DOI: https://doi.org/10.26642/ten-2025-2(96)-90-94
УДК 004.56

А.С. Глазунов, аспірант
А.М. Гуржій, д.т.н., проф.
Національний університет біоресурсів і природокористування України

Метод раннього виявлення інсайдерів у хмарних середовищах

У статті розглянуто проблему виявлення інсайдерських загроз у хмарних сервісах, яка набула актуальності у зв'язку зі стрімко цифровізацією бізнес-процесів. Встановлено, що, попри наявність широкого спектра технічних засобів забезпечення інформаційної безпеки (ІБ), таких як IDS, DLP, SIEM і ACS-системи, більшість організацій виявляються недостатньо підготовленими до протидії складним загрозам з боку внутрішніх порушників. Це пояснюється тим, що наявні засоби ІБ здебільшого орієнтовані на виявлення зовнішніх атак і не забезпечують достатньої гнучкості в умовах зміни поведінки співробітників із правами розширеного доступу. У статті запропоновано вдосконалений метод раннього виявлення інсайдерів у хмарних середовищах, який базується на використанні модифікованої моделі баєсівської мережі. Новизною методу є включення до структури мережі спеціалізованих вузлів, що відображають організаційні та поведінкові індикатори рівня ризику, а також цифрові сліди, які залишають співробітники під час взаємодії з хмарною інфраструктурою. Вперше формалізовано і змодельована ймовірність шахрайських дій саме з боку керівного персоналу компанії, що істотно підвищує точність виявлення загроз. Запропоновану модель реалізовано програмно й апробовано на синтетичному наборі даних. Отримані результати демонструють працездатність підходу та підтверджують його доцільність для подальшого впровадження у системи підтримки прийняття рішень в інформаційній безпеці.

Ключові слова: *інсайдерська загроза; внутрішній порушник; хмарні сервіси; інформаційна безпека; баєсівська мережа; цифрові сліди; поведінкові індикатори; апріорна ймовірність; апостеріорна ймовірність; адаптивне виявлення; прогнозування ризиків; система підтримки прийняття рішень; аналіз аномалій.*

Актуальність теми. Впровадження хмарних сервісів (ХС) в інформаційну інфраструктуру компаній, установ та органів державного управління посприяло цифровізації ключових секторів економіки. Це зокрема, фінанси, охорона здоров'я, енергетика, логістика й освіта [1, 2]. Хмарні обчислення (ХО) забезпечили масштабованість, високу доступність та гнучкість в управлінні обчислювальними ресурсами компаній та установ. Але, попри очевидні переваги, збільшився рівень інформаційних ризиків. Передусім тих, що пов'язані з діяльністю внутрішніх зловмисників – інсайдерів. Актуальність виявлення інсайдерських загроз у хмарних середовищах обумовлена не лише їхнім високим деструктивним потенціалом, але й складністю своєчасного виявлення через відсутність чітко виражених ознак поведінки, що відрізняють дії інсайдера від легітимної активності користувача. Попри наявність великого спектра технічних засобів кіберзахисту (КІБ) (DLP, SIEM, IDS/IPS тощо), більшість з них орієнтована на виявлення зовнішніх атак або стандартних аномалій, що не дозволяє ефективно протидіяти складним сценаріям інсайдерської поведінки. Проблема ускладнюється у випадках, коли йдеться про співробітників, які мають розширені права доступу або займають керівні посади [3]. Такі загрози часто реалізуються у вигляді шахрайських дій із затриманим ефектом або в обхід формальних правил доступу.

В умовах озброєної агресії проти нашої країни хмарні інфраструктури активно інтегруються в бізнес-процеси приватних компаній, установ і державних органів, забезпечуючи гнучкий доступ до ресурсів та даних. Однак разом із перевагами зростає ймовірність складних інформаційних загроз з боку співробітників, які мають легітимний доступ до систем, особливо тих, хто обіймає керівні посади. Наявні технічні засоби інформаційної безпеки (ІБ) орієнтовані переважно на виявлення зовнішніх атак або технічно орієнтованих аномалій в мережі, і не здатні ефективно протидіяти поведінковим сценаріям інсайдерської активності. Передусім складними є випадки, коли потенційні загрози маскуються під легальні дії користувача в межах його посадових повноважень. Відсутність моделей, здатних інтегрувати цифрові сліди, поведінкові ознаки та організаційний контекст у єдину систему оцінювання рівня ризику, створює потребу у побудові нових інструментів для виявлення інсайдерів. Тому виникла необхідність у розробленні моделі, що дозволяла б оцінювати рівень ризику інсайдерської загрози до настання інциденту та підтримувала прийняття обґрунтованих рішень у реальному часі.

Аналіз останніх досліджень та публікацій, на які спираються автори. Наявні наукові підходи пропонують використання моделей машинного навчання та штучного інтелекту, серед яких можна виділити баєсівські мережі, здатні моделювати причинно-наслідкові зв'язки між ризик-факторами та оцінювати рівень загрози в умовах невизначеності. У працях українських і зарубіжних дослідників

(С.М. Шевченко, Ю.Д. Жданова, П.М. Складанний, С.В. Бойко [4], A.Wall, I.Agrafiotis [9], N.Elmrabit, S.H. Yang, L.Yang, H.Zhou [8], N.d'Ambrosio, G.Perrone, S.P. Romano [7] та ін.) проаналізовано можливості побудови систем поведінкової аналітики, заснованої на дослідженнях цифрових слідів користувача. Проте значна частина наявних рішень не враховує складну багаторівневу структуру ризиків, пов'язаних із посадовими повноваженнями, специфікою взаємодії з хмарними сервісами та аспектами поведінки.

Таким чином, актуальним є розроблення математично обґрунтованої моделі для виявлення інсайдерських загроз у хмарних сервісах, яка б ураховувала технічні, поведінкові та організаційні індикатори, дозволяла оцінювати рівень ризику до фактичного порушення та була придатною для програмної реалізації у вигляді компонента системи підтримки прийняття рішень (СППР) у сфері КІБ.

Метою статті є розроблення та формалізація імовірнісної моделі виявлення інсайдерських загроз у хмарних сервісах на основі модифікованої баєсівської мережі, яка дозволяє враховувати технічні, поведінкові та організаційні індикатори ризику, зокрема для користувачів з розширеними правами доступу, з метою підвищення точності раннього виявлення потенційних порушень інформаційної безпеки.

Викладення основного матеріалу. Нехай $B = \langle G, \Theta \rangle$, де B – модифікована баєсівська мережа, $G = \langle V, E \rangle$ – орієнтований ациклічний граф (DAG), $V = \{I, T.B.O, R\} \cup V_{cloud}$ – множина вузлів, де I – змінна «Інсайдер», T – технічні індикатори (логування, права доступу, DLP), B – поведінкові індикатори (активність, шаблони, відхилення), O – організаційні індикатори (посада, повноваження, історія), R – рівень ризику доступу до інформаційних ресурсів, V_{cloud} – вузли, пов'язані з інфраструктурою хмарних сервісів.

Тоді ймовірнісну модель для пошуку інсайдера запишемо так:

$$P = \{I.TB, O, R\} = \prod_{v \in V} P\big(v|pa(v)\big),$$

де $pa(v)$ – множина батьківських вузлів для v.

Відповідно облік спеціалізованих вузлів (керівний персонал), який може буди інсайдером, запишемо так. Нехай $O = \{O_1, O_2 \dots, O_k\}$ – множина організаційних індикаторів, зокрема:

$O_{pos} \in \{\text{рядовий , керівник}\}$, $O_{auth} \in \{\text{низький , високий}\}$, O_{susp} – історія підозрілих дій керівника.

Урахування організаційного статусу співробітника, зокрема перебування на керівній посаді, дозволило деталізувати модель інсайдерської поведінки на рівні внутрішньої структури компанії або підприємства. Проте для забезпечення ефективного функціонування моделі необхідно також формалізувати вхідні ознаки, які репрезентують цифрові сліди та техніко-поведінкові індикатори активності користувача. Саме такий рівень деталізації дозволив баєсівській мережі адекватно реагувати на зміни поведінки користувача.

Модель дозволила оцінювати умовну ймовірність інсайдерської загрози для керівника:

$$P\big(I = 1|O_{pos} = \text{керівник}, O_{auth}, O_{susp}, T.B\big) \geq \tau,$$

де τ – поріг спрацьовування (порогове правило).

Після формалізації множини вхідних ознак, що відображають ризикоорієнтовану поведінку користувача, виникає потреба в гнучкому механізмі їх оцінювання у часі. Статична оцінка ймовірності загрози в умовах ХС є недостатньою для практичних задач. Тому наступним кроком стала побудова моделі, яка підтримує оновлення апостеріорної ймовірності та прийняття рішення залежно від контексту і встановленого порогового значення, що змінюється з урахуванням функцій втрат і значущості ознак.

Формалізуємо цифрові індикатори за якими можна зробити висновок про інсайдерську діяльність на керівній посаді. Нехай $x = (x_1, x_2 \dots, x_n)$ – спостереження цифрових слідів (за допомогою систем DLP, SIEM, IDS/IPS тощо). Тоді апріорна ймовірність інсайдерської загрози визначається так: $P(I = 1)$ та апостеріорна так:

$$P(I = 1|x) = \frac{P(I = 1|x)P(I = 1)}{P(x)},$$

де $P_{(x)} = P(x|I = 1)P(I = 1) + p(x|I = 0)P(I = 0)$.

Відповідно для виявлення загроз інсайдерської діяльності визначимо послідовне баєсівське правило:

$$\pi_t = p\big(I = 1|X_{1,\dots}x_t\big);$$

$$\delta^*(t) = \begin{cases} 1, \text{якщо } \pi_1 \geq \tau_1, \\ 0, \text{інакше}, \end{cases}$$

де τ_1 – динамічний поріг, який адаптується на основі контексту, функцій втрат та ваг факторів.

Адаптація порогів прийняття рішень забезпечує чутливість моделі до змін у поведінкових або технічних характеристиках. Проте це не враховує повною мірою нерівноцінність наслідків хибнопозитивних і хибнонегативних рішень. У реальних умовах ціна помилки суттєво різниться залежно від типу інциденту, ролі користувача та критичності інформаційного ресурсу у ХС.

Отже, наступним етапом є побудова функції ризику з нелінійними залежностями, що дозволила б точно калібрувати рішення та мінімізувати очікувані втрати, що обґрунтовує застосування оптимальних баєсівських правил у процесі виявлення інсайдерських загроз для ХС.

Тоді функція апостеріорного ризику для прийняття рішення δ про інсайдерську діяльність на керівній посаді буде такою:

$$R(\delta) = c_{fp} \cdot P(\delta = 1|I = 0) + c_{fn} \cdot P(\delta = 0|I = 1),$$

де c_{fp} – вартість хибнопозитивного спрацьовування системи виявлення інсайдеру, c_{fn} – вартість пропуску інсайдера.

Відповідно оптимальне рішення запишемо так

$$\delta^*(t) = \begin{cases} 1 \frac{P(I=1|x)}{P(I=0|x)} \geq \frac{c_{fp}}{c_{fn}}. \\ 0, \text{інакше} \end{cases}$$

Зведена ієрархія моделі може бути подана так:

- рівень ознак (індикаторів) – T, B, O;
- рівень апостеріорної оцінки –$P(I|T, B, O)$;
- рівень оптимального рішення – $\delta^*(t)$;
- рівень стратегічного реагування – побудова СППР.

У модифікованій баєсівській мережі, як зображено на рисунку 1, зв'язки між вузлами реалізовані у вигляді спрямованих дуг, які відображають причинно-наслідкові залежності між факторами ризику. Наприклад, зниження морального стану персоналу (вузол, що належить до організаційної групи індикаторів) може спричинити зростання рівня незадоволення співробітника (вузол з атрибутивної підгрупи), що своєю чергою підвищує ймовірність інсайдерської активності (рис. 1).

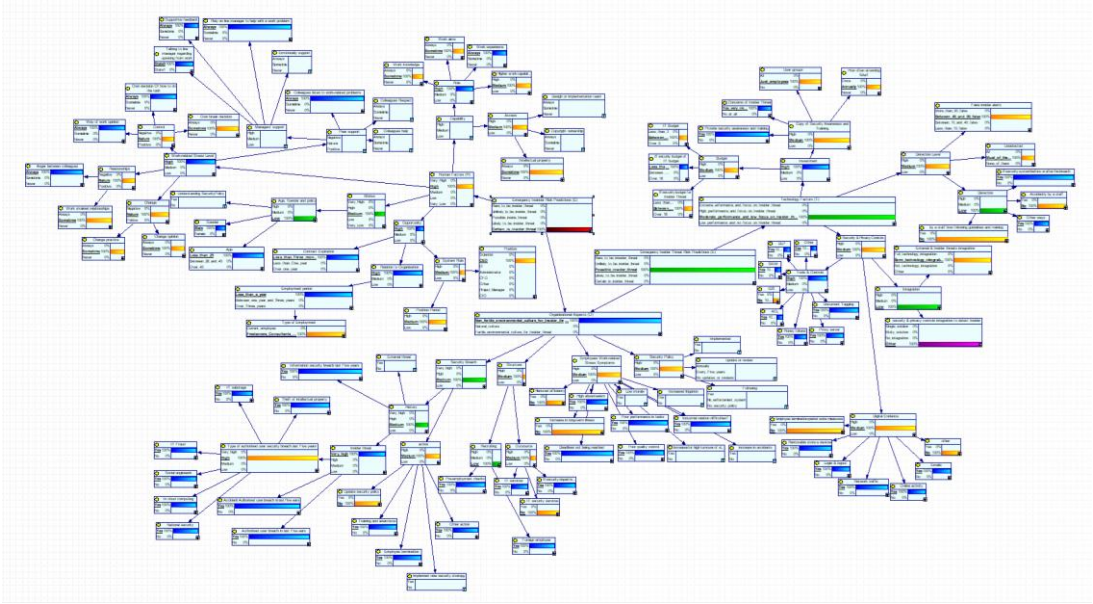

Рис. 1. Модифікована мережа Байєса для СППР та моделювання ймовірності виявлення інсайдерів, з урахуванням специфіки хмарних сервісів, що використовуються в організації

Застосування такої моделі в середовищі GeNIe/SMILE дозволило здійснювати кількісну оцінку ризику інсайдерських загроз у хмарних сервісах на основі вхідних даних – як об'єктивних цифрових слідів, так і експертно визначених параметрів.

У результаті, для кожного вузла мережі для компанії, яка розглядалася під час дослідження, встановлені апріорні або емпірично уточнені ймовірності, що дало змогу моделювати різноманітні сценарії розвитку подій та ідентифікувати вразливі компоненти ХС.

Дані для побудови та апробації моделі модифікованої мережі Байєса для СППР та моделювання ймовірності виявлення інсайдерів, з урахуванням специфіки хмарних сервісів надані компанією ТОВ «Аджілівей», що надала узагальнені статистичні відомості щодо взаємодії співробітників із хмарними сервісами, а також анонімізовані цифрові сліди користувачів. Це дозволило під час обчислювальних експериментів сформувати репрезентативний набір даних, на основі якого здійснено навчання моделі та верифікацію її ефективності для виявлення потенційних інсайдерських загроз.

На відміну від базової моделі, запропонованої в [5, 6], розроблена модифікована мережа враховує специфіку ризиків, притаманних саме хмарним середовищам. Запропонована модель забезпечує більш точну інтеграцію організаційних, поведінкових і технічних факторів, що виникають під час взаємодії користувачів з хмарною інфраструктурою, та дозволило здійснювати комплексну оцінку потенційної загрози в умовах неповноти або невизначеності інформації яка стосується інсайдерської діяльності на керівних посадах.

Запропонована модель реалізована як окремий модуль СППР на мові програмування Python. На рисунку 2 представлено результуюче розподілення ймовірності інсайдерської загрози серед співробітників, одного відділу. Кожен стовпчик на гістограмі рисунку 2 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. Таким чином, в результаті досліджень було побудовано модель мережі Баєса для моделювання внутрішніх порушників безпеки та інсайдерів. Модель дає можливість оцінити ймовірність інсайдерської загрози для кожного співробітника компанії на підставі трьох факторів: людського, організаційного і технологічного.

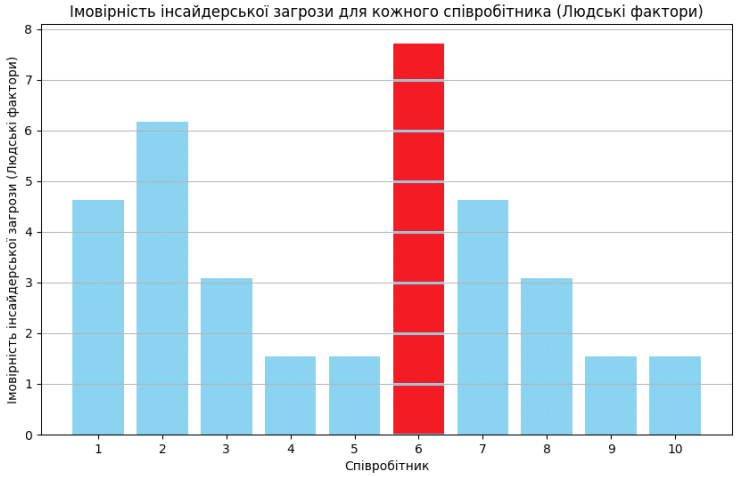

Рис. 2. Результуюче розподілення ймовірності інсайдерської загрози серед співробітників одного відділу

Висновки та перспективи подальших досліджень. 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.

Вперше запропоновано модель мережі Баєса, 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 Баєса, яка для синтетичного набору даних показала свою працездатність, це дало можливість говорити про те, що вона доцільна для імплементації до структури контурів ІБ.

Отримав подальший розвиток метод раннього виявлення інсайдерів в організаціях, що використовують ХС, заснований на використанні мережі Баєса 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.

Список використаної літератури:

1. *Голячук Н.В.* Хмарні обчислення: завтрашній день бізнесу / *Н.В. Голячук, С.Є. Голячук, В.С. Рихлюк* // Економічні науки. Серія «Облік і фінанси». – 2014. – Вип. 11 (1). – С. 37–43.
2. *Продеус К.І.* Особливості застосування хмарних технологій у малому бізнесі / *К.І. Продеус* // Математичні методи, моделі та інформаційні технології в управлінні підприємством : тези доповідей ІІ студентської вузівської наукової конференції. – С. 137–140.
3. *Поночовний Ю.Л.* Аналіз загроз і заходів із забезпечення безпеки в системах хмарних обчислень з послугою PaaS / *Ю.Л. Поночовний, І.О. Черницька, І.В. Замковець* // Збірник наукових праць Харківського університету Повітряних Сил. – 2016. – Вип. 3. – С. 104–107.
4. Інсайдери та інсайдерська інформація: суть, загрози, діяльність та правова відповідальність / *С.М. Шевченко, Ю.Д. Жданова, П.М. Складанний, С.В. Бойко* // Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». – 2022. – № 15 (3). – С. 175–185.
5. *Wall A.* A Bayesian approach to insider threat detection / *A.Wall, I.Agrafiotis* // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. – 2021. – Vol. 12, Issue 2. – P. 48–84.
6. Insider threat risk prediction based on Bayesian network / *N.Elmrabit, S.H. Yang, L.Yang, H.Zhou* // Computers & Security. – 2020. – Vol. 96.

7. *d'Ambrosio N.* Including insider threats into risk management through Bayesian threat graph networks / *N.d'Ambrosio, G.Perrone, S.P. Romano* // Computers & Security. – 2023. – Vol. 133.
8. *Cappelli D.M.* The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud) / *D.M. Cappelli, A.P. Moore, R.F. Trzeciak*. – Addison-Wesley, 2012.
9. Proactive insider threat detection through graph learning and psychological context / *O.Brdiczka, J.Liu, B.Price and other* // In Proc. of the 2012 IEEE Symposium on Security and Privacy Workshops (SPW'12). – San Francisco, California, USA. – P. 142–149.

References:

1. Holiachuk, N.V., Holiachuk, S.Ye. and Rykhliuk, V.S. (2014), «Khmarni obchyslennia: zavtrashnii den biznesu», *Ekonomichni nauky. Seriia «Oblik i finansy»*, Issue 11 (1), pp. 37–43.
2. Prodeus, K.I., «Osoblyvosti zastosuvannia khmarnykh tekhnolohii u malomu biznesi», *Matematychni metody, modeli ta informatsiini tekhnolohii v upravlinni pidpryiemstvom*, tezy dopovidei II studentskoi vuzivskoi naukovoi konferentsii, pp. 137–140.
3. Ponochovnyi, Yu.L., Chernytska, I.O. and Zamkovets, I.V. (2016), «Analiz zahroz i zakhodiv iz zabezpechennia bezpeky v systemakh khmarnykh obchyslen z posluhoiu PaaS», *Zbirnyk naukovykh prats Kharkivskoho universytetu Povitrianykh Syl*, Issue 3, pp. 104–107.
4. Shevchenko, S.M., Zhdanova, Yu.D., Skladannyi, P.M. and Boiko, S.V. (2022), «Insaidery ta insaiderska informatsiia: sut, zahrozy, diialnist ta pravova vidpovidalnist», *Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika»*, No. 15 (3), pp. 175–185.
5. Wall, A. and Agrafiotis, I. (2021), «A Bayesian approach to insider threat detection», *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, Vol. 12, Issue 2, pp. 48–84.
6. Elmrabit, N., Yang, S.H., Yang, L. and Zhou, H. (2020), «Insider threat risk prediction based on Bayesian network», *Computers & Security*, Vol. 96.
7. d'Ambrosio, N., Perrone, G. and Romano, S.P. (2023), «Including insider threats into risk management through Bayesian threat graph networks», *Computers & Security*, Vol. 133.
8. Cappelli, D.M., Moore, A.P. and Trzeciak, R.F. (2012), «The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud)», *Addison-Wesley*.
9. Brdiczka, O., Liu, J., Price, B. et al. (2012), «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, pp. 142–149.

Глазунов Андрій Сергійович – аспірант факультету інформаційних технологій Національного університету біоресурсів і природокористування України.

Наукові інтереси:

– моделі системи технології захисту інформації в інформаційних середовищах.

Гуржій Андрій Миколайович – доктор технічних наук, професор кафедри інформаційних систем і технологій Національного університету біоресурсів і природокористування України.

Наукові інтереси:

– технології інформаційно-комунікаційного забезпечення освітнього процесу.

Hlazunov A.S., Gurzhii A.M.

Early detection method for insiders in cloud environments

The article examines the problem of detecting insider threats in cloud services (CS), which has become pressing due to the rapid digitalization of business processes. It is established that despite a wide range of information security (IS) tools – such as IDS, DLP, SIEM, and access control systems (ACS) – most organizations prove insufficiently prepared to counter sophisticated threats from internal malicious actors. This is because existing IS tools are largely oriented toward detecting external attacks and do not provide sufficient flexibility amid changing behavior of employees with elevated access rights.

The article proposes an improved method for early detection of insiders in cloud environments based on a modified Bayesian network model. The novelty of the method lies in incorporating specialized nodes into the network structure that reflect organizational and behavioral risk indicators, as well as the digital footprints left by employees when interacting with the cloud infrastructure. For the first time, the probability of fraudulent actions specifically by a company's managerial staff is formalized and modeled, which significantly increases threat detection accuracy. The proposed model is implemented in software and validated on a synthetic dataset. The obtained results demonstrate the viability of the approach and confirm its suitability for further integration into decision-support systems in information security.

Keywords: insider threat; internal malicious actor; cloud services; information security; Bayesian network; digital footprints; behavioral indicators; prior probability; posterior probability; adaptive detection; risk prediction; decision support system; anomaly analysis.

Стаття надійшла до редакції 02.09.2025.