих дослідженнях Байєсівські мережі використовувалися для моделювання ймовірності того, що співробітник є ненадійним, на основі сукупності ознак. Як показали автори, методи машинного навчання допомагають виявити закономірності та аномалії даних, які є неочевидними для людини. Вони автоматизують процес аналізу даних та виявлення аномалій, що робить їх ефективними інструментами для виявлення потенційно ненадійних співробітників, зокрема в компаніях, пов'язаних з роботою хмарних сервісів.

Виявлення внутрішніх порушників ІБ, включаючи потенційних інсайдерів, може відіграти вирішальну роль у мінімізації поверхні атак та підвищенні рівня захисту хмарних сервісів. Так, приміром, Amazon Web Services надає низку інструментів та сервісів для виявлення і моніторингу потенційних порушників, включаючи Amazon GuardDuty для виявлення аномальної активності в мережі, AWS CloudTrail для відстеження дій користувачів та AWS Config для оцінки відповідності конфігурації хмарних ресурсів вимогам безпеки. Аналогічні можливості є і в Microsoft Azure, який за допомогою Azure Security Center надає можливості виявлення загроз і порушників у хмарній інфраструктурі, включаючи виявлення аномальної активності, вразливостей і неправильної конфігурації ресурсів. Azure Sentinel дає можливість аналізувати дані журналів та створювати адаптивні правила для виявлення загроз. У Google Cloud Platform є Cloud Security Command Center, який необхідний для виявлення загроз та порушників у хмарному середовищі, а також надає інструменти для моніторингу та аналізу активності користувачів і ресурсів, такі як Cloud Monitoring та Cloud Logging. IBM Cloud Security Advisor надає інструменти виявлення загроз і порушників, включаючи аналіз аномальної активності та моніторинг подій безпеки. IBM QRadar дає змогу виявляти та аналізувати загрози на основі даних із різних джерел.

У таблиці 1.6 систематизовано специфіку виявлення внутрішніх порушників ІБ хмарних сервісів.

Таблиця 1.6 – Специфіка виявлення внутрішніх порушників ІБ хмарних сервісів та програмні продукти різних вендорів на ринку хмарних сервісів (Складено автором)

Використовувані методи та засоби	Особливості
Аналіз поведінки користувачів та співробітників	Моніторинг аномальної активності, незвичайні спроби входу, доступ до конфіденційних даних, зміни конфігурації системи. Використання інструментів машинного навчання для виявлення підозрілих патернів поведінки.
Контроль доступу	Впровадження принципу найменших привілеїв, надання користувачам лише тих прав доступу, які їм необхідні. Регулярний авдит прав доступу та відстеження несанкціонованого доступу до даних.

Продовження таблиці 1.6

Шифрування даних	На прикладі методів шифрування, що використовуються в AWS. Шифрування на стороні клієнта. Amazon S3 Client-Side Encryption дає можливість шифрувати дані перед завантаженням у S3. AWS KMS Customer Master Key (CMK) дозволяє використовувати власний ключ шифрування для захисту даних в AWS. Шифрування на стороні сервера. Amazon S3 Server-Side Encryption (SSE) дає можливість шифрувати дані на серверах AWS. AWS EBS Encryption дає можливість шифрувати томи EBS. AWS RDS Encryption дає можливість шифрувати бази даних RDS. Шифрування «від кінця до кінця». AWS KMS Customer Master Key (CMK) дає можливість використовувати власний ключ шифрування для захисту даних в AWS. AWS Nitro Enclaves забезпечує безпечне середовище для виконання конфіденційних обчислень. Токенізація. Гомоморфне шифрування. AWS CloudHSM дає можливість використовувати апаратні модулі безпеки (HSM) для захисту ключів шифрування. AWS Nitro Enclaves забезпечує безпечне середовище для виконання конфіденційних обчислень.
Використання інструментів DLP (Data Loss Prevention) для запобігання витоку конфіденційних даних	Інструменти DLP (Data Loss Prevention) в AWS 1. AWS CloudTrail відстежує дії користувачів та зміни конфігурації в AWS. Дає можливість виявити підозрілу активність, спроби доступу до конфіденційних даних. 2. AWS Config оцінює та моніторить конфігурацію AWS-ресурсів. Дає змогу виявити несанкціоновані зміни в конфігурації, що призведе до витоку даних. 3. AWS GuardDuty виявляє загрози та аномальну активність в середовищі AWS. Дає змогу виявити спроби витоку конфіденційних даних. 4. AWS Inspector автоматично сканує AWS-ресурси щодо вразливостей. Дає можливість виявити вразливості, можливо використати для атаки на AWS-середовище та крадіжки даних. 5. AWS Macie забезпечує класифікацію та захист конфіденційних даних в AWS.
Моніторинг системи	Відстеження подій безпеки, таких як спроби злому, зміни у файлах, аномалії мережі. Використання інструментів Security Information and Event Management (SIEM) для централізованого моніторингу та аналізу подій безпеки.
Інформаційна обізнаність	Навчання співробітників основам інформаційної безпеки та правилам роботи з хмарними сервісами. Створення культури кібербезпеки у компанії.
Приклади для вендорів	
Amazon Web Services	AWS CloudTrail – сервіс для запису та моніторингу дій користувачів, API-дзвінків та змін конфігурації в AWS. AWS GuardDuty – сервіс для виявлення загроз та аномальної активності в середовищі AWS. AWS Identity and Access Management (IAM) – сервіс для керування доступом до AWS-ресурсів.

	AWS Config – сервіс для оцінки та моніторингу конфігурації AWS-ресурсів.

Продовження таблиці 1.6

Microsoft Azure	Azure Active Directory (AD) – керування доступом на основі ролей (RBAC) для визначення, хто має доступ до яких ресурсів Azure. Azure AD Identity Protectio для виявлення та реагування на підозрілу активність користувачів. Azure AD Conditional Access для застосування додаткових політик безпеки для доступу користувачів. 2. Microsoft Cloud App Security (MCAS) – виявлення та захист конфіденційних даних у хмарних додатках, включаючи Microsoft 365 та Azure. MCAS Cloud Discovery для виявлення та оцінки хмарних програм, що використовуються в організації. MCAS Conditional Access App Control для застосування політик безпеки для доступу до хмарних програм. 3. Azure Monitor – збір та аналіз журналів безпеки для виявлення підозрілої активності. Azure Monitor Log Analytics для створення запитів користувача для виявлення загроз. Azure Monitor Sentinel для використання машинного навчання для виявлення загроз. 4. Azure Security Center – єдина консоль для керування безпекою Azure. Azure Security Center Advanced Threat Protection для виявлення та реагування на складні загрози. Azure Security Center Just-In-Time VM Access для обмеження доступу до віртуальних машин Azure. 5. Microsoft Intune – керування мобільними пристроями для захисту корпоративних даних на мобільних пристроях. Intune App Protection – для застосування політик безпеки для доступу до корпоративних програм на мобільних пристроях. Intune Conditional Access – для застосування додаткових політик безпеки для доступу до корпоративних ресурсів з мобільних пристроїв.

Нові дослідження в галузі забезпечення ІБ інстансів хмарної інфраструктури, з використанням методів машинного навчання та мережі Байєса, відіграють значну роль у підвищенні ефективності виявлення потенційно ненадійних працівників. Методи машинного навчання дають змогу аналізувати великі обсяги даних аномальної поведінки співробітників, що допомагає виявити інсайдерів, які завдають шкоди чи діють несанкціоновано. Мережі Байєса, у свою чергу, ґрунтуючись на різних ознаках та поведінкових даних, та їх використовують для моделювання ймовірності того, що конкретний співробітник є потенційним порушником. Отже, такі дослідження приведуть до розробки більш точних та ефективних систем виявлення інсайдерських загроз, що допоможе організаціям запобігати витоку даних, зберігати конфіденційність і забезпечувати безперервність бізнес-

процесів, заточених на використання хмарних сервісів. Крім того, розвиток нових методів та підходів до виявлення загроз може сприяти більш ефективному захисту від внутрішніх атак та підвищенню рівня безпеки хмарних сервісів загалом.

Висновки за розділом 1

У розділі отримано такі основні результати та зроблено наступні висновки.

Показано, що хмарні обчислення стали невід'ємною частиною бізнес-процесів, надаючи об'єктам інформаційної діяльності можливості оперативно моніторити і реагувати на зміни ринку та керувати бізнес-процесами.

Встановлено, що у різних галузях хмарні сервіси використовуються для оптимізації виробничих процесів, керування фінансами, обробки медичних даних, організації освітнього процесу, автоматизації торгівлі, оптимізації логістики тощо. Застосування ХОб підвищує ефективність бізнесу за рахунок зменшення витрат на ІТ-інфраструктуру та поліпшення доступності до даних та додатків. Крім того, хмарні сервіси дають можливість компаніям швидко масштабувати свої операції та впроваджувати нові технології.

Встановлено, що інформаційна безпека хмарних сервісів є невід'ємним елементом для успішного ведення бізнесу, забезпечуючи захист даних, безперервність бізнес-процесів, відповідність нормативним вимогам та довіру клієнтів. Проблематика ІБ хмарних сервісів притаманна всім вендорам через спільні вразливості, загрози та специфіки технології і навіть вимог клієнтів до високого рівня захисту даних.

Встановлено, що нові дослідження у сфері забезпечення ІБ хмарних сервісів, за допомогою методів машинного навчання і мережі Байєса, зіграють вирішальну роль для підвищення ефективності виявлення потенційно ненадійних співробітників, фактично мінімізувати частину внутрішніх загроз ІБ хмарних сервісів. Методи машинного навчання дають змогу аналізувати великі обсяги даних для виявлення аномалій у поведінці співробітників, а мережі Байєса, ґрунтуючись на різних ознаках та даних про

поведінку, використовують для моделювання ймовірності того, що конкретний співробітник є потенційним порушником. Такі дослідження можуть привести до розробки більш точних та ефективних систем виявлення інсайдерських загроз, що допоможе організаціям запобігати витоку даних, зберігати конфіденційність і забезпечувати безперервність бізнес-процесів.

РОЗДІЛ 2.
ЗАСТОСУВАННЯ МЕРЕЖ БАЄСА ТА МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ВНУТРІШНІХ ЗАГРОЗ У БІЗНЕС-ПРОЦЕСАХ, ЗАСНОВАНИХ НА ХМАРНИХ СЕРВІСАХ

Внутрішні атаки становлять для організацій загрозу, що постійно зростає, адже співробітники – шахраї та/або інсайдери, маючи законний доступ до комп'ютерних систем (КС), у тому числі до хмарних сервісів, що використовуються у бізнесових процесах, а також володіючи інформацією про політику ІБ (або ПІБ) в організації, можуть уникнути виявлення. Організації недостатньо готові до виявлення, стримування та пом'якшення складних внутрішніх, у тому числі інсайдерських атак, оскільки їхні методи ІБ адаптовані переважно до зовнішніх загроз. Проведений у першому розділі роботи аналіз публікацій з виявлення, в тому числі, інсайдерських загроз, надає теоретичну базу для розуміння мотивів, поведінки та моделей таких атак. Більшість існуючих моделей виявлення аномалій інсайдерських загроз орієнтовані на обробку мережних даних. У дослідженні, представленому в межах другого розділу дисертації, ми розглядаємо архітектуру мереж Байєса, здатних враховувати аспекти поведінки разом з мережними даними. Наш підхід використовує методи машинного навчання для аналізу даних. Також ми вводимо функції, що базуються на теоретичних засадах моделювання інсайдерських загроз. Такий підхід, на нашу думку, допоможе аналітикам ІБ враховувати поведінкові особливості співробітників, щоб зробити бізнес-процеси, побудовані у хмарних сервісах, більш безпечними. Ми застосували наші моделі до синтетичних даних, що доводить, як оказано в поточному розділі дисертації, ефективність викладеного підходу для захисту від внутрішніх загроз, в першу чергу від інсайдерів. Розглянуті атаки на синтетичному наборі даних характеризувалися низькою кількістю помилкових спрацьовувань, що свідчить про ефективність запропонованого варіанта рішення.

2.1. Інсайдерська загроза. Огляд методів та моделей для її виявлення

Відповідальність за ІБ хмарних сервісів, які використовує організація, зазвичай лежить на обох сторонах. Перше, це хмарний провайдер, оскільки саме провайдер хмарного сервісу відповідає за забезпечення безпеки інфраструктури хмарної платформи, включаючи фізичну безпеку дата-центрів, мережний захист, своєчасне оновлення ПЗ, а також захист від DDoS-атак та інших загроз. Друге, це користувач – організація та її менеджмент, служби ІБ, інформаційні служби, які використовують хмарні сервіси і також несуть відповідальність за безпечне користування цими сервісами. Принаймні, користувач повинен подбати про безпеку доступу до своїх даних та програм, використовувати надійні паролі, регулярно оновлювати ПЗ, а також забезпечити захист даних під час їх передачі та зберігання.

Так, приміром, Amazon Web Services (AWS) надає широкий спектр інструментів та послуг для забезпечення безпеки. У цей перелік входять роботи, що вже згадувалися в першому розділі, – AWS Identity and Access Management (IAM), AWS WAF (Web Application Firewall) та AWS Shield для захисту від DDoS-атак. Google Cloud Platform (GCP) також пропонує подібні послуги. Скажімо, Identity and Access Management (IAM), Cloud Armor для захисту веб-застосунків та Cloud Security Command Center для моніторингу безпеки хмарних ресурсів. Організація, у свою чергу, повинна правильно налаштувати і використовувати ці інструменти, а також стежити за безпекою своїх даних та додатків у хмарі.

Наведені в таблиці 2.1 приклади випадків, коли дії співробітників призводили до негативних наслідків для компаній, які використовують хмарні сервіси, мотивують вчених розробляти нові методи і технології для виявлення потенційних інсайдерів з кількох причин.

Таблиця 2.1 – Приклади ситуацій, коли ненавмисні чи навмисні дії співробітників (у тому числі інсайдерів) призводили до негативних наслідків для компаній, які використовують хмарні сервіси у своїх бізнес-процесах

(складено автором на підставі аналізу літературних джерел, зазначених у таблиці)

Джерело інформації	Компанія та галузь	Короткий опис інциденту
[104]	Capital One (американська банківська холдингова компанія, що спеціалізується на кредитних картках та автокредитах)	У 2019 році інженер з програмного забезпечення Capital One, Paige Thompson, вкрала дані 106 мільйонів клієнтів. Вона отримала доступ до даних через просту помилку конфігурації хмарного середовища AWS. Наслідки – витік даних спричинив штраф у розмірі $80 мільйонів для Capital One, а також тюремне ув'язнення Thompson на 5 років.
[105]	Uber (компанія, що створила однойменний мобільний додаток для пошуку, виклику та оплати таксі або приватних водіїв та доставки їжі)	У 2016 році колишній співробітник Uber вкрав дані 57 мільйонів користувачів та водіїв. Він отримав доступ до даних через несанкціонований доступ до облікового запису AWS. Наслідки – Uber оштрафовано на $148 мільйонів за порушення правил конфіденційності даних.
[106]	Microsoft (один із найбільших у світі розробників у сфері пропрієтарного ПЗ)	2020 року співробітник Microsoft вкрав вихідний код Azure. Він використовував свій службовий обліковий запис для доступу до коду і виклав його у відкритий доступ. Наслідки – Microsoft не розкрила інформацію про наслідки цього витоку, але він міг призвести до серйозних уразливостей в Azure.
[107]	Verizon (американська телекомунікаційна компанія, найбільший у США постачальник послуг бездротового зв'язку)	У 2017 році співробітник Verizon продав дані 6 мільйонів клієнтів на чорному ринку. Він отримав доступ до даних через несанкціонований доступ до облікового запису AWS. Наслідки – Verizon оштрафували на $1.35 мільйона за порушення правил конфіденційності даних.
[108]	Tesla (американська компанія, виробник електромобілів та рішень для зберігання електроенергії)	У 2018 році співробітник Tesla здійснив витік конфіденційних даних про виробничі процеси компанії. Наслідки – постраждали конкурентоспроможність та безпека компанії.
[109]	Dropbox (Компанія з розробки програмного забезпечення)	У 2014 році інсайдер з Dropbox отримав доступ до облікових записів користувачів без їхнього дозволу. Наслідки порушення конфіденційності даних негативно позначилися на репутації компанії.
[110]	NASA (США, Національне управління з аеронавтики та дослідження космічного простору)	У 2011 році зафіксовано випадок, що колишній співробітник NASA потай отримав доступ до чутливої інформації і передав її третій стороні. Наслідки – витік конфіденційних даних та збитки для організації.

Перше, такі випадки (в таблиці 2.1 показано лише незначну кількість подібних інцидентів) свідчать, що існуючі методи захисту від інсайдерських загроз є недостатньо ефективними. Інсайдери, володіючи знаннями про внутрішні процеси компанії та доступом до цінних даних, спроможні обійти стандартні заходи безпеки. Це підштовхує вчених та інженерів до розробки більш надійних та інноваційних методів для виявлення подібних загроз.

Друге, такі випадки наголошують на необхідності розробки методів, які можуть ефективно виявляти різницю між нормальною та потенційно небезпечною поведінкою співробітників. Це розробка алгоритмів МН, здатних аналізувати та інтерпретувати дані про активність користувачів, щоб виявляти аномальну поведінку, яка може свідчити про можливу загрозу.

Як видно з прикладів, наведених у таблиці 2.1, витік конфіденційної інформації або несанкціонований доступ до даних приводять до фінансових втрат, шкоди репутації та клієнтам, а також до порушення законодавства про захист даних. Такі інциденти підкреслюють необхідність поліпшення методів виявлення та запобігання подібним загрозам.

Багато теоретичних робіт з інсайдерських загроз, зокрема, [111-117], досліджують мотиви та засоби інсайдерів. Як показано в цих публікаціях, інсайдерські атаки зазвичай ініційовані різними мотивами. У [114] проведено класифікацію інсайдерських атак. Відповідно до такої класифікації можна, як мінімум, виділити три типи атак, які, відповідно, спрямовані на: крадіжку інтелектуальної власності; шахрайство; саботаж.

Загрози інтелектуальній власності зазвичай спрямовані на отримання бізнес-переваг, продаж конфіденційної інформації. У [114] показано, що більшість крадіжок інтелектуальної власності чиняться технічними інсайдерами, які крадуть інтелектуальну власність за допомогою технічних уразливостей у системах, про які добре обізнані. Інсайдери, які не мають технічного доступу до обладнання або програмного забезпечення, у тому числі коли йдеться про хмарні сервіси, з меншою ймовірністю матимуть доступ до більшої частини інтелектуальної власності. Відповідно, вони швидше за все не

зможуть використовувати її самостійно за межами організації, приміром, продати або передати третім особам. У [101, 114, 117] наголошується, що технічні інсайдери рідко крадуть інтелектуальну власність з метою її прямого продажу. Натомість вони використовують подібну інформацію у своїх інтересах. У [101] і [104] наводяться приклади, коли такі дії інсайдерів посприяли їм самим у відкритті власного конкуруючого бізнесу. Також можлива передача інтелектуальної власності конкурентам чи іноземним державам. Інсайдерське шахрайство полягає у використанні інсайдером своєї авторизації/доступу або для навмисного порушення цілісності даних організації з метою особистої вигоди, або для крадіжки інформації, що призводить до злочину з використанням особистих даних [118, 119].

Шахрайство не потребує технічних знань, і як правило, доступне для реалізації навіть технічно не підготовленому співробітнику, який працює, з хмарними сервісами в організації. Відповідно, такі дії чинять насамперед співробітники, які обіймають нижчі посади [114]. Випадки інсайдерського шахрайства, проаналізовані в [114], тривали щонайменше п'ять місяців і часто призводили до серйозних крадіжок чи порушень цілісності.

Як показано в більшості розглянутих робіт, присвячених діям інсайдерів [111-119], фінансова вигода є основним мотиватором подібних вчинків. Це стосується співробітників, які зазнають матеріальних труднощів і, відповідно, перебувають у скрутному фінансовому становищі.

Саботаж пов'язаний із порушенням доступності активів кіберпростору та заподіянням шкоди окремим особам. Зазвичай його вчиняють особи, які обіймають технічні посади, як-то, системні адміністратори, котрі мають необхідні повноваження і навички, що може потенційно завдати значної шкоди інформаційним активам компанії. Однак у роботах [111, 112, 114] наведено й інші випадки інсайдерського IT-саботажу, приміром, коли інсайдер не є тим, хто безпосередньо вчиняє саботаж, а натомість допомагає іншим особам вчиняти правопорушення. Проблема полягає в тому, що багато дій, які виконуються інсайдерами, аналогічні їхнім повсякденним робочим завданням,

і це ускладнює виявлення зловмисних дій, якщо використовувати DLP системи. Одним із прикладів може бути випадок, коли співробітник, який для виконання своїх робочих обов'язків має доступ до конфіденційних даних у хмарі, починає копіювати ці дані на свої особисті пристрої або завантажувати їх на особисті хмари. Поведінка такого співробітника може бути аналогічна його звичайним завданням роботи з даними. Відповідно сигнал для системи DLP не спрацює, оскільки копіювання даних може розглядатися як нормальна частина роботи такого співробітника.

Ще один випадок – використання хмарного сервісу для передачі конфіденційної інформації між співробітниками, що також може бути стандартною практикою для роботи в команді. Якщо співробітник почне передавати дані, не зважаючи на правила безпеки або наявність ПІБ, це може бути непоміченим для системи DLP через подібність до звичайних операцій.

Такі сценарії наголошують на важливості не тільки виявлення аномальної поведінки, але й аналізу контексту використання даних та активності співробітників для більш точного виявлення підозрілих дій. Для того, щоб виявити інсайдерські загрози, які схожі зі звичайною діяльністю співробітників, необхідно використовувати не тільки технічні засоби, такі як системи DLP, але й аналізувати контекст дій та поведінку користувачів. Доцільно враховувати такі фактори:

- Обсяг та частота доступу. Якщо співробітник раптово почав часто вимагати доступу до даних, які він раніше не запитував, це може бути ознакою аномальної активності.
- Час доступу. Якщо доступ до даних здійснюється в незвичайний час, приміром, у неробочий час або під час відпустки, це також може бути ознакою підозрілої активності.
- Передача даних. Моніторинг передачі даних між пристроями та хмарними сховищами може допомогти виявити несанкціоноване переміщення конфіденційної інформації.

- Обсяг даних. Раптове копіювання великого обсягу даних із хмари або завантаження їх на зовнішні пристрої може бути індикатором витоку інформації.
- Поведінка у мережі. Аналіз мережної активності співробітників може виявити незвичайні спроби доступу до ресурсів або використання несанкціонованих програм.

Використання аналітики поведінки користувачів та методів МН потенційно дає можливість створити моделі, здатні виявляти підозрілі дії, навіть якщо вони здаються стандартними для робочої діяльності.

У науковій літературі описано кілька підходів до виявлення інсайдерських загроз, як-от в [102, 120] авторами розглянуті методи виявлення аномалій. Ці методи можна поділити на три групи: машинне навчання; статистичний аналіз; інтелектуальний аналіз даних (ІАД).

Переваги та недоліки методів МН ми детально розглянули у таблиці 1.5. Що стосується недоліків статистичного аналізу та ІАД під час виявлення інсайдера, то їх коротко можна узагальнити так:

- ІАД може дати помилкові спрацьовування або неоднозначні результати, які потребують додаткової перевірки, що може призвести до перевантаження системи безпеки, у тому числі хмарного сервісу.
- Статистичний аналіз може мати низьку точність у виявленні інсайдерів або недооцінювати реальні загрози через складність аналізу контексту та мінливість поведінки співробітників.
- Використання статистичних методів та методів ІАД може викликати питання щодо конфіденційності та безпеки даних співробітників, що потребує ретельного керування доступом до даних.

У [121, 122] автори розглянули можливості застосування марковських моделей у завданні виявлення інсайдерів. Зауважимо, що в цих роботах автори звертають увагу на той факт, що приховані моделі Маркова (ПММ) є простими екземплярами динамічних мереж Байєса.

Байєсова мережа (БМ) і ПММ [121, 122] узагальнені в динамічні байєсові мережі. Приховані марковські моделі корисні для глибшого розуміння БМ, які описують модель інсайдера. Параметри ПММ виведені із даних з використанням алгоритму Баума-Велча [123]. Автори в роботах [121, 122, 124-126] показали, що ПММ є багатообіцяючим підходом до виявлення інсайдерських загроз. Проте, як зазначають самі автори даних робіт, використання ПММ потребує значних обчислювальних ресурсів, а для оцінки їх ефективності потрібні подальші дослідження. Можливість використання ПММ у завданнях, як-от, пов'язаних зі складнішими моделями поведінки інсайдера, поки що залишається недослідженою.

У роботі [127] автори розглянули можливості методу «аналіз головних компонентів» (або PCA) щодо вирішення завдання з виявлення інсайдера. На думку авторів, PCA може бути корисним у зазначеному завданні для зниження розмірності даних та виділення найбільш значущих ознак. Це корисно під час роботи з великими обсягами інформації, характерними для завдань виявлення інсайдерів. PCA дає можливість виділити найбільш значущі ознаки, які пов'язані з нелояльністю співробітників. Це допомагає сфокусуватися на головних аспектах поведінки працівників під час аналізу даних. Також PCA може допомогти виявити аномалії у даних, які можуть свідчити про нелояльну поведінку співробітників. Приміром, аномальні зміни у зразку використання ресурсів або взаємодії із системами можуть вказувати на потенційного інсайдера. З погляду візуалізації результатів PCA також зручний, оскільки дає змогу візуалізувати дані в меншій кількості вимірювань, що може допомогти виявити закономірності або кластери, пов'язані з нелояльною поведінкою співробітників. Проте відзначимо, що хоча PCA є потужним інструментом зменшення розмірності даних і, отже, складності проблеми виявлення аномалій у поведінці співробітників, він може втратити цінну інформацію.

За останні роки досить велика кількість досліджень, зокрема, роботи [128-133], присвячені застосуванню нейронних мереж в завданні виявлення інсайдера. У цих роботах автори пропонують методи виявлення інсайдерських

загроз з використанням штучних нейронних мереж (ШНМ) та використовують різні підходи до навчання ШНМ, а саме: аналіз журналів активності користувачів [128, 133], одночасне навчання на даних із різних джерел [129], використання автоенкодерів (тип ІНС, який навчається реконструювати вхідні дані на виході, використовуючи внутрішнє приховане подання даних. У завданні виявлення інсайдерів автоенкодер може бути використаний для виділення найбільш значущих ознак із даних та виявлення аномалій) [131].

У [130] автори порівнюють ефективність різних методів виявлення інсайдерських загроз, а в [132] розробляють інтегровані моделі, що враховують проблему незбалансованості даних. Загалом, проаналізовані роботи доводять потенціал ШНМ для ефективного виявлення інсайдерських загроз. Також зауважимо, що в роботі [134] проведений ретельний огляд різних методів виявлення інсайдерських загроз, в тому числі використання ШНМ, а в роботі [135] автори виконали не менш ретельний огляд переваг та недоліків різних методів МН для виявлення інсайдерських загроз.

Як зазначають автори розглянутих публікацій [128-135], використання моделей глибокого навчання пов'язане з низкою недоліків.

Ми виділили такі: збір даних про реальні інсайдерські інциденти є складним завданням. А нестача даних може призвести до перенавчання ШНМ та зниження її ефективності на реальних даних. ШНМ необхідно постійно навчати на нових даних, щоб вона залишалася ефективною; кількість випадків інсайдерських інцидентів, як правило, значно менша, ніж випадків нормальної поведінки, отже, це може призвести до того, що ШНМ оптимізована для виявлення нормальної поведінки та пропускати інсайдерські інциденти; ШНМ є «чорними ящиками», що ускладнює інтерпретацію їхніх рішень. Це може зробити складним обґрунтування рішень ІНС та вжиття заходів щодо реагування на інсайдерські загрози; дані, що використовуються для навчання ШНМ, можуть містити конфіденційну інформацію. Відповідно, це може призвести до проблем з безпекою та конфіденційністю; інсайдери можуть змінити свою поведінку, щоб уникнути виявлення ШНМ, а це може призвести

до того, що ШНМ стане менш ефективною з часом; для розробки та використання ШНМ потрібні знання в галузі машинного навчання та кібербезпеки, отже, це може обмежити можливості використання ШНМ у деяких організаціях, що використовують хмарні послуги.

Усі вище розглянуті недоліки та складності справедливі і до провайдерів хмарних сервісів. Це стосується пункту про навчання ШНМ для завдання з виявлення інсайдера. Приміром, AWS для допомоги організаціям у виявленні інсайдерських загроз пропонує низку інструментів і послуг: Amazon GuardDuty (сервіс для виявлення загроз, який може виявити підозрілу активність в хмарному середовищі); Amazon CloudTrail (сервіс авдиту, що допомагає відстежувати всі дії); Amazon Macie (сервіс для виявлення та захисту конфіденційних даних). AWS, проте, не може отримати доступ до даних про інсайдерські інциденти в самій компанії, яка використовує хмарний сервіс, оскільки є обмеження через конфіденційність даних усередині організації.

Отже, використання ШНМ у завданні виявлення інсайдера має низку обмежень. У даному випадку ми розглядаємо AWS, однак аналогічні висновки будуть справедливими і для хмарних сервісів Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud, Oracle Cloud. Перерахуємо їх:

1) AWS не має доступу до даних, що зберігаються у хмарних сервісах AWS, за винятком випадків, коли користувач явно надає такий доступ.

2) Відповідальність за захист даних від інсайдерських загроз лежить на організації, що використовує AWS (або Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud, Oracle Cloud).

Крім моделей виявлення інсайдерських загроз з урахуванням аномалій, існують підходи, створені задля розпізнавання поведінкових аспектів. Такі моделі можуть пролити світло на глибинні взаємозв'язки між аномаліями, виявленими, наприклад, за допомогою DLP, та мотивацією інсайдерів.

Одним із методів, який може сприяти у виявленні внутрішніх загроз, є ймовірнісне латентно-семантичне індексування. Його можна застосовувати до

електронних листів, щоб дізнатися про інтереси співробітників та їх соціальні зв'язки [136].

Згідно із [102, 128-135, 142], інсайдер відрізняється від звичайного внутрішнього порушника ІБ тим, що він є частиною організації та має легальний доступ до систем і даних. Інсайдер зазвичай має більш глибокі знання про політики ІБ та методи моніторингу компанії. Відповідно, такі знання роблять його дії складнішими. У компаніях, які використовують хмарні сервіси у своїх бізнес-процесах, інсайдер може використовувати знання про системи та сервіси для вчинення умисних або ненавмисних дій, які можуть призвести до порушення ІБ.

У категорії технічних підходів, які зазвичай використовують для виявлення внутрішніх порушників та/або інсайдерів, є дві основні підкатегорії [102, 142]. Кожна з цих підкатегорій ґрунтується на доступних методах виявлення інсайдерських загроз. Перша підкатегорія містить методи виявлення будь-якої несанкціонованої діяльності. Друга підкатегорія передбачає методи виявлення будь-яких змін у поведінці, що можуть призвести до зловмисної інсайдерської загрози. Хоча системи виявлення вторгнень (IDS), DLP-системи (запобігання витоку даних), SIEM-системи (системи керування ІБ (SIM) та керування подіями безпеки (SEM)), ACS-системи контролю доступу майже завжди можуть досить результативно виявляти аномальну поведінку звичайного внутрішнього порушника ІБ, проте стосовно інсайдера ця проблема залишається невирішеною.

Резюмуючи результати, викладені в даному параграфі цього розділу роботи, можна зробити такі узагальнення, що дають можливість продовжити дослідження у вибраному напрямку:

інсайдери мають легальний доступ до систем і даних, тому їхні дії можуть здаватися легітимними, отже, вони можуть виконувати завдання під час роботи з ХС, які схожі на їхні звичайні робочі обов'язки, що ускладнює виявлення аномальної поведінки за допомогою штатних IDS, DLP, SIEM, ACS-систем;

інсайдери можуть обходити DLP, SIEM, ACS-системи, використовуючи знання організаційної структури та слабких місць в організації ІБ;

використання хмарних сервісів вносить додаткову складність у моніторинг і виявлення аномальної поведінки через відмінності в архітектурі та методах забезпечення безпеки для таких провайдерів як AWS, Microsoft Azure, GCP, IBM Cloud, Oracle Cloud та ін.;

інформація про поведінку співробітників у хмарних сервісах є обмеженою або недоступна для внутрішніх систем моніторингу, що знижує ефективність виявлення;

інсайдери, що свідомо діють зловмисно та/або керуючись фінансовими мотивами, є небезпечними, оскільки вони знають, як уникати виявлення і можуть завдати значної шкоди організації.

2.2. Байєсівський метод раннього виявлення інсайдерів в організаціях, які використовують хмарні послуги

Як показано у першому розділі дисертації, а також у попередньому параграфі роботи, існує безліч досліджень, присвячених протидії зовнішнім загрозам інформаційної безпеки (ІБ). Розроблено повноцінні методології та спеціалізоване програмне забезпечення. І якщо говорити про захист хмарних провайдерів, таких як AWS, Microsoft Azure, Google Cloud Platform, IBM Cloud, Oracle Cloud, то питання протидії зовнішнім загрозам методологічно, організаційно й технічно вирішено, про що свідчить неухильне зниження кількості інцидентів з інформаційною безпекою під час роботи компаній з хмарними платформами. Проте, як ми показали у попередньому параграфі, інструментарій протидії внутрішнім загрозам інформаційної безпеки опрацьований все ще недостатньо добре. Це підтверджує і той факт, що на думку багатьох керівників компаній та фахівців з кібербезпеки, основні небезпеки, пов'язані з витоком інформації, походять від внутрішніх загроз, і нерідко це безпосередньо є наслідком нелояльної чи злочинної поведінки співробітників та/або технічного персоналу [137-139].

Основним елементом ефективної протидії внутрішнім порушникам є їх дострокове або ж раннє виявлення. Події та обставини, наявність яких дає підстави з деякою мірою ймовірності припустити, що певний співробітник реалізує або може реалізувати загрозу для ІБ хмарного сервісу, який використовується в діяльності компанії, називаються індикаторами загрози. Індикатори можуть бути поведінковими, що характеризують соціальну поведінку потенційного інсайдера, або технічними, що пов'язані з його діями в інформаційній системі організації або під час роботи з хмарними сервісами.

Частково технічні індикатори (метрики ІБ) ми згадували раніше. До цього списку можна додати:

1) Спроби доступу до даних із різних місць або пристроїв, що може свідчити про намагання обійти системи безпеки. Приміром, спроба доступу до даних з IP-адреси, яка не відповідає звичайній IP-адресі пристрою користувача. Або спроба доступу до даних із нового пристрою, який раніше не використовувався для цього. Або спроба доступу до даних у незвичайний час, який не відповідає звичайному часу доступу користувача. Або раптове збільшення кількості запитів до даних із одного або декількох пристроїв, що частково свідчить про спробу масового доступу чи атаки. А також спроба доступу до даних відразу з декількох пристроїв або місць, що вказує на скоординовану атаку.

2) Використання незвичайних чи незнайомих команд, запитів або дій в інтерфейсі хмарного сервісу, що свідчить про спроби несанкціонованого доступу чи дій. Приміром, несподівана спроба доступу до захищених даних або ресурсів, до яких користувач не має необхідних прав. Або спроба змінити налаштування безпеки, такі як правила групи безпеки або політики IAM (AWS identity and Assess Management), без попереднього повідомлення або не за встановленими процедурами. Або створення чи видалення інфраструктурних ресурсів (EC2-інстансів, S3-бакетів) без відповідного дозволу або не за встановленими процедурами. Або зміна параметрів ХС, таких як Amazon RDS або Amazon S3, що може призвести до порушення працездатності програми

або витоку конфіденційної інформації. Або незвичайна активність в API, безліч невдалих спроб автентифікації або виклики API із незвичайних джерел.

3) Спроби зміни налаштувань безпеки, спроби обходу двофакторної автентифікації тощо. Приміром, спроба створити, змінити або видалити IAM-користувачів або їх права для отримання несанкціонованого доступу.

Аналогічно розглянемо й технічні індикатори (метрики ІБ). До них можна віднести такі: 1) Підвищена активність чи інтерес співробітника до даних або інформації, до яких він не має прямої необхідності чи дозволу доступу; 2) Частота запитів на доступ до конфіденційних даних, які нетипові для посади запитувача.

У разі мотивованих інсайдерських порушень поведінкові індикатори зазвичай виникають задовго перед технічними. Загроза IT-саботажу починається із незадоволеності співробітника, яка може призвести до протиправних дій під час роботи з хмарним сервісом. Для загроз IT-шахрайства та IT-шпигунства характерно, що злочин передує періоду підготовки та раціоналізації [101, 130]. А це швидше за все позначиться на поведінці інсайдера. Проте поведінкові індикатори менш застосовні до загрози крадіжки інтелектуальної власності, оскільки інсайдери завжди усвідомлюють порушення своїх дій. Також поведінкові індикатори практично не застосовуються до невмотивованих порушників, які діють без попередньої підготовки та ненавмисно. Відповідно, це ускладнює їх виявлення як за поведінковими, так і технічними індикаторами (метриками ІБ).

Формалізація показників ІБ та оголошення базового набору таких показників є важливими кроками для виявлення внутрішнього порушника та/або інсайдерів. Показники ІБ можуть містити різні метрики і параметри, які відображають стан ІБ ХС. Ці показники можуть містити дані про доступ до системи, активність користувачів, події безпеки та інші аспекти роботи системи.

Оголошення базового набору показників ІБ для хмарного сервісу можна описати так:

$$SM = \left\{ \bigcup_{i=1}^{n} SM_i \right\} = \{SM_1, \ldots, SM_n\}, \tag{2.1}$$

де $SM_i \subseteq SM\left(i = \overline{1,n}\right)$ – множина метрик ІБ хмарного сервісу.

Метрики ІБ містять показники, що відображають різні аспекти безпеки хмарних сервісів, у тому числі внутрішні загрози з боку співробітників компанії. Це повною мірою стосується й інсайдерів. Інсайдери, які мають законний доступ до хмарного сервісу та даних компанії, можуть становити серйозну загрозу ІБ, тому слід мати метрики, які можуть допомогти виявити подібні загрози.

Формалізація показників ІБ та визначення базового набору метрик пов'язані із завданням виявлення внутрішніх інсайдерів, оскільки дають змогу компаніям оцінити ефективність своїх заходів щодо забезпечення безпеки та виявити аномальну поведінку співробітників. Набір (2.1) може бути представлений у вигляді зв'язкового списку або системи підмножин:

$$SM = \left\{ \bigcup_{j=1}^{m_i} SM_{ij} \right\} = \{SM_{i.1}, \ldots, SM_{i.m}\}, \tag{2.2}$$

де $SM_{ij}\left(i = \overline{1,n},\ j = \overline{1,m_i}\right)$– список метрик параметра i (цінність метрики визначається відповідно до стандартів ІБ та рекомендованих практик для кожного конкретного хмарного сервісу);

m_i – кількість метрик в i параметрі.

Для виявлення внутрішніх порушників ІБ, у тому числі на об'єктах інформаційної діяльності, які використовують хмарні сервіси у своїх бізнес-процесах, потрібно збирати поведінкові й технічні індикатори загроз та

оцінювати ймовірність того, що конкретний співробітник реалізує ту чи іншу загрозу ІБ. Існує припущення, що наявність деяких індикаторів не завжди вдається визначити з використанням стандартних засобів захисту, таких як DLP, IDS/IPS, SIEM, в цілому. Або для конкретного провайдера, такого як Amazon, (Amazon GuardDuty, Amazon CloudTrail, Amazon Macie). У разі перевищення певного порогу ймовірності реалізації загрози співробітник переходить до списку потенційних інсайдерів. А для інсайдерів вже застосовуються відповідні контрзаходи. Потрібно визначити оптимальний поріг ймовірності реалізації загрози, при якому досягається мінімум помилок першого та другого роду. Більшість моделей загроз, крім невмотивованого порушника ІБ, виявляють заздалегідь на основі чинних методів. Для розробки математичної моделі раннього виявлення невмотивованого порушника інформаційної безпеки потрібні додаткові дослідження його поведінки та можливих індикаторів.

Мережа Байєса (БМ) – це спрямований ациклічний граф. Кожній його вершині відповідає випадкова змінна [140, 141]. Якщо вузли (змінні) не з'єднані дугами, вважають, що вони умовно незалежні [140]. Якщо з вершини (A) виходить дуга у вершину (B), то вершина (A) – батько вершини (B). Відповідно, (B) – нащадок вершини (A). Множину вершин-батьків вершини (v_i) позначимо $(parents(v_i))$. Відповідно, якщо (V) – безліч усіх вершин, а (v_i)– значення $i-ой$ вершини, справедливий наступний вираз, що описує повний спільний розподіл ймовірності:

$$P(v_1,...,v_2)=\prod_{i=1}^{n} P(v_i|parents(v_i)). \qquad (2.3)$$

Розглянемо невеликий приклад. Для опису вершин-батьків вершини у БМ можна використовувати структуру даних, наприклад, словник у Python, де ключами будуть самі вершини, а значеннями – їхні батьки. Якщо у нас є

вершина (v_1) з батьками (v_2) і (v_3), то це може бути описано так: *parents = { 'v1': ['v2', 'v3'], 'v2': [], 'v3': [] }.* Цей код прикладу створює словник '*parents*', у якому в кожної вершини зазначені її батьки. У даному випадку у вершин (v_2) і (v_3) немає батьків, а у вершини (v_1) батьками є вершини (v_2) і (v_3). Опис батьків вершини впливає на опис повного спільного розподілу ймовірності, оскільки вершина залежатиме від батьків. При описі вершин-батьків ми враховуємо ці залежності та визначаємо, як зміна стану батьків може вплинути на ймовірність стану вершини (v_i). Модифікуємо приклад у контексті розглянутого нами в даному параграфі завдання з виявлення невмотивованого порушника ІБ. Припустимо, у нас є БМ, яка моделює поведінку співробітника в організації, у бізнес-процесах якої використовуються хмарні сервіси. У цій мережі у нас є вершина, яка є ймовірністю того, що співробітник вчинить порушення правил ІБ, не маючи явних мотивів для цього. Для моделювання такої БМ ми можемо визначити батьків вершини як набір факторів, які можуть впливати на невмотивоване порушення. Наприклад, батьками вершини є такі фактори:

1) Частота доступу до захищених даних. Логічно, чим частіше співробітник має доступ до захищених даних, тим вища ймовірність, що він вчинить порушення без явних мотивів.

2) Рівень привілеїв у системі. Чим вище рівень привілеїв у співробітника, тим більше можливостей у нього вчинити порушення правил ІБ без явних мотивів.

3) Історія попередніх порушень. Якщо у співробітника були випадки порушень правил ІБ у минулому, це може збільшити ймовірність того, що він вчинить порушення і в майбутньому без явних мотивів.

Опис батьків вершини дасть можливість врахувати різні фактори, які можуть впливати на ймовірність невмотивованого порушення правил ІБ співробітником.

Щоб врахувати цю залежність, ми можемо визначити таку структуру вершин-батьків: *parents = { 'vi': ['access_frequency', 'privilege_level', 'previous_violations'], 'access_frequency': [], 'privilege_level': [], 'previous_violations': [] }.* Цей код описує ситуацію, коли вершина (v_i) залежить від трьох факторів: частоти доступу до захищених даних (access_frequency), рівня привілеїв у системі (privilege_level) та історії попередніх порушень (previous_violations). Кожен із цих чинників може вплинути на ймовірність невмотивованого порушення правил ІБ під час роботи з хмарними сервісами.

БМ є модель для опису ймовірних зв'язків між подіями, а також відсутності таких зв'язків. У цій моделі зв'язок $(A \to B)$ від події (A) до події (B) вважається причинним, якщо подія (A) впливає на виникнення події (B) та визначає її значення. Для визначення ймовірності приналежності співробітника до певного класу внутрішніх порушників ІБ можна використовувати БМ кожного класу. Переваги застосування БМ у цьому контексті передбачають простоту побудови та інтерпретації, можливість роботи з неточними та неповними даними, а також можливість навчання в процесі роботи з низькими обчислювальними витратами.

Входами кожної БМ є індикатори, які свідчать про потенційні порушення ІБ хмарних сервісів потенційним внутрішнім порушником. Виходом кожної БМ є можливість приналежності співробітника до певного класу внутрішніх порушників. Кожна вершина в мережі являє собою випадкову величину, яка може приймати значення «1» (якщо індикатор спостерігається) або «0» (інакше). Дуги між вершинами БМ є імовірнісні залежності між величинами, які визначаються за допомогою таблиці умовної ймовірності. Значення у таблиці умовної ймовірності кожної вершини визначаються відповідно (2.3).

Для навчання БМ необхідно вибрати алгоритм її навчання для виявлення внутрішніх порушників і/або інсайдерів. Сьогодні алгоритми навчання БМ добре вивчені, і для подібного завдання, як показано в роботах [102, 139-142],

найбільше підходять: ЕМ-алгоритм; методи – релевантних векторів, Монте-Карло тощо. Для бази знань, що розробляється, необхідно правильно описати БМ і визначити, що власне будуть представляти входи в неї. У ситуації з моделюванням дій внутрішніх порушників входи до БМ – індикатори подій ІБ, пов'язані з діями внутрішніх порушників. Але оскільки в ситуації з невмотивованим внутрішнім порушником судити про його дії складно, то подібна інформація для бази знань слабо структурованою, що у свою чергу ускладнює процедуру суджень щодо прояву деяких індикаторів, приміром, поведінкових. Відповідно, в моделі БМ з'являються не тільки слабо структуровані, а й приховані дані. Виходячи з вищесказаного, для моделі БМ та її навчання обрано ЕМ-алгоритм [140]. Даний алгоритм має такі переваги порівняно з альтернативними варіантами: Зі зростанням кількості вихідних даних відбувається лінійне збільшення складності алгоритму [140], що прийнятно для постановки завдання з моделювання дій внутрішніх порушників; ЕМ-алгоритм стійкий до «шумів» [140, 141]; ЕМ-алгоритм дає можливість працювати зі слабо структурованими та прихованими даними; Реалізація ЕМ-алгоритму будь-якою високорівневою мовою програмування не становить складності.

ЕМ-алгоритм містить такі етапи або кроки: expectation step (E – крок); maximization step (M – крок).

Нехай є набір даних (Y) – індикатори ІБ хмарних сервісів, які об’єкт інформаційної діяльності використовує у своїх бізнес-процесах. Частина цих даних спостерігалася (X). Інша частина не спостерігалася – (Z). Фактично дані (Z) приховані або Zh. Приклади (X), (Z) або (Zh) наведено у таблиці 2.2.

У такій ситуації правомірний запис:

$$Y = X \bigcup Zh. \tag{2.4}$$

На початковому етапі роботи ЕМ-алгоритму задаємо для (Zh) деяке початкове значення, яке буде лише припущенням.

Таблиця 2.2 – Приклади індикаторів ІБ хмарних сервісів

№	Індикатори ІБ хмарних сервісів (Y)	Видимі індикатори ІБ хмарних сервісів (X)	Приховані індикатори ІБ хмарних сервісів (Zh)
1	Декілька невдалих спроб входу в систему або спроби входу з незвичайних місць	Журнали подій системи виявлення вторгнень (IDS), що містять інформацію про аномальну активність	Незвичайні запити до бази даних або зміни у файловій структурі, які не були зареєстровані
2	Несподівано великий обсяг даних, що передаються між внутрішніми та зовнішніми вузлами	Журнали системи запобігання витоку даних (DLP), що містять інформацію про спроби НСД до даних	Спроби доступу до хмарного сервісу ззовні з використанням облікових даних співробітника
3	Спроби доступу до API хмарного сервісу не характерні для звичайного робочого процесу	Журнали системи керування подіями безпеки (SIEM), що містять інформацію про спроби входу в систему або зміни в конфігурації хмарного сервісу	Переміщення або копіювання великого обсягу даних поза звичайним робочим процесом
4	Зміни в налаштуваннях без попередження або узгодження	Журнали контролю доступу (ACS) містять інформацію про спроби доступу до захищених ресурсів	Зміни у звичайному робочому розкладі чи звичках користувачів, що вказують на потенційну компрометацію облікових даних

Крок E:

$$M(h) = E[\ln p(y \mid h) \mid X], \tag{2.5}$$

де $M(h)$ – математичне очікування натурального логарифму для змінних, що становлять вибірку спостерігача та залежать від кількості прихованих даних (h).

Крок M (розрахунок максимального значення математичного очікування від $Q(h)$:

$$h_1 = \arg\max_h M(h). \tag{2.6}$$

В результаті роботи алгоритму покроково визначатимемо значення (h) при $M(h)$ для кроку E. Реалізовуватимемо кроки до моменту, поки послідовність (h_k) не стане сходитися.

За допомогою ЕМ-алгоритму знаходитимемо нові оцінки максимальної правдоподібності параметрів БМ, використовуючи наявні вибіркові дані. Отримана підсумкова оцінка дасть можливість переглядати БМ та значення апріорних ймовірностей подій ІБ, пов'язаних із персоналом. Для навчання БМ що більше інцидентів ІБ, то точнішим є результат. Навчена БМ у складі БЗ допоможе з великим ступенем точності визначати внутрішнього порушника політики ІБ компанії.

Для розробки моделі БМ на основі наданих даних спочатку використано синтетичний набір даних. Потім описано мовою Python структуру БМ та визначено умовні розподіли ймовірностей (CPD). Для виведення ймовірностей внутрішнього порушника використано інференцію [143].

Нище показано фрагмент коду, який описує згенеровані випадкові значення для індикаторів, що спостерігаються (X), для прихованих індикаторів (Zh), а також об'єднані спостережувані та приховані індикатори для створення повного набору даних (Y).

```
# Features related to security indicators (Y)
failed_login_attempts = np.random.randint(0, 5, n_samples)
data_transfer_volume = np.random.randint(1, 100, n_samples)
api_access_attempts = np.random.randint(0, 3, n_samples)
config_changes = np.random.randint(0, 2, n_samples)
# Features observed (X)
ids_logs = np.random.randint(0, 2, n_samples)
dlp_logs = np.random.randint(0, 2, n_samples)
siem_logs = np.random.randint(0, 2, n_samples)
acs_logs = np.random.randint(0, 2, n_samples)
# Combine features into a DataFrame
df = pd.DataFrame({
    'Failed_Login_Attempts': failed_login_attempts,
    'Data_Transfer_Volume': data_transfer_volume,
    'API_Access_Attempts': api_access_attempts,
    'Config_Changes': config_changes,
    'IDS_Logs': ids_logs,
    'DLP_Logs': dlp_logs,
    'SIEM_Logs': siem_logs,
    'ACS_Logs': acs_logs
})
```

Можливість невірного входу в систему (X_1) впливає на ймовірність прихованого порушника (Zh_1). Використовую інференцію для обчислення

ймовірності, що прихований порушник активний, з урахуванням індикатора, який спостерігається $(X_1 = 1)$. Інференція в БМ дає нам змогу обчислити ймовірність гіпотези або стану змінної на основі наявних даних та моделі мережі. У завданнях виявлення прихованого внутрішнього порушника ІБ це необхідно для визначення ймовірності того, що порушник справді активний і становить загрозу для ІБ хмарного сервісу. Якщо у нас є дані про кілька невдалих спроб входу до хмарного сервісу, несподівано великий обсяг передачі даних і спроб доступу до API, модель БМ може допомогти визначити, наскільки ймовірно, що ці події пов'язані з активністю внутрішнього порушника та/або інсайдера. Інференція дає змогу оцінити ймовірність того, що дані, які спостерігаються, відповідають активності прихованого порушника, враховуючи структуру залежностей між змінними в БМ. Це допоможе офіцеру з ІБ приймати більш обґрунтовані рішення щодо виявлення та запобігання загрозам ІБ.

Описана БМ реалізована мовою Python серед Spyder (Anaconda) (див. рис. 2.1). На рис. 2.2 показан результат візуалізації роботи такої простої БМ.

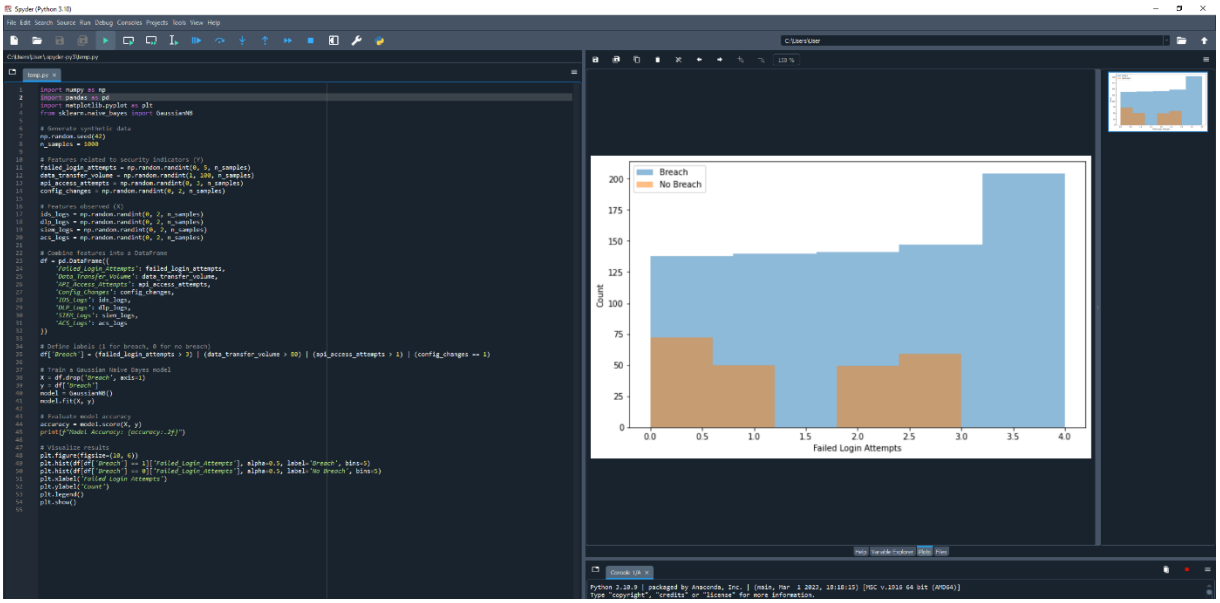


Рис. 2.1 – Реалізація найпростішої БМ для виявлення внутрішнього порушника ІБ мовою Python у середовищі Spyder (Anaconda)

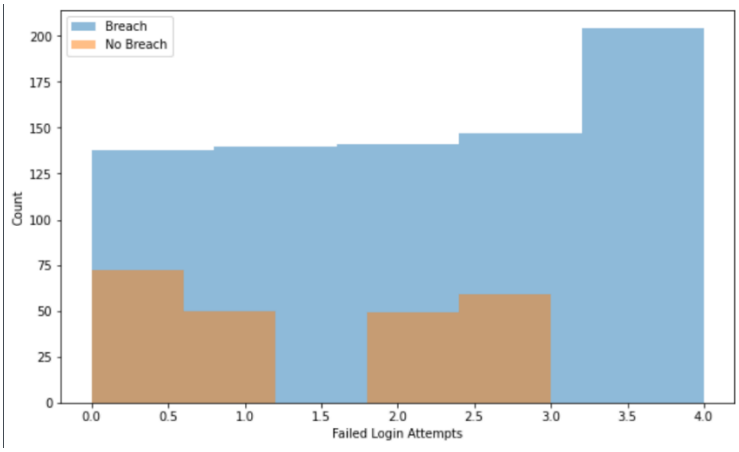


Рис. 2.2 – Результати візуалізації роботи елементарної БМ виявлення внутрішнього порушника ІБ

На гістограмі, яку показано на рис. 2.2, бачимо дві групи стовпців:

1) Breach (Порушення) – ця група представляє випадки, коли індикатори ІБ вказують на можливого порушника (значення «1» у стовпці «Breach»).

2) – No Breach (Без порушення ІБ) – ця група містить випадки, коли індикатори ІБ не вказують на порушення (значення «0» у стовпці «Breach»).

По осі абсцис показано кількість невірних спроб входу до системи (Failed Login Attempts). Стовпці показують, скільки зафіксовано невірних спроб входу до системи.

Стовпці зі значенням «1» (Breach (Порушення)) вказують на випадки, коли виявлено неодноразове порушення ІБ (багато невірних спроб входу).

Стовпці зі значенням «0» (No Breach (Без порушення)) вказують на випадки, коли не було зафіксовано порушення ІБ.

Для синтетичного набору вихідних даних видно, що у гістограмі випадки порушень (Breach) зазвичай мають більше невірних спроб входу у систему, ніж випадки без порушень (No Breach).

Зрозуміло, така проста БМ не дає можливості описати всі ситуації та варіанти дій внутрішнього порушника, а тим більше інсайдера, проте вона ілюструє концептуально вірний підхід до застосування БМ для виявлення

внутрішнього порушника чи інсайдера, а синтез складнішої БМ, яку можна застосовувати на практиці в реальних хмарних сервісах, описано далі у роботі.

Крім того, на подальших етапах дослідження можна збільшити кількість інцидентів у вибірці.

На поточному етапі дослідження вибірку, яка використовувалася для навчання БМ, вже можна додатково поповнити інцидентами, віднесеними до таких категорій:

1) саботаж (проявом саботажу в хмарному сервісі з боку внутрішнього порушника ІБ може бути навмисне некоректне заповнення БД компанії. Наприклад, співробітник, який має доступ до БД клієнтів, може змінити або видалити частину даних, що призведе до спотворення інформації та потенційних проблем для компанії);

2) шахрайські дії на керівних посадах (спотворення даних звітів компанії у власних інтересах. Керівник, який має доступ до хмарного сервісу для аналізу фінансової звітності, може змінити дані, щоб створити помилкове враження про фінансове становище компанії перед інвесторами або стейкхолдерами. Такі дії можуть призвести до негативних наслідків для компанії та її репутації);

3) шахрайські дії рядових співробітників (спотворення особистої інформації під час влаштування на роботу. Співробітник може підробити своє резюме, включивши до нього неправдиві відомості про попередній досвід роботи або освіту, щоб отримати посаду, для якої не має необхідної кваліфікації. Використання хмарного сервісу в цьому випадку може спростити доступ до резюме та його редагування, що потенційно дає змогу співробітнику вчинити шахрайство);

4) шпигунство (прикладом шпигунства з використанням хмарних сервісів може бути ситуація, коли співробітник компанії, маючи доступ через хмарний сервіс до конфіденційної інформації про бізнес компанії, збирає та передає цю інформацію конкурентам. Співробітник може завантажувати файли з планами розвитку компанії або даними про клієнтів на свій особистий

хмарний обліковий запис і далі передавати їх конкурентам, що може призвести до серйозних збитків для компанії);

5) розкрадання інформаційних ресурсів (прикладом розкрадання інформаційних ресурсів з використанням хмарних сервісів може бути ситуація, коли співробітник компанії, маючи доступ до БД клієнтів через хмарний сервіс, копіює цю БД на свій пристрій або завантажує її на особистий хмарний обліковий запис. Далі, використовуючи вкрадені дані, співробітник може, приміром, звернутися до клієнтів компанії від свого імені або продати БД конкурентам, що завдасть значних збитків компанії).

Подібна чи інша більш детальна класифікація допомагає краще зрозуміти природу загроз та способи запобігання їм. Приміром, заходи щодо запобігання саботажу можуть відрізнятися від заходів щодо запобігання розкраданню інформаційних ресурсів. Кожна категорія загрози має свої особливості та може потребувати унікальних методів виявлення і захисту, а класифікація допомагає зосередити зусилля на ключових питаннях ІБ хмарних сервісів. Різні категорії загроз мають різний потенціал для заподіяння шкоди організації, відповідно, розуміння цього допомагає оцінити ризики та розробити відповідні заходи щодо їх зниження.

Розглянемо ще один приклад реалізації БМ. Але на відміну від попереднього прикладу для моделювання БМ, використовуємо програмний пакет GeNIe Modeler [144]. Зауважимо, що GeNIe Modeler – це спеціалізований інструмент для ймовірнісного моделювання й побудови БМ, які, як було показано вище, широко використовуються під час моделювання порушень ІБ. GeNIe Modeler (навіть у безкоштовній версії 2.0) пропонує графічний інтерфейс для створення та аналізу БМ, що спрощує візуалізацію та розуміння складних взаємозв'язків між змінними. GeNIe також забезпечує розширені можливості для чутливого аналізу, виведення та навчання на основі даних, що є принциповим для моделювання внутрішніх порушень безпеки, де відносини між змінними недостатньо зрозумілі або можуть змінюватися з часом. І хоча Python має великі бібліотеки для МН та аналізу даних, включно з бібліотеками

для БМ, такими як pgmpy і pomegranate, його застосування потребує знань і зусиль у програмуванні, що може виходити за компетенції співробітників відділу ІБ. У такому аспекті GeNIe Modeler має переваги завдяки своєму зручному інтерфейсу та спеціалізованим функціям для моделювання БМ, що робить його в низці ситуацій більш придатним для користувачів, які цінують простоту використання та візуалізацію. Python, з іншого боку, пропонує велику гнучкість та контроль для досвідчених користувачів, які володіють програмуванням та хочуть широко налаштовувати свій підхід до моделювання.

За допомогою експертної оцінки (залучалися експерти в галузі ІБ зі стажем не менше 5 років) були виділені відповідні індикатори частково з наведених вище категорій і частково на підставі [102, 114]. У результаті відібрано як поведінкові, так і технічні індикатори, які узагальнені в таблиці 2.3.

Таблиця 2.3 – Індикатори для побудови БМ

№	Категорія індикатора	Опис	Умовні позначення
1	Технічний (TI)	Підозріла транзакція з облікового запису співробітника	(TI_1)
2		Операції, що потрапляють під категорію шахрайських [102, 114]	(TI_2)
3		Невідповідність даних, заявлених співробітником, результатам авдиту	(TI_3)
4		Факти фальшування документів	(TI_4)
1	Поведінковий (BI)	Виявлені проблеми фінансового характеру у співробітника	(BI_1)
2		Підозрілі джерела отримання доходів	(BI_2)
3		Стресовий стан співробітника без видимих причин	(BI_3)

Крім індикаторів, наведених у таблиці 2.3, можна також використовувати вже згадані раніше ознаки, приміром, частоту доступу до конфіденційної інформації; незвичайні мережні патерни; незвичайну активність усередині мережі; аномальну активність на робочому пристрої (встановлення нових програм або зміна системних налаштувань без попереднього повідомлення служб ІБ) та ін.

Для мінімізації кількості інформативних індикаторів для БМ можна використовувати як методи МН, що розглядаються в роботі, так і алгоритми відбору ознак. Ці методи дають можливість автоматично визначити найбільш інформативні ознаки великого набору даних, зменшуючи тим самим розмірність простору ознак і підвищуючи ефективність моделі (див. рис. 2.3).

Гістограма на (рис. 2.3) показує вагомість кожної ознаки для алгоритму відбору ознак в БМ. Кожен стовпець на гістограмі представляє одну ознаку, довжина якої відповідає значенням вагомості цієї ознаки. Чим довше стовпець, тим вагоміша ознака. Гістограма допомагає візуалізувати і порівняти вагомість різних ознак, що може бути корисно в процесі ухвалення рішення про те, які ознаки залишити для подальшого аналізу.

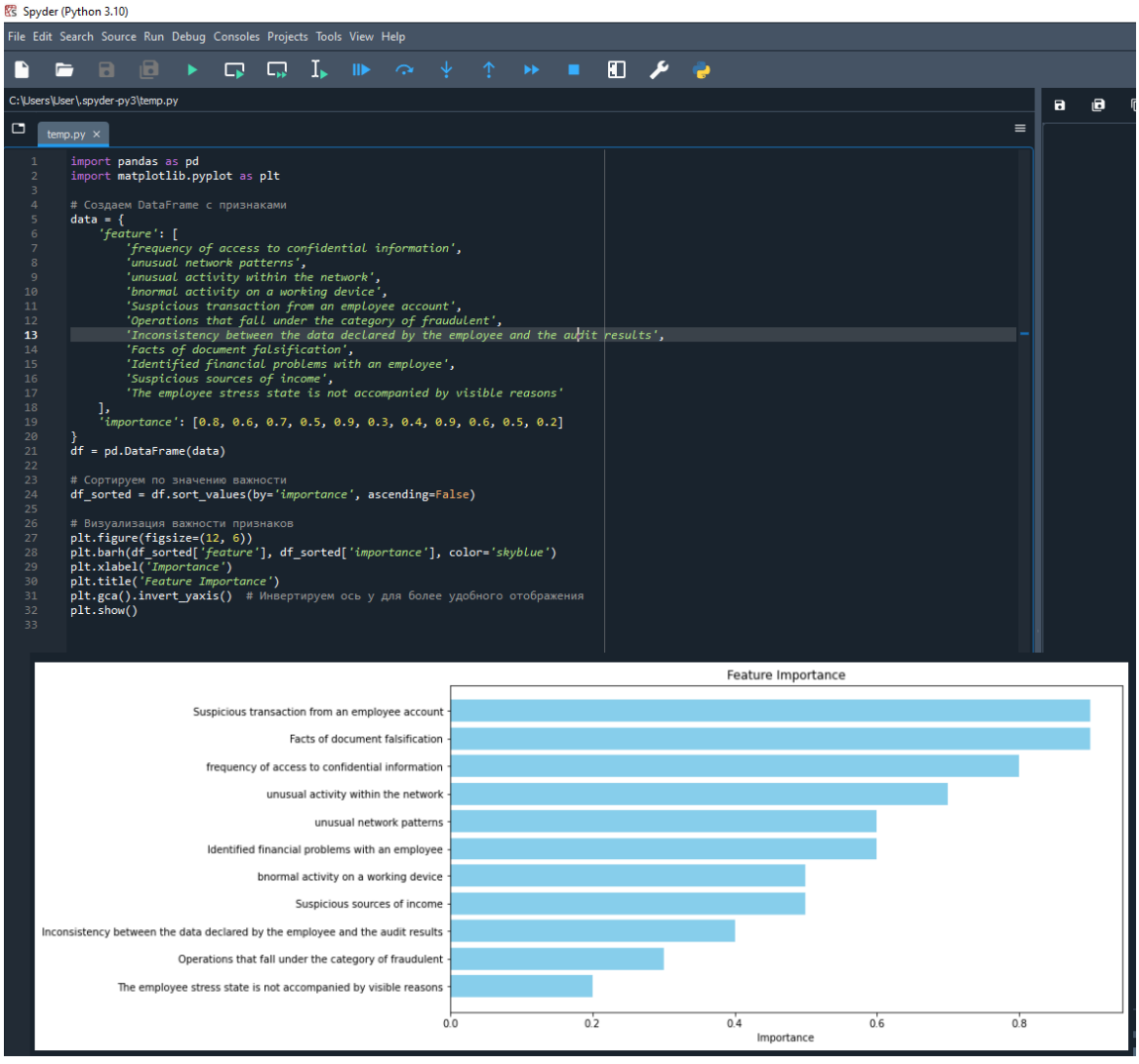


Рис. 2.3 – Реалізація алгоритму відбору ознак

Під час побудови БМ для оцінки шахрайських дій внутрішнього порушника ІБ або інсайдера на керівних посадах компанії, яка використовує хмарні сервіси, краще залишити ті ознаки, котрі не так легко виявити за допомогою DLP і SIEM систем. А саме такі: підозріла транзакція з облікового запису співробітника; операції, що підпадають під категорію шахрайських; невідповідність даних, заявлених співробітником, результатам авдиту; факти фальшування документів; виявлені проблеми фінансового характеру у працівника; підозрілі джерела отримання доходів; стресовий стан співробітника, що не пояснюється видимими причинами.

Ці ознаки є більш специфічними для оцінки поведінки співробітника і є прихованими або менш очевидними, що робить їх більш цінними для виявлення потенційних інсайдерських загроз. Крім того, вони безпосередньо пов'язані з шахрайською діяльністю, на відміну від загальних ознак, таких як незвичайна активність на робочому пристрої, які можуть пояснюватися і не шахрайськими мотивами.

Тому в наступному прикладі розглянемо лише варіант побудови БМ для ситуації можливих шахрайських дій на керівних посадах компанії, що використовує у своїх бізнес-процесах хмарні сервіси (див. рис. 2.4).

На рис. 2.4 вершині, яка позначена (FM), поставимо у відповідність апріорне значення ймовірності того факту, що співробітник належить до категорії керівної посади. Тоді відповідні значення ймовірностей будуть записані так: для $(BI_1 - BI_3) - P(BI_k \mid FM)$; для $(PI_1 - PI_4) - P(TI_k \mid FM)$; де $k, j = 1,2,3,4$ – порядковий номер індикатора у таблиці 2.3.

І як було показано в [145], альтернативна модель у вигляді наївного байєсівського класифікатора також дає змогу з великим ступенем точності вирішити це завдання. Опис батьків вершини дасть можливість врахувати різні

фактори, які можуть впливати на ймовірність невмотивованого порушення правил ІБ співробітником.

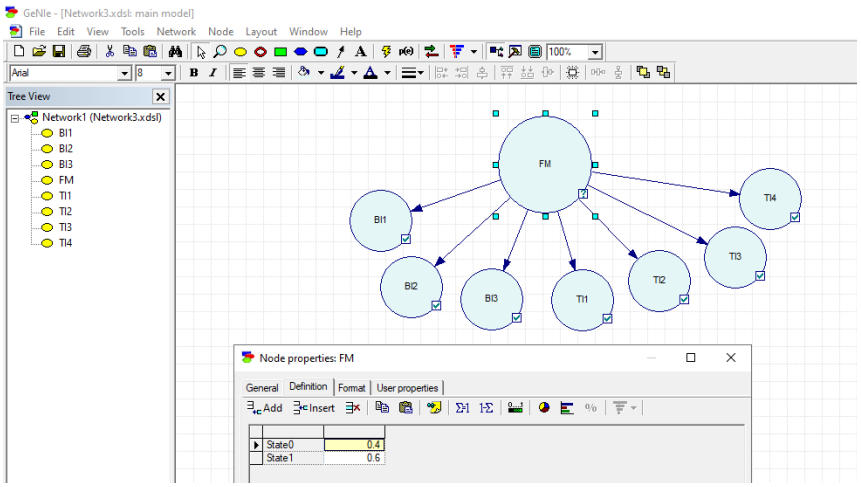


Рис. 2.4 – БМ для ситуації шахрайських дій на керівних посадах компанії

На наступному етапі побудови БМ необхідно заповнити таблиці апріорних ймовірностей (див., рис. 2.5).

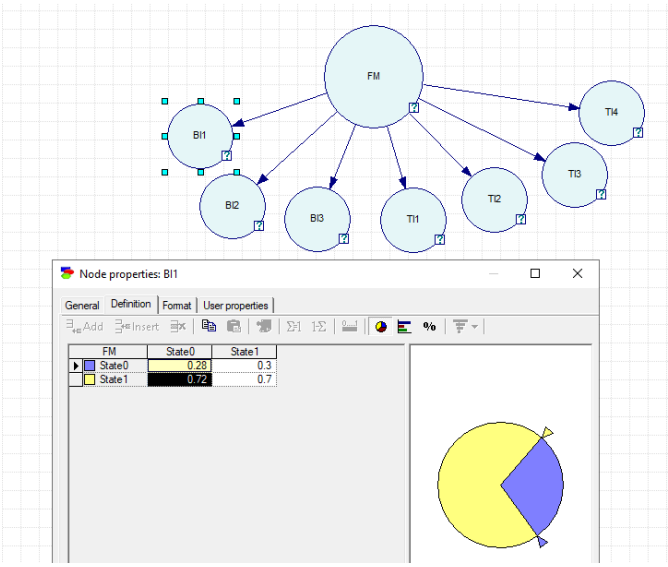


Рис. 2.5 – Заповнення таблиці апріорних ймовірностей БМ для ситуації шахрайських дій на керівних посадах компанії

Для створення БМ, що виявляє шахрайство на керівних посадах у компанії, яка використовує хмарні сервіси у своїх бізнес-процесах, наступним кроком є заповнення таблиці апріорних ймовірностей параметрів БМ, на підставі експертної думки або об'єктивних даних, отриманих від систем DLP, IDS/IPS, SIEM. Після цього проводиться навчання БМ із коригуванням значень ймовірностей. Для початку роботи з БМ необхідно опитати спостерігача (експерта) про виявлені можливим порушником індикатори або зібрати ці дані з об'єктивних засобів – DLP, IDS/IPS, SIEM, як-от, Splunk (див. рис. 2.6).

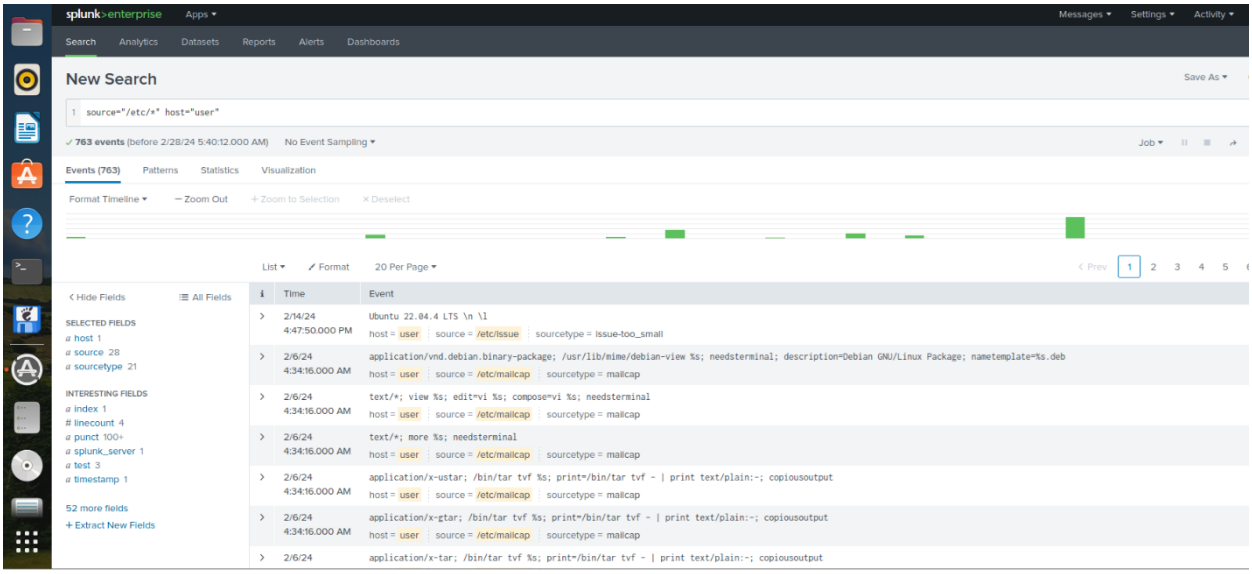


Рис. 2.6 – Збір інформації про дії персоналу в SIEM Splunk

Для отримання інформації про технічні індикатори можна використовувати програмні засоби моніторингу ІБ та протидії шахрайству. Для Amazon це Amazon GuardDuty, AWS Config, AWS WAF, Amazon Macie. Однак зауважимо, що зазначені програмні засоби не гарантують стовідсоткову ІБ під час шахрайських дій співробітників. Деталі таких інцидентів часто є конфіденційною інформацією і, відповідно, не завжди доступні для громадського обговорення. Однак у таблиці 2.4 ми систематизували загальні сценарії, в яких шахраї могли б спробувати обійти засоби забезпечення ІБ від Amazon. Робота з БМ починається з моменту фіксації спостерігачем, скажімо,

співробітником відділу ІБ, одного з індикаторів, наприклад, описаних у таблиці 2.3. Зрозуміло, можна використовувати й інші індикатори, які є в системах контролю роботи персоналу (DLP). Для того, щоб почати роботу з БМ, необхідно опитати спостерігача про виявлені ймовірним порушником індикатори. Потрібно відзначити, що для отримання інформації про технічні індикатори можна використовувати програмні засоби моніторингу ІБ та протидії шахрайству.

Таблиця 2.4 – Загальні сценарії, в яких шахраї могли б спробувати обійти засоби забезпечення ІБ хмарних сервісів (на прикладі Amazon)

№	Засіб	Варіанти дій з боку внутрішнього порушника
1.	Amazon GuardDuty	Зловмисники можуть використовувати методи обфускування для маскування шкідливої активності. Атаки «нульового дня» можуть експлуатувати невідомі вразливості, яких ще не виявлено GuardDuty. ВП можуть використовувати легітимні інструменти та методи для досягнення своєї мети, не викликаючи підозр GuardDuty.
2	AWS Config	Зловмисники можуть отримати доступ до конфігурації AWS-середовища, використовуючи вкрадені облікові дані. ВП можуть змінити конфігурацію щоб уникнути правил безпеки AWS Config. ВП можуть використовувати методи соціальної інженерії, щоб обдурити користувачів із правами доступу до AWS Config.
3	Amazon Macie	Зловмисники можуть використовувати методи шифрування для приховування конфіденційних даних. Вони можуть використовувати методи стеганографії для приховування конфіденційних даних у зображеннях чи інших файлах. Зловмисники можуть використовувати легітимні методи передачі конфіденційних даних, не викликаючи підозр Amazon Macie.

Поведінкові індикатори можна визначити у вигляді спостереження. Наприклад, співробітник відділу ІБ зафіксував фінансові поведінкові індикатори, рядок 1 у таблиці 2.2 для TI і рядок 1 у таблиці 2.3 для BI. Це відповідає такому запису:

$$TI_1 = BI_1 = True;\ BI_2 = BI_3 = TI_2 = TI_3 = TI_4 = False.$$

У цьому випадку ймовірність того, що співробітник віднесений до внутрішнього порушника, можна обчислити, скориставшись виразом:

$$P(FM \mid BI_1,\ldots,BI_3,TI_1,\ldots,TI_4) = \\ = \frac{P(BI_1 \mid FM)\cdot\ldots\cdot P(BI_3 \mid FM)}{Z}\cdot \\ \frac{P(TI_1 \mid FM)\cdot\ldots\cdot P(TI_4 \mid FM)}{Z}, \tag{2.7}$$

де $\prod_{i,j=1}^{i=3,j=4} P(BI_i \mid FM)\cdot P(TI_j \mid FM)\cdot P(FM) + \\ + \prod_{i,j=1}^{i=3,j=4} P(BI_i \mid \overline{FM})\cdot P(TI_j \mid \overline{FM})\cdot P(\overline{FM})$.

Для навчання нашої БМ потрібен синтетичний набір даних, який містить інформацію про різні ознаки та цільову змінну (порушення ІБ). Структура зазначеного набору даних може бути такою відповідно до таблиці 2.3 (розглядаємо найпростіший варіант):

Ознаки (Features): Підозріла транзакція з облікового запису співробітника (бінарна ознака: 0 – ні, 1 – так);

Операції, що потрапляють під категорію шахрайських (бінарна ознака: 0 – ні, 1 – так);

Невідповідність даних, заявлених співробітником, результатам авдиту (бінарна ознака: 0 – ні, 1 – так);

Факти фальсифікації документів (бінарна ознака: 0 – ні, 1 – так);

Виявлені проблеми фінансового характеру у співробітника (бінарна ознака: 0 – ні, 1 – так);

Підозрілі джерела отримання доходів (бінарна ознака: 0 – ні, 1 – так);

Стресовий стан співробітника не пояснюється видимими причинами (бінарна ознака: 0 – ні, 1 – так).

Цільова змінна (Target): Порушення інформаційної безпеки (бінарна ознака: 0 – ні, 1 – так).

Зауважимо, що в будь-якій великій компанії служба ІБ може використовувати різні методи та інструменти для виявлення підозрілих транзакцій співробітника або його фінансових проблем. Якщо говорити про

Amazon (як приклад), то служба ІБ компанії може використовувати засоби моніторингу та аналітики для аналізу фінансових транзакцій співробітників. Наприклад, несподівані перекази коштів або незвичайні витрати з облікового запису співробітника вказують на фінансові проблеми або підозрілі активності. Взаємодія з фінансовими відділами компанії також у більшості випадків допомагає оперативно виявляти фінансові проблеми співробітників, такі як неоплачені рахунки або заборгованості, які пов'язані з несумлінною діяльністю.

Для імплементації навчального набору даних у коді Python скористаємося бібліотекою pandas для роботи з даними та створення датафрейму. Нижче наведено приклад коду, який створює датафрейм на основі запропонованого в даному параграфі набору даних.

```
import pandas as pd

# Створення набору даних
data = {
    'Підозріла_транзакція': [1, 0, 0, 1],
    'Шахрайські_операції': [0, 1, 0, 1],
    'Невідповідність_даних': [1, 0, 1, 0],
    'Факти_фальсифікації_документів': [0, 1, 0, 0],
    'Проблеми_фінансового_характеру': [0, 1, 1, 1],
    'Підозрілі_джерела_доходів': [0, 1, 1, 0],
    'Стресовий_стан': [1, 0, 1, 0],
    'Порушення_ІБ': [1, 1, 0, 1]}

# Створення датафрейму
df = pd.DataFrame(data)

# Виведення на екран
print(df)
```

Цей код створює датафрейм df із заданими ознаками та цільовою змінною. Відповідно, офіцер ІБ може використовувати цей чи інший датафрейм для навчання мережі Байєса або інших моделей машинного навчання.

Тоді отримаємо таку гістограму (див. рис. 2.7). На гістограмі блакитні стовпці становлять ймовірність події «True» (справжнє), а помаранчевий

стовпець – ймовірність події «False» (хибне). У цьому контексті «True» може означати, що співробітник пов'язаний з певним фактором (підозрілою транзакцією), а «False» – що він не пов'язаний із цим фактором. Ширина стовпців відображає можливість кожної події. Чим ширший стовпець, тим вища ймовірність цієї події.

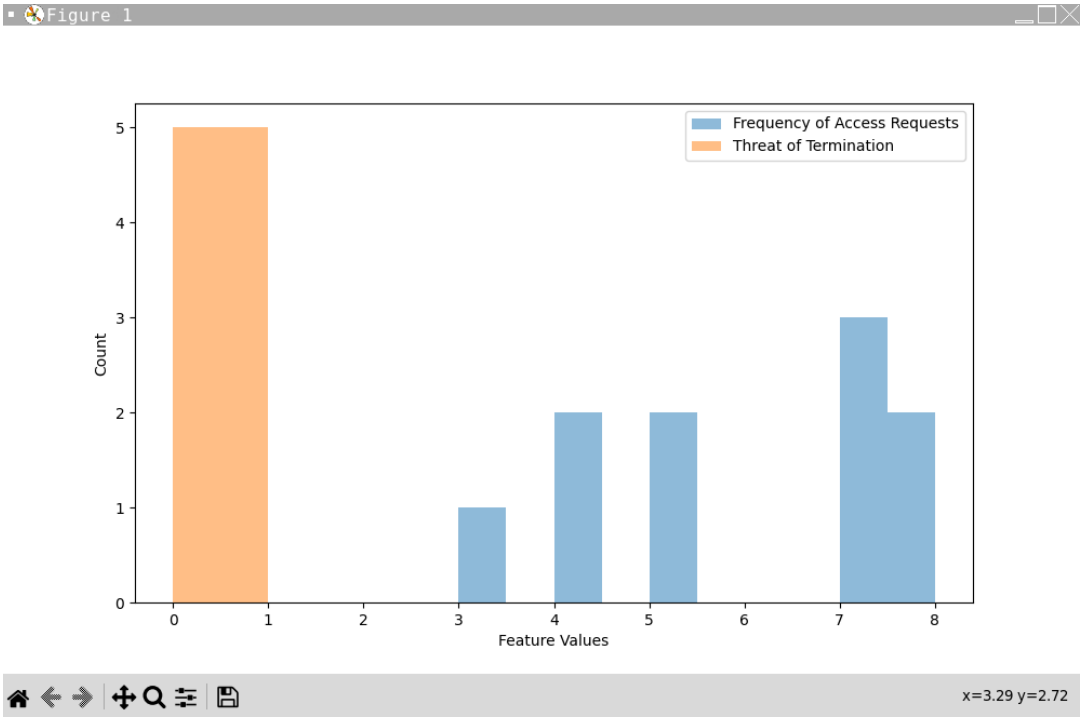


Рис. 2.7 – Візуалізація роботи БМ для ситуації шахрайських дій на керівних посадах компанії

Якщо блакитний стовпець ширший, це означає, що ймовірність події «True» вище, ніж ймовірність події «False». З гістограми можна зробити висновки про те, які фактори більш ймовірно пов'язані зі співробітником, якщо він є потенційно внутрішнім порушником та/або інсайдером. Якщо блакитний стовпець для «Підозрілої транзакції (TI_1)» ширше, це може свідчити, що співробітник схильний до таких транзакцій. Для поліпшення за допомогою БМ моделювання поведінки внутрішнього порушника та/або інсайдера служба ІБ може використовувати конкретні дані у форматі цифрових слідів, застосовуючи для цього, як-от, DLP, SIEM та інше ПЗ.

Для вершини (TI_4) «Факти фальсифікації документів» цифрові сліди (ЦС) містять такі дані: логи доступу до документів або хмарних сервісів, що

показують несанкціонований доступ або зміну документів; історія змін у документах, яка може свідчити про фальсифікацію; авдиторські звіти або відгуки, що виявляють невідповідності в документах або їхню справжність.

Ці ЦС використовують для розрахунку апостеріорної ймовірності фактів фальшування документів. Якщо збільшується кількість невідповідностей в авдиторських звітах, а також НСД до документів, це може збільшити ймовірність фальсифікації документів. Подібні факти можливо виявити за допомогою вже згаданих DLP або DFT (Digital Forensics Tools – інструментів для аналізу метаданих та вмісту документів, щоб виявити зміни або фальсифікацію), DMS (Document Management Systems – систем керування документами) тощо.

Припустимо, у нас є такі дані: P (Факти фальсифікації документів = True | Керівна посада = True) = 0.1 P (Факти фальсифікації документів = False | Керівна посада = True) = 0.9. У результаті моделювання отримаємо загальний вигляд БМ (див. рис. 2.8 та гістограму, див. рис. 2.9).

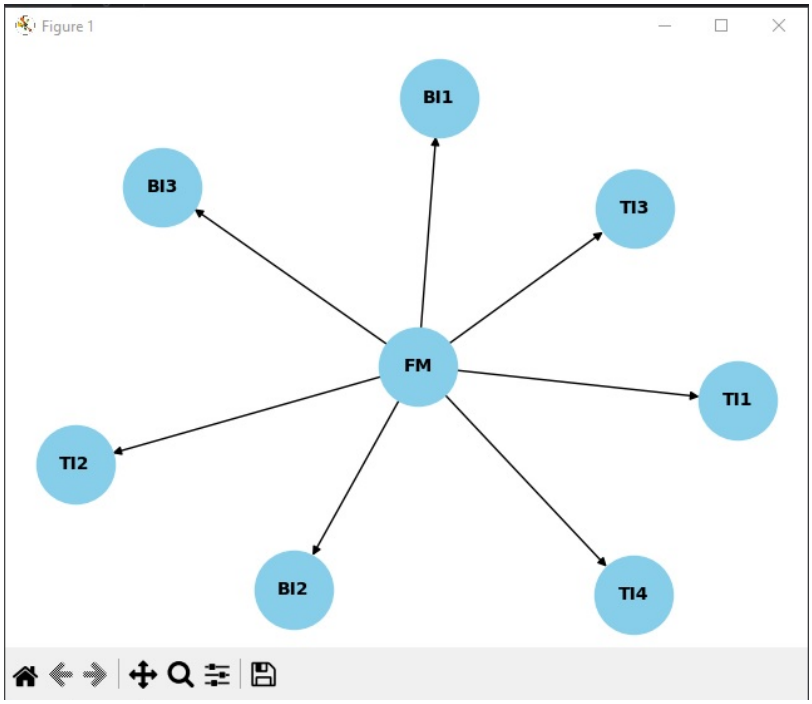


Рис. 2.8 – БМ, що моделює загрозу шахрайства особи, яка перебуває на керівній посаді в компанії, що використовує хмарні сервіси

Треба розуміти, що це лише модель, і ймовірності налаштовують залежно від конкретної ситуації. Гістограма, яку представлено на рис. 2.9, допоможе офіцеру служби ІБ візуалізувати ці ймовірності і робити висновки на підставі наявних даних.

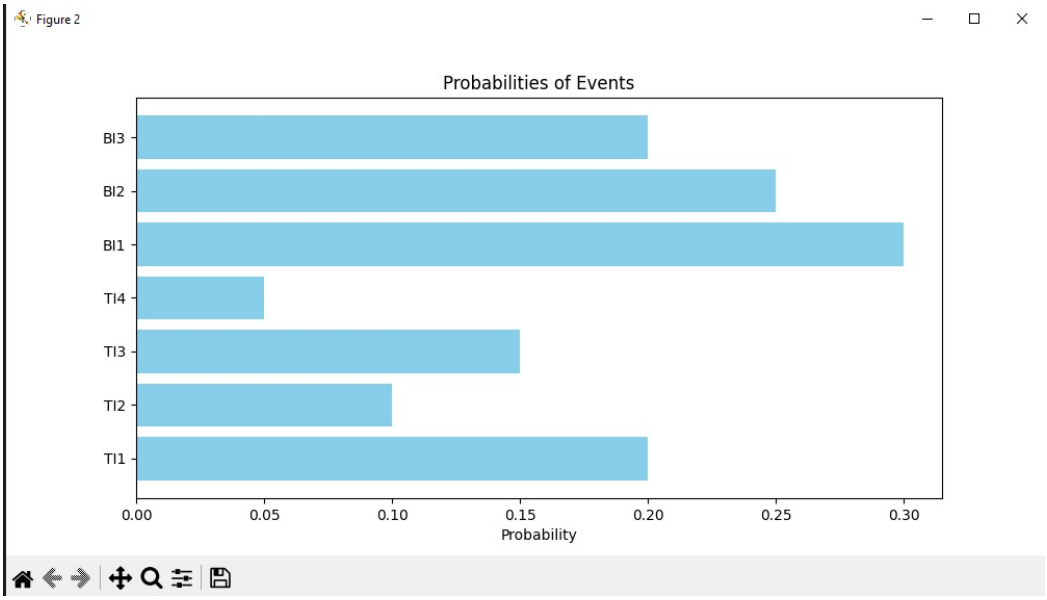


Рис. 2.9 – Результати візуалізації роботи БМ, що моделює загрозу шахрайства особи, яка перебуває на керівній посаді в компанії, що використовує хмарні сервіси

Гістограма, яку показано на рис. 2.9, є стовпчастою діаграмою, де кожен горизонтальний стовпець відповідає певній події. Вісь абсцис показує ймовірність різних подій (вершин графа, показаного на рис. 2.7). Вісь ординат позначає самі вершини (події), які ми розглядали у таблиці 2.3. Висота кожного стовпця відповідає ймовірності цієї події. Так ймовірність становить $(TI_1 = 0.2)$. Це означає, що подія (TI_1) відбувається із ймовірністю 20%. І так далі. Подія $(TI_4 = 0{,}05)$ має найменшу ймовірність (5%). Гістограма дає можливість наочно порівняти ймовірність різних подій.

Під час використання цієї або іншої БМ для виявлення внутрішнього порушника та/або інсайдера цифрові сліди враховуються у вигляді апріорної та апостеріорної ймовірності подій. Якщо є цифрові сліди, що свідчать про

факти фальсифікації документів, можна використовувати ці дані для уточнення ймовірності такої події в БМ.

Служба інформаційної безпеки (СІБ) компанії, яка використовує хмарні сервіси, відстежує цифрові сліди, що свідчать про порушення політики ІБ, наприклад, фальсифікації документів особою, котра перебуває на керівній посаді, під час роботи з хмарним сервісом Amazon. Для цього використовується аналіз метаданих (див., рис. 2.10).

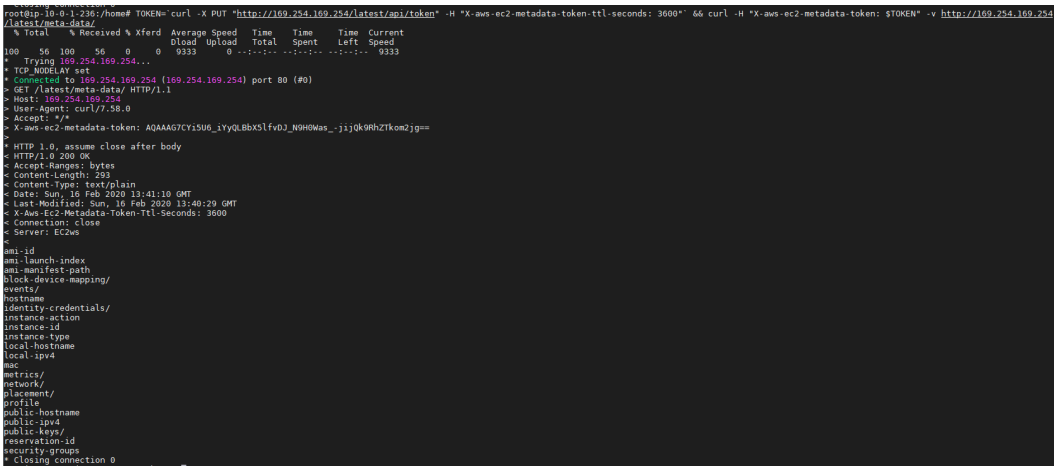


Рис. 2.10 – Аналізу метаданих під час роботи хмарного сервісу Amazon

Подібний аналіз або за допомогою корпоративних сервісів, або за допомогою DLP допомагає зібрати необхідну інформацію про ЦС, наприклад, таку: дата і час створення, зміни та доступу до документів; використовувані пристрої та IP-адреси; збережені версії документів та ін. Крім того, врахувати апріорну та апостеріорну ймовірності подій пов'язаних з вершиною (TI_4), можна використовуючи засоби аналізу змісту документів, що дають можливість: виявляти протиріччя у датах, цифрах чи фактах; невідповідність стилістики чи формату документа; факти використання підроблених підписів або печаток тощо (див. таблицю 2.5).

Більшу частину подібної інформації про цифрові сліди надають системи DLP, однак завдання з вивчення цифрових слідів користувачів, що працюють з хмарними сервісами, не входило до переліку завдань, які вирішуються в межах даного дисертаційного дослідження.

Таблиця 2.5 – Порівняльний аналіз програмних продуктів, що використовуються для виявлення фактів шахрайства під час роботи з документами, зокрема, осіб, які перебувають на керівних посадах (складено автором на підставі аналізу літературних джерел [146-149]).

Назва ПП	Переваги	Недоліки
IBM Watson for Document Analysis	Потужний інструмент для аналізу документів, здатний виявляти патерни та аномалії у поведінці співробітників	Потребує складного налаштування та інтеграції з іншими системами для повного використання у хмарних сервісах
Google Cloud Natural Language API	Має хорошу підтримку для аналізу природної мови	Може бути обмежений у можливості точного виявлення фальшування документів без додаткового налаштування
Amazon Comprehend	Має інтеграцію з іншими сервісами AWS, що полегшує використання у хмарному середовищі	Може бути менш точним у визначенні фальсифікації документів порівняно з більш спеціалізованими інструментами, наведеними в цій таблиці
Nuix	Потужний інструмент для цифрового аналізу, аналізу документів та медіафайлів	Потребує високої кваліфікації для ефективного використання, складний у налаштуванні
X-Ways Forensics и Magnet Forensics	Спеціалізовані інструменти для цифрового слідства, здатні обробляти різні типи доказів, пов'язаних із фальсифікацією документів	Є надмірними для простих завдань аналізу документів, які потребують додаткової експертизи для ефективного використання; значна вартість

Якщо врахувати у коді варіант використання цифрового сліду, для вершини «Факт фальшування документів», тобто (TI_4), то отримаємо такий результат (див. рис. 2.11). Відповідно, маємо таку інформацію:

Співробітник А – апріорна ймовірність того, що він на керівній посаді, 0.1. Факт фальшування документів – виявлений (за цифровим слідом на підставі даних, отриманих від Amazon Comprehend).

Співробітник В – апріорна ймовірність того, що він на керівній посаді, 0.3. Факт фальшування документів – не виявлений (Amazon Comprehend не зафіксувала інциденту, пов'язаного з фальсифікацією документів).

Співробітник С – апріорна ймовірність того, що він на керівній посаді, 0.5. Факт фальсифікації документів – виявлено (за цифровим слідом).

На гістограмі, показаній на рис. 2.11, можна побачити різницю між ситуацією, коли факт фальшування не був виявлений (як у співробітника В) і коли він був виявлений (як у співробітників А і С), спираючись на цифровий слід. Гістограма показує, що використання цифрового сліду допомогло точніше виявити факти фальсифікації документів.

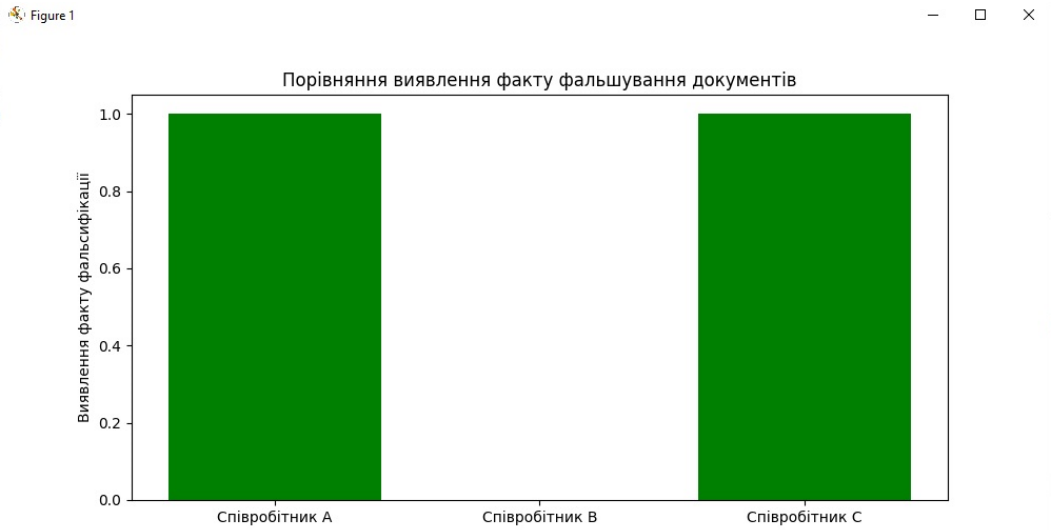


Рис. 2.11 – Гістограма апостеріорної та апріорної ймовірності в БМ уточнені на підставі цифрового сліду

Поведінкові індикатори можна виявити шляхом спостереження та/або за допомогою вже багаторазово згаданих у цьому розділі систем DLP, IPS/IDS, SIEM тощо. Якщо були помічені лише фінансові проблеми та підозрілі транзакції, то значення змінних будуть наступними, для врахування такої залежності ми можемо визначити таку структуру вершин-батьків:

```
parents = {
    'vi': ['access_frequency', 'privilege_level', 'previous_violations'],
    'access_frequency': [],
    'privilege_level': [],
    'previous_violations': []
}
```

Цей фрагмент коду описує ситуацію, коли вершина залежить від трьох факторів: Частоти доступу до захищених даних (access_frequency); Рівня

привілеїв у системі (privilege_level); Історії попередніх порушень (previous_violations).

Кожен із цих чинників може вплинути на ймовірність невмотивованого порушення правил ІБ під час роботи з хмарними сервісами.

БМ є модель для опису ймовірнісних зв'язків між подіями, а також відсутності таких зв'язків. У розглянутій моделі зв'язок $(A \to B)$ від події (A) до події (B) вважається причинним, якщо подія (A) впливає на виникнення події (B) та визначає її значення. Для визначення ймовірності приналежності співробітника до певного класу внутрішніх порушників ІБ можна використовувати БМ кожного класу. Перевагами застосування БМ є простота побудови та інтерпретації, можливість роботи з неточними і неповними даними, а також можливість навчання в процесі роботи з низькими обчислювальними витратами. Входами кожної БМ будуть індикатори, які свідчать про потенційні порушення ІБ хмарних сервісів, що проявляються потенційним внутрішнім порушником. Виходом кожної БМ є можливість приналежності співробітника до певного класу внутрішніх порушників.

Заповнення таблиць виконується на підставі спеціалізованих ПП, таких як IDS, DLP, SIEM, ACS-систем та інших, або за допомогою експертів, як внутрішніх, приміром, співробітників ІБ компанії, так і зовнішніх (авдитори ІБ). Коли всі таблиці заповнені, виконується навчання БМ і за потреби коригуються отримані значення ймовірностей.

Отже, відносно нескладна БМ для виявлення внутрішніх порушників ІБ чи інсайдерів у компаніях, що використовують хмарні сервіси, доводить принципову можливість використання математичного апарату БМ для поліпшення методів забезпечення ІБ. Така БМ допоможе системі інформаційної безпеки: якісніше оцінювати ризики ІБ, оскільки БМ дає змогу оцінювати ймовірність різних подій і порушень ІБ на підставі наявної інформації, зокрема, отриманої за результатами аналізу цифрового сліду; ухвалювати більш аргументовані рішення, оскільки аналіз ймовірностей у БМ

допоможе, спираючись на фактичні дані та апріорні знання, аналізувати причинно-наслідкові зв'язки, які створюють проблеми для ІБ з боку внутрішніх порушників або інсайдерів; поліпшувати процеси забезпечення ІБ, оскільки БМ може оптимізувати контрольні заходи чи виділення ресурсів з урахуванням оцінки ризиків ІБ. БМ може бути легко модифікована й адаптована до умов, які змінюються, і нових загроз, що робить її ефективним інструментом для забезпечення ІБ в такому середовищі, як хмарний сервіс.

Синтез складнішої мережі, що враховує взаємозв'язки різних факторів, також має великий потенціал для поліпшення методів забезпечення ІБ хмарних сервісів (див. рис. 2.12), (мережа ненавчена). Така мережа, яка далі розглядається в межах третього розділу дисертації, може допомогти виявляти більш складні візерунки та взаємозв'язки між різними подіями, що підвищить ефективність і точність виявлення потенційних загроз ІБ в хмарних сервісах з боку внутрішніх порушників. Однак для цього потрібні додаткове дослідження та розробка моделей, а також велика база даних для навчання й аналізу.

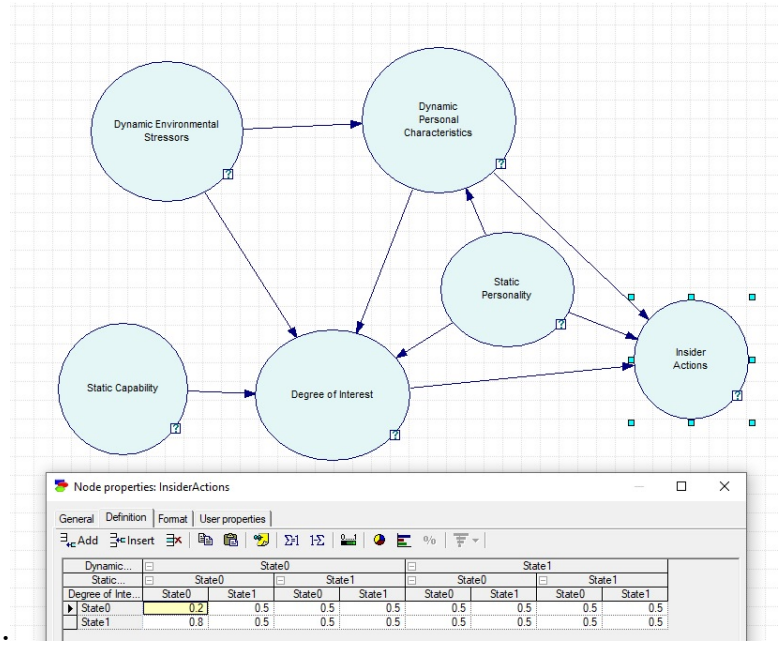


Рис. 2.12 – Концептуальний вигляд БМ, яка враховує поведінкові аспекти внутрішнього порушника ІБ (або інсайдера)

Представлена концептуальна модель БМ (рис. 2.12) описує різні категорії змінних, які, розглянуто під час подальших досліджень. Ці категорії містять динамічні й статичні стресори навколишнього середовища, особисті характеристики співробітника, а також фактори, пов'язані з інсайдерськими діями на робочому місці, такі як контрпродуктивна поведінка і ступінь зацікавленості в реалізації інсайдерської атаки. Вважаємо, що динамічні стресори навколишнього середовища для співробітника компанії можуть містити тимчасові фактори, приміром, зміни в робочих процесах або несподівані події, які впливають на його емоційний стан та працездатність. Також це термінові завдання, зміни в проєктах або несподівані проблеми з хмарною інфраструктурою.

Статичні стресори навколишнього середовища містять постійні фактори, які впливають на співробітника протягом тривалого часу. Це високі вимоги до роботи, невизначеність у кар'єрному зростанні або конфліктні ситуації на робочому місці. Обидва типи стресорів суттєво впливають на емоційний стан співробітника та його здатність ефективно працювати з хмарними сервісами та іншими бізнес-процесами. Однак для реального застосування така модель потребує валідації, щоб переконатися в її ефективності й точності передбачень.

Для навчання показаної на рис. 2.12, подібної або більш складної БМ з використанням методів МН можна застосувати підходи, засновані на статистичному аналізі даних. Однак для цього знадобиться як мінімум синтетичний набір даних. Зібрати конкретні дані щодо інцидентів ІБ, пов'язаних із порушенням ІБ внутрішніми порушниками, досить складно, оскільки більшість компаній таку інформацію не оприлюднює, і вона вважається конфіденційною. Створення синтетичного набору даних дасть можливість змоделювати різні сценарії інцидентів ІБ, які виникають в компаніях, що використовують хмарні сервіси. Цей набір даних може містити різні параметри, такі як тип інциденту, дії внутрішнього порушника, використовувані методи атаки, а також різні фактори, що впливають на

ймовірність виникнення інциденту, такі як посада співробітника, його поведінка, доступ до інформації і т. д. За допомогою синтетичного набору даних можна навчити мережу Байєса та провести аналіз її ефективності у виявленні потенційних загроз від внутрішніх порушників.

Тому в третьому розділі ми пропонуємо використовувати синтетичні дані, які будуть містити інформацію про різні події або характеристики, пов'язані з внутрішніми порушниками ІБ. Більш детально ці питання розглянуто у третьому, кінцевому розділі дисертації.

Під час розробки загальних алгоритмів контролю дій внутрішніх порушників інформаційної безпеки та/або інсайдерів у компаніях, включно з тими, чиї бізнес-процеси базуються на хмарних сервісах, необхідно враховувати витрати, пов'язані з проведенням такого контролю (йдеться про витрати часу, матеріальних ресурсів, фінансів). У роботі [150] показано, що існує нижній поріг інтенсивності передбачення, наприклад, несанкціонованого доступу до ресурсів об'єкта інформаційної діяльності. Автори роблять висновок, що прогнозування несанкціонованого доступу може бути ефективним для головних обчислювальних вузлів (у нашому випадку вузлів хмарних сервісів), тобто екземплярів з чітко вираженими безперервними властивостями, що містять значну кількість компонентів, процеси яких відрізняються сильною взаємообумовленістю.

Вузол хмарного сервісу зазвичай належить до віртуального або фізичного обчислювального ресурсу, що надається клієнту для виконання завдань чи обробки даних у хмарі. Вузол може бути представлений у вигляді віртуальної машини, контейнера або іншої форми обчислювальної одиниці, яка може бути запущена, керована та масштабована у хмарі, тобто екземпляром. Коло найважливіших питань, пов'язаних із проблемою прогнозу несанкціонованого доступу зовнішнього порушника до екземплярів хмарного сервісу, досить велике. Вичерпне дослідження всіх цих питань є доцільним у межах окремої дисертаційної роботи. Тому не всі перелічені проблеми розглянуті в цьому розділі однаково. Більше того, деякі питання взагалі не

будуть порушені у цій роботі. Однак, у наступному розділі дисертації вважаємо за доцільне зупинитися на розвитку моделей пошуку оптимальних послідовних байєсівських правил під час прогнозування несанкціонованого доступу внутрішніх порушників до екземплярів хмарних сервісів у компанії.

Висновки за розділом 2

У другому розділі роботи отримано наступні основні результати та зроблено такі висновки.

Показано, що внутрішні атаки становлять для організацій постійно зростаючу загрозу, адже співробітники-шахраї та/або інсайдери, котрі мають законний доступ до комп'ютерних систем, у тому числі до хмарних сервісів, які використовуються у бізнес-процесах компанії, а також володіючи інформацією про політику інформаційної безпеки (ІБ) в організації, можуть уникнути виявлення.

Встановлено, що незважаючи на великий арсенал технічних систем для виявлення внутрішніх порушників інформаційної безпеки, зокрема, таких як IDS, DLP, SIEM, ACS-системи, організації, як і раніше, недостатньо готові до виявлення, стримування та пом'якшення складних внутрішніх, у тому числі інсайдерських атак, тому що їхні методи ІБ адаптовані до переважно зовнішніх загроз.

Отримав подальший розвиток метод раннього виявлення інсайдерів в організаціях, що використовують хмарні сервіси, заснований на використанні мережі Байєса. Цей метод враховує технічні та поведінкові категорії індикаторів під час виявлення шахрайських дій співробітника, який обіймає керівну посаду компанії, що використовує у своїх бізнес-процесах хмарні сервіси.

Вперше запропоновано модель мережі Байєса, яка може бути корисною службі інформаційної безпеки під час виявлення внутрішніх порушників і яка відрізняється від аналогічних рішень тим, що в ній врахована загроза шахрайства особи, яка перебуває на керівній посаді в компанії, що

використовує хмарні сервіси, а в завданні апріорних та апостеріорних ймовірностей подій, пов'язаних із відібраними індикаторами, беруться до уваги цифрові сліди, що залишаються співробітником під час роботи з комп'ютерними системами компанії.

Виконано програмну реалізацію запропонованої моделі мережі Байєса, яка для синтетичного набору даних показала свою працездатність, це дає можливість говорити про те, що вона може бути імплементована до структури контурів інформаційної безпеки компанії.

Показано, що навіть відносно нескладна мережа Байєса для виявлення внутрішніх порушників інформаційної безпеки або інсайдерів у компаніях, які використовують хмарні сервіси, доводить принципову можливість використання математичного апарату БМ для поліпшення методів забезпечення ІБ. Обґрунтовано, у наступному розділі роботи доцільно зупинитися на розвитку моделей пошуку оптимальних послідовних байєсівських правил під час прогнозування НСД внутрішніх порушників до екземплярів хмарних сервісів у компанії.

Обґрунтовано, що синтез складнішої мережі, яка враховує взаємозв'язки різних факторів, також має великий потенціал для поліпшення методів забезпечення інформаційної безпеки хмарних сервісів. Однак для цього потрібні додаткове дослідження та розробка моделей, а також велика база даних для навчання й аналізу.

РОЗДІЛ 3.
ПОСЛІДОВНІ БАЙЄСІВСЬКІ ПРАВИЛА ДЛЯ ПРОГНОЗУВАННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ВНУТРІШНЬОГО ПОРУШНИКА АБО ІНСАЙДЕРА ДО ХМАРНИХ СЕРВІСІВ КОМПАНІЇ

У заключному розділі дисертаційного дослідження ми представимо результати, пов’язані з вирішенням завдання прогнозування несанкціонованого доступу (НСД) з боку внутрішніх порушників та/або інсайдерів до хмарних сервісів, які використовуються компаніями для своїх бізнес-процесів. У цьому розділі ми описуємо оптимальні послідовні правила для досягнення цієї мети, ґрунтуючись на ідеї порівняння апостеріорної ймовірності гіпотези зі змінним порогом під час перевірки багатоальтернативних гіпотез (приміром, щодо наявності порушення політики інформаційної безпеки – ПІБ або виявлення інсайдера).

У випадку оптимальних послідовних байєсівських правил для прогнозування несанкціонованого доступу з боку внутрішнього порушника та/або інсайдера до хмарних сервісів критерієм оптимальності може слугувати мінімізація апостеріорного ризику під час прийняття рішення. Тобто правила для мережі Байєса повинні бути побудовані так, щоб за наявності НСД ймовірність прийняття правильного рішення (виявлення порушення) була максимальною, а ризик помилки (хибного спрацювання) – мінімальним. Тоді граничні умови можуть включати, наприклад, імовірність хибного спрацювання, коли необхідно мінімізувати ймовірність помилкового виявлення несанкціонованого доступу за його відсутності, а також імовірність пропуску виявлення дій внутрішнього порушника, коли потрібно мінімізувати ймовірність невиявлення НСД за його наявності. Окрім того, необхідно враховувати ціну хибних спрацювань і пропусків виявлення, оскільки вони є різними й матють різні наслідки для компанії. Варто зауважити, що різні кроки прийняття рішення можуть мати різну важливість, і це також слід враховувати під час визначення оптимальних правил. Для успішного вирішення завдання

необхідно знайти явне вираження для межі, яка залежить від розподілу ймовірностей спостережень. Коли гіпотези істотно віддалені одна від одної, оптимальне послідовне вирішальне правило полягає у виборі на кожному кроці номера гіпотези з максимальною апостеріорною ймовірністю та порівнянні її з випадковим порогом. Можна стверджувати, що оптимальні послідовні байєсівські правила будуються так, щоб досягти балансу між точністю виявлення дій внутрішнього порушника, ціною помилок та іншими факторами, з урахуванням специфіки завдання прогнозування несанкціонованого доступу в хмарних сервісах. У завершальному розділі роботи ми проаналізуємо проблему прогнозування несанкціонованого доступу з боку внутрішніх порушників до хмарних сервісів, що використовуються компанією, і запропонуємо модель оптимального послідовного вирішального правила, яка базується на виборі на кожному кроці гіпотези з максимальною апостеріорною ймовірністю та її порівнянні з випадковим порогом.

3.1. Стратегія перевірки гіпотез і мінімізації ризику неправильного визначення внутрішнього порушника або інсайдера під час роботи з хмарними сервісами

Оптимальні послідовні байєсівські правила (БП) є математичним інструментом, який можна використовувати для прогнозування несанкціонованого доступу з боку внутрішніх порушників до хмарних сервісів компаній. Ці правила ґрунтуються на байєсівській статистиці та являють собою послідовність рішень, що ухвалюються на кожному кроці на підставі наявної інформації про попередні події або кіберінциденти. Згідно із [150, 151, 152], оптимальні послідовні БП можуть застосовуватись для аналізу різних ознак та індикаторів, які можуть свідчити про можливе порушення безпеки.

На кожному етапі алгоритму оптимальні послідовні БП дають змогу аналітику з кібербезпеки компанії оцінити ймовірність того, що спостережувані ознаки відповідають нормальній поведінці або ж вказують на

присутність несанкціонованого доступу. БП можуть враховувати різноманітні чинники, такі як попередні аномалії, динаміка зміни ознак тощо, це робить їх ефективним інструментом для прогнозування й запобігання несанкціонованому доступу в межах хмарних сервісів. Опишемо загальний метод послідовної перевірки гіпотез, який можна застосовувати для вирішення завдання з виявлення внутрішнього порушника або інсайдера під час роботи з хмарними сервісами компанії. Існують інформативні параметри $(\theta_m, m = 1,2,...)$, які можуть являти собою різні характеристики або дії. Ці інформативні параметри можуть вказувати на наявність або відсутність порушення безпеки. Наприклад, це вже раніше згадані в другому розділі роботи нетипові мережні патерни, виявлення яких може свідчити про спроби несанкціонованого доступу, або ж аномальна активність на робочому пристрої, виявлення якої також може вказувати на компрометацію пристрою.

Спостереження $(x_n, n = \overline{1,N})$ характеризуються різними ознаками або подіями, які можна спостерігати в межах використання хмарних сервісів, наприклад, нетипова активність співробітника під час роботи з конфігураційним файлом хмарного сервісу (для AWS конфігураційний файл може бути представлений у форматі JSON або YAML). Прості гіпотези за вектором спостереження $(x_n, n = \overline{1,N})$ означають, що розглянуті гіпотези щодо стану хмарної системи – наприклад, порушення безпеки або його відсутність –ґрунтуються на спостережуваних ознаках, представлених у вигляді вектора. Кожна компонента цього вектора відображає окремі характеристики або параметри, такі як частота доступу, мережні патерни, активність усередині мережі та інші, згадані раніше. Для формалізації цього викладу опишемо невеликий фрагмент на Python, у якому створимо клас (або структуру) даних, що представляє вектор спостереження.

```
class SecurityObservationVector:
    def __init__(self, access_frequency, network_patterns, internal_activity, device_activity, ...):
        self.access_frequency = access_frequency
        self.network_patterns = network_patterns
        self.internal_activity = internal_activity
        self.device_activity = device_activity
        ...

# ------
observation = SecurityObservationVector(
    access_frequency=5,
    network_patterns=[1, 0, 1, 1, 0],
    internal_activity=3,
    device_activity=2,
    ..
)
```

У цьому прикладі для ілюстрації як вектор спостереження $\left(x_n, n=\overline{1,N}\right)$ розглянуто чотири ознаки: частота доступу до конфіденційної інформації; нетипові мережні патерни (незвично високий трафік або підозрілі запити, тощо); нетипова активність усередині мережі, до прикладу, неочікувані запити на доступ до ресурсів або файлів; аномальна активність на робочому пристрої співробітника (незвичні спроби доступу до даних, запити на зміну конфігураційного файлу хмарного сервісу або встановлення несанкціонованого програмного забезпечення, тощо).

Такий підхід дає можливість описати стан системи через набір ознак і проаналізувати його на підставі цих або ширшого кола параметрів. При цьому перевірка гіпотези щодо стану системи здійснюється шляхом порівняння апостеріорної ймовірності відповідної гіпотези зі змінним порогом, який залежить від апостеріорних ймовірностей інших гіпотез [150-153].

Гіпотези $\left(H_i : \theta = i, i = \overline{0, M-1}\right)$ пов'язані з різними сценаріями або припущеннями щодо наявності порушення безпеки хмарного сервісу.

Втрати $\left(g_{ij}(n)\right)$ при $\left(\theta = i, u_n = j, i, j = \overline{0, M-1}\right)$ можуть являти собою шкоду, якої може зазнати компанія у разі порушення безпеки. Апостеріорний ризик

(АР) пов’язаний із ймовірністю прийняття неправильного рішення на кожному етапі $(n-ом)$ кроці рішення $(u_n = j)$.

Тоді, якщо припустити, що ми спостерігаємо за інформативними параметрами $(\theta_m, m = 1,2,...)$, що приймають кінцеву кількість значень $(0,1,...,M-1)$ з ймовірностями $(P(\theta = i))$, то завдання полягатиме в послідовній перевірці (M) простих гіпотез щодо векторного спостереження $(x_n, n = \overline{1,N})$, у припущенні, що задані втрати $(g_{ij}(n))$ при $(\theta = i, u_n = j, i, j = \overline{0,M-1})$ і апостеріорний ризик $(R_n(j, x_1^n))$ можна, згідно із [150-153], у загальному вигляді записати так:

$$(R_{nj}(P(\theta = i))) = \sum_{i=0}^{M-1} g_{ij}(n) \cdot P(\theta = i), n = \overline{1,N}, \tag{3.1}$$

де $P(\theta = i | x_1^n) = \pi_{ni} = \pi_{ni}(x_1^n)$ – апостеріорна ймовірність $(i-ої)$ гіпотези після спостереження $n-$го значення, а вектор спостережень від 1 до n ($x_1, x_2, ..., x_n$).

Якщо припустити існування гіпотези про те, що співробітник вчиняє підозрілі дії з даними в хмарі. Існує апріорна ймовірність цієї гіпотези, що дорівнює 0.3. Нехай після аналізу спостережень – наприклад, отриманих із систем контролю витоку даних (DLP) або платформ для керування інформаційною безпекою (SIEM), – дані узгоджуються з цією гіпотезою із ймовірністю 0.8. Зміна апостеріорної ймовірності гіпотези після врахування цих спостережень дає змогу оновити наші уявлення про ймовірність її істинності на підставі нових даних.

Описаний вище метод виявлення несанкціонованого доступу до хмарних сервісів є стандартним. Тому, щоб побудувати оптимальні послідовні байєсівські правила для прогнозування, зокрема, несанкціонованого доступу до хмарних сервісів, необхідно реалізувати певну послідовність кроків. Серед них: визначення гіпотез, що нас цікавлять (несанкціонований проти авторизованого доступу до хмарних сервісів); вказання апріорних ймовірностей гіпотез (тобто надання числових значень нашим початковим уявленням про ймовірність кожної гіпотези – ці значення базуються на досвіді фахівців з інформаційної безпеки, інтуїції або даних з інших джерел, таких як DLP, SIEM тощо); визначення функції правдоподібності, яка описує ймовірність отриманих спостережень за кожною гіпотезою; застосування теореми Байєса для обчислення апостеріорних ймовірностей гіпотез; визначення функції втрат, яка враховує ціну прийняття хибного рішення; розрахунок очікуваних втрат для кожного рішення (прогнозування несанкціонованого доступу, тоді як насправді доступ був авторизованим); вибір рішення, що мінімізує очікувані втрати. Цей процес можна повторювати послідовно в міру надходження нових даних. Апостеріорні ймовірності з попереднього кроку можуть використовуватись як апріорні ймовірності для наступного етапу.

Згідно з [150], функція

$$\left(R_n^0\left(P(\theta = i)\right) = \min_{j \in 0, M-1} R_{nj}\left(P(\theta = i)\right) \right) \tag{3.2}$$

є угнутою на $[0,1] = [0,1]^{M-1}$. Угнута функція характеризується тим, що її графік лежить нижче будь-якої дотичної, проведеної до цього графіка. Припустімо, твердження про те, що функція, яка описує апостеріорний ризик, є вгнутою на інтервалі [0,1], має безпосереднє значення для побудови оптимальних послідовних байєсівських правил для прогнозування несанкціонованого

доступу до хмарних сервісів компанії. І справді, апостеріорний ризик у нашому завданні можна розглядати як міру втрат або ризику, пов'язаного з ухваленням конкретного рішення щодо прогнозування несанкціонованого доступу.

Якщо функція, що описує апостеріорний ризик, є угнутою на інтервалі [0,1], це означає, що зі зростанням ймовірності несанкціонованого доступу (апостеріорної ймовірності) ризик зростає нелінійно. Відповідно, під час побудови оптимальних послідовних байєсівських правил необхідно враховувати цю нелінійну залежність між ймовірністю та ризиком. Оптимальні правила слід формувати так, щоб мінімізувати апостеріорний ризик під час ухвалення рішення про наявність або відсутність несанкціонованого доступу до хмарних сервісів.

Угнутість функції апостеріорного ризику вказує на необхідність прийняття більш консервативних рішень при вищих рівнях ймовірності несанкціонованого доступу з метою зниження ризику. Припустімо, що виконується умова

$$p_{n+1}\left(x_{n+1}\middle|x_1^n\right)=p_{n+1}\left(x_{n+1}\middle|\pi_n\right),\ n>1 \tag{3.3}$$

та послідовність статистик $\{\pi_n, n\geq 1\}$ є транзитивною.

Йдеться про те, що умова (3.3) гарантує достатню «роздільність» між апостеріорними ймовірностями різних гіпотез після певної кількості спостережень $(n\geq 2)$, або ж, у міру накопичення даних, стає дедалі очевидніше, яка з гіпотез є правильною. Відповідно, транзитивність послідовності статистик означає, що коли статистика «віддає перевагу» гіпотезі 1 над гіпотезою 2, а також гіпотезі 2 над гіпотезою 3 після певної кількості спостережень, то вона також надасть перевагу гіпотезі 1 над гіпотезою 3.

Під час оцінювання апостеріорного ризику несанкціонованого доступу з боку внутрішніх порушників або інсайдерів до хмарних сервісів транзитивність статистик означає: що «підозрілішою» є поведінка користувача, то вище значення статистики, а отже й оцінюваний ризик. Ця властивість є вагомою для забезпечення узгодженості статистичних висновків.

Тоді функція (R), розглянута вище у виразі (3.2), може використовуватись для оцінки «втрат» у разі вибору неправильної гіпотези.

Розглянемо кілька прикладів. Нехай, необхідно розробити рішення, яке прогнозує ймовірність несанкціонованого доступу до хмарних сервісів з боку внутрішнього порушника. Загалом можна сформулювати дві гіпотези: (θ_0) – користувач не є порушником; (θ_1) – користувач є порушником.

Вектор спостереження $(x_n, n=\overline{1,N})$ у найпростішому вигляді може формуватися з урахуванням логів активності користувача, таких як час доступу, IP-адреси, тип дій, використовувані ресурси тощо.

Апостеріорна ймовірність (π_{ni}) – це ймовірність того, що користувач є порушником з огляду на його історію активності, а AP – це потенційні втрати, пов'язані з неправильною класифікацією користувача (хибне спрацювання або пропуск порушника). Тоді функція збитку (R) може складатися зі збитку від класифікації легітимного користувача як порушника (хибне спрацювання) та збитку від пропуску порушника (хибне заперечення). Зауважимо, що пропуск порушника небезпечніший за хибне спрацювання.

Алгоритм машинного навчання за допомогою мережі Байєса аналізує дані $(x_n, n=\overline{1,N})$ і обчислює апостеріорну ймовірність (π_{ni}). При цьому умова (3.3) гарантує, що зі зростанням обсягу даних про поведінку користувача

система стає більш впевненою в його класифікації (порушник чи ні). Нехай, система безпеки спостерігає за активністю користувача й фіксує нетипові дії, такі як доступ до конфіденційних файлів у неробочий час або з невідомої IP-адреси. Це призводить до зростання апостеріорної ймовірності (π_{n1}) (користувач – порушник). Якщо (π_{n1}) перевищить визначений поріг, система може заблокувати доступ користувача або надіслати сповіщення адміністратору з інформаційної безпеки.

Розглянемо завдання визначення оптимальної стратегії перевірки гіпотез. Припустимо, необхідно розробити стратегію перевірки гіпотез, яка мінімізує ризик неправильної класифікації користувача з одночасним урахуванням витрат на додаткові перевірки. Для розробки такої стратегії потрібно врахувати, що апостеріорна ймовірність (π_{ni}) оновлюватиметься з урахуванням результатів додаткових перевірок, а апостеріорний ризик враховує витрати на проведення таких перевірок.

Зазначимо, що під час виявлення внутрішніх порушників та/або інсайдерів додаткові перевірки можуть включати різноманітні методи, спрямовані на збір більш детальної інформації про поведінку користувачів і підтвердження їхньої особи. Метою таких перевірок є зменшення невизначеності та підвищення точності класифікації користувача як порушника або легітимного користувача.

Для подібних перевірок зазвичай використовують відстеження відхилень від звичних шаблонів поведінки, таких як час доступу, місцезнаходження, використовувані застосунки і типи файлів. Також може аналізуватися емоційний стан користувача на основі текстових повідомлень, наприклад, у корпоративному чаті чи інших каналах комунікації.

У такому разі логічно припустити, що функція втрат (R) може бути модифікована з урахуванням витрат на різні типи перевірок. Окрім того,

застосовується складніший алгоритм, який ухвалює рішення про доцільність проведення додаткових перевірок на підставі апостеріорної ймовірності та оцінки витрат і ризиків.

У випадку, коли система виявляє підозрілу активність користувача, але апостеріорна ймовірність (π_{n1}) недостатньо висока для блокування доступу, тоді система може ініціювати додаткову перевірку, наприклад, двофакторну автентифікацію або підтвердження особи. Відповідно, результати цієї перевірки використовують для подальшого уточнення (π_{ni}) та прийняття фінального рішення.

За деяких значень параметрів апріорного розподілу та спостережуваних даних функція байєсівського ризику може бути угнутою. Це означає, що оптимальне рішення міститься всередині інтервалу можливих варіантів.

Згідно з [150], можна записати:

$$M\left[R_{n+1}^{N}\left(T_{n+1}\left(x_1^{n+1}\right)\right)\middle|T_n\right]=\int\limits_{X_{n+1}} R_{n+1}^{N}\left(f_{n+1}\left(T_n,x_{n+1}\right)\right)p_{x+1}\left(x_n+1\middle|T_n\right)dx_{n+1},\ n=\overline{1,N-1},\tag{3.4}$$

де T_n – це статистика, яка використовується для перевірки гіпотези про те, що вибір $n-$го елемента не залежить від вибору $(n-1)$-го елемента;

$f-$ це функція, яка використовується для визначення ймовірності спостереження події (A) за умови, що подія (B) вже відбулася;

$p-$ це ймовірність спостереження події (A).

У виразі (3.4) інтеграл використовується для обчислення апостеріорного ризику, що дає змогу врахувати всі можливі значення (θ_i). Наприклад, припустімо, що функція втрат дорівнює «1», якщо ми не виявили інсайдера, і

«0», якщо виявили. Тоді апостеріорний ризик – це очікуване значення функції втрат, тобто ймовірність того, що ми не виявимо інсайдера, помножена на 1.

Далі, $M-$ це кількість можливих дій, які може вчинити інсайдер або внутрішній порушник інформаційної безпеки. Достатня статистика розмірності $(M-1)$ дасть можливість зробити висновки щодо ймовірності того, що інсайдер або внутрішній порушник вчинив інсайдерську дію. Припустімо $(M=3)$, тобто маємо три можливі дії: $A-$ легальна дія; $B-$ інсайдерська дія; $C-$ легальна дія.

Отже, достатня статистика розмірності $(M-1)=2$, тобто вона містить інформацію про 2 легальні дії. Ця інформація допоможе нам зробити висновки про ймовірність того, що дія (B) є інсайдерською.

Розглянемо наступний простий сценарій. Припустімо, існує компанія, що використовує хмарні сервіси й занепокоєна загрозою інсайдерських атак. Для оцінки ризику і виявлення потенційних внутрішніх порушників та інсайдерів компанія використовує мережу Байєса, яка містить такі вузли (див. рис. 3.1):

1) доступ до чутливих даних $(D)-$ бінарний вузол, що вказує, чи мав співробітник доступ до чутливих даних (так/ні) або (yes/no).

2) нетипова поведінка $(B)-$ бінарний вузол, що вказує на наявність нетипової поведінки, такої як робота в неробочий час, завантаження великих обсягів даних, спроби доступу до заборонених ресурсів або спроба редагування конфігураційного файлу (Yes/No).

3) фінансові проблеми $(F)-$ бінарний вузол, що вказує на наявність фінансових проблем у співробітника (Yes/No). Як-от, співробітник часто просить у колег позичити гроші.

4) Інсайдер $(I)-$ бінарний вузол, що вказує, чи є співробітник інсайдером (так/ні) або (yes/no).

Тоді дуги від (I) до (D), (B) та (F) відображають вплив статусу інсайдера на ймовірність доступу до даних, нетипової поведінки та фінансових проблем. Відповідно, апріорний розподіл $(I = Yes)$ – низька ймовірність, наприклад, 0.01 (припускаємо, що більшість співробітників є лояльними). Припустімо, для конкретного співробітника було виявлено, що він мав доступ до чутливих даних $(D = Yes)$ і демонстрував нетипову поведінку $(B = Yes)$. Інформація про фінансові проблеми – відсутня $(F = ?)$. Використовуючи наявні дані та мережу Байєса, обчислимо апостеріорний розподіл для $(P(I = yes|D = yes, B = yes))$.

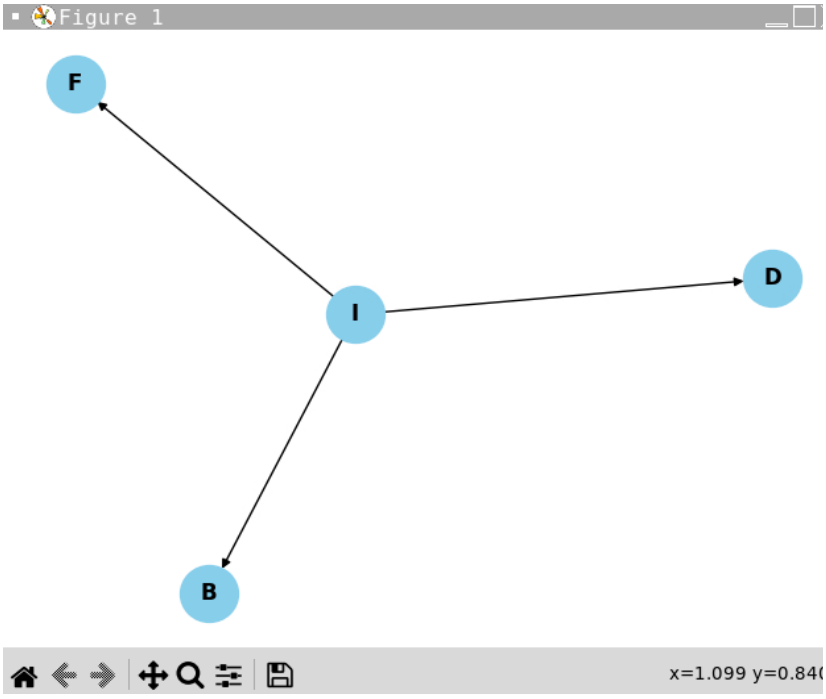


Рис. 3.1 – мережа Байєса, яка ілюструє найпростіший сценарій виявлення інсайдера

Цей розподіл вказує на оновлену ймовірність того, що співробітник є інсайдером, з урахуванням спостережуваних даних. Далі визначається функція втрат, яка враховує ціну хибнопозитивних і хибнонегативних рішень.

Наприклад, хибнопозитивне рішення (звинувачення лояльного співробітника) може призвести до втрати репутації компанії та зниження морального духу колективу, тоді як хибнонегативне рішення (невиявлення справжнього інсайдера) може спричинити витік даних і фінансові збитки.

Угнутість функції ризику дає змогу розробляти більш гнучкі й деталізовані правила прийняття рішень. Замість простої класифікації співробітників на «інсайдерів» і «не інсайдерів» можна використовувати порогове значення ймовірності та застосовувати різні заходи залежно від рівня ризику. Якщо функція байєсівського ризику, яка базується на апостеріорному розподілі та функції втрат, є угнутою, це означає, що існує оптимальний поріг ймовірності, перевищення якого веде до класифікації співробітника як потенційного інсайдера, що потребує подальшого розслідування. Цей поріг міститься усередині інтервалу можливих значень, а не на його межах.

Приклади заходів: низький ризик – моніторинг активності співробітника; середній ризик – обмеження доступу до чутливих даних; високий ризик – внутрішнє розслідування, залучення служби безпеки.

Угнутість функції байєсівського ризику в завданні виявлення інсайдерів і/або внутрішніх порушників дає можливість розробляти більш гнучкі та ефективні правила прийняття рішень, які враховують як ймовірність інсайдерської загрози, так і потенційні наслідки помилок.

Втім, слід зазначити, що в інших випадках функція байєсівського ризику може бути опуклою. Це означає, що оптимальне рішення розміщується на межі інтервалу можливих рішень.

Проілюструємо це для завдання виявлення внутрішнього порушника інформаційної безпеки та/або інсайдера.

Аналогічно до попереднього прикладу, розглянемо ще один сценарій. Існує компанія, що працює з конфіденційними даними в хмарних сервісах і занепокоєна загрозою інсайдерських витоків. Для виявлення потенційних

інсайдерів, як і в попередньому випадку, використовується байєсівський підхід із застосуванням мережі Байєса. Маємо такі вузли мережі Байєса:

- Доступ до конфіденційних даних $(D)-$ бінарний вузол (Yes/No);
- Незвична поведінка $(B)-$ бінарний вузол (Yes/No);
- Інсайдер $(I)-$ бінарний вузол (Yes/No).

І відповідні дуги від (I) до (D) та (B), які відображають вплив статусу інсайдера на ймовірність доступу до даних і на нетипову поведінку.

З огляду на серйозні наслідки витоку даних, хибнонегативне рішення (пропуск інсайдера) має значно вищу ціну, ніж хибнопозитивне (необґрунтоване звинувачення лояльного співробітника). Може використовуватись лінійна функція втрат із коефіцієнтом 10 для хибнонегативних рішень і коефіцієнтом 1 – для хибнопозитивних.

Після спостереження за даними (якщо співробітник мав доступ до конфіденційних даних і проявляв нетипову поведінку) обчислюється апостеріорний розподіл $(P(I = yes|D, B))$. Тоді байєсівський ризик обчислюється для двох можливих рішень: «вважати співробітника інсайдером» і «вважати співробітника не інсайдером», із використанням апостеріорного розподілу та функції втрат. Відповідно, через асиметричну функцію втрат функція байєсівського ризику може бути опуклою. А оптимальне рішення розміщуватиметься на межі інтервалу й полягатиме в тому, щоб класифікувати співробітника як інсайдера, навіть якщо апостеріорна ймовірність $(P(I = yes|D, B))$ не надто значна.

Проілюструємо це на простому прикладі: якщо ціна витоку даних значно перевищує ціну хибного звинувачення, то навіть за невеликої ймовірності того, що співробітник є інсайдером (приміром, 30%), оптимальним рішенням

може бути вжиття заходів, таких як обмеження доступу до даних, проведення розслідування або звільнення співробітника.

У разі опуклої функції ризику поріг для застосування заходів проти потенційних інсайдерів буде нижчим, ніж у випадку симетричної функції втрат. Це пояснюється тим, що компанія прагне мінімізувати ризик катастрофічних наслідків витоку даних, навіть за рахунок підвищеного ризику хибних звинувачень. У такій ситуації правила прийняття рішень будуть зосереджені на запобіганні інсайдерським загрозам, а не на виявленні інсайдерів після того, як витік уже стався.

Код, наведений нижче (див. рис. 3.2), ілюструє, як опукла функція байєсівського ризику приводить до більш консервативних правил ухвалення рішень, коли навіть невелика ймовірність інсайдерської загрози може стати підставою для вжиття заходів, аби уникнути потенційно катастрофічних наслідків,

```
import numpy as np
import matplotlib.pyplot as plt
# --- Параметри ---
p_insider = 0.3       # Імовірність того, що співробітник є інсайдером
cost_fn = 10          # Базова вартість хибнонегативного рішення
cost_fp_base = 1      # Базова вартість хибнопозитивного рішення
fp_scale_factor = 0.1  # Коефіцієнт масштабування для хибнопозитивних рішень
# --- Асиметрична функція втрат ---
def loss_function(decision, actual):
  if decision == 1 and actual == 0:  # Хибнопозитивне
    return cost_fp_base * (1 + fp_scale_factor * p_insider)
  elif decision == 0 and actual == 1:  # Хибнонегативне
    return cost_fn
  else:
    return 0
# --- Обчислення байєсівського ризику ---
decisions = [0, 1]  # 0 - не інсайдер; 1 - інсайдер
bayes_risks = []
for decision in decisions:
  risk = p_insider * loss_function(decision, 1) + (1 - p_insider) * loss_function(decision, 0)
  bayes_risks.append(risk)
# --- Візуалізація ---
plt.plot(decisions, bayes_risks, marker='o')
plt.xlabel("Рішення (0 - не інсайдер, 1 - інсайдер)")
plt.ylabel("Байєсовський ризик ")
plt.title("Приклад функції байєсовського ризику з асиметричною функцією втрат ")
plt.xticks(decisions)
plt.grid(True)
plt.show()
# --- Висновок оптимального рішення ---
optimal_decision = np.argmin(bayes_risks)
print("Оптимальне вирішення:", optimal_decision)
```

Рис. 3.2 – Ілюстрація випадку, коли функція байєсівського ризику приводить до більш консервативних правил прийняття рішень

У наведеному прикладі коду з використанням асиметричної функції втрат функція байєсівського ризику не є строго опуклою (див. рис. 3.3).

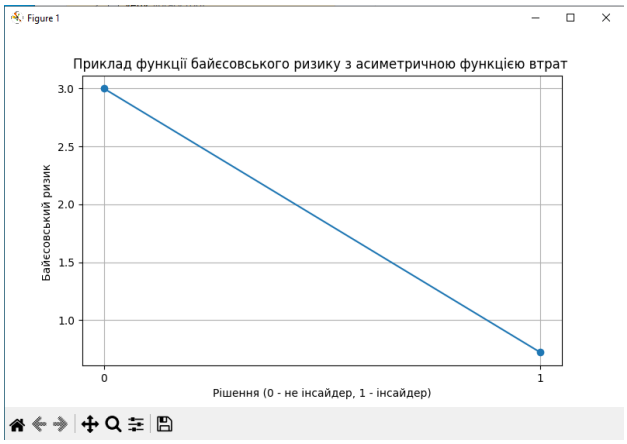


Рис. 3.3 – Ілюстрація прикладу, коли використовується асиметрична функція втрат

Форма функції залежатиме від конкретних значень параметрів: p_insider, cost_fn, cost_fp_base і fp_scale_factor.

Для випадку строго опуклої функції ми дещо змінили код, який тепер має такий вигляд (див. рис. 3.4):

```
import numpy as np
import matplotlib.pyplot as plt
# --- Параметри ---
p_insider = 0.3          # Імовірність того, що співробітник є інсайдером
cost_fn = 100           # Висока вартість помилковонегативного рішення
cost_fp_base = 1         # Базова вартість хибнопозитивного рішення
fp_scale_factor = 0.2   # Коефіцієнт масштабування (незначний)
# --- Асиметрична функція втрат ---
def loss_function(decision, actual):
      if decision == 1 and actual == 0:  # Хибнопозитивне
        return cost_fp_base * (1 + fp_scale_factor * p_insider)
      elif decision == 0 and actual == 1:  # Хибнонегативне
        return cost_fn  # Висока вартість
      else:
        return 0
# --- Обчислення байєсовського ризику ---
decisions = [0, 1]  # 0 - не інсайдер, 1 - інсайдер
bayes_risks = []
for decision in decisions:
  risk = p_insider * loss_function(decision, 1) + (1 - p_insider) * loss_function(decision, 0)
  bayes_risks.append(risk)
# --- Візуалізація ---
plt.plot(decisions, bayes_risks, marker='o')
plt.xlabel("Рішення (0 - не інсайдер, 1 - інсайдер)")
plt.ylabel("Байєсовський ризик ")
plt.title("Приклад функції байєсовського ризику з асиметричною функцією втрат ")
plt.xticks(decisions)
plt.grid(True)
plt.show()

# --- Висновок оптимального рішення ---
optimal_decision = np.argmin(bayes_risks)
print("Оптимальне рішення:", optimal_decision)
```

Рис. 3.4 – Початковий код для асиметричної функції втрат

Строга опуклість означає, що графік функції, зображений на рис. 3.3, розташований строго вище за будь-яку дотичну, проведену до цього графіка. Фрагмент реалізації в середовищі PyCharm наведено нижче.

```python
import matplotlib.pyplot as plt
# --- Параметри ---
p_insider = 0.3          # Імовірність того, що співробітник є інсайдером
cost_fn = 100            # Висока вартість помилковонегативного рішення
cost_fp_base = 1         # Базова вартість хибнопозитивного рішення
fp_scale_factor = 0.2    # Коефіцієнт масштабування (незначний)
# --- Асиметрична функція втрат ---
2 usages
def loss_function(decision, actual):
    if decision == 1 and actual == 0:  # Хибнопозитивне
        return cost_fp_base * (1 + fp_scale_factor * p_insider)
    elif decision == 0 and actual == 1:  # Хибнонегативне
        return cost_fn  # Висока вартість
    else:
        return 0
# --- Обчислення байєсовського ризику ---
decisions = [0, 1]  # 0 - не інсайдер, 1 - інсайдер
bayes_risks = []
for decision in decisions:
    risk = p_insider * loss_function(decision, actual: 1) + (1 - p_insider) * loss_function(decision, actual: 0)
    bayes_risks.append(risk)
# --- Візуалізація ---
plt.plot( *args: decisions, bayes_risks, marker='o')
plt.xlabel("Рішення (0 - не інсайдер, 1 - інсайдер)")
plt.ylabel("Байєсовський ризик ")
plt.title("Приклад функції байєсовського ризику з асиметричною функцією втрат ")
plt.xticks(decisions)
plt.grid(True)
plt.show()

# --- Висновок оптимального рішення ---
optimal_decision = np.argmin(bayes_risks)
print("Оптимальне рішення:", optimal_decision)
```

Рис. 3.5 – Реалізація асиметричної функції втрат у середовищі PyCharm

Рис. 3.6 – Візуалізація байєсівського ризику з урахуванням «невизначеності»

Отриманий результат (див. рис. 3.6) ілюструє, як кусково-лінійна опукла функція баєсівського ризику може бути використана для моделювання завдання з виявлення інсайдерів з урахуванням невизначеності та різної ціни помилок. Ця кусково-лінійна функція складається з трьох лінійних сегментів, які з’єднуються у точках зламу (при рішеннях 1 та 2). Оскільки графік функції розташований вище будь-якого відрізка, що з’єднує дві точки на графіку,

функція є опуклою. Проте вона не є строго опуклою, оскільки містить лінійні ділянки. Строго опукла функція повинна мати вигин у кожній точці.

Як видно з графіка, мінімум байєсівського ризику досягається при рішенні 1 (інсайдер). Це означає, що в цьому випадку оптимальним є класифікувати співробітника як інсайдера. Введення третього рішення – «невпевненість» (2) – дало змогу створити злам у функції ризику та зробити її опуклою. Форма графіка показує, що ціна хибнонегативного рішення (пропустити інсайдера) є вищою, ніж ціна хибнопозитивного (помилково звинуватити лояльного співробітника). Це відображається у більш крутому нахилі сегмента між рішеннями 0 та 1 порівняно із сегментом між рішеннями 1 та 2.

У цьому випадку оптимальне рішення приймається на підставі порогового значення ймовірності p_insider. Якщо ймовірність перевищує певний поріг, співробітник класифікується як інсайдер. Рішення «невпевненість» може використовуватись у випадках, коли значення p_insider близьке до порогового, і службі інформаційної безпеки потрібна додаткова інформація або аналіз для ухвалення остаточного рішення (див. рис. 3.7).

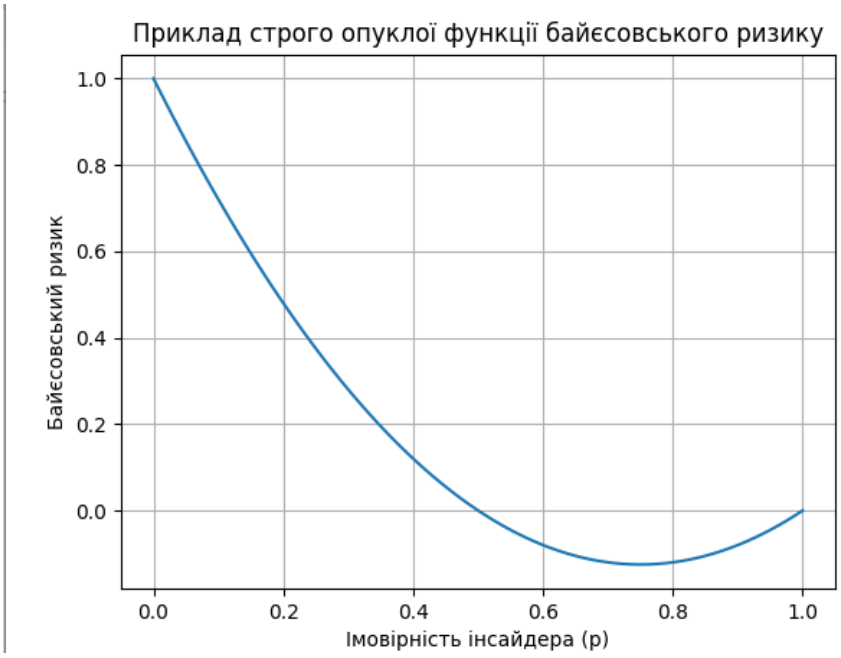


Рис. 3.7 – Графік візуалізації опуклої функції ризику несанкціонованого доступу до хмарних сервісів

У цьому прикладі ми створюємо масив `p_insider_values`, який являє собою неперервний діапазон ймовірностей від 0 до 1 (див. рис. 3.8).

```python
import numpy as np
import matplotlib.pyplot as plt

# --- Синтетичні дані ---
p_insider_values = np.linspace( start: 0,  stop: 1,  num: 100) # Безперервний діапазон ймовірностей

# --- Параметри функції ризику ---
a = 2
b = 3

# --- Суворо опукла функція ризику ---
1 usage
def bayesian_risk(p):
    return a * p**2 - b * p + 1 # Приклад суворо опуклої функції

# --- Обчислення ризику для кожної ймовірності ---
bayes_risks = [bayesian_risk(p) for p in p_insider_values]
```

Рис. 3.8 – Код для опуклої функції ризику несанкціонованого доступу до хмарних сервісів

Далі визначимо параметри a та b, які впливають на форму опуклої функції. Визначимо функцію *bayesian_risk(p)*, яка є опуклою. У цьому прикладі використовувалась квадратична функція з додатним коефіцієнтом при квадратичному члені. У конкретному випадку можна застосовувати будь-яку опуклу функцію для *bayesian_risk(p)*, наприклад, експоненційну функцію або функцію з логарифмом. Функція *bayesian_risk(p)* може використовуватись, коли потрібно враховувати різні види ризиків та їх взаємозв'язок. Якщо ми хочемо врахувати не лише ймовірність порушення безпеки, а й ступінь шкоди від такого порушення (фінансові збитки, втрата даних або репутації), то доцільно застосувати опуклу функцію *bayesian_risk(p)* для агрегування цих параметрів у єдиний показник ризику. Зазначимо, що експоненційну функцію доцільно використовувати тоді, коли необхідно враховувати експоненційне зростання ризику зі збільшенням певних параметрів. Якщо ймовірність порушення безпеки зростає експоненційно зі збільшенням кількості спроб доступу до хмарної системи, то експоненційну функцію можна використати для моделювання цього зростання.

Логарифмічну функцію можна застосовувати для моделювання ризиків, що зменшуються зі збільшенням певних параметрів. Якщо ризик порушення безпеки зменшується зі збільшенням кількості впроваджених захисних заходів, спрямованих проти внутрішнього порушника або інсайдера, то логарифмічна функція може бути використана для моделювання цього зменшення.

Наведемо приклад використання експоненційної функції. Припустімо, що ризик порушення безпеки подвоюється з кожною новою спробою доступу до хмарної системи або конкретного хмарного сервісу. Тоді функція ризику може бути виражена як $\exp(n)$, де $n-$ кількість спроб доступу.

І другий приклад використання логарифмічної функції. Припустімо, що ризик порушення безпеки зменшується вдвічі з кожним новим захисним заходом, спрямованим проти внутрішнього порушника або інсайдера. Тоді функцію ризику можна виразити як $\log(n)$.

На рис. 3.7 функція має мінімум при певному значенні ймовірності інсайдера (приблизно 0.6). Це означає, що в завданні ухвалення рішень, пов'язаному із цією функцією ризику, існує оптимальне рішення. Інакше кажучи, у цьому випадку оптимальне рішення залежить від конкретного значення $p\_insider$. Форма графіка показує, що ціна помилок (як хибнопозитивних, так і хибнонегативних) зростає в міру віддалення від оптимального значення $p\_insider$. Це відображає такий факт: що далі ми від оптимального рішення, то вищим є ризик ухвалення неправильного рішення. У цьому випадку оптимальне рішення не ґрунтується на одному пороговому значенні. Натомість необхідно враховувати конкретне значення $p\_insider$ і приймати рішення, яке мінімізує ризик для цього конкретного значення. Область навколо точки мінімального ризику можна розглядати як зону

невизначеності, де незначні зміни $p\_insider$ не призводять до суттєвих змін ризику. У цій зоні може виникнути потреба в додаткових даних або аналізі для ухвалення остаточного рішення.

Для нашого завдання прогнозування несанкціонованого доступу з боку внутрішніх порушників або інсайдерів до хмарних сервісів, які використовуються компаніями у своїх бізнес-процесах, оптимальне послідовне правило перевірки багатоальтернативних гіпотез за прийнятих припущень полягає в порівнянні апостеріорних ймовірностей гіпотез, як описано у виразі (3.5), зі змінним (випадковим) порогом. Цей поріг залежить від сукупності апостеріорних ймовірностей інших гіпотез:

$$u_n^o(\pi_n)=\begin{cases} k,\ \pi_{nk} \geq B_{nK}^N\left(\pi_n^k\right); \\ u,\ \pi_{nk} < B_{nK}^N\left(\pi_n^{(k)}\right),\ n=\overline{1,N} \end{cases}, \tag{3.6}$$

де π_n – вектор апостеріорних ймовірностей гіпотез щодо наявності несанкціонованого доступу до хмарних сервісів на n–ому кроці спостереження;

π_{nk} – k–та компонента вектора π_n, тобто апостеріорна ймовірність k–тої гіпотези на n–ому кроці;

B_{nK}^N – межа або область, де застосовуються різні стратегії прийняття рішень або використовуються різні пороги для віднесення співробітника до категорії внутрішнього порушника або інсайдера.

При цьому на $(N-м)$, $B_{nK}^N\left(\pi_n^{(k)}\right)=D_{Nk}\left(\pi_n^{(k)}\right)$ де D_{Nk} можна знайти, використовуючи вираз (3.7). А остаточне рішення ухвалюється з ймовірністю 1. Повне вирішення завдання полягатиме у знаходженні явного виразу для межі $B_{nK}^N\left(\pi_n^{(k)}\right),\ n=\overline{1,N}$. А вигляд цієї межі буде визначатися розподілом

ймовірностей спостережень. Для нашого завдання припускаємо, що умова (3.3) виконується лише в тому випадку, коли ймовірність дорівнює 1.

$$D_{Nk}\left(\pi_n^{(k)}\right)=\max_{j\neq k,M-1}\left\{\frac{1}{g_{kj}(n)-g_{kk}(n)}\cdot\sum_{i=0,i\neq k}^{M-1}\pi_{ni}\left[g_{kj}(n)-g_{kk}(n)\right]\right\}. \tag{3.7}$$

На основі вище наведених міркувань можна створити як достатньо прості, так і складні мережі Байєса для моделювання внутрішніх порушників інформаційної безпеки або інсайдерів. Нижче ми розглядаємо приклад синтезу мережі Байєса, в якій визначається ймовірність інсайдерської загрози (E) з урахуванням людського фактора (H), організаційного впливу (O) і технологічного аспекту (T). Для розрахунку ймовірності інсайдерської загрози (E) була використана така залежність [153]:

$$P(E|H,O,T)=P(E)\frac{P(H|E)P(O|E)P(T|E)}{\sum_i\left[P(E_i)P(H|E_i)P(O|E_i)P(T|E_i)\right]}, \tag{3.8}$$

де $P(E)-$ ймовірність інсайдерської загрози або загрози внутрішнього порушника безпеки;

$P(H|E)-$ ймовірність людського фактора за умови ймовірності інсайдерської загрози при визначеному рівні ризику, який може бути пов'язаний з оцінкою ймовірності виникнення інсайдерської загрози та її потенційних наслідків для безпеки хмарних сервісів. Тут можна врахувати результати, отримані в другому розділі роботи.

$P(O|E)-$ймовірність організаційного впливу за умови ймовірності інсайдерської загрози при визначеному рівні ризику;

$P(T|E)$ – ймовірність технологічного аспекту за умови ймовірності інсайдерської загрози при визначеному рівні ризику. При цьому загалом технологічні аспекти можуть містити різні аспекти безпеки хмарних сервісів, пов'язані із захистом даних, моніторингом та авдитом, а також процесами конфігурації та оновлення хмарної системи і хмарних сервісів;

$\sum_i [P(E_i)P(H|E_i)P(O|E_i)P(T|E_i)]$ – сума ймовірностей для всіх рівнів ризику, починаючи з дуже низького ризику.

Величина $P(E|H,O,T)$ – остаточний прогноз ризику того, що співробітник може бути внутрішнім порушником або інсайдером.

На відміну від [153], у наших розрахунках ми припускаємо, що ситуації шахрайських дій на керівних посадах компанії, описані за допомогою мережі Байєса у другому розділі роботи, можна віднести до людського фактора (H) і організаційного фактора (O). Людський фактор (H) пов'язаний з діями, поведінкою та рішеннями людей, в даному разі керівників компанії. Шахрайство на керівних посадах є результатом недобросовісних або незаконних дій конкретних осіб, можливо, з метою отримати неправомірну вигоду чи обманути організацію. А організаційний фактор (O) належить до аспектів, пов’язаних з організацією та керуванням компанії, таких як політики, процедури, контроль та системи, які можуть створювати умови, що сприяють або запобігають виникненню шахрайських дій. Наприклад, слабкі системи внутрішнього контролю, відсутність належного моніторингу або непрозорі процеси провокують несумлінних керівників до шахрайства і сприяти його приховуванню.

Зауважимо, що технологічний фактор (T) зазвичай не є основною причиною шахрайських дій на керівних посадах. Однак технологічні засоби відіграють вирішальну роль у виявленні або запобіганні шахрайства,

наприклад, через системи моніторингу, аналізу даних або системи ідентифікації та автентифікації в хмарних сервісах.

Нижче наведено приклад імплементації в коді програми моделювання інсайдера функції $calculate\_insider\_threat\_risk()$, яка приймає три списки як вхідні дані, що представляють рівні ризику для кожного фактора (людський, організаційний, технологічний).

Матриця $(p\_e\_given\_hot)$ містить умовні ймовірності інсайдерської загрози (E) при різних рівнях людського фактора (H), організаційних (O) і технологічних (T) факторів. У процесі навчання мережі Байєса можна замінювати ці значення реальними ймовірностями, отриманими з експертних оцінок або аналізу даних.

Вектори (p_h, p_o, p_t) містять апріорні ймовірності для кожного рівня ризику кожного фактора. Значення векторів також можна замінити реальними ймовірностями для конкретної компанії.

У процесі машинного навчання мережі Байєса значення ймовірностей, таких як $p\_e\_given\_hot, p\_h, p\_o$ та p_t, можна змінювати й уточнювати на підставі реальних даних та експертних оцінок, власне цей процес і є навчанням мережі Байєса.

Далі в наведеному фрагменті коду обчислюється спільна ймовірність $(joint\_probability)$ з використанням формули (3.8) і векторизованих операцій NumPy. Потім сумує спільну ймовірність по всіх рівнях ризику для отримання (p_e), вектора ймовірностей інсайдерської загрози для кожного рівня ризику. Потім нормалізує (p_e) для забезпечення сумування до 1. У результаті

програма повертає ймовірність рівня ризику для співробітника як остаточний прогноз.

У процесі машинного навчання, наприклад, можна створити приклади списків: $human\_factors$; organizational_aspects; technology_factors, з рівнями ризику для кожного фактора. За необхідності ці дані можна замінити реальними значеннями для конкретної компанії, яка використовує хмарні сервіси.

Зазначимо, що наведений нижче фрагмент коду (див. рис. 3.9) надає базовий приклад реалізації алгоритму, і для його практичного застосування будуть потрібні більш складна обробка даних, валідація моделі та інтерпретація результатів. Про це піде мова нижче.

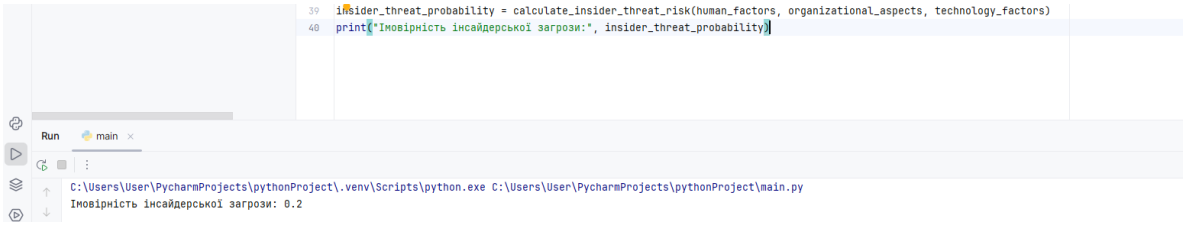


Рис. 3.9 – Фрагмент висновку для визначення умовних ймовірностей інсайдерської загрози (E) при різних рівнях людського фактора (H), організаційних (O) і технологічних (T) факторів

Для навчання мережі Байєса можна використовувати реальний набір даних, який містить приклади випадків з відомими значеннями для всіх вузлів, включаючи вузол прогнозу (у цьому випадку – ризик інсайдерської загрози). Однак компанії, як правило, не надають таку інформацію стороннім організаціям. Винятком може бути ситуація, коли проводиться авдит безпеки компанії і відповідно до договору на проведення такого авдиту компанія-авдитор може вимагати реальні дані щодо проявів дій інсайдерів і внутрішніх порушників.

Більш повний варіант коду та результати машинного навчання мережі Байєса на синтетичному наборі даних ми розглянемо в наступному параграфі роботи.

3.2. Розробка і тестування мережі Байєса для моделювання внутрішнього порушника безпеки або інсайдера

Після етапу визначення оптимальної стратегії перевірки гіпотез і мінімізації ризику неправильного визначення внутрішнього порушника безпеки або інсайдера під час роботи з хмарними сервісами доцільно виконати моделювання мережі Байєса, використовуючи програмне забезпечення для байєсівського мережного моделювання та аналізу даних, наприклад, таке як BayesiaLab (див. рис. 3.10), Netica, Hugin, GeNIe/SMILE, Bayes Server (див. рис. 3.11).

Нижче наведено систематизовані результати аналізу переваг і недоліків такого програмного забезпечення (див. табл. 3.1).

Використання спеціалізованого програмного забезпечення для байєсівського мережного моделювання й аналізу даних допомагає, за наявності навичок роботи з ним і відповідної кваліфікації, зручно та ефективно будувати й аналізувати мережі Байєса, роблячи процес моделювання і аналізу більш точним та інформативним. Однак зазначимо, що програмне забезпечення для байєсівського мережного моделювання, таке як BayesiaLab, Netica, Hugin, GeNIe/SMILE та Bayes Server, має певні недоліки, серед яких – складність для неспеціалістів з моделювання, ліцензійні обмеження та функціональність. На нашу думку, в прикладних дослідженнях у сфері кібербезпеки ці недоліки можливо подолати при використанні алгоритмічної мови Python і бібліотек для роботи з мережами Байєса, таких як pgmpy, pomegranate і libpgm.

Крім того, деякі програми, наприклад, BayesiaLab, Netica, Hugin, мають досить складний інтерфейс або потребують спеціальних навичок для роботи,

що може ускладнити їх використання для нових користувачів. Водночас, використання Python і бібліотек для роботи з мережами Байєса зазвичай є більш інтуїтивно зрозумілим і доступним для широкого кола користувачів.

Як бачимо в в таблиці 3.1, за винятком GeNIe/SMILE, всі інші спеціалізовані програмні продукти (BayesiaLab, Netica, Hugin, Bayes Server) є платними, що може бути перешкодою для їх використання. Тоді як Python і бібліотеки для роботи з мережами Байєса зазвичай поширюються за вільними ліцензіями, такими як MIT або BSD, що забезпечує більш вільне використання. Деякі програми, наприклад, Hugin і GeNIe/SMILE, мають обмеження з функціоналу, оскільки підтримують обмежену кількість ймовірнісних моделей. Використання Python і бібліотек дає змогу більш гнучко налаштовувати моделі й вирішувати різноманітні завдання аналізу даних.

Таблиця 3.1 – Аналіз переваг і недоліків програмного забезпечення для байєсівського мережного моделювання (складено автором на основі аналізу сайтів компаній-виробників цього ПЗ)

ПО для байєсівського мережного моделювання	Переваги	Недоліки
BayesiaLab	Має інтуїтивно зрозумілий інтерфейс. Надійні можливості для аналізу байєсівських мереж. Підтримує різні типи ймовірнісних моделей.	Платне ПЗ
Netica	Має широкі можливості для моделювання і аналізу байєсівських мереж. Зручний інтерфейс та інструменти для роботи з мережами Байєса.	Платне ПЗ
Hugin	Має потужні алгоритми для аналізу байєсівських мереж. Підтримує різні типи ймовірнісних моделей. Забезпечує гнучкість у налаштуванні та розширенні функціональності.	Платне ПЗ
GeNIe/SMILE	Безкоштовне ПЗ, доступне для використання без додаткових витрат. Широкі можливості для моделювання і аналізу байєсівських мереж. Підтримує різні типи ймовірнісних моделей.	Інтерфейс може здатися менш інтуїтивним порівняно з деякими іншими інструментами

Bayes Server	Потужні алгоритми та інструменти для аналізу байєсівських мереж. Підтримує різні типи ймовірнісних моделей.	Платне ПЗ, потребує ліцензування

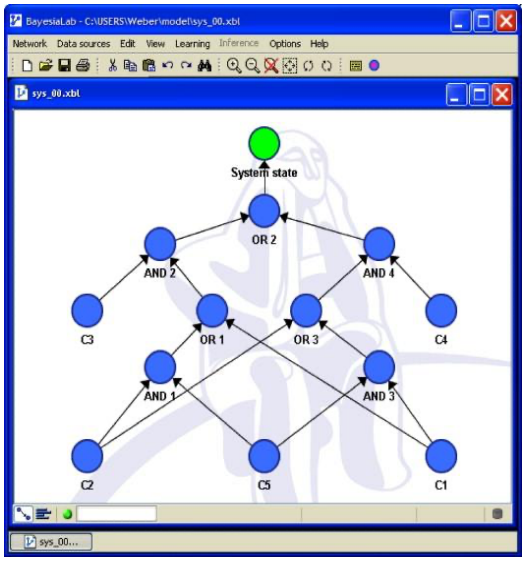


Рис. 3.10 – Фрагмент мережі Байєса, побудованої за допомогою програмного забезпечення BayesiaLab

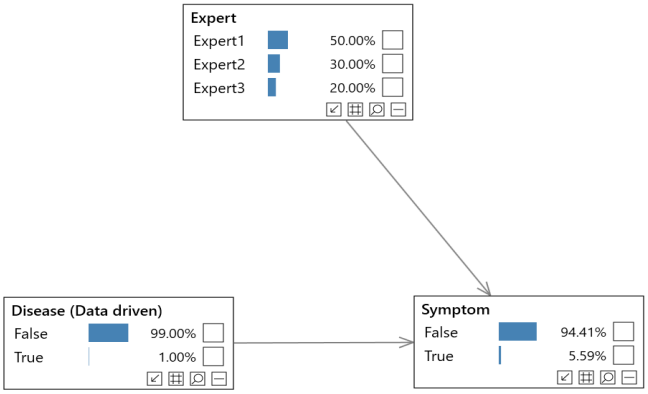


Рис. 3.11 – Структура найпростішої мережі Байєса для визначення ризику, побудованої за допомогою програмного забезпечення Bayes Server

Прототипне моделювання в спеціалізованому програмному забезпеченні, наприклад, такому як GeNIe/SMILE, має низку переваг перед виконанням моделювання мережі Байєса безпосередньо в Python із використанням бібліотек для роботи з мережами Байєса. Спеціалізоване ПЗ зазвичай має інтуїтивно зрозумілий інтерфейс і надає графічні інструменти для моделювання, що робить процес розробки та відлагодження моделі більш зручним для користувачів з різним рівнем досвіду. Також спеціалізоване ПЗ часто пропонує багатий набір функцій та можливостей для моделювання,

аналізу та візуалізації мереж Байєса, що може бути корисним під час дослідження різних аспектів моделі мережі Байєса, наприклад, інсайдера. Використання спеціалізованого ПЗ дало змогу зосередитись на проєктуванні моделі та аналізі результатів, тоді як написання коду на Python займає більше часу та зусиль.

Наприклад, за основу нашої мережі Байєса можна взяти мережу Байєса, запропоновану дослідниками університету Глазго [153]. Представлена в [153] мережа Байєса пропонує комплексний підхід до оцінки ризику інсайдерських загроз всередині організації. Вона містить різні чинники, пов'язані з демографією та зайнятістю (посада, тип зайнятості, досвід роботи, знання, продуктивність, рівень доступу тощо); поведінкові індикатори (незадоволеність, рівень стресу, зміна робочих звичок, ставлення до політик безпеки, стосунки з колегами, незвичайна активність у хмарних сервісах); людські фактори (розуміння політик інформаційної безпеки, обізнаність про загрози, схильність до соціальної інженерії, рівень знань про інформаційну безпеку); культура безпеки; керування і підтримка; технологічні фактори (інфраструктура безпеки, надійність контролю доступу, системи моніторингу і шифрування даних) тощо.

Для нашого завдання на етапі проєктування мережа Байєса була модифікована шляхом додавання нових вузлів. Додані вузли, пов'язані: з хмарними технологіями (репутація і надійність постачальника хмарних послуг CSP, сертифікати відповідності, рівень безпеки інфраструктури, методи шифрування даних, процедури реагування на інциденти); з інсайдерськими загрозами – прямі спостереження (порушення політик безпеки хмарних сервісів, несанкціонований доступ, витік даних, підозріла активність, спроби обходу механізмів безпеки), непрямі індикатори (зміни в поведінці співробітників, зниження продуктивності, фінансові труднощі, підвищений інтерес до конфіденційних даних у хмарі); з виявленням і реагуванням (ефективність механізмів виявлення, здатність системи виявляти інсайдерські загрози в хмарному середовищі на підставі аналізу різних індикаторів,

стратегії реагування на інциденти, плани реагування на інциденти, адаптовані до хмарних середовищ, в тому числі процедури збереження доказів, співпраця з CSP, правові та регуляторні аспекти). Також були додані вузли для ситуацій шахрайських дій на керівних посадах компанії, що раніше розглянуто у другому розділі роботи.

Вузли в мережі Байєса, як це показано на рис. 3.12, пов’язані направленими дугами, які відображають вплив одних факторів на інші. Наприклад, низький моральний дух співробітників (вузол в організаційних аспектах) може збільшити ймовірність незадоволення (вузол в атрибутах співробітника) (див. рис. 3.13), що, в свою чергу, підвищує ризик інсайдерської загрози.

За допомогою мережі Байєса, побудованої в GeNIe/SMILE, можна провести оцінку ризику інсайдерських загроз у хмарних сервісах організації за наявності вихідних даних, що дають можливість виставити значення відповідних ймовірностей. Шляхом аналізу даних і експертних оцінок для конкретної організації, яка використовує хмарні сервіси, можна для конкретного вузла призначити відповідні ймовірності, що дає змогу моделювати різні сценарії і виявляти найбільш уразливі місця. На відміну від початкового варіанта роботи, викладеного в [153], модифікована мережа Байєса враховує специфіку хмарних середовищ і пов’язані з ними ризики, оскільки вона дає можливість проводити комплексну оцінку ризиків, враховуючи взаємодію різних факторів під час роботи з хмарними сервісами.

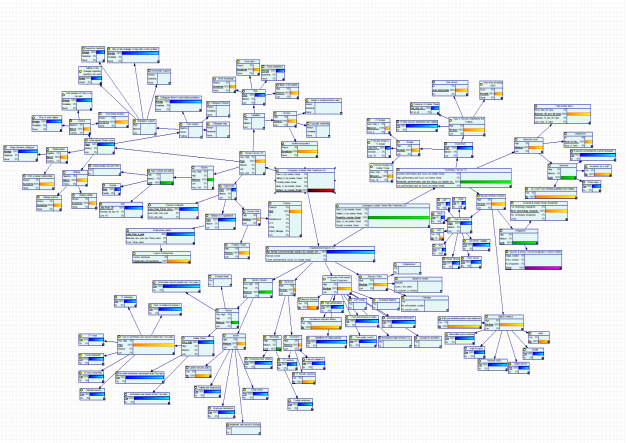


Рис. 3.12 – Модифікована мережа Байєса для моделювання внутрішніх порушників інформаційної безпеки та/або інсайдерів, з урахуванням специфіки хмарних сервісів, що використовуються в організації

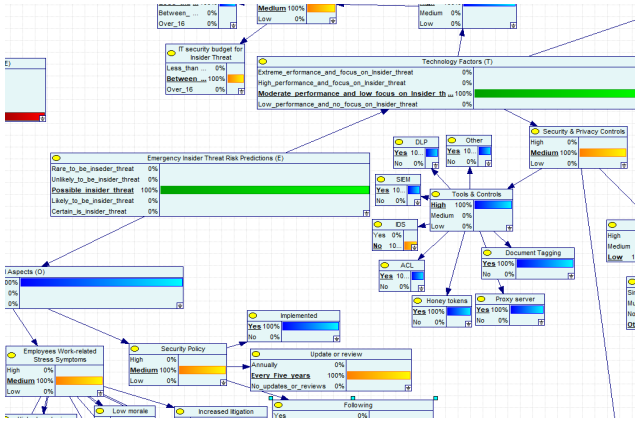


Рис. 3.14 – Фрагмент мережі Байєса для моделювання внутрішніх порушників інформаційної безпеки та/або інсайдерів, з урахуванням специфіки хмарних сервісів, що використовуються в організації

Частково вузли мережі Байєса показані в таблиці А.1 (додаток А) зі значеннями, отриманими в процесі машинного навчання.

Запропонована модифікація допомагає визначити пріоритетні напрямки для зміцнення безпеки хмарних сервісів і сприяє розробці ефективних стратегій виявлення та реагування на інсайдерські загрози.

Проте GeNIe/SMILE має обмежений набір алгоритмів машинного навчання порівняно з Python. Це може обмежити можливості для оптимізації та налаштування моделі під конкретні завдання.

Використання Python і бібліотек для роботи з мережами Байєса надає більш гнучкі та доступні інструменти для моделювання і аналізу даних, а також має низку переваг порівняно з традиційними програмами для байєсівського аналізу. Тому, на нашу думку, такий підхід, заснований на використанні Python, має свої переваги для побудови мережі Байєса порівняно зі спеціалізованим програмним забезпеченням. По-перше, Python є потужною мовою програмування з багатою системою бібліотек, що робить її ідеальним інструментом для створення мережі Байєса будь-якої складності та масштабу. Під час створення подібного проєкту можна легко розширити функціональність за допомогою різних бібліотек і реалізувати адаптовані рішення під конкретне завдання. Також Python має багату систему для аналізу даних і машинного навчання, що дає можливість інтегрувати побудову мережі Байєса з іншими етапами аналізу даних і моделювання.

Переконавшись у працездатності мережі Байєса, показаної на рис. 3.12, далі ми зосередимо увагу на програмній реалізації даної моделі за допомогою Python.

Отже, для кожного з факторів вводяться значення від 0 до 2, щоб вказати рівень ризику, пов'язаний з цим фактором для конкретного співробітника. Ці значення потім використовуються в алгоритмі для обчислення ймовірності інсайдерської загрози.

У цьому прикладі, як і в раніше розглянутому варіанті, описаному в попередньому параграфі, ми використовуємо функцію $calculate\_insider\_threat\_risk$, яка приймає три аргументи: рівень людських факторів, рівень організаційних аспектів та рівень технологічних факторів. Всередині функції визначена умовна ймовірність $p\_e\_given\_hot$, яка містить ймовірності інсайдерської загрози для різних комбінацій рівнів факторів. Потім функція використовує передані аргументи, щоб обчислити ймовірність інсайдерської загрози для цього співробітника на основі формули (3.8).

Цей програмний продукт реалізований у середовищі PyCharm (див. рис. 3.15). А спрощену блок-схему показано на рис. 3.16.

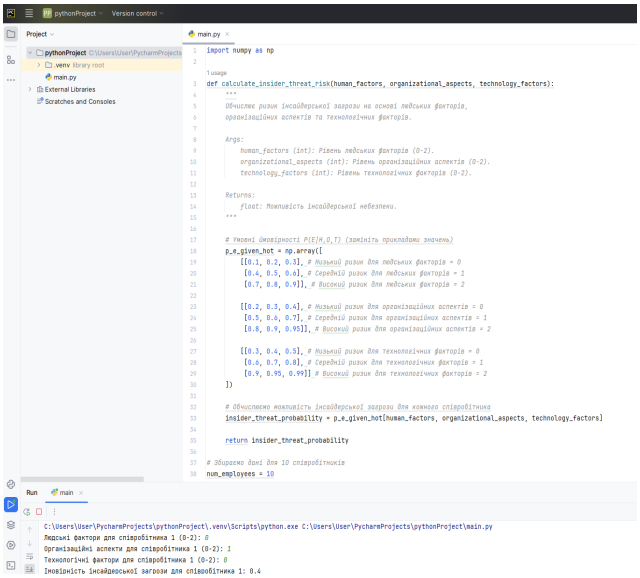
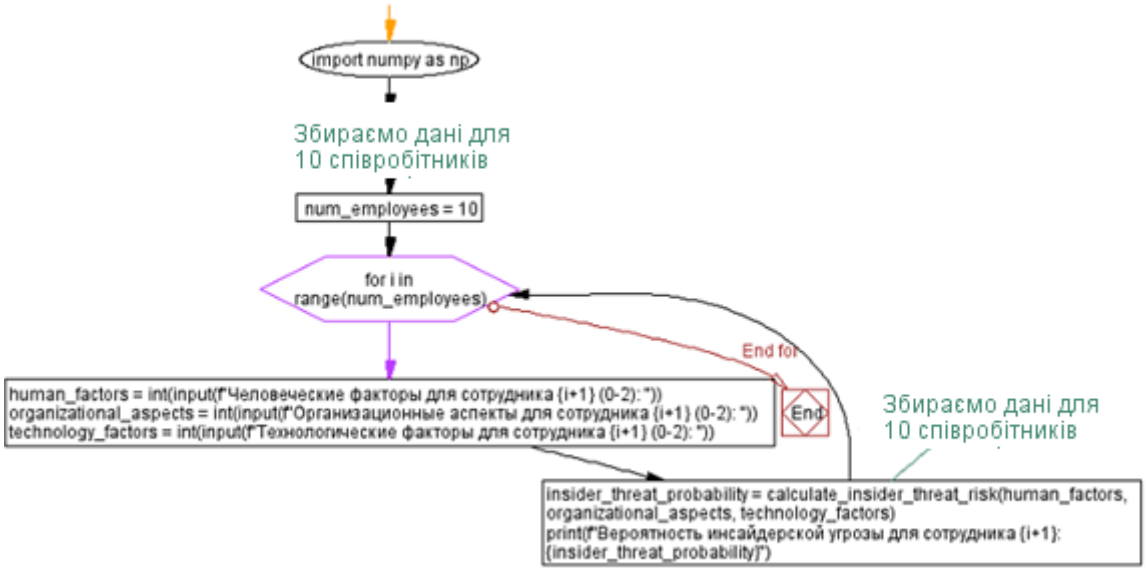


Рис. 3.15 – Програмна реалізація функції *calculate_insider_threat_risk*



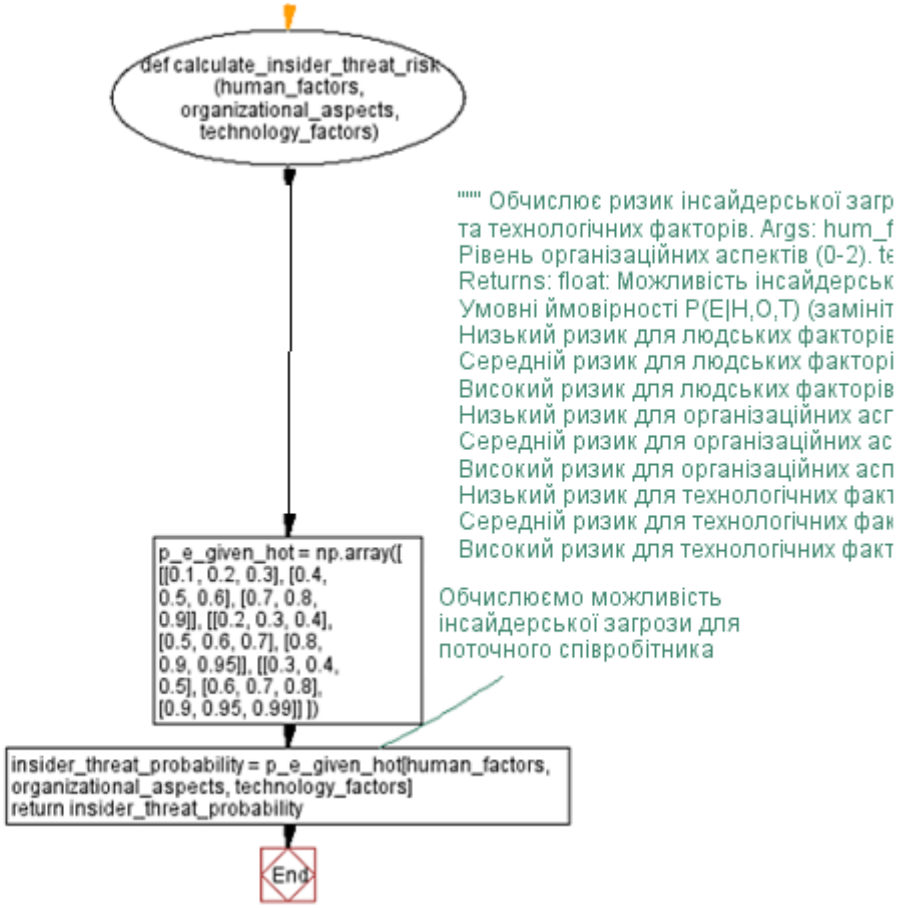


Рис. 3.16 – Спрощена блок-схема для реалізації функції *calculate_insider_threat_risk*

Для того, щоб зробити висновок більш наочним, ми додали можливість виведення результатів у вигляді гістограми (див. рис. 3.17 і 3.18).

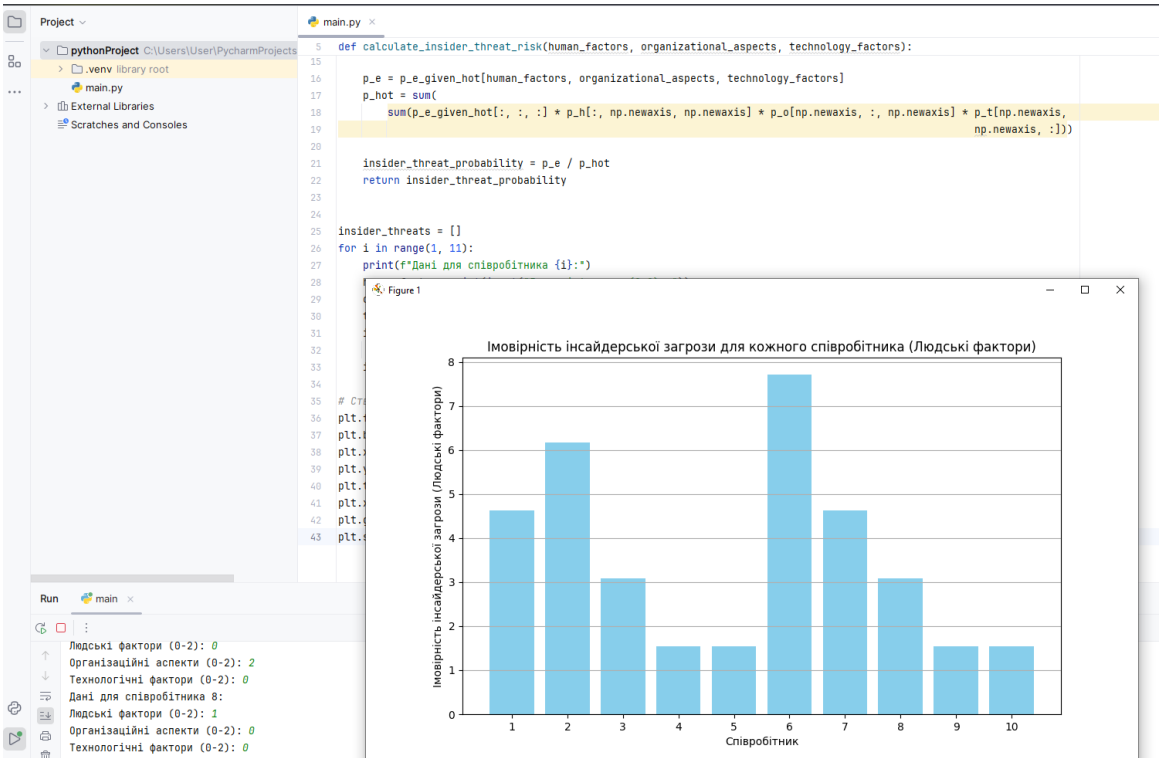


Рис. 3.17 – Програмна реалізація функції

calculate_insider_threat_risk з можливістю виведення результатів оцінки для кожного із співробітників у вигляді гістограми (показана тільки для людських факторів)

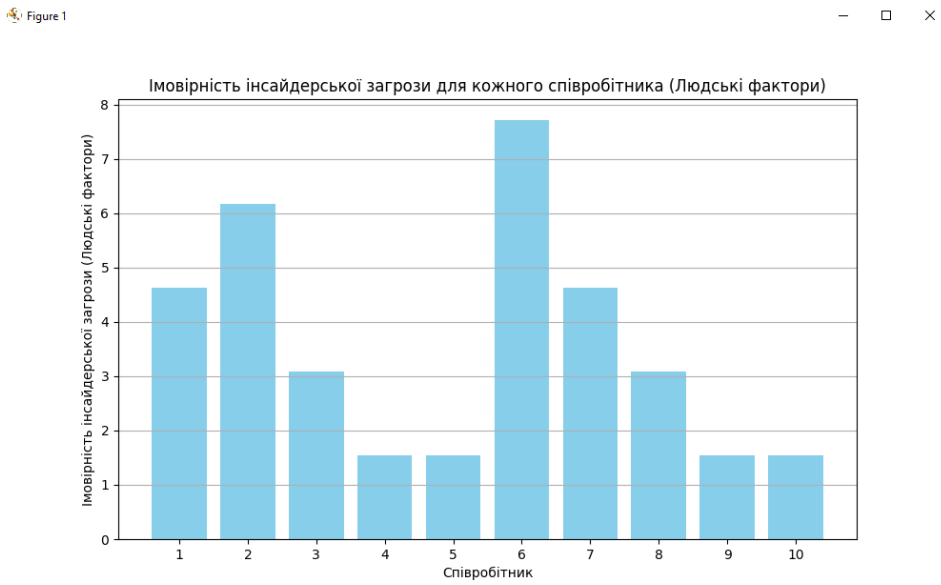


Рис. 3.18 – Гістограма, що відображає оцінку інсайдерської загрози для кожного із співробітників (на прикладі людських факторів)

На рис. 3.18 показано розподіл ймовірностей інсайдерської загрози серед умовних 10 співробітників компанії за людськими факторами. Кожен стовпчик на гістограмі представляє одного співробітника, при цьому висота стовпця відповідає ймовірності інсайдерської загрози для цього співробітника. Наприклад, якщо для співробітника 1 обчислена ймовірність інсайдерської загрози – *calculate_insider_threat_risk* по людських факторах становить 0.1, то у відповідного стовпця на гістограмі є висота, що відповідає 0.1. Гістограма дає змогу більш наочно візуалізувати й порівняти ймовірності загроз для різних співробітників, наприклад, відділу компанії, що працює з хмарними сервісами, і визначити, у кого з них ймовірність є вищою або нижчою.

Для зручності роботи з програмою ми додали в неї віконні елементи (див. рис. 3.19), а також спрощену блок-схему (рис. 3.20 і 3.21).

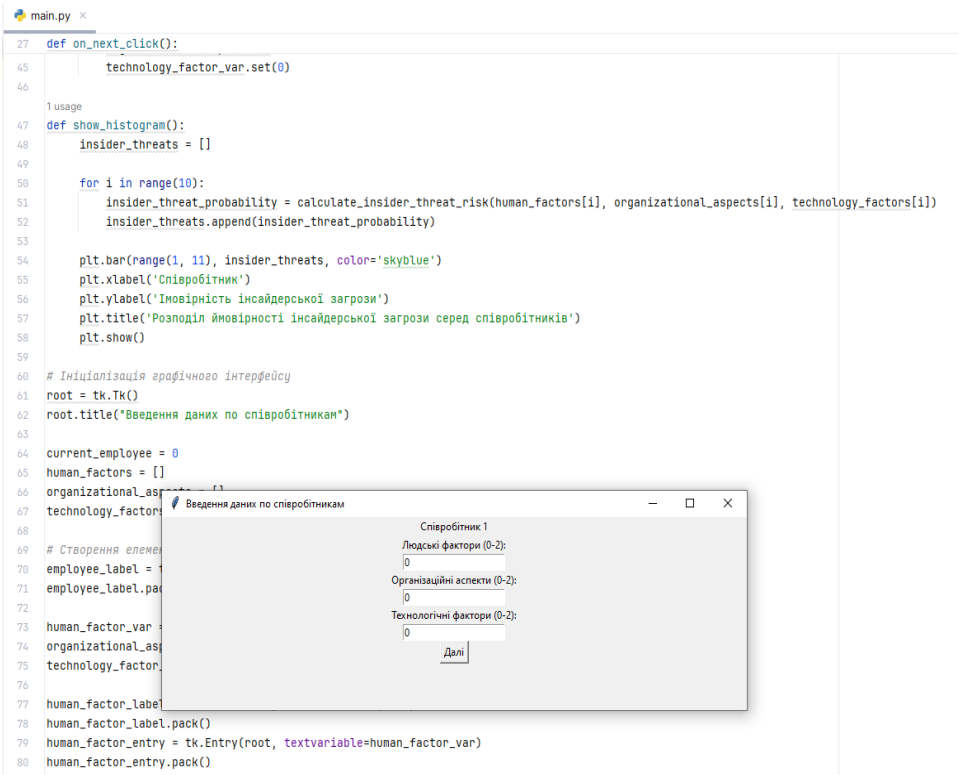
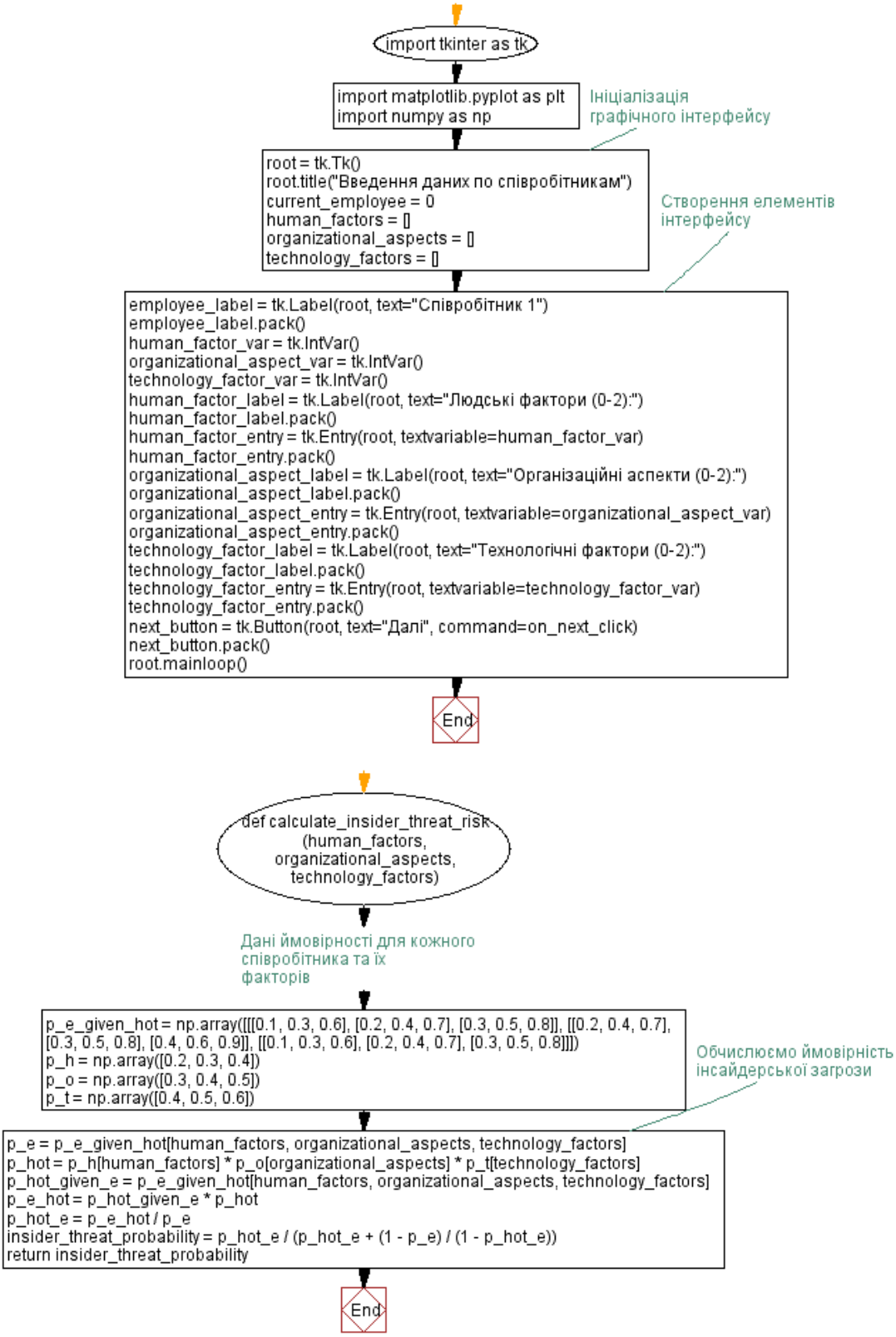
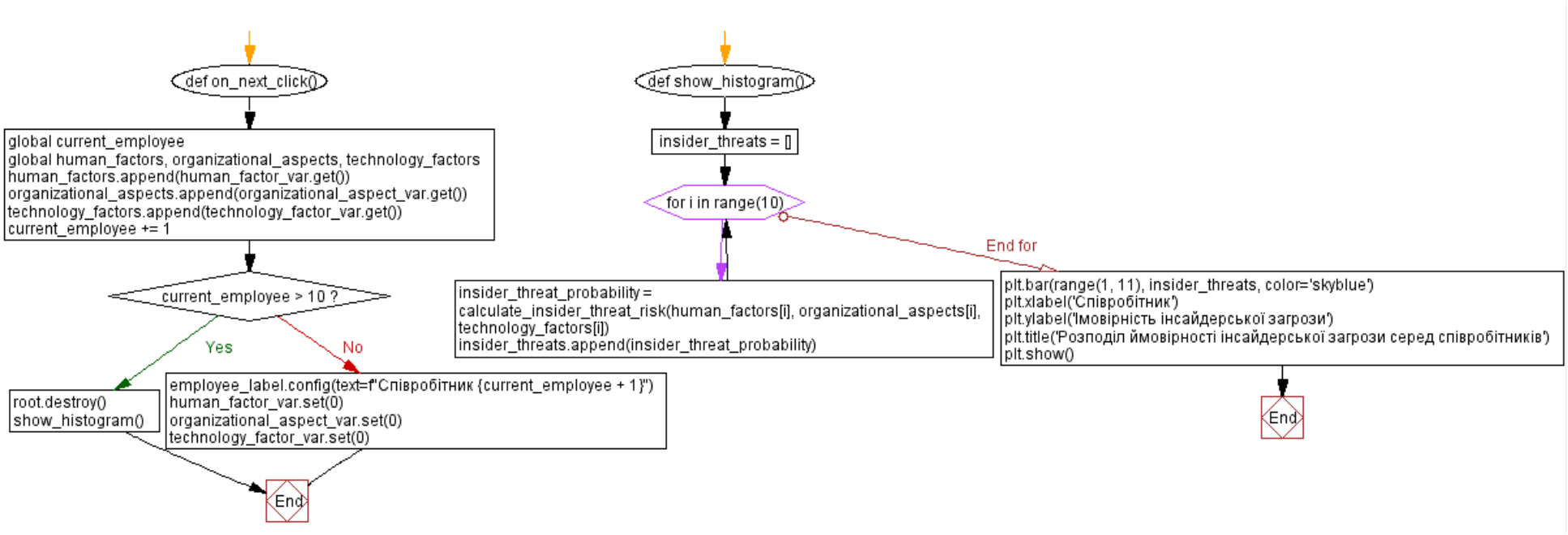


Рис. 3.19 – Додавання віконних елементів у програму для зручності її використання службою інформаційної безпеки



а) початок блок-схеми

Рис. 3.20 – Спрощена блок-схема алгоритму роботи виявлення внутрішнього порушника або інсайдера



б) закінчення блок-схеми

Рис. 3.21 – Спрощена блок-схема алгоритму роботи виявлення внутрішнього порушника або інсайдера

Використання віконних елементів для введення даних по кожному з факторів (людський, організаційний, технологічний), на наш погляд, має низку переваг, для прототипного проєктування системи підтримки прийняття рішень (СППР) для виявлення внутрішніх порушників (ВН) та інсайдерів у компаніях, що використовують хмарні сервіси. Віконні елементи (див. рис. 3.19) забезпечують зручний та інтуїтивно зрозумілий інтерфейс для введення даних, і співробітнику відділу безпеки легше вводити значення для кожного фактора окремо, що поліпшує загальне сприйняття системи. Покрокове заповнення даних для кожного співробітника дасть можливість збирати інформацію поступово, що знижує ймовірність помилок і полегшує процес введення даних. Зазначимо, що віконні елементи дадуть змогу наочно відображати введені дані, це допоможе співробітникам служби безпеки краще розуміти, які значення вони вводять і як це в кінцевому підсумку вплине на результати.

Після заповнення даних для всіх співробітників гістограма, виведена в окремому вікні СППР, допоможе легко аналізувати і порівнювати ймовірності інсайдерської загрози для кожного співробітника (див. рис. 3.22), при цьому співробітник(-и), що становить найбільшу загрозу, виділений червоним кольором.

На рис. 3.22 представлено результуюче розподілення ймовірності інсайдерської загрози серед співробітників, наприклад, одного відділу. Кожен стовпчик на гістограмі відповідає одному співробітнику. Висота стовпця відображає ймовірність інсайдерської загрози для кожного співробітника, тобто чим вищий стовпець, тим вища ймовірність того, що цей співробітник є потенційним інсайдером.

В результаті досліджень ми побудували модель мережі Байєса для моделювання внутрішніх порушників безпеки та інсайдерів. Ця модель дасть можливість оцінити ймовірність інсайдерської загрози для кожного співробітника компанії на підставі трьох факторів: людського, організаційного і технологічного.

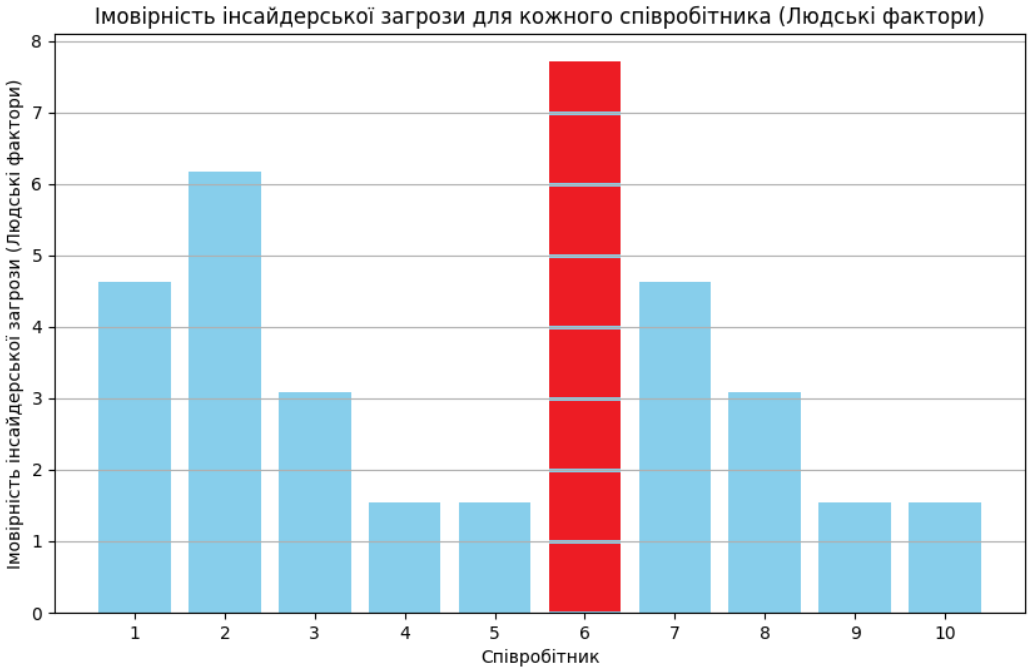


Рис. 3.22 – Результуюче розподілення ймовірності інсайдерської загрози серед співробітників, наприклад, одного відділу

Після введення даних для всіх співробітників і обчислення ймовірностей гістограма (див. рис. 3.22) дасть змогу візуалізувати розподіл ймовірностей серед співробітників, що допоможе працівникам служби безпеки виявити потенційних інсайдерів серед них.

Для навчання цієї мережі Байєса необхідно для конкретної компанії або організації зібрати дані про минулі інциденти, пов'язані з внутрішніми порушниками. На цьому етапі можна використовувати дані, зібрані, наприклад, за допомогою систем DLP, SIEM, IDS/IPS, про дії порушників, їх ролі в організації, використані технології та інші фактори. Оскільки у нас такої можливості не було, для навчання використовувалися синтетичні набори даних з урахуванням кодування категоріальних змінних, масштабування числових змінних і поділу даних на навчальний і тестовий набори. Розглянемо цей етап більш детально на конкретному прикладі. Припустімо, що у нас є синтетичний набір даних про співробітників компанії, яка працює з хмарними сервісами, і ми хочемо виявити потенційних внутрішніх порушників безпеки і/або інсайдерів. Припустимо, що у нас є такі дані: Категоріальні змінні: Роль

співробітника в компанії (адміністратор, розробник, менеджер, аналітик тощо); Рівень доступу до хмарного сервісу (високий, середній, низький); Використовувані технології – Amazon Web Services, Microsoft Azure, Google Cloud Platform тощо.

Числові змінні: Час з моменту останнього входу в систему; Кількість запитів до хмарних сервісів за останній місяць; Обсяг переданих даних через хмарні сервіси за останній місяць.

Для використання цих даних у моделі машинного навчання нам необхідна їх попередня обробка, яка передбачає кодування категоріальних змінних. Тобто необхідно перетворити категоріальні змінні в числовий формат, оскільки більшість алгоритмів машинного навчання потребують числових даних. У програмі було використано метод кодування One-Hot Encoding. Цей метод перетворює кожну категорію в окремий стовпець з бінарними значеннями. Реалізовано масштабування числових змінних для забезпечення однакової значущості кожної з них у моделі. Ми використовували метод стандартизації, який приводить значення до середнього, рівного нулю, і стандартного відхилення, рівного одиниці.

Для перетворення категоріальних змінних у числовий формат за допомогою методу кодування One-Hot Encoding у роботі використовувалася бібліотека pandas (Python). Фрагмент коду наведено нижче (див. рис. 3.23).

```
import pandas as pd
# Створюємо вихідні дані
data = {
     'Роль': ['адміністратор', 'розробник', 'менеджер', 'аналітик'],
     'Рівень доступу': ['високий', 'середній', 'низький', 'високий'],
     'Технології': ['Amazon Web Services', 'Amazon Web Services', 'Amazon Web Services', 'Amazon Web Services'],

     'Час останнього входу': [10, 20, 15, 5],
     'Запити за місяць': [100, 200, 150, 50],
     'Обсяг даних за місяць': [1000, 2000, 1500, 500]
}
df = pd.DataFrame(data)
# Перетворюємо категоріальні змінні на числовий формат за допомогою One-Hot Encoding
df_encoded = pd.get_dummies(df, columns=['Роль', 'Рівень доступу', 'Технології'])
print(df_encoded)
```

Рис. 3.23 – Перетворення категоріальних змінних у числовий формат за допомогою методу кодування One-Hot Encoding

У цьому невеликому прикладі метод pd.get_dummies() використаний для перетворення категоріальних змінних «Роль», «Рівень доступу» і «Технології»

у числовий формат за допомогою One-Hot Encoding. Кожна категорія кожної змінної перетворюється в окремий стовпець з бінарними значеннями, що показують приналежність до категорії.

Далі реалізовано поділ даних на навчальний і тестовий набори. Навчальний набір використовувався для навчання моделі, а тестовий набір – для перевірки її ефективності. Співвідношення між навчальним і тестовим наборами становило 80 до 20.

Далі йде етап регуляризації моделі для запобігання перенавчанню і поліпшення узагальнюючої здатності моделі. Щодо завдання виявлення внутрішніх порушників і/або інсайдерів, регуляризація моделі може бути реалізована на основі використання L1 або L2 регуляризації у випадку лінійної або логістичної регресії. Регуляризація додавала штраф до функції втрат моделі за великі ваги параметрів, що дало можливість зменшити їх значення і запобігти перенавчанню.

Нижче показаний фрагмент коду для L2 регуляризації до моделі логістичної регресії з використанням бібліотеки scikit-learn в Python (див. рис. 3.24).

```
from sklearn.linear_model import LogisticRegression
від sklearn.model_selection import train_test_split
від sklearn.preprocessing import StandardScaler
від sklearn.metrics import accuracy_score
від sklearn.datasets import make_classification
# Генеруємо синтетичні дані
X, y = make_classification(n_samples=1000, n_features=10, n_informative=5, random_state=42)
# Поділяємо дані на навчальний та тестовий набори
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.3, random_state=42)
# Масштабуємо дані
scaler = StandardScaler()
X_train_scaled = scaler.fit_transform(X_train)
X_test_scaled = scaler.transform(X_test)
# Навчаємо модель з L2 регуляризацією
model = LogisticRegression(penalty='l2', C=1.0, random_state=42)
model.fit(X_train_scaled, y_train)
# Передбачаємо мітки класів для тестового набору
y_pred = model.predict(X_test_scaled)
# Оцінюємо якість моделі
accuracy = accuracy_score(y_test, y_pred)
print(f'Accuracy: {accuracy}')
```

Рис. 3.24 – Фрагмент регуляризації до моделі логістичної регресії з використанням бібліотеки scikit-learn

У прикладі коду $penalty='l2'$ вказує на застосування L2 регуляризації, а параметр C контролює силу регуляризації (менші значення C відповідають більшій силі регуляризації).

Етап інтерпретації ми пропускаємо, оскільки цей етап розглядався неодноразово під час описання графіків і гістограм, наведених вище в розділі. Загалом зазначимо, що цей етап є необхідним для виявлення найбільш значущих факторів, що впливають на ймовірність інсайдерської загрози. Однак він у багатьох випадках визначається специфікою бізнес-процесів компанії. Специфіка інтерпретації може залежати від конкретної сфери бізнесу та специфіки компанії. У банківському секторі може бути доцільним визначити, які саме дії співробітників свідчать про потенційну загрозу безпеці даних клієнтів. У технологічній компанії потрібно зрозуміти, які технології або рівні доступу є найбільш вразливими для інсайдерських атак.

Інтерпретація результатів моделювання має такий вигляд для умовної компанії:

1. Роль співробітника. Адміністратори мають вищу ймовірність реалізації інсайдерської загрози, ніж аналітики. Це пов'язано з більшим доступом до систем і даних.

2. Рівень доступу до хмарного сервісу. Співробітники з високим рівнем доступу мають вищу ймовірність реалізації інсайдерської загрози, ніж ті, у яких рівень доступу середній або низький. Це також пов'язано з можливістю більш широкого впливу на системи і дані.

3. Використовувані технології. Співробітники, які використовують Amazon Web Services, можуть мати вищу ймовірність реалізації інсайдерської загрози, якщо не дотримуються правил безпеки та моніторингу, що пов'язано з властивостями цієї платформи.

Припустимо, у нас є DataFrame data, що містить дані про співробітників, як це показано нижче:

```
data = pd.DataFrame({
    'Role': ['administrator', 'developer', 'manager', 'analyst'],
    'Access Level': ['high', 'medium', 'low', 'high'],
    'Technologies': ['Amazon Web Services', 'Amazon Web Services',
'Google Cloud Platform', 'Microsoft Azure']
})
```

Тоді застосуємо кодування категоріальних змінних.

```
encoder = OneHotEncoder(sparse=False)
encoded_data = encoder.fit_transform(data[['Role', 'Access Level',
'Technologies']])
encoded_df = pd.DataFrame(encoded_data, columns=
encoder.get_feature_names(['Role', 'Access Level', 'Technologies']))
```

Для масштабування числових змінних використовувався StandardScaler з бібліотеки sklearn.

```
from sklearn.preprocessing import StandardScaler
scaler = StandardScaler()
scaled_data = scaler.fit_transform(data[['Time since last login',
'Number of requests', 'Amount of data transferred']])
scaled_df = pd.DataFrame(scaled_data, columns=['Time since last login',
'Number of requests', 'Amount of data transferred'])
```

І реалізація поділу даних на навчальний і тестовий набори.

```
from sklearn.model_selection import train_test_split
X = pd.concat([encoded_df, scaled_df], axis=1)
y = data['Інсайдерська загроза']
X_train, X_test, y_train, y_test =
= train_test_split(X, y, test_size=0.2, random_state=42)
```

Ми проілюстрували етапи підготовки даних для моделювання ймовірності інсайдерської загрози, використовуючи кодування категоріальних змінних, масштабування числових змінних і поділ даних на навчальний і тестовий набори з урахуванням вибраної специфіки компанії.

Інтерпретація результатів моделювання дає можливість виявити вирішальні фактори, які слід враховувати під час розробки стратегій для запобігання інсайдерським загрозам.

Підсумовуючи, можна стверджувати, що проведені в межах цього розділу дослідження дали змогу розробити прототип системи підтримки прийняття рішень для моделювання внутрішнього порушника інформаційної безпеки і/або інсайдера. У ході досліджень були продемонстровані на синтетичному наборі даних процеси збору даних про співробітників, аналізу їхньої поведінки та факторів, що впливають на ймовірність інсайдерської загрози.

Зазначимо, що в для навчання такої мережі Байєса необхідні дані про минулі інциденти в компаніях, що може бути ускладнено конфіденційністю даних і політиками компаній щодо їх обробки та зберігання. Крім того, компанії не завжди готові розкривати таку інформацію стороннім особам.

Тим не менш, наш прототип системи показав можливості моделювання внутрішніх та інсайдерських загроз і може бути доопрацьований та адаптований для конкретної компанії за наявності відповідних даних і узгодження з політиками безпеки та конфіденційності.

Розроблена мережа Байєса була реалізована програмно (весь код не наводиться за вимогами компанії, на базі якої була апробована та впроваджена система, що підтверджується Актом про впровадження, додаток А). Крім того, результати дослідження впроваджені у освітній процес (додаток Б).

З огляду на все вищезаначене, можна вважати, що всі поставлені завдання виконані, мета дослідження досягнута і отримані нові як теоретичні, так і практичні результати.

Висновки за розділом 3

У межах кінцевого розділу роботи були отримані такі результати і зроблені наступні висновки:

Розглянуті теоретичні аспекти вирішення завдання зі складання оптимальних послідовних байєсівських правил для прогнозування несанкціонованого доступу (несанкціонований доступ) внутрішнього порушника (внутрішній порушник) і/або інсайдера до хмарних сервісів компаній та організацій. При цьому порівнюється апостеріорна ймовірність гіпотези зі змінним порогом під час перевірки багатоальтернативних гіпотез, наприклад, про наявність порушення політики інформаційної безпеки в компанії.

Показано, що в разі оптимальних послідовних байєсівських правил (БП) для прогнозування несанкціонованого доступу внутрішнього порушника і/або інсайдера до хмарних сервісів критерієм оптимальності може бути мінімізація апостеріорного ризику в процесі ухвалення рішення. Тобто БП, розглянуті в цьому розділі роботи, побудовані так, щоб під час виникнення несанкціонованого доступу ймовірність прийняття правильного рішення (детектування порушення) була максимальною, а ризик помилки (хибного спрацьовування) мінімальним. Тоді граничні умови в такому випадку містили ймовірність хибного спрацьовування, коли було необхідно на вимогу замовника мінімізувати ймовірність помилкового виявлення несанкціонованого доступу за його відсутності, а також ймовірність пропуску виявлення дій внутрішнього порушника, коли необхідно мінімізувати ймовірність недетектування несанкціонованого доступу за його наявності. Також в ході дослідження було встановлено, що доцільно враховувати ціну хибних спрацьовувань та пропусків виявлення, оскільки вони є різними і матють різні наслідки для компанії. Зауважимо, що різні етапи прийняття рішення мають різну вагу, і це також потрібно врахувати під час визначення оптимальних правил.

Досліджено оптимальну стратегію перевірки гіпотез і мінімізації ризику неправильного визначення внутрішнього порушника і/або інсайдера під час роботи з хмарними сервісами та показано, що оптимальні послідовні байєсівські правила є математичним інструментом, який можна

використовувати для прогнозування несанкціонованого доступу внутрішнього порушника до хмарних сервісів організацій і компаній.

Встановлено, що оптимальні послідовні байєсівські правила доцільно використовувати для аналізу різних ознак та індикаторів, які вказують на можливе порушення безпеки, при цьому на кожному етапі алгоритму оптимальні послідовні байєсівські правила дають можливість аналітику кібербезпеки компанії оцінити ймовірність того, що спостережувані ознаки відповідають нормальній поведінці або ж вказують на наявність несанкціонованого доступу. Показано, що байєсівські правила враховують різні фактори, такі як попередні аномалії, динаміку зміни ознак і т.д., що робить їх ефективним інструментом для прогнозування і запобігання несанкціонованому доступу в хмарні сервіси.

Отримав розвиток метод виявлення несанкціонованого доступу до хмарних сервісів, що відрізняється від використовуваних рішень застосуванням спроєктованої та програмно реалізованої байєсівської мережі, яка може моделювати ймовірність виникнення зловмисної внутрішньої загрози або інсайдерської загрози до того, як відбудеться порушення. При цьому запропоновано програмний опис байєсівської мережі, яка розглядає технічні, організаційні та людські фактори, і під час побудови оптимальних послідовних байєсівських правил враховані нелінійні залежності між ймовірністю реалізації внутрішніх (інсайдерських загроз) і ризиком, наприклад, несанкціонованого доступу до хмарних сервісів, що допомагає за рахунок використання в програмному рішенні оптимальних правил для мінімізації апріорного ризику ухвалювати рішення про наявність або відсутність несанкціонованого доступу до хмарних сервісів.

Розглянуті приклади використання різних байєсівських правил для моделювання внутрішніх порушників і/або інсайдера, а також випадки вирішення завдання з визначення оптимальної стратегії перевірки гіпотез, що дає можливість мінімізувати ризик неправильної класифікації користувача при одночасному врахуванні витрат на додаткові перевірки.

Запропонована модифікована байєсівська мережа для завдання пошуку внутрішніх порушників і/або інсайдера шляхом додавання вузлів, пов'язаних з хмарними технологіями: постачальник хмарних послуг (репутація і надійність постачальника, сертифікати відповідності, рівень безпеки інфраструктури, методи шифрування даних, процедури реагування на інциденти); вузли, пов'язані з інсайдерськими загрозами – прямі спостереження (порушення політик безпеки хмарних сервісів, несанкціонований доступ, витік даних, підозріла активність, спроби обходу механізмів безпеки), непрямі індикатори (зміни в поведінці співробітників, зниження продуктивності, фінансові труднощі, підвищений інтерес до конфіденційних даних в хмарі); вузли, пов'язані з виявленням і реагуванням (ефективність механізмів виявлення, здатність системи виявляти інсайдерські загрози в хмарному середовищі на підставі аналізу різних індикаторів, стратегії реагування на інциденти, плани реагування на інциденти, адаптовані до хмарних середовищ, в тому числі процедури збереження доказів, співпраця з постачальником хмарних послуг, правові і регуляторні аспекти), а також додано вузли для ситуацій шахрайських дій на керівних посадах компанії, що раніше розглянуто в другому розділі роботи.

Доповнено модель для розрахунку ймовірності інсайдерської загрози, яка, на відміну від існуючих досліджень, дає можливість також оцінювати шахрайські дії на керівних посадах компанії. При цьому обґрунтовано, що в такій моделі ці дії доцільно віднести до людського фактора або/і до організаційного фактора, оскільки людський фактор пов'язаний з діями, поведінкою і рішеннями людей, в даному випадку керівників компанії. При цьому технологічний фактор, як показано, зазвичай не є основною причиною шахрайських дій на керівних посадах під час роботи з хмарними сервісами.

Виконано розробку і тестування мережі Байєса для моделювання внутрішнього порушника безпеки або інсайдера за допомогою програмного забезпечення GeNIe/SMILE, а також алгоритмічної мови Python. Показано, що використання програмного забезпечення для байєсівського мережного

моделювання і аналізу даних дає змогу зручно та ефективно будувати й аналізувати байєсівські мережі, роблячи процес моделювання і аналізу більш точним та інформативним.

Обґрунтовано, що для практичного застосування більш доцільним є використання мови Python. Спроєктовано і апробовано на рівні прототипу варіант системи підтримки прийняття рішень (СППР) для виявлення внутрішніх порушників та інсайдерів у компаніях, що використовують хмарні сервіси, в якому віконні елементи забезпечують зручний та інтуїтивно зрозумілий інтерфейс для введення даних, і співробітнику відділу безпеки легше вводити значення для кожного фактора окремо, що поліпшує загальне сприйняття системи. Окрім того, покрокове заповнення даних для кожного співробітника дасть можливість збирати інформацію поступово, що зменшує ймовірність помилок і полегшує процес введення даних. На синтетичному наборі даних отримані результати навчання такої байєсівської мережі, а також результати роботи СППР у вигляді гістограми для порівняння ймовірності інсайдерської загрози для кожного співробітника. Показано, що для повноцінного навчання такої байєсівської мережі необхідно для конкретної компанії або організації зібрати дані про минулі інциденти, пов'язані з внутрішніми порушниками, використовуючи системи DLP, SIEM, IDS/IPS.

Розроблена байєсівська мережа була реалізована програмно, фрагмент коду показаний в додатку А (весь код не наводиться за вимогами замовника, який впровадив цю систему, що підтверджується Актом про впровадження).

Зважаючи на все вищезазначене, можна стверджувати, що всі поставлені завдання, викладені у введенні, були успішно виконані. Мета дослідження досягнута, і отримані нові як теоретичні, так і практичні результати.

ВИСНОВКИ

У роботі отримано такі основні наукові результати та зроблено наступні висновки.

1. Показано, що хмарні обчислення (ХОб) стали невід'ємною частиною бізнес-процесів, надаючи об'єктам інформаційної діяльності можливості оперативно моніторити і реагувати на зміни ринку та керувати бізнес-процесами. Встановлено, що у різних галузях хмарні сервіси (ХС) використовують для оптимізації виробничих процесів, керування фінансами, опрацювання медичних даних, організації освітнього процесу, автоматизації торгівлі, оптимізації логістики тощо. Доведено, що інформаційна безпека (ІБ) ХС є невід'ємним елементом для успішного ведення бізнесу, забезпечуючи захист даних, безперервність бізнес-процесів, відповідність нормативним вимогам та довіру клієнтів. Встановлено, що незважаючи на великий арсенал технічних систем для виявлення внутрішніх порушників ІБ, зокрема, таких як IDS, DLP, SIEM, ACS-системи, організації, як і раніше, недостатньо готові до виявлення, стримування та пом'якшення складних внутрішніх, у тому числі інсайдерських атак, тому що їхні методи ІБ адаптовані до переважно зовнішніх загроз.

2. Отримав подальший розвиток метод раннього виявлення інсайдерів в організаціях, що використовують ХС, заснований на використанні мережі Байєса та який на відміну від чинних рішень враховує технічні та поведінкові категорії індикаторів під час виявлення шахрайських дій співробітника, який обіймає керівну посаду компанії, що використовує у своїх бізнес-процесах ХС.

3. Вперше запропоновано модель мережі Байєса, яка є корисною службі ІБ під час виявлення внутрішніх порушників і яка відрізняється від аналогічних рішень тим, що в ній врахована загроза шахрайства особи, яка перебуває на керівній посаді в компанії, що використовує ХС, а в завданні апріорних та апостеріорних ймовірностей подій, пов'язаних із відібраними індикаторами, беруться до уваги цифрові сліди, що залишаються

співробітником під час роботи з комп'ютерними системами компанії. Виконано програмну реалізацію запропонованої моделі мережі Байєса, яка для синтетичного набору даних показала свою працездатність, це дає можливість говорити про те, що вона доцільна для імплементації до структури контурів ІБ. Цей висновок підтверджено актом не впровадження розробленої моделі.

4. Удосконалено метод виявлення несанкціонованого доступу до ХС, що відрізняється від використовуваних рішень застосуванням розробленої байєсівської мережі, яка моделює ймовірність виникнення зловмисної внутрішньої загрози або інсайдерської загрози до того, як відбудеться порушення, Запропоновано опис байєсівської мережі, яка розглядає технічні, організаційні та людські фактори, і під час побудови оптимальних послідовних байєсівських правил враховані нелінійні залежності між ймовірністю реалізації внутрішніх (інсайдерських загроз) і ризиком.

5. Запропонована модель модифікованої байєсівскої мережі для завдання пошуку внутрішніх порушників і/або інсайдера шляхом додавання вузлів, пов'язаних з хмарними технологіями: постачальник хмарних послуг (репутація і надійність постачальника, сертифікати відповідності, рівень безпеки інфраструктури, методи шифрування даних, процедури реагування на інциденти); вузли, пов'язані з інсайдерськими загрозами – прямі спостереження (порушення політик безпеки ХС, несанкціонований доступ, витік даних, підозріла активність, спроби обходу механізмів безпеки), непрямі індикатори (зміни в поведінці співробітників, зниження продуктивності, фінансові труднощі, підвищений інтерес до конфіденційних даних в хмарі); вузли, пов'язані з виявленням і реагуванням (ефективність механізмів виявлення, здатність системи виявляти інсайдерські загрози в хмарному середовищі на підставі аналізу різних індикаторів, стратегії реагування на інциденти, плани реагування на інциденти, адаптовані до хмарних середовищ, в тому числі процедури збереження доказів, співпраця з постачальником хмарних послуг, правові і регуляторні аспекти), а також додано вузли для ситуацій шахрайських дій на керівних посадах компанії.

6. Доповнено модель для розрахунку ймовірності інсайдерської загрози, яка, на відміну від існуючих досліджень, дає можливість також оцінювати шахрайські дії на керівних посадах компанії. При цьому обґрунтовано, що в такій моделі ці дії доцільно віднести до людського фактору або/і до організаційного фактора, оскільки людський фактор пов'язаний з діями, поведінкою і рішеннями людей, в даному випадку керівників компанії. При цьому технологічний фактор, як показано, зазвичай не є основною причиною шахрайських дій на керівних посадах під час роботи з ХС.

7. Виконано розробку і тестування мережі Байєса для моделювання внутрішнього порушника безпеки або інсайдера за допомогою програмного забезпечення GeNIe/SMILE, а також алгоритмічної мови Python. Показано, що використання програмного забезпечення для байєсівського мережного моделювання і аналізу даних дає змогу зручно та ефективно будувати й аналізувати байєсівські мережі, роблячи процес моделювання і аналізу більш точним та інформативним. Спроєктовано і апробовано на рівні прототипу варіант системи підтримки прийняття рішень (СППР) для виявлення внутрішніх порушників та інсайдерів у компаніях, що використовують ХС, в якому віконні елементи забезпечують зручний та інтуїтивно зрозумілий інтерфейс для введення даних, і співробітнику відділу безпеки буде легше вводити значення для кожного фактора окремо, що поліпшує загальне сприйняття системи. Окрім того, покрокове заповнення даних для кожного співробітника дає можливість збирати інформацію поступово, що зменшує ймовірність помилок і полегшує процес введення даних. На синтетичному наборі даних продемонстровані результати навчання такої байєсівської мережі, а також результати роботи СППР у вигляді гістограми для порівняння ймовірності інсайдерської загрози для кожного співробітника. Показано, що для повноцінного навчання такої байєсівської мережі буде необхідно для конкретної компанії або організації зібрати дані про минулі інциденти, пов'язані з внутрішніми порушниками, використовуючи системи DLP, SIEM, IDS/IPS. Розроблена байєсівська мережа реалізована програмно, фрагмент

коду показаний в додатку А (весь код не наводиться за вимогами замовника, який впровадив цю систему, що підтверджується Актом про впровадження).

Зважаючи на все вищезазначене, можна стверджувати, що всі поставлені завдання, викладені у введенні, успішно виконані. Мета дослідження досягнута, і отримані нові як теоретичні, так і практичні результати.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Архіпова, Т. Л., & Зайцева, Т. В. (2013). Використання хмарних обчислень у вищій школі. Інформаційні технології в освіті, (17), 99-108.

2. Поночовний, Ю. Л., Черницька, І. О., & Замковець, І. В. (2016). Аналіз загроз і заходів із забезпечення безпеки в системах хмарних обчислень з послугою PaaS. Збірник наукових праць Харківського університету Повітряних Сил, (3), 104-107.

3. Наконечний, А. Й., & Пазан, Р. Г. (2015). Опрацювання сигналів з використанням сучасних хмарних технологій. Вісник Національного університету Львівська політехніка. Автоматика, вимірювання та керування, (821), 8-16.

4. Голячук, Н. В., Голячук, С. Є., & Рихлюк, В. С. (2014). Хмарні обчислення: завтрашній день бізнесу. Економічні науки. Серія: Облік і фінанси, (11 (1)), 37-43.

5. Продеус, К. І. Особливості застосування хмарних технологій у малому бізнесі. Математичні методи, моделі та інформаційні технології в управлінні підприємством: тези доповідей II студентської вузівської наукової конференції, 137-140.

6. Weinhardt, C., Anandasivam, A., Blau, B., Borissov, N., Meinl, T., Michalk, W., & Stößer, J. (2009). Cloud computing–a classification, business models, and research directions. Business & Information Systems Engineering, 1, 391-399.

7. Chang, V., Bacigalupo, D., Wills, G., & De Roure, D. (2010, May). A categorisation of cloud computing business models. In 2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing (pp. 509-512). IEEE.

8. Che, J., Duan, Y., Zhang, T., & Fan, J. (2011). Study on the security models and strategies of cloud computing. Procedia Engineering, 23, 586-593.

9. Sakr, S.; Liu, A.; Batista, D.M.; AlOmari, M. A Survey of Large Scale Data Management Approaches in Cloud Environments. IEEE Commun. Surv. Tutor. 2011, 13, 311–336.

10. Fox, A.; Griffith, R.; Katz, R.H.; Joseph, A.D.; Konwinski, A.; Lee, G.; Patterson, D.A.; Rabkin, A.; Stoica, I.; Zaharia, M.; et al. Above the Clouds: A Berkeley View of Cloud Computing; Department of Electrical Engineering and Computer Sciences, University of California: Berkeley, CA, USA, 2009; p. 28.

11. Reese, G. Cloud Application Architectures: Building Applications and Infrastructure in the Cloud; O'Reilly Media: Sebastopol, CA, USA, 2009.

12. Patidar, S.; Rane, D.; Jain, P. A Survey Paper on Cloud Computing. In Proceedings of the 2012 Second International Conference on Advanced Computing & Communication Technologies, Los Angeles, CA, USA, 27–29 June 2012.

13. Sun, L.; Dong, H.; Ashraf, J. Survey of Service Description Languages and Their Issues in Cloud Computing. In Proceedings of the 2012 Eighth International Conference on Semantics, Knowledge and Grids, Beijing, China, 22–24 October 2012.

14. Ahmed, E.; Khan, S.; Yaqoob, I.; Gani, A.; Salim, F. Multi-objective optimization model for seamless application execution in mobile cloud computing. In Proceedings of the 2013 5th International Conference on Information and Communication Technologies, Ohrid, Macedonia, 12–15 September 2013.

15. Ojala, A. (2016). Discovering and creating business opportunities for cloud services. Journal of Systems and Software, 113, 408-417.

16. Motahari-Nezhad, H. R., Stephenson, B., & Singhal, S. (2009). Outsourcing business to cloud computing services: Opportunities and challenges. IEEE Internet Computing, 10(4), 1-17.

17. Ali, A., Warren, D., & Mathiassen, L. (2017). Cloud-based business services innovation: A risk management model. International Journal of Information Management, 37(6), 639-649.

18. Quarati, A., Clematis, A., & D'Agostino, D. (2016). Delivering cloud services with QoS requirements: Business opportunities, architectural solutions and energy-saving aspects. Future Generation Computer Systems, 55, 403-427.

19. Boillat, T., & Legner, C. (2013). From on-premise software to cloud services: the impact of cloud computing on enterprise software vendors' business models. Journal of theoretical and applied electronic commerce research, 8(3), 39-58.

20. Vasiljeva, T., Shaikhulina, S., & Kreslins, K. (2017). Cloud computing: Business perspectives, benefits and challenges for small and medium enterprises (case of Latvia). Procedia Engineering, 178, 443-451.

21. Hon, W. K., & Millard, C. (2018). Banking in the cloud: Part 1–banks' use of cloud services. Computer law & security review, 34(1), 4-24.

22. Li, F., Lu, H., Hou, M., Cui, K., & Darbandi, M. (2021). Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality. Technology in Society, 64, 101487.

23. Ghule, S., Chikhale, R., & Parmar, K. (2014). Cloud computing in banking services. International Journal of Scientific and Research Publications, 4(6), 1-8.

24. Casola, V., Castiglione, A., Choo, K. K. R., & Esposito, C. (2016). Healthcare-related data in the cloud: Challenges and opportunities. IEEE cloud computing, 3(6), 10-14.

25. Fosch-Villaronga, E., Felzmann, H., Ramos-Montero, M., & Mahler, T. (2018, October). Cloud services for robotic nurses? Assessing legal and ethical issues in the use of cloud services for healthcare robots. In 2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS) (pp. 290-296). IEEE.

26. Zafar, Z., Islam, S., Aslam, M. S., & Sohaib, M. (2014). Cloud computing services for the healthcare industry. Int J Multidiscip Sci Eng, 5, 25-29.

27. Kiryakova, G. (2017). Application of cloud services in education. Trakia Journal of Sciences, 15(4), 277-284.

28. Alharthi, A., Yahya, F., Walters, R. J., & Wills, G. B. (2015, May). An overview of cloud services adoption challenges in higher education institutions. In Workshop on Emerging Software as a Service and Analytics (Vol. 2, pp. 102-109). SCITEPRESS.

29. Garg, S. K., Vecchiola, C., & Buyya, R. (2013). Mandi: a market exchange for trading utility and cloud computing services. The Journal of Supercomputing, 64, 1153-1174.

30. Menychtas, A., Gomez, S. G., Giessmann, A., Gatzioura, A., Stanoevska, K., Vogel, J., & Moulos, V. (2012). A marketplace framework for trading cloud-based services. In Economics of Grids, Clouds, Systems, and Services: 8th International Workshop, GECON 2011, Paphos, Cyprus, December 5, 2011, Revised Selected Papers 8 (pp. 76-89). Springer Berlin Heidelberg.

31. Sergi, I., Montanaro, T., Benvenuto, F. L., & Patrono, L. (2021). A smart and secure logistics system based on IoT and cloud technologies. Sensors, 21(6), 2231.

32. Koliadenko, S., Golubkova, I., Babachenko, M. L. T., & Burmaka, L. (2020). Development and use of it solutions in logistics. Фінансово-кредитна діяльність: проблеми теорії та практики: зб. наук. пр. Україна: Харків. 2020.№ 3 (34). С. 230-236.

33. Subramanian, N., Abdulrahman, M. D., & Zhou, X. (2014). Integration of logistics and cloud computing service providers: Cost and green benefits in the Chinese context. Transportation Research Part E: Logistics and Transportation Review, 70, 86-98.

34. Huang, H. Y., Ku, E. C., & Chen, C. D. (2022). Cloud infrastructure enhancing product competitive advantage of tourism SMEs on online consumption values of tourists. Business Process Management Journal, 28(4), 1146-1163.

35. Stănciulescu, G. C., & Dumitrescu, F. (2014). Optimizing the IT structures of tourism SMEs using modern applications and resources (Cloud). Procedia Economics and Finance, 15, 1769-1778.

36. Tselios, C., Politis, I., Tselios, V., Kotsopoulos, S., & Dagiuklas, T. (2012, September). Cloud computing: a great revenue opportunity for telecommunication industry. In FITCE Congress (FITCE), 51st (Vol. 6).

37. Chang, Y. J., Hari, A., Koppol, P., Martin, A., & Stathopoulos, T. (2012). Scalable and elastic telecommunication services in the cloud. Bell Labs Technical Journal, 17(2), 81-96.

38. Buyya, R., Beloglazov, A., & Abawajy, J. (2010). Energy-efficient management of data center resources for cloud computing: A vision, architectural elements, and open challenges. arXiv preprint arXiv:1006.0308.

39. Jayaprakash, S., Nagarajan, M. D., Prado, R. P. D., Subramanian, S., & Divakarachari, P. B. (2021). A systematic review of energy management strategies for resource allocation in the cloud: Clustering, optimization and machine learning. Energies, 14(17), 5322.

40. Xu, M., Toosi, A. N., & Buyya, R. (2020). A self-adaptive approach for managing applications and harnessing renewable energy for sustainable cloud computing. IEEE Transactions on Sustainable Computing, 6(4), 544-558.

41. Bui, D. M., Yoon, Y., Huh, E. N., Jun, S., & Lee, S. (2017). Energy efficiency for cloud computing system based on predictive optimization. Journal of Parallel and Distributed Computing, 102, 103-114.

42. Yang, X., Wallom, D., Waddington, S., Wang, J., Shaon, A., Matthews, B., & Kershaw, P. (2014). Cloud computing in e-Science: research challenges and opportunities. The Journal of Supercomputing, 70, 408-464.

43. Artem, K., Holoshchuk, R., Kunanets, N., Shestakevysh, T., & Rzheuskyi, A. (2019). Information support of scientific researches of virtual communities on the Platform of Cloud Services. In Advances in Intelligent Systems and Computing III: Selected Papers from the International Conference on Computer Science and Information Technologies, CSIT 2018, September 11-14, Lviv, Ukraine (pp. 301-311). Springer International Publishing.

44. Marienko, M. V. (2021). Tools and services of the cloud-based systems of open science formation in the process of teachers' training and professional

development. In Digital Transformation: 13th PLAIS EuroSymposium on Digital Transformation, PLAIS EuroSymposium 2021, Sopot, Poland, September 23, 2021, Proceedings 13 (pp. 108-120). Springer International Publishing.

45. Singh, S., & Chana, I. (2013). Cloud based development issues: a methodical analysis. International Journal of Cloud Computing and Services Science, 2(1), 73.

46. Sivakumaren, K. S., Swaminathan, S., & Karthikeyan, G. (2012). Growth and Development of publication on cloud computing: A scientometric Study. International Journal of Information Library and Society, 1(1), 37.

47. Аулов, І. Ф., & Горбенко, І. Д. (2013). Хмарні обчислення та аналіз питань інформаційної безпеки в хмарі. Прикладная радиоэлектроника, (Том 12, № 2), 194-201.

48. Гудзовата, О.О. (2013). Інформаційна безпека хмарних сервісів. Науковий вісник Львівського державного університету внутрішніх справ. Серія економічна, (2), 228-239.

49. Комiссар, Д. О., & Луппол, Є. Ю. (2013). Хмарні технології безпеки. Вісник Східноукраїнського національного університету імені Володимира Даля, (15 (1)), 83-87.

50. Коломійцев, О., Третяк, В., Рибальченко, А., Любченко, О., Полтавський, Е., Кривчун, В., & Третяк, А. (2023). Використання методів рангового підходу до рішення задачі оптимізації розміщення засобів захисту інформації в хмарному середовищі. Scientific Collection «InterConf+», (29 (139)), 274-292.

51. Lim, S.Y.; Kiah, M.M.; Ang, T.F. Security Issues and Future Challenges of Cloud Service Authentication. Polytech. Hung. 2017, 14, 69–89.

52. Borylo, P.; Tornatore, M.; Jaglarz, P.; Shahriar, N.; Cholda, P.; Boutaba, R. Latency and energy-aware provisioning of network slices in cloud networks. Comput. Commun. 2020, 157, 1–19.

53. Carmo, M.; Dantas Silva, F.S.; Neto, A.V.; Corujo, D.; Aguiar, R. Network-Cloud Slicing Definitions for Wi-Fi Sharing Systems to Enhance 5G Ultra-Dense Network Capabilities. Wirel. Commun. Mob. Comput. 2019, 2019, 8015274.

54. Mathkunti, N. Cloud Computing: Security Issues. Int. J. Comput. Commun. Eng. 2014, 3, 259–263.

55. Stefan, H.; Liakat, M. Cloud Computing Security Threats And Solutions. J. Cloud Comput. 2015, 4, 1.

56. Khan, A.N.; Fan, M.Y.; Malik, A.; Memon, R.A. Learning from Privacy Preserved Encrypted Data on Cloud Through Supervised and Unsupervised Machine Learning. In Proceedings of the International Conference on Computing, Mathematics and Engineering Technologies, Sindh, Pakistan, 29–30 January 2019; pp. 1–5.

57. Khilar, P.; Vijay, C.; Rakesh, S. Trust-Based Access Control in Cloud Computing Using Machine Learning. In Cloud Computing for Geospatial Big Data Analytics; Das, H., Barik, R., Dubey, H., Roy, D., Eds.; Springer: Cham, Switzerland, 2019; Volume 49, pp. 55–79.

58. Subashini, S.; Kavitha, V. A Survey on Security Issues in Service Delivery Models of Cloud Computing. J. Netw. Comput. Appl. 2011, 35, 1–11.

59. Bhamare, D.; Salman, T.; Samaka, M.; Erbad, A.; Jain, R. Feasibility of Supervised Machine Learning for Cloud Security. In Proceedings of the International Conference on Information Science and Security, Jaipur, India, 16–20 December 2016; pp. 1–5.

60. Yuhong, L.; Yan, S.; Jungwoo, R.; Syed, R.; Athanasios, V. A Survey of Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions. J. Comput. Sci. Eng. 2015, 9, 119–133.

61. Фролов, В. В. (2020). Analysis of approaches providing security of cloud sevices. Radioelectronic and Computer Systems, (1), 70-82.

62. Selamat, N.; Ali, F. Comparison of malware detection techniques using machine learning algorithm. Indones. J. Electr. Eng. Comput. Sci. 2019, 16, 435.

63. Alsolami, E. Security threats and legal issues related to Cloud based solutions. Int. J. Comput. Sci. Netw. Secur. 2018, 18, 156–163.

64. Xue, M.; Yuan, C.; Wu, H.; Zhang, Y.; Liu, W. Machine Learning Security: Threats, Countermeasures, and Evaluations. IEEE Access 2020, 8, 74720–74742.

65. Deshpande, P.; Sharma, S.C.; Peddoju, S.K. Security threats in cloud computing. In Proceedings of the International Conference on Computing, Communication and Automation, Greater Noida, India, 11–14 December 2011; pp. 632–636.

66. Varun, K.A.; Rajkumar, N.; Kumar, N.K. Survey on security threats in cloud computing. Int. J. Appl. Eng. Res. 2014, 9, 10495–10500.

67. Kazim, M.; Zhu, S.Y. A survey on top security threats in cloud computing. Int. J. Adv. Comput. Sci. Appl. 2015, 6.

68. Barona, R.; Anita, M. A survey on data breach challenges in cloud computing security: Issues and threats. In Proceedings of the International Conference on Circuit, Power and Computing Technologies (ICCPCT), Paris, France, 17–18 September 2017; pp. 1–8.

69. Aawadallah, N. Security Threats of Cloud Computing. Int. J. Recent Innov. Trends Comput. Commun. 2015, 3, 2393–2397.

70. Nadeem, M. Cloud Computing: Security Issues and Challenges. J. Wirel. Commun. 2016, 1, 10–15.

71. Le Duc, T.; Leiva, R.G.; Casari, P.; Östberg, P.O. Machine Learning Methods for Reliable Resource Provisioning in Edge-Cloud Computing: A Survey. ACM Comput. Surv. 2019, 52, 1–39.

72. Callara, M.; Wira, P. User Behavior Analysis with Machine Learning Techniques in Cloud Computing Architectures. In Proceedings of the 2018 International Conference on Applied Smart Systems, Médéa, Algeria, 24–25 November 2018; pp. 1–6.

73. Khan, M. A survey of security issues for cloud computing. J. Netw. Comput. Appl. 2016, 71, 11–29.

74. Маковоз, К. О. (2012). Методи виявлення вторгнень у хмарних системах відеоспостереження. Хмарні технології в освіті: матеріали Всеукраїнського науково-методичного Інтернет-семінару (Кривий Ріг–Київ–Черкаси–Харків, 21 грудня 2012 р.). – Кривий Ріг: Видавничий відділ КМІ, 2012. – 173 с.

75. Шимчук, Г., Голотенко, О., & Золотий, Р. З. (2022). Основні проблеми та загрози хмарної безпеки. Матеріали науково-технічної конференції „Інформаційні моделі, системи та технології “Тернопільського національного технічного університету імені Івана Пулюя, 59-60.

76. Горбань, О., & Браіловський, М. Захист хмарної інфраструктури від DDoS атак. Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 27-28 жовтня 2022 року; Київський національний університет імені Тараса Шевченка / Редкол.: В.В. Ільченко. (голова) та ін. – К.: ВПЦ "Київський університет", 2022. – 159 с.

77. Lin, C.; Lu, H. Response to Co-resident Threats in Cloud Computing Using Machine Learning. In Proceedings of the International Conference on Advanced Information Networking and Applications, Caserta, Italy, 15–17 April 2020; Volume 926, pp. 904–913.

78. Venkatraman, S.; Mamoun, A. Use of data visualisation for zero-day malware detection. Secur. Commun. Netw. 2018, 1–13.

79. Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., & Piran, M. J. (2020). A review of machine learning algorithms for cloud computing security. Electronics, 9(9), 1379.

80. Sarma, M.; Srinivas, Y.; Ramesh, N.; Abhiram, M. Improving the Performance of Secure Cloud Infrastructure with Machine Learning Techniques. In Proceedings of the International Conference on Cloud Computing in Emerging Markets (CCEM), Bangalore, India, 19–21 October 2016; pp. 78–83.

81. Sulistio, A., Reich, C., & Doelitzscher, F. (2009). Cloud infrastructure & applications–CloudIA. In Cloud Computing: First International Conference,

CloudCom 2009, Beijing, China, December 1-4, 2009. Proceedings 1 (pp. 583-588). Springer Berlin Heidelberg.

82. Salah, K., Hammoud, M., & Zeadally, S. (2015). Teaching cybersecurity using the cloud. IEEE Transactions on Learning Technologies, 8(4), 383-392.

83. Yau, S. S., Buduru, A. B., & Nagaraja, V. (2015, June). Protecting critical cloud infrastructures with predictive capability. In 2015 IEEE 8th International Conference on Cloud Computing (pp. 1119-1124). IEEE.

84. Elzamly, A.; Hussin, B.; Basari, A.S. Classification of Critical Cloud Computing Security Issues for Banking Organizations: A Cloud Delphi Study. Int. J. Grid Distrib. Comput. 2016, 9, 137–158.

85. Sayantan, G.; Stephen, Y.; Arun-Balaji, B. Attack Detection in Cloud Infrastructures Using Artificial Neural Network with Genetic Feature Selection. In Proceedings of the IEEE 14th International Conference on Dependable, Autonomic and Secure Computing, Athens, Greece, 12–15 August 2016; pp. 414–419.

86. Lee, Y.; Yongjoon, P.; Kim, D. Security Threats Analysis and Considerations for Internet of Things. In Proceedings of the International Conference on Security Technology (SecTech), Jeju Island, Korea, 25–28 November 2015; pp. 28–30.

87. Al-Janabi, S.; Shehab, A. Edge Computing: Review and Future Directions. REVISTA AUS J. 2019, 26, 368–380.

88. Hittmeir, M., Ekelhart, A., & Mayer, R. (2019, August). On the utility of synthetic data: An empirical evaluation on machine learning tasks. In Proceedings of the 14th International Conference on Availability, Reliability and Security (pp. 1-6).

89. Abdallah, E. E., & Otoom, A. F. (2022). Intrusion Detection Systems using supervised machine learning techniques: a survey. Procedia Computer Science, 201, 205-212.

90. Zhao, J., Shetty, S., & Pan, J. W. (2017, October). Feature-based transfer learning for network security. In MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM) (pp. 17-22). IEEE.

91. Elzamly, A., Hussin, B., Abu-Naser, S. S., Shibutani, T., & Doheir, M. (2017). Predicting critical cloud computing security issues using Artificial Neural Network (ANNs) algorithms in banking organizations.

92. Nita, S. L., & Mihailescu, M. I. (2018, June). On artificial neural network used in cloud computing security-a survey. In 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) (pp. 1-6). IEEE.

93. Negi, A., Singh, M., & Kumar, S. (2015). An efficient security framework design for cloud computing using artificial neural networks. In International Journal of Computer Applications (Vol. 129, No. 4, pp. 17-21). Foundation of Computer Science (FCS).

94. Azeez, N. A., & Van der Vyver, C. (2019). Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. Egyptian Informatics Journal, 20(2), 97-108.

95. Haag, S., & Eckhardt, A. (2014). Organizational cloud service adoption: a scientometric and content-based literature analysis. Journal of Business Economics, 84, 407-440.

96. Ali, O., Shrestha, A., Chatfield, A., & Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. Government Information Quarterly, 37(1), 101419.

97. Huang, C., Min, G., Wu, Y., Ying, Y., Pei, K., & Xiang, Z. (2017). Time series anomaly detection for trustworthy services in cloud computing systems. IEEE Transactions on Big Data, 8(1), 60-72.

98. Weng, Y., & Liu, L. (2019). A collective anomaly detection approach for multidimensional streams in mobile service security. IEEE Access, 7, 49157-49168.

99. Hussain, W., Hussain, F. K., Saberi, M., Hussain, O. K., & Chang, E. (2018). Comparing time series with machine learning-based prediction approaches for violation management in cloud SLAs. Future Generation Computer Systems, 89, 464-477.

100. Dwivedi, A. K. (2023). Nonlinear Time Series Analysis for Anomaly Detection in Cybersecurity using Cloud IoT. Advances in Nonlinear Variational Inequalities, 26(3), 01-15.

101. Wall, A., & Agrafiotis, I. (2021). A Bayesian approach to insider threat detection. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 12(2). pp. 48-84.

102. Elmrabit, N., Yang, S. H., Yang, L., & Zhou, H. (2020). Insider threat risk prediction based on Bayesian network. Computers & Security, 96, 101908.

103. d'Ambrosio, N., Perrone, G., & Romano, S. P. (2023). Including insider threats into risk management through Bayesian threat graph networks. Computers & Security, 133, 103410.

104. Novaes Neto, N., Madnick, S., de Paula, M. G., & Malara Borges, N. (2020). A case study of the capital one data breach. Stuart E. and Moraes G. de Paula, Anchises and Malara Borges, Natasha, A Case Study of the Capital One Data Breach (January 1, 2020).

105. Bodie, M. T. (2022). The Law of Employee Data: Privacy, Property, Governance. Ind. Lj, 97, 707.

106. Microsoft: Lapsus$ Used Employee Account to Steal Source Code. https://threatpost.com/microsoft-lapsus-compromised-one-employees-account/179048/

107. Verizon confirms data of 6 million customers was leaked. https://www.washingtonpost.com/business/economy/verizon-confirms-data-of-6-million-customers-was-leaked/2017/07/13/f9340746-67d4-11e7-8eb5-cbccc2e7bfbf_story.html

108. Tesla sues ex-employee for hacking, theft, and leaking to the press. https://www.theverge.com/2018/6/20/17484030/tesla-sues-employee-hacking-theft-leaking

109. Nearly 7 Million Dropbox Passwords Have Been Hacked. https://www.businessinsider.com/dropbox-hacked-2014-10

110. NASA says was hacked 13 times last year. https://www.reuters.com/article/us-nasa-cyberattack-idUKTRE8211G320120303/

111. I. Agrafiotis, A. Erola, M. Goldsmith, and S. Creese. A tripwire grammar for insider threat detection. In Proc. of the 8th ACM CCS International Workshop on Managing Insider Security Threats (MIST'16), Vienna Austria, pp. 105–108. ACM, October 2016.

112. I. Agrafiotis, J. R. Nurse, O. Buckley, P. Legg, S. Creese, and M. Goldsmith. Identifying attack patterns for insider threat detection. Computer Fraud & Security, 2015(7), pp. 9–17.

113. W. Eberle, J. Graves, and L. Holder. Insider threat detection using a graph-based approach. Journal of Applied Security Research, 6(1) pp. 32–81, December 2010.

114. D. M. Cappelli, A. P. Moore, and R. F. Trzeciak. The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud). Addison-Wesley, January 2012.

115. O. Brdiczka, J. Liu, B. Price, J. Shen, A. Patil, R. Chow, E. Bart, and N. Ducheneaut. Proactive insider threat detection through graph learning and psychological context. In Proc. of the 2012 IEEE Symposium on Security and Privacy Workshops (SPW'12), San Francisco, California, USA, pages 142–149. IEEE, May 2012.

116. M. Bishop and C. Gates. Defining the insider threat. In Proc. of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead (CSIIRW'08), Oak Ridge, Tennessee, USA, page 15. ACM, May 2008.

117. Нечипуренко К. О. Способи виявлення інсайдерів на підприємстві. *Актуальні проблеми кібербезпеки:* матеріали Всеукраїнської наук.-практ. конф. (Київ, 22 жовт. 2020 р.). Київ, 2020. С. 138.

118. T. Lewellen, A. P. Moore, D. M. Cappelli, R. F. Trzeciak, D. Spooner, and R. M. Weiland. Spotlight on: Insider threat from trusted business partners.

version 2: Updated and revised. Technical report, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University (PA, USA), October 2012.

119. R. M. Weiland, A. P. Moore, D. M. Cappelli, R. F. Trzeciak, and D. Spooner. Spotlight on: Insider threat from trusted business partners. CERT Program, February 2010.

120. A. Patcha and J.-M. Park. An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer networks, 51(12):3448–3470, August 2007.

121. M. R. Randazzo, M. Keeney, E. Kowalski, D. M. Cappelli, and A. P. Moore. Insider threat study: Illicit cyber activity in the banking and finance sector. Technical report, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, June 2005.

122. T. Rashid, I. Agrafiotis, and J. R. Nurse. A new take on detecting insider threats: exploring the use of hidden markov models. In Proc. of the 2016 International Workshop on Managing Insider Security Threats (MIST'16), Vienna Austria, pages 47–56. ACM, October 2016.

123. Lindberg, D. V., & Omre, H. (2015). Inference of the transition matrix in convolved hidden Markov models and the generalized Baum–Welch algorithm. IEEE Transactions on Geoscience and Remote Sensing, 53(12), 6443-6456.

124. Лаптєв О. А. Модель інформаційної безпеки на основі марковських випадкових процесів. *Зв'язок*. 2018. № 6. С. 45–49.

125. Довбешко С. В., Толюпа С. В., Шестак Я. В. Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак. *Сучасний захист інформації.* 2019. № 1(37). С. 6–15.

126. Толюпа С., Пархоменко І., Терейковська Л., Квасніков В. Побудова систем виявлення кібератак за допомогою прихованої марківської моделі. *Технічні науки та технології.* 2021. № 1 (23). С. 53–61.

127. I. Agrafiotis, A. Erola, J. Happa, M. Goldsmith, and S. Creese. Validating an insider threat detection system: A real scenario perspective. In Proc. of the 2016

IEEE Security and Privacy Workshops (SPW'16), San Jose, California, USA, pages 286–295. IEEE, May 2016.

128. Yuan, F., Cao, Y., Shang, Y., Liu, Y., Tan, J., & Fang, B. (2018). Insider threat detection with deep neural network. In Computational Science–ICCS 2018: 18th International Conference, Wuxi, China, June 11–13, 2018, Proceedings, Part I 18 (pp. 43-54). Springer International Publishing.

129. Liu, L., Chen, C., Zhang, J., De Vel, O., & Xiang, Y. (2019). Insider threat identification using the simultaneous neural learning of multi-source logs. IEEE Access, 7, 183162-183176.

130. Williams, A. D., Abbott, S. N., Shoman, N., & Charlton, W. S. (2021). Results from invoking artificial neural networks to measure insider threat detection & mitigation. Digital Threats: Research and Practice (DTRAP), 3(1), 1–20.

131. Saminathan, K., Mulka, S. T. R., Damodharan, S., Maheswar, R., & Lorincz, J. (2023). An Artificial Neural Network Autoencoder for Insider Cyber Security Threat Detection. Future Internet, 15(12), 373.

132. Al-Mhiqani, M. N., Ahmed, R., Abidin, Z. Z., & Isnin, S. N. (2021). An integrated imbalanced learning and deep neural network model for insider threat detection. International Journal of Advanced Computer Science and Applications, 12(1).

133. Савченко В. А. Нейромережева технологія виявлення інсайдерських загроз на основі аналізу журналів активності користувачів / Савченко В. А., Савченко В. В., Довбешко С. В., Мацько О. Й., Зідан А. М. *Сучасний захист інформації.* 2018. № 4. С. 36.

134. Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. ACM Computing Surveys (CSUR), 52(2), 1–40.

135. Bin Sarhan, B., & Altwaijry, N. (2022). Insider Threat Detection Using Machine Learning Approach. Applied Sciences, 13(1), 259.

136. J. S. Okolica, G. L. Peterson, and R. F. Mills. Using plsi-u to detect insider threats by datamining e-mail. International Journal of Security and Networks, 3(2):114–121, January 2008.

137. Lois, P., Drogalas, G., Karagiorgos, A., & Tsikalakis, K. (2020). Internal audits in the digital era: opportunities risks and challenges. EuroMed Journal of Business, 15(2), 205–217.

138. Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. Computers & Security, 90, 101709.

139. Шевченко С. М., Жданова Ю. Д., Складанний П. М., Бойко С. В. Інсайдери та інсайдерська інформація: суть, загрози, діяльність та правова відповідальність. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 2022. № 15(3). С. 175–185.

140. Згуровський М. З., Бідюк П. І., Терентьєв О. М., Просянкіна-Жарова Т. І. Байєсівські мережі в системах підтримки прийняття рішень. Київ: «Едельвейс», 2015. 300 с.

141. Бідюк П. І., Терентьєв О. М., Коновалюк М. М. Байєсівські мережі в технологіях інтелектуального аналізу даних. *Наукові праці [Чорноморського державного університету імені Петра Могили]. Сер.: Комп'ютерні технології.* 2010. Т. 134. Вип. 121. С. 6–16.

142. Elmrabit, N., Yang, S.H., Yang, L., 2015. Insider Threats in Information Security Categories and Approaches, in: 2015 21st International Conference on Automation and Computing (ICAC), IEEE, Glasgow, United Kingdom. pp. 1–6.

143. Darwiche, A. (2003). A differential approach to inference in Bayesian networks. Journal of the ACM (JACM), 50(3), 280–305.

144. Hikal, A., Gaebel, J., Neumuth, T., Dietz, A., & Stoehr, M. (2023). A treatment decision support model for laryngeal cancer based on Bayesian networks. Biomedicines, 11(1), 110.

145. Axelrad, E. T., Sticha, P. J., Brdiczka, O., & Shen, J. (2013, May). A Bayesian network model for predicting insider threats. In 2013 IEEE security and privacy workshops (pp. 82–89). IEEE.

146. Kumar, A., Tejaswini, P., Nayak, O., Kujur, A. D., Gupta, R., Rajanand, A., & Sahu, M. (2022, May). A survey on IBM watson and its services. In Journal of Physics: Conference Series (Vol. 2273, No. 1, p. 012022). IOP Publishing.

147. Lee, S., Kim, T., Park, S., & Lee, Y. (2018). DBpedia Web Search Application using Google Cloud Natural Language API. In Proceedings of the Korea Information Processing Society Conference (pp. 509–511). Korea Information Processing Society.

148. Guzman, B., Metzger, I., Aphinyanaphongs, Y., & Grover, H. (2020). Assessment of amazon comprehend medical: Medication information extraction. arXiv preprint arXiv:2002.00481.

149. Rosalina, V., Suhendarsah, A., & Natsir, M. (2016). Analisis Data Recovery Menggunakan Software Forensic: Winhex and X-Ways Forensic. PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer, 3(1).

150. Опірський І. Р., Головатий Т. І. Послідовна перевірка кількох прогнозів несанкціонованого доступу в байєсівській постановці задачі. *Науковий вісник НЛТУ України.* 2016. № 26 (4). С. 359–368.

151. Опірський І. Р. Технології попередження та прогнозування НСД на основі математичного апарату Баєсовських усічених процесів прийняття рішень. *Інформаційна безпека*. 2014. № 2 (14). С. 125–134.

152. Опірський І. Р. Технології попередження та прогнозування НСД на основі математичного апарату Баєсовських не усічених процесів прийняття рішень. *Інформаційна безпека*. 2014. № 3 (15). С. 52–60.

153. Elmrabit, N., Yang, S. H., Yang, L., & Zhou, H. (2020). Insider threat risk prediction based on Bayesian network. Computers & Security, 96, 101908.

Додаток А

Таблиця А.1. – Фрагмент прикладу таблиці з результатами навчання мережі Байєса для виявлення внутрішніх порушників та/або інсайдерів у компанії

Назва вузла англійською	Назва вузла українською	Параметри, задані для вершини в ході МН
Organizational Aspects (O)	Організаційні аспекти (O)	*Non fertile environmental culture for Insider threat* = 1.29%
		Natural culture = 98 %
		Fertile environmental culture for Insider threat = 0.07%
Security Breach	Порушення безпеки	*Very high* = 0.01%
		High = 4.5%
		Medium = 85%
		Low = 11%
History	Історія	*Very high* = 0.02%
		High = 6.5%
		Medium = 19.7%
		Low = 74.6%
External threat	Зовнішня загроза	*Yes* = 50%
		No = 50%
Information security breach last Five years	Порушення ІБ за останні п'ять років	*Yes* = 50%
		No = 50%
Insider threat	Внутрішня загроза	*Very high* = 0.02%
		High = 7.1%
		Medium = 18%
		Low = 74.6%
Type of authorized user security breach last Five years	Тип порушення безпеки авторизованого користувача у ХС за останні п'ять років	*Very high* = 0.03%
		High = 7.8%
		Medium = 17.4
		Low = 74.9%
Accident authorized user breach in last Five years	Випадкове порушення авторизованих користувачів за останні п’ять років	*Yes* = 50%
		No = 50%
Authorized user breach in last Five years	Авторизовані порушення користувача за останні п'ять років	*Yes* = 50%
		No = 50%
Theft of intellectual property	Крадіжка інтелектуальної власності	*Yes* = 50%
		No = 50%
IT sabotage	IT-диверсія	*Yes* = 50%
		No = 50%
IT Fraud	IT-шахрайство (на посаді)	*Yes* = 50%
		No = 50%
Social engineering	Соціальна інженерія	*Yes* = 50%
		No = 50%
In cloud computing		*Yes* = 50%

	У хмарних обчисленнях (постачальник хмарних послуг (CSP); репутація і надійність CSP, сертифікати відповідності, рівень безпеки інфраструктури та ін.)	*No* = 50%
National security	Порушення національної безпеки	*Yes* = 50%
		No = 50%
Action	Дії	*Low* = 57.8%
		Medium = 38.9%
		High = 3.4%
Update security policy	Оновити політику безпеки	*Yes* = 50%
		No = 50%
Training and awareness	Навчання та обізнаність з ІБ	*Yes* = 50%
		No = 50%
Employee termination	Звільнення працівника	*Yes* = 50%
		No = 50%
Implement new security strategy	Реалізувати нову стратегію ІБ	*Yes* = 50%
		No = 50%
Other action	Інші дії ІБ	*Yes* = 50%
		No = 50%
Structure	Структура	*High* = 5.2%
		Medium = 92.2%
		Low = 2.8%
Recruiting	Рекрутинг	*High* = 7.6%
		Medium = 86.1%
		Low = 6.3%
Outsource	Аутсорсинг для ІБ	*High* = 9.5%
		Medium = 89.2%
		Low = 1.2%
Pre-employment checks	Перевірки перед прийомом на роботу	*Yes* = 50%
		No = 50%
Foreign employee	Іноземні працівники	*Yes* = 50%
		No = 50%
IT services CS	IT послуги ХС	*Yes* = 50%
		No = 50%
IT security services	Послуги безпеки IT	*Yes* = 50%
		No = 50%
IT security department	Відділ IT безпеки	*Yes* = 50%
		No = 50%
Employees Work-related Stress Symptoms	Симптоми стресу, пов’язані з роботою працівників	*High* = 0.01%
		Medium = 99.1%
		Low = 0.2%
Reduced efficiency	Знижена працездатність	*Yes* = 50%
		No = 50%
High absenteeism	Високий абсентеїзм	*Yes* = 50%
		No = 50%

Low morale	Низький моральний дух	*Yes* = 50%
		No = 50%
Increased litigation	Збільшення судових процесів	*Yes* = 50%
		No = 50%
Increase in long-tern illness	Збільшення тривалості хвороби	*Yes* = 50%
		No = 50%
Poor performance in tasks	Погана продуктивність у виконанні завдань	*Yes* = 50%
		No = 50%
Industrial relation difficulties?	Труднощі виробничих відносин	*Yes* = 50%
		No = 50%
Deadlines not being reached	Дедлайни не досягнуті	*Yes* = 50%
		No = 50%
Poor quality control	Поганий контроль якості	*Yes* = 50%
		No = 50%
increased or high turnover of staff	Підвищена або велика плинність кадрів	*Yes* = 50%
		No = 50%
increase in accidents	Збільшення аварійності	*Yes* = 50%
		No = 50%
Security Policy	Політика ІБ	*High* = 1.5 %
		Medium = 98.1%
		Low = 0.11%
Update or review	Оновлення або перегляд	*Annually* = 20%
		Every_Five_years = 50%
		No_updates_or_reviews = 30%
Following	Підтримка ІБ	*Yes* = 50%
		No_enforcement_system = 20%
		No_security_policy = 30%
Implemented	Реалізація ІБ	*Yes* = 50%
		No = 50%
Emergency Insider Threat Risk Predictions (E)	Прогнозування ризику внутрішньої загрози	*Rare_to_be_inseder_threat* = 0.06 %
		Unlikely_to_be_insider_threat = 32.9 %
		Possible_insider_threat = 51 %
		Likely_to_be_insider_threat = 13 %
		Certain_is_insider_threat = 5.4 %
Technology Factors (T)	Технологічні фактори (T)	*Extreme_erformance_and_focus_on_Insider_threat* = 0.01 %
		High_performance_and_focus_on_Insider_threat = 3.2 %
		*Moderate_performance_and_low_focus_on_*ln*sider_threat* = 96.8 %
		Low_performance_and_no_focus_on_Insider_threat = 0.01%
Investment	Інвестиції у ІБ	*High* = 0.05%
		Medium = 10.5%

		Low = 88.6%
Budget	Бюджет ІБ	*High* = 0.01%
		Medium = 4.9%
		Low = 95.0%
Copy of Security Awareness and Training	Копія інформації про безпеку та навчання	*High* = 0.3%
		Medium = 0.02%
		Low = 97.5%
IT Budget	ІТ-бюджет	*Less_than*_3 = 20%
		*Between*_3_*and*_9 = 60%
		*Over*_9 = 20%
IT security budget of IT budget	Бюджет ІТ безпеки ІТ бюджету	*Less_than*_10 = 60%
		*Between*_10_*and*_16 = 20%
		*Over*_16 = 20%
IT security budget for Insider Threat	Бюджет ІТ-безпеки для боротьби з внутрішніми загрозами	Less_than_10 = 60%
		*Between*_10_*and*_16 = 20%
		*Over*_16 = 20%
How often attending SAaT	Як часто ви відвідуєте SAaT	*Once* = 20%
		Annually = 20%
		Never =40%
User groups	Групи користувачів	*All* = 41.5 %
		Just_employess = 30.2 %
		No = 29.3 %
Concerns of Insider Threat	Занепокоєння щодо внутрішньої загрози	*Yes* = 50%
		No = 50%
Provide security awareness and training	Забезпечити обізнаність та навчання з питань безпеки	*Yes* = 50%
		No = 50%
Detection Level	Рівень виявлення	*High* = 40.5%
		Medium = 30.3%
		Low = 29.3%
Undetected	Непомічені порушення	*All* = 35.8 %
		Must_of_them = 44.0 %
		None_of_them = 20.1 %
Detection	Виявлення порушень	*High* = 1.8%
		Medium = 98.1%
		Low = 0.2%
Fails insider alerts	Не вдається отримати інсайдерські сповіщення	*More_than*_90_*false* = 27.2 %
		*Between*_40_*and*_90_*false* = 23.1 %
		*Between*_10_*and*_40_*false* = 33.4 %
		*Less_than*_10_*false* = 16 %
IT security system before or after the breach	Система ІТ-безпеки до або після порушення	*Yes* = 50%
		No = 50%
Accidently by a staff	Випадковий співробітник	*Yes* = 50%
		No = 50%
Other ways	Інші способи	*Yes* = 50%
		No = 50%
		Yes = 50%

by a staff how following guidelines and training	Дотримання персоналом інструкцій та проведення тренінгів	*No* = 50%
Emergency_Insinder_Risk_Predictions	Прогнози ризиків надзвичайних ситуацій	*Rare_to_be_insider_threat* = = 0.06%
		Unlikely_to_be_insider_threat = = 30.8 %
		Possible_inside_threat = 51.0 %
		Likely_to_be_insider_threat = = 12.76 %
		Certain_is_insider_threat = 5.35 %
Human Factors (H)	Людський фактор (H)	Very high = 10.1%
		High = 47.2%
		Medium = 41.2%
		Low = 1.4%
		Very Low = 0.04%
Capability	Спроможність	*High* = 67.0%
		Medium = 30.1%
		Low = 1.4%
Role	Роль	*High* = 66.7%
		Medium = 33.4%
		Low = 0.01%
Work knowledge	Знання про роботу	*Always* =20%
		Sometimes = 60 %
		Never =20%
Work aims	Цілі роботи	*Always* =60%
		Sometimes = 20 %
		Never =20%
Work experience	Досвід роботи	*Always* =60%
		Sometimes = 20 %
		Never =20%
Higher work capabilities	Вищі робочі можливості	*High* = 66.7%
		Medium = 33.3%
		Low = 0.01%
Access	Доступ	*High* = 59.1%
		Medium = 40.9%
		Low = 0.01%
Desigh or implementation team	Команда проєктування або впровадження	*Always* =20%
		Sometimes = 60 %
		Never =20%
Copyright ownership	Право власності на авторські права	*Always* =40%
		Sometimes = 40 %
		Never =20%
Intellectual property	Інтелектуальна власність	*Always* =20%
		Sometimes = 40 %
		Never =40%
Opportunity	Можливість	*High* = 0.02 %
		Medium = 83.2%

		Low = 16.8%
Contract Expiration	Закінчення терміну дії контракту	*Less_than_Three_months* = 20%
		Less_than_One_year = 20 %
		Over_one_year = 60%
Relation to Organization	Ставлення до організації	*High* = 1.04%
		Medium = 82.8%
		Low = 7.6%
System Role	Системна роль	*High* = 7.7%
		Medium = 75.4%
		Low = 17.2%
Employment period	Період працевлаштування	*Less_than_a_year* = 20 %
		Between_one_year_and_ _Three_years = 60 %
		Over_Three_years = 20 %
Position Period	Період позиції	*High* = 40%
		Medium = 40%
		Low = 20%
Type of Employment	Тип зайнятості	*Current_employee* = 80 %
		Freelancers_Consul tan *ts_Contractors_ _and_Agency_staff* = 80 %
Motive	Мотиви	*Very high* = 18.9%
		High = 48.9%
		Medium = 31.5%
		Low = 0.7%
		Very Low = 0.04%
Age, Gender and position	Вік, стать і посада	*High* = 70.3%
		Medium = 29.4%
		Low = 0.29%
Understanding SecurityPolicy	Розуміння політики безпеки	*Yes* = 50%
		No = 50%
Gender	Стать	*Male* = 50 %
		Female = 50 %
Age	Вік	*Less_than_25* = 20%
		Between_26_and_45 = 60%
		Over_45 = 20%
Work-related Stress Level	Рівень стресу, пов'язаного з роботою	*High* = 76.2%
		Medium = 23.4%
		Low = 0.36%
Peer support	Підтримка однолітків	*Negative* =97.1%
		Nature =3.0%
		Positive = 0.01%
Control	Контроль	*Nature* =4.3%
		Negative =95.4%
		Positive = 0.4%
Relationships	Стосунки	*Negative* =13.67%
		Nature =84.1%

		Positive = 2.3%
Change	Зміна	*Negative* =71.0%
		Nature =28.4%
		Positive = 0.7%
Change practice	Змінити практику	*Always* =20%
		Sometim = 60%
		Never =20%
Change opinion	Змінити думку	*Always* =20%
		Sometim = 60%
		Never =20%
Anger between colleagues	Злість між колегами	*Always* =20%
		Sometim = 60%
		Never =20%
Work strained relationships	Напружені стосунки на роботі	*Always* =20%
		Sometim = 60%
		Never =20%
Way of work opinion	Думка про спосіб роботи	*Always* =20%
		Sometim = 60%
		Never =20%
Own decision Of how to do the task	Власне рішення про те, як виконати завдання	*Always* =20%
		Sometim = 60%
		Never =20%
Own break decision	Власне рішення про перерву	*Always* =40%
		Sometim = 40%
		Never =20%
Colleagues_help	Допомога колег	*Always* =20%
		Sometim = 40%
		Never =40%
Colleagues listen to work-related problems	Колеги вислуховують проблеми, пов'язані з роботою	*Always* =40%
		Sometim = 40%
		Never =20%
Colleagues Respect	Повага колег	*Always* =40%
		Sometim = 20%
		Never =40%
Managers' support	Підтримка менеджерів	*High* = 20%
		Medium = 40%
		Low = 40%

Emotionally support	Емоційна підтримка	*Always* =20%
		Sometim = 20%
		Never =60%
Rely on line manager to help with a work problem	Покладатися на допомогу лінійного керівника у вирішенні робочих проблем	*Always* =20%
		Sometim = 40%
		Never =40%
Supportive feedback	Схвальні відгуки	*Always* =20%
		Sometim = 40%
		Never =40%
Talking to line manager regarding upsetting from work	Розмова з безпосереднім керівником щодо розладів на роботі	*Yes* = 50%
		No = 50%

Додаток Б

Акт впровадження результатів дисертаційного дослідження у виробничий процес ТОВ «Інфобіт»

ПОГОДЖЕНО

Проректор з наукової роботи та інноваційної діяльності Національного університету біоресурсів і природокористування України доктор сільськогосподарських наук, професор

_____ Оксана ТОНХА

«16» _____ 2026 р.

ЗАТВЕРДЖУЮ

Директор ТОВ «Інфобіт»

_____ Анастасія КРИЦАК

«16» січня 2026 р.

А К Т
про впровадження/використання результатів дисертації на здобуття ступеня доктора філософії у виробничий процес

Цим актом стверджується, що результати дисертації на тему: «**Комп'ютерні баєсівські моделі виявлення інсайдерів у хмарних сервісах»**, що представлена на здобуття наукового ступеня доктора філософії з галузі знань 12 – Інформаційні технології та спеціальності 122 – Комп'ютерні науки, виконаної Глазуновим Андрієм Сергійовичем, впроваджено у Товаристві з обмеженою відповідальністю «Інфобіт».

1. Вид впроваджуваних результатів	Модифікована модель баєсівської мережі для виявлення інсайдерських загроз у хмарних сервісах інформаційних систем
2. Новизна отриманих результатів	Вперше розроблено модифіковану модель баєсівської мережі для виявлення інсайдерських загроз у хмарних сервісах інформаційних систем. На відміну від наявних рішень, модель включає спеціалізовані вузли для врахування дій осіб, які займають керівні посади, і моделює ризики шахрайської поведінки з боку такого персоналу. Модель враховує цифрові сліди, які формуються під час взаємодії користувача з хмарними застосунками, що дозволяє оцінювати ймовірність внутрішніх загроз до моменту фактичного порушення. Структура розробленої моделі включає опис апріорних і апостеріорних ймовірностей для вирішальних технічних, поведінкових та організаційних індикаторів, що забезпечує глибше причинно-наслідкове моделювання ситуацій загрози в умовах неповної інформації.
3. Практичне впровадження/ використання результатів	Реалізовано алгоритмічну процедуру побудови оптимальних послідовних баєсівських правил, яка забезпечує гнучку адаптацію порогів прийняття рішень відповідно до накопичених апостеріорних ймовірностей та враховує ймовірнісні витрати помилкових рішень, як хибнопозитивних, так і хибнонегативних, а також змінну етапів ухвалення рішення в системах інформаційної безпеки хмарних сервісів для підприємства з урахуванням специфіки політики безпеки, кадрових структур та хмарної архітектури. Програмна реалізація моделі здійснена за допомогою середовища GeNIe/SMILE та мови програмування Python, що дозволяє забезпечити модульність,

	масштабованість та інтеграцію з типовими інструментами кіберзахисту, такими як SIEM, DLP, IDS/IPS. У моделі реалізовано вузли, які описують як технічні й поведінкові ознаки активності користувачів, так і фактори, пов'язані з організаційним контекстом і управлінськими повноваженнями. Протестовано та впроваджено систему підтримки прийняття рішень (СППР), адаптовану для використання фахівцями підрозділів інформаційної безпеки. СППР забезпечує покроковий інтерфейс введення даних, що дозволяє поступово формувати індивідуальний профіль ризику співробітника, здійснювати автоматичний аналіз на основі заданої моделі та візуалізувати результати у зручному вигляді.
4. Значущість отриманих результатів	Практичне значення дисертаційного дослідження полягає у розробленні, програмній реалізації та апробації інтелектуальної моделі виявлення інсайдерських загроз у хмарних середовищах з використанням модифікованої баєсівської мережі, що дає змогу здійснювати багатофакторну оцінку ризику, пов'язаного з поведінкою співробітників, які взаємодіють із хмарними сервісами, зокрема з урахуванням можливих шахрайських дій з боку осіб, які займають керівні посади. У структурі баєсівської мережі враховано цифрові сліди, поведінкові аномалії та організаційні фактори ризику, що дозволяє підвищити точність виявлення внутрішніх порушників на ранніх етапах.

Від Національного університету біоресурсів і природокористування України

Декан факультету
інформаційних технологій
д.т.н., професор

_____ Ігор БОЛБОТ
(підпис) (ПІБ)
«16» 01 2026 р.

Заступник декана
з наукової роботи
д.е.н., професор

_____ Володимир КРАВЧЕНКО
(підпис) (ПІБ)
«14» 01 2026 р.

Від організації

Керівник підрозділу, де безпосередньо впроваджені результати дисертаційної роботи

"ІНФОБІТ" Ідентифікаційний код 45134665

_____ Ігор ПАСЕМКО
(підпис) (ПІБ)
« 16 » січня 2026 р.

Додаток В

Акт впровадження результатів дисертаційного дослідження у освітній процес НУБіП України

ЗАТВЕРДЖУЮ

Проректор з наукової роботи та інноваційної [illegible]льності Націона[illegible]ету біоресурсів і приро[illegible] України доктор [illegible]ких наук, профе[illegible]

______ [illegible] ТА[illegible]ХА

«12» ______ 2025 р.

ПОГОДЖЕНО

Керівник центру забезпечення якості освіти Національного університету біоресурсів і природокористування України кандидат педагогічних наук, доцент

______ **Ярослав РУДИК**

«12» грудня **2025 р.**

А К Т

про впровадження/використання результатів дисертації на здобуття ступеня доктора філософії у навчальний процес

Цим актом стверджується, що результати дисертації на тему: «**Комп'ютерні баєсівські моделі виявлення інсайдерів у хмарних сервісах**»

яку представлено на здобуття ступеня доктора філософії з галузі знань 12 – Інформаційні технології та спеціальності 122 – Комп'ютерні науки, виконаної Глазуновим Андрієм Сергійовичем,

впроваджено у освітній процес під час викладання дисциплін «Технології хмарних обчислень» та «Технології захисту інформації» на кафедрі інформаційних систем і технологій у процесі підготовки фахівців ступеня вищої освіти «Бакалавр» зі спеціальності Інформаційні системи та технології та освітнього ступеня «Магістр» освітньо-професійної програми Інформаційно-комунікаційні технології в освіті у Національному університеті біоресурсів і природокористування України.

При викладанні дисципліни «Технології хмарних обчислень» здобувачі освіти ознайомлені з принципами захисту даних у хмарних сервісах, Моделями загроз у Cloud-середовища, зовнішніх та внутрішніх атаках, класифікацією інсайдерів, інструментами для моніторингу та аудиту активності у хмарах. Запропоновано лабораторну роботу з моделювання сценарію інсайдерської атаки в Cloud-середовищі.

При викладанні дисципліни «Технології захисту інформації» було запропоновано матеріали для теоретичного навчання з моделювання профілю порушника в інформаційних системах. Розроблена постановка лабораторної роботи з побудови імовірнісного портрету інсайдера з використанням баєсівського підходу для відрізнення помилки легітимного користувача від цілеспрямованої крадіжки даних.

Декан факультету інформаційних технологій
д.т.н., професор — Ігор БОЛБОТ

Заступник декана з наукової роботи
д.е.н., професор — Володимир КРАВЧЕНКО

Завідувач кафедри
к.е.н., доцент, почесний професор — Михайло ШВИДЕНКО