КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.25.103117
УДК 004.56

Глазунов Андрій Сергійович
аспірант спеціальності 122 Комп'ютерні науки
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID: 0009-0003-8631-8430
glasgarick2013@gmail.com

РОЗРОБКА БАЙЄСІВСЬКИХ МЕРЕЖ ДЛЯ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ПІД ЧАС АНАЛІЗУ ВНУТРІШНІХ КІБЕРЗАГРОЗ

Анотація. Сьогодні хмарні обчислення стали важливою технологічною парадигмою, що набула широкого впровадження в діяльності сучасних організацій, у тому числі в Україні. Перехід до хмарних сервісів (ХС) дозволяє компаніям підвищити ефективність, гнучкість та конкурентоспроможність, а також оптимізувати операційні витрати та ризики, пов'язані з інформаційною безпекою (ІБ). Хмарні технології забезпечують доступність, масштабованість та надійність корпоративних програмних додатків і систем, що сприяє їх широкому застосуванню в сучасному бізнес-середовищі. Разом з тим, використання ХС породжує нові виклики та загрози ІБ, серед яких чільне місце займають внутрішні порушники. Внутрішні загрози ІБ можуть становити найбільшу небезпеку для компаній. Це можуть бути як навмисні дії з боку нелояльних співробітників, так і ненавмисні помилки чесних працівників. Внутрішні порушники можуть мати прямий доступ до конфіденційної інформації та систем, що ускладнює виявлення та протидію цим загрозам. Ефективне управління ризиками внутрішніх загроз вимагає комплексного підходу, що включає технічні, організаційні та кадрові заходи безпеки. Ця робота є спробою розробки методу раннього виявлення таких порушників, що базується на застосуванні мереж Байєса. Запропонована в дослідженні класифікація внутрішніх порушників та визначені індикатори їх активності становлять новий підхід до аналізу та виявлення загроз ІБ в хмарному середовищі. Реалізація моделі, що навчається, мовою Python і GeNIe Modeler демонструє можливість створення ефективних засобів виявлення порушників, які можуть доповнити наявні DLP-системи. Застосування сучасних інструментів розробки та моделювання робить цю роботу актуальною та інноваційною в галузі захисту хмарних сервісів від внутрішніх загроз інформаційної безпеки. Подальші дослідження передбачають деталізацію запропонованого методу, а також аналіз інших математичних підходів, що можуть бути використані для вирішення поставленого завдання, з оцінкою результатів їх застосування.

Ключові слова: хмарні сервіси; інформаційна безпека; внутрішні порушники; мережа Байєса.

ВСТУП

Хмарні сервіси стали невід'ємною частиною корпоративних процесів через ряд переваг, які вони пропонують. По-перше, хмарні сервіси забезпечують гнучкість і масштабованість, дозволяючи компаніям швидко адаптуватися до потреб, що змінюються, а також вимогам ринку. Вони дозволяють легко масштабувати обчислювальні ресурси в залежності від навантаження, що сприяє оптимальному використанню ресурсів та економії витрат. По-друге, хмарні срвіси пропонують високу доступність та надійність. Постачальники хмарних послуг забезпечують резервне копіювання даних, географічну реплікацію та безліч механізмів забезпечення безперервної роботи систем. Це дозволяє компаніям мінімізувати ризики простоїв та втрати даних, що особливо важливо для критично важливих програм та бізнес-процесів.

Третя перевага хмарних сервісів — це економічна вигода. Замість необхідності інвестувати значні кошти у власну інфраструктуру та обладнання, компанії можуть використовувати модель оплати за використання та платити лише за реально споживані ресурси. Це знижує капітальні витрати та дозволяє більш ефективно керувати бюджетом ІТ. Нарешті, хмарні сервіси надають великий вибір інструментів та сервісів для розробки, розгортання та керування програмами. Це дозволяє компаніям зосередитись на своїй основній діяльності, а не на управлінні інфраструктурою. Хмарні сервіси також сприяють інноваціям та швидкій доставці нових продуктів та послуг на ринок. Забезпечення інформаційної безпеки (ІБ) в хмарних сервісах є пріоритетом як для провайдерів хмарних послуг, так і для компаній, які використовують ці послуги. У провайдерів хмарних послуг ІБ забезпечується через широкий набір заходів та механізмів. Наприклад, провідні провайдери хмарних послуг, такі як Amazon Web Services (AWS), Microsoft Azure та Google Cloud, приділяють велику увагу безпеці своїх інфраструктурних компонентів. Вони забезпечують фізичну безпеку своїх дата-центрів, мають різні зони доступності, контролюють доступ до обладнання та ресурсів, регулярно аудитуються та сертифікуються сторонніми аудиторами. Крім того, провайдери хмарних послуг пропонують широкий набір інструментів та сервісів для забезпечення безпеки на рівні додатків та даних. Це включає можливості керування доступом, шифрування даних, моніторингу та виявлення інцидентів, а також автоматизації процесів безпеки. Такі сервіси, як AWS Identity and Access Management (IAM), AWS Key Management Service (KMS), AWS CloudTrail та AWS GuardDuty, надають засоби контролю доступу, шифрування, аудиту та виявлення потенційних загроз.

Аналіз останніх досліджень і публікацій. У компаніях, що використовують хмарні сервіси, ІБ також відіграє важливу роль. Компанії повинні вживати заходів для захисту своїх даних та ресурсів у хмарі [1] – [10]. Це включає розробку та реалізацію політик безпеки, навчання співробітників, управління доступом, моніторинг активності користувачів та виявлення внутрішніх загроз. Для розпізнавання внутрішніх загроз, включаючи загрози від інсайдерів, компанії використовують різні механізми та інструменти. Наприклад, системи моніторингу та аналітики допомагають аналізувати активність користувачів, виявляти незвичайні чи підозрілі дії, а також моніторити доступ до чутливих даних та ресурсів [6] – [10]. Також можуть застосовуватися техніки машинного навчання та аналізу поведінки для виявлення аномалій та потенційних загроз.

Багато теоретичних робіт з інсайдерських загроз, наприклад, [9] – [14], досліджують мотиви та засоби інсайдерів. Як показано в цих публікаціях, інсайдерські атаки зазвичай ініційовані різними мотивами. У [11] було 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 інтелектуальної власності зазвичай спрямовані на отримання бізнес-переваг, продаж конфіденційної інформації. У [11] показано, що більшість крадіжок інтелектуальної власності відбувається технічними інсайдерами, які крадуть інтелектуальну власність за допомогою технічних вразливостей 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, наприклад, продати або передати її третім особам. У [11], [14] наголошується, що технічні інсайдери рідко крадуть інтелектуальну власність з метою її прямого продажу.

Натомість вони використовують подібну інформацію у своїх інтересах. Так у [1] наводяться приклади, коли такі дії інсайдерів сприяли останнім 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 [15], [16].

Шахрайство не вимагає технічних знань, і як правило доступніше для реалізації навіть технічно не підготовленим співробітником, який працює з хмарними сервісами в організації. Відповідно, такі дії здійснюють співробітники, які обіймають нижчі посади [11]. Випадки інсайдерського шахрайства, проаналізовані [11], тривали щонайменше п’ять місяців і включали часті випадки серйозних крадіжок чи порушень цілісності.

Як показано в більшості розглянутих робіт, присвячених діям інсайдерів [8] – [16], фінансова вигода є основним мотиватором подібних дій. Особливо це стосується співробітників, які зазнають матеріальних труднощів, і відповідно, які перебувають у скрутному чи тяжкому фінансовому становищі.

Саботаж пов’язаний з порушенням доступності активів кіберпростору та заподіянням шкоди окремим особам. Зазвичай його здійснюють особи, які займають технічні посади, наприклад, системні адміністратори, які мають необхідні повноваження і навички, що може потенційно завдати значної шкоди інформаційним активам компанії. Однак у роботах [8], [9], [11] наведено й інші випадки інсайдерського IT-саботажу, наприклад, коли інсайдер не є тим, хто безпосередньо вчиняє саботаж, а натомість допомагає іншим особам вчиняти правопорушення. Проблема полягає в тому, що багато дій, що виконуються інсайдерами, аналогічні їхнім повсякденним робочим завданням, що ускладнює виявлення зловмисних дій, використовуючи, наприклад, DLP системи. Одним із прикладів може бути випадок, коли співробітник, який має доступ до конфіденційних даних у хмарі для виконання своїх робочих обов’язків, 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 одним прикладом може бути використання хмарних сервісів для передачі конфіденційної інформації між співробітниками, що також може бути стандартною практикою для роботи в команді. Якщо співробітник почне передавати дані, незважаючи 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 можуть бути схожі зі звичайною діяльністю співробітників, важливо використовувати не тільки технічні засоби, такі як системи DLP, але й аналізувати контекст дій та поведінку користувачів. Наприклад, можна враховувати такі фактори:

1. Об’єм та частота доступу. Якщо співробітник раптово почав часто запитувати доступ до даних, які він раніше не запитував, це може бути ознакою аномальної активності.
2. Час доступу. Якщо доступ до даних здійснюється в незвичайний час, наприклад, у неробочий час або під час відпустки, це також може бути ознакою підозрілої активності.

3. Передача даних. Моніторинг передачі даних між пристроями та хмарними сховищами може допомогти виявити несанкціоноване переміщення конфіденційної інформації.
4. Об’єм даних. Раптове копіювання великого обсягу даних з хмари або їх завантаження на зовнішні пристрої може бути індикатором витоку інформації.
5. Поведінка у мережі. Аналіз мережної активності співробітників може виявити незвичайні спроби доступу до ресурсів або використання несанкціонованих програм.

Таким чином, використання аналітики поведінки користувачів та методів машинного навчання потенційно дозволяє створити моделі, які можуть виявляти підозрілі дії, навіть якщо вони здаються стандартними для робочої діяльності.

Мета статті. Апробація можливості моделювання дій внутрішніх порушників інформаційної безпеки хмарних сервісів на підставі застосування мереж Байєса.

МЕТОДИКА ДОСЛІДЖЕННЯ

Внутрішні атаки становлять загрозу для організацій, яка постійно зростає, адже співробітники-шахраї та/або інсайдери, які мають законний доступ до комп’ютерних систем (КС), у тому числі до хмарних сервісів, які використовують у своїх бізнес-процесах, а також володіючи інформацією про політику ІБ в організації, що можуть уникнути виявлення. Організації недостатньо готові до виявлення, стримування та пом’якшення складних внутрішніх, у тому числі інсайдерських атак, оскільки їх методи ІБ адаптовані до переважно зовнішніх загроз. Аналіз публікацій, проведених у рамках першого розділу роботи, 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 обробку мережевих даних. У даному дослідженні, яке представлено в рамках другого розділу дисертації, розглядається архітектура мереж Байєса, здатних враховувати аспекти поведінки разом з мережевими даними. Даний підхід використовує методи машинного навчання для аналізу даних. А також ми вводимо функції, що базуються на теоретичних засадах моделювання інсайдерських загроз. Такий підхід, дозволить аналітикам ІБ враховувати поведінкові особливості співробітників, роблячи бізнес-процеси, побудовані у хмарному сервісі більш безпечними. Застосувавши моделі до синтетичних даних, що буде показано в розділі дисертації, демонструє ефективність викладеного підходу для захисту від внутрішніх загроз, в першу чергу інсайдерів. Розглянуті атаки на синтетичному наборі даних характеризувалися низькою кількістю помилкових спрацьовувань, що свідчить про ефективність запропонованого варіанта рішення.

Відповідальність за ІБ хмарних сервісів, які використовує організація, зазвичай лежить обох сторонах. По-перше, це хмарний провайдер, оскільки саме провайдер хмарного сервісу відповідає за забезпечення безпеки інфраструктури хмарної платформи, включаючи фізичну безпеку дата-центрів, мережевий захист, оновлення та патчінг ПЗ, а також захист від DDoS-атак та інших загроз. По-друге, це користувач. Організація, менеджмент, служби ІБ, інформаційні служби, що використовують хмарні сервіси, також несуть відповідальність за безпечне використання цих сервісів. Принаймні, користувач повинен забезпечити 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, наприклад, 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. Наприклад, 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 та використовувати ці інструменти, а також стежити за безпекою своїх даних та додатків у хмарі.

Наведені в табл. 1 приклади випадків, коли дії співробітників призводили до негативних наслідків для компаній, які використовують хмарні сервіси, мотивують вчених розробляти нові методи та технології для виявлення потенційних інсайдерів з кількох причин.

Таблиця 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	Компанія	Короткий опис інциденту
[1]	Capital One	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.
[2]	Uber	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 був оштрафований на $148 мільйонів за порушення правил конфіденційності даних.
[3]	Microsoft	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 вона могла призвести до серйозних уразливостей в Azure.
[4]	Verizon	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.
[5]	Tesla	У 2018 році співробітник Tesla здійснив витік конфіденційних даних про виробничі процеси компанії. Наслідки — конкурентоспроможність та безпека компанії.
[6]	Dropbox	У 2014 році інсайдер з Dropbox отримав доступ до облікових записів користувачів без їх дозволу. Наслідки порушення конфіденційності даних та негативно позначилося на репутації компанії.
[7]	NASA	У 2011 році зафіксовано випадок, коли колишній співробітник NASA потай отримав доступ до чутливої інформації і передав її третій стороні. Наслідки — витік конфіденційних даних та збитків для організації.

По-перше, такі випадки (а в табл. 1 показано лише незначну кількість подібних інцидентів) показують, що існуючі методи захисту від інсайдерських загроз можуть бути недостатньо ефективними. Інсайдери, володіючи знаннями про внутрішні процеси компанії та доступом до цінних даних, можуть обійти стандартні заходи безпеки. Це підштовхує вчених та інженерів до розробки більш надійних та інноваційних методів для виявлення подібних загроз.

По-друге, такі випадки наголошують на необхідності розробки методів, які можуть ефективно розрізняти між нормальною та потенційно небезпечною поведінкою співробітників. Це включає розробку алгоритмів машинного навчання, здатних аналізувати та інтерпретувати дані про активність користувачів, щоб виявляти аномальну поведінку, яка може свідчити про можливу загрозу.

Як видно з прикладів, наведених у табл. 1, виток конфіденційної інформації або несанкціонований доступ до даних можуть призвести до фінансових втрат, шкоди репутації та клієнтам, а також порушення законодавства про захист даних. Такі інциденти демонструють необхідність поліпшення методів виявлення та запобігання подібним загрозам.

Зауважимо, що хоча з точки зору технічної реалізації мережеві атаки залишаються найскладнішими, зловживання персоналу, який працює з хмарними сервісами та категорія кіберинцидентів, які можна віднести до внутрішніх загроз, залишаються найбільш небезпечними з точки зору більшості менеджменту компаній та організацій у всьому світі. При цьому процедура прийняття рішення для оцінки ситуації, пов’язаної із внутрішньою загрозою та прогнозування наслідків від реалізації внутрішньої загрози для організації інформаційної безпеки, потребує чітких алгоритмів дії з боку служб інформаційної безпеки.

У такій ситуації для того, щоб успішно протидіяти внутрішнім порушникам, необхідно не тільки виявити їх протиправні дії на ранній стадії, але й змоделювати подальші кроки з тим чи іншим ступенем ймовірності, а також прорахувати наслідки від реалізації кожного з варіантів дій такого внутрішнього порушника. В подібній ситуації саме байєсівська мережа дозволяє виконати зазначені дії. Також зауважимо, що дії внутрішніх поруників описуються набором подій та фактів. Дані про подібні події та факти з боку захисту організації інформаційної безпеки дозволяють з достатньою ймовірністю зробити висновок, що певний співробітник компанії або може реалізувати, або вже реалізував загрозу ІБ. Таким чином, подібні дані про події та факти можна віднести до індикаторів загроз. Подібні індикатори загроз, залежно від способу отримання інформації, можна поділити на такі категорії:

- технічні (наприклад, отримані за допомогою системи контролю над діями персоналу);
- поведінкові (результат спостережень та фіксації неправомірних дій співробітника з боку служби ІБ).

Поведінкові індикатори відображають поведінку потенційного інсайдера, шкода від дій якого може багаторазово перевершити шкоду від будь-якої, навіть технічно досконалої мережевої атаки. Якщо дії внутрішнього порушника (інсайдера) мотивовані, то як правило, ці дії можуть стати першим етапом цільової атаки на інформаційні ресурси компанії і в такій ситуації поведінкові індикатори, передуватимуть технічним індикаторам [1]. У спеціальних дослідженнях, присвячених вивченню дій інсайдерів, досить докладно описані типові випадки таких дій [1] – [6]. Наприклад, якщо йдеться про потенційний ІТ-саботаж, то на першому етапі з’являється невдоволення співробітника. Якщо служба ІБ проігнорує подібні прояви, то внутрішній порушник

може перейти до реальних дій, наприклад, розкрадання чи псування інформаційних ресурсів. Зауважимо, що дії невмотивованого внутрішнього порушника виявити складно. Абсолютна більшість таких порушень реалізується ненавмисно і без попередньої підготовки.

Для досягнення мети дослідження необхідно вибрати алгоритм навчання байєсівської мережі для завдання з виявлення внутрішнього порушника. Сьогодні алгоритми навчання байєсівських мереж добре вивчені і для подібного завдання, як показано в роботах [17] – [19] найбільш підходять:

- ЕМ-алгоритм;
- методи — релевантних векторів, Монте-Карло, тощо.

Для бази шаблонів байєсівської мережі, що розробляється, важливо правильно описати байєсівську мережу і визначити, що буде входами до неї. У ситуації з моделюванням дій внутрішнього порушника, входи до байєсівської мережі — індикатори подій ІБ, пов'язані з діями внутрішнього порушника. В ситуації, наприклад, з невмотивованим внутрішнім порушником, судити про його дії складно, то подібна інформація для бази знань буде слабоструктурованою, що у свою чергу ускладнює процедуру суджень про прояв деяких індикаторів, наприклад, поведінкових. Отже, в моделі байєсівської мережі з'являються не тільки слабоструктуровані, а й приховані дані. Виходячи з вище сказаного, для моделі байєсівської мережі та її навчання було обрано ЕМ-алгоритм. Даний алгоритм має такі переваги в порівнянні з альтернативними варіантами:

1. Зі зростанням кількості вихідних даних відбувається лінійне збільшення складності алгоритму [17], [20], що прийнятно для постановки задачі моделювання дій внутрішнього порушника;
2. ЕМ-алгоритм стійкий до «шумів» [17];
3. ЕМ-алгоритм дозволяє працювати зі слабоструктурованими та прихованими даними;
4. Реалізація ЕМ-алгоритму будь-якою високорівневою мовою програмування не становить складності. ЕМ-алгоритм включає наступні етапи або кроки:
   - expectation step ($E-$крок);
   - maximization step ($M-$крок). Наприклад маємо набір даних (Y) — індикатори ІБ.

Частина цих даних спостерігалася (X). Інша частина не спостерігалася — (Z). Фактично дані (Z) приховані або Zh. У такій ситуації правомірний запис:

$$Y = X \text{ Y } Zh. \tag{1}$$

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

Крок E:

$$Q(h) = E\left[\ln p(y \mid h) \mid X\right], \tag{2}$$

де $Q(h)$ — 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 $Q(h)$:

$$h_1 = \arg\max_h Q(h). \tag{3}$$

Таким чином, в результаті роботи алгоритму покроково визначатимемо значення (h) при $Q(h)$ для кроку E. Реалізовуватимемо кроки до моменту, поки послідовність (h_k) не стане сходитись.

Таким чином, за допомогою ЕМ-алгоритму знаходитимемо нові оцінки максимальної правдоподібності параметрів байєсівської мережі, використовуючи наявні вибіркові дані. Отримана підсумкова оцінка дасть можливість переглядати байєсівську мережу та значення апріорних ймовірностей подій ІБ, пов'язаних із персоналом. Для навчання байєсівської мережі, чим більше інцидентів ІБ, то точнішим буде результат. Навчена байєсівська мережа, дозволить з великим ступенем точності визначати внутрішніх порушників політики ІБ компанії.

На даному етапі досліджень було згенеровано вибірку з даних, представлених у звітах низки компаній [1], [2] для 100 інцидентів ІБ, які пов'язані з діями інсайдерів. На наступних етапах дослідження кількість інцидентів у вибірці може бути збільшена за рахунок даних, зібраних на підприємствах.

Для навчання мережі розроблено статистичну базу, що складається з понад 100 різних інсайдерських інцидентів. Усі інциденти взяті із відкритих джерел, база постійно поповнюється.

У вибірці, яка використовувалася для навчання, були використані інциденти, віднесені до таких категорій:

1. саботаж (наприклад, некоректне заповнення баз даних);
2. шахрайські дії на керівних посадах (наприклад, спотворення даних звітів компанії у власних інтересах);
3. шахрайські дії рядових співробітників (наприклад, спотворення особистої інформації при влаштуванні на роботу);
4. шпигунство (наприклад, збір інформації для конкурентів);
5. розкрадання інформаційних ресурсів (наприклад, розкрадання БД клієнтів компанії).

За допомогою експертної оцінки (залучалися експерти в галузі ІБ зі стажем не менше 5 років) виділено відповідні індикатори. В результаті опитування було проаналізовано як поведінкові, так і технічні індикатори, які узагальнено у табл. 2.

Таблиця 2

Індикатори для побудови байєсівської мережі

№	Категорія індикатора	Опис	Умовні позначення
1	Технічний (TI)	Підозріла транзакція з облікового запису співробітника	(TI_1)
2		Операції, що підпадають під категорію шахрайських [1] – [6]	(TI_2)
3		Невідповідність даних, заявлених співробітником, результатам аудиту	(TI_3)
4		Факти фальшування документів	(TI_4)
1	Поведінковий (BI)	Виявлені проблеми фінансового характеру у співробітника	(BI_1)
2		Підозрювальні джерела отримання доходів	(BI_2)
3		Стресовий стан співробітника не супроводжуються видимими причинами	(BI_3)

ISSN 2663 - 4023

У статті розглянемо приклад побудови мережі Байєса для ситуації шахрайських дій на керівних посадах компанії, див. рис. 1.

На рис. 1, вершина 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 — порядковий номер індикатора табл. 2.

На рис. 1 наочно продемонстровано, що вибір моделі умовно і значення індикаторів взаємозалежні. Залежність індикаторів від моделі не істотно впливає на потенційну точність ідентифікації внутрішнього порушника. І як було показано в [9], [20] і альтернативна модель у вигляді наївного байєсівського класифікатора, також дозволяє з великим ступенем точності вирішити це завдання.

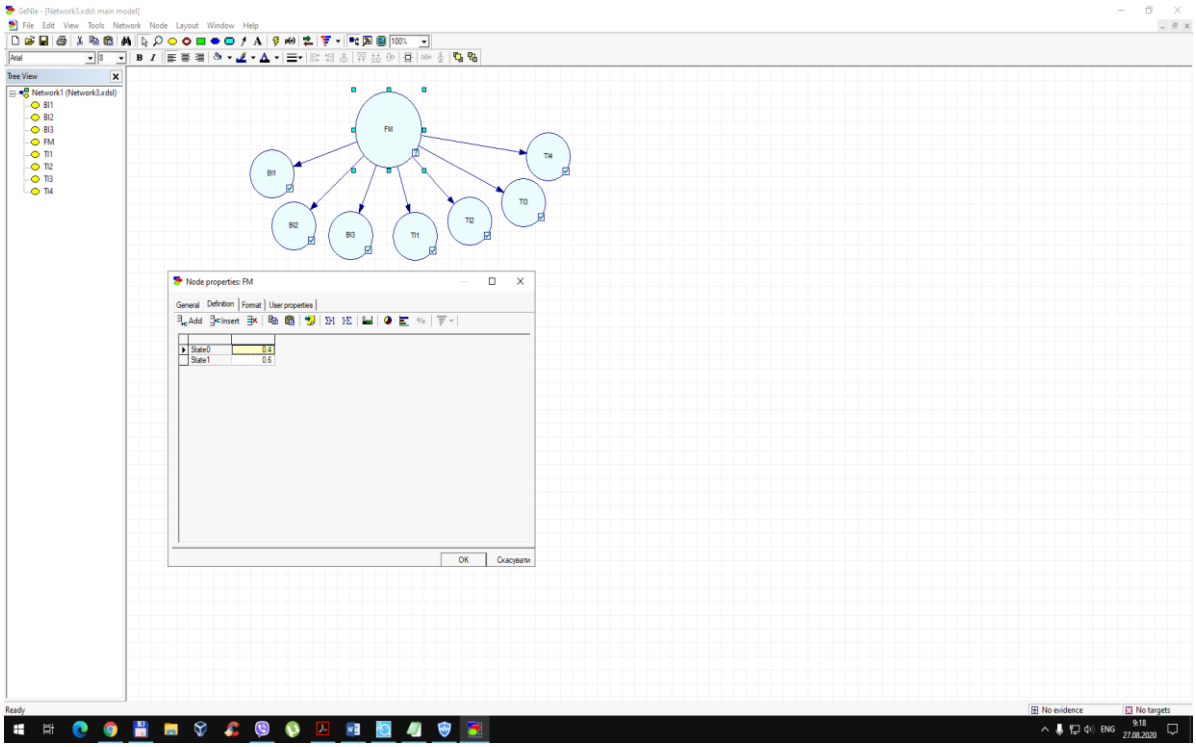

Рис. 1. Байєсівська мережа для ситуації шахрайських дій на керівних посадах компанії.

На наступному етапі побудови байєсівської мережі необхідно заповнити таблиці апріорних ймовірностей (рис. 2).

ISSN 2663 - 4023

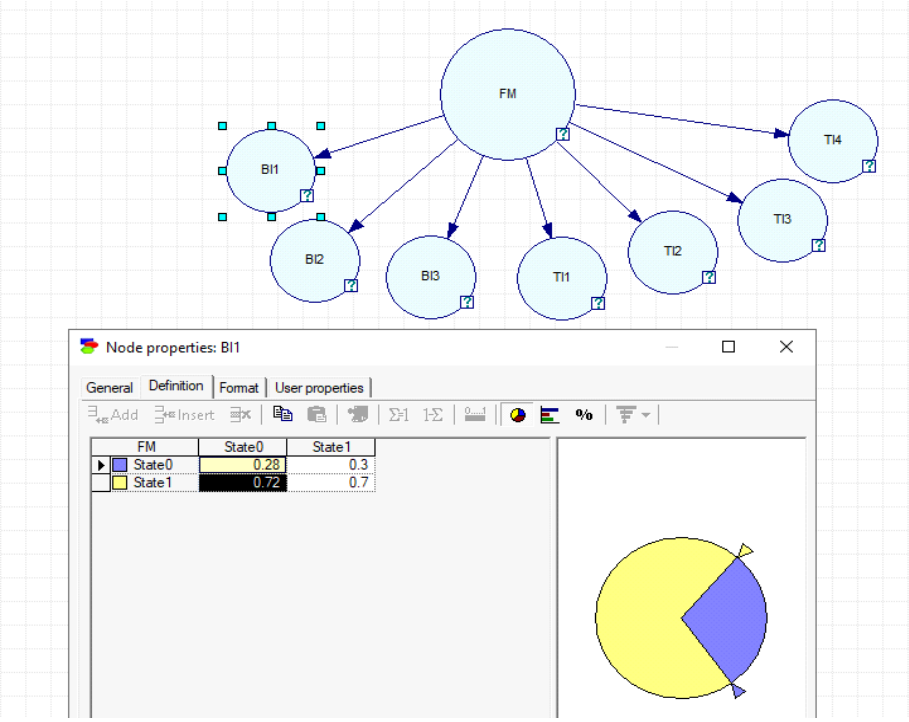

Рис. 2. Заповнення таблиці апріорних ймовірностей байєсівсбкої мережі для ситуації шахрайських дій на керівних посадах компанії

Таким чином, опис батьків вершини дозволить врахувати різні фактори, які можуть впливати на ймовірність невмотивованого порушення правил ІБ співробітником.

Щоб врахувати дану залежність, ми можемо визначити наступну структуру вершин-батьків:

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

Цей код описує ситуацію, коли вершина 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.

Таким чином, баєсівська мережа представляє собою модель для опису ймовірнісних зв'язків між подіями, а також відсутності таких зв'язків. У даній моделі зв'язок $(A \to B)$ від події (A) до події (B) вважається причинною, якщо подія (A) впливає виникнення події (B) та визначає його значення. Для визначення ймовірності приналежності співробітника до певного класу внутрішніх порушників ІБ можна використовувати байєсівську мережу для кожного класу. Переваги застосування байєсівських мереж у цьому контексті включають простоту побудови та інтерпретації,

можливість роботи з неточними та неповними даними, а також можливість навчання в процесі роботи з низькими обчислювальними витратами.

Входами кожної байєсівської мережі є індикатори, які свідчать про потенційні порушення ІБ хмарного сервісу, що виявляються потенційним внутрішнім порушником. Виходом кожної байєсівсбкої мережі 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 байєсівської мережі є імовірнісні залежності між величинами, які визначаються за допомогою таблиці умовної ймовірності.

Заповнення таблиць виконується опираючись на думки експертів, як внутрішніх, співробітників ІБ компанії, так і зовнішніх.

Коли всі таблиці заповнені, виконується навчання байєсівської мережі і в разі потреби коригуються отримані значення ймовірностей.

Початок роботи з байєсівськими мережами відбувається з моменту фіксації спостерігачем, наприклад, співробітником відділу ІБ, одного з індикаторів, наприклад, описаних у табл. 2. Зрозуміло, можна використовувати інші індикатори, які присутні в сучасних системах контролю роботи персоналу. Для того щоб почати роботу з мережею Байєса, необхідно опитати спостерігача про виявлені імовірним порушником індикаторів. Необхідно відзначити, що для отримання інформації про технічні індикатори можна використовувати програмні комплекси моніторингу ІБ та протидії шахрайству. Поведінкові індикатори можна визначити за допомогою спостереження.

Наприклад, співробітник відділу ІБ зафіксував фінансові поведінкові індикатори, рядок 1 для TI та рядок 1 для BI, у табл. 2, відповідно. 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 буде віднесений до внутрішніх порушників, можна обчислити, скориставшись виразом:

$$P(FM \mid BI_1,...,BI_3,TI_1,...,TI_4) = \\ = \frac{P(BI_1 \mid FM)\cdot ... \cdot P(BI_3 \mid FM)}{Z} \cdot \\ \frac{P(TI_1 \mid FM)\cdot ... \cdot P(TI_4 \mid FM)}{Z}, \quad (4)$$

де

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

Нижче розглянуто результати тестування шаблону мережі Байєса (рис. 2) для бази знань. Як і в минулих обчислювальних експериментах, тестова вибірка включала 30 записів.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Результати експериментів показано на рис. 3. На графіках показані результати моделювання ймовірностей коректного визначення та трактування шахрайських дій на керівних посадах компанії. Отримано дані для похибки 1-го роду та 2-го роду. Мережа

навчалася з використання ЕМ алгоритму (лінії 1 та 3. Відповідно, 1 — пунктирна лінія червоного кольору, 3 — лінія помаранчевого кольору) та РС алгоритму (лінії 2 та 4. Відповідно, 2 — суцільна лінія синього кольору, 4 — лінія зеленого кольору).

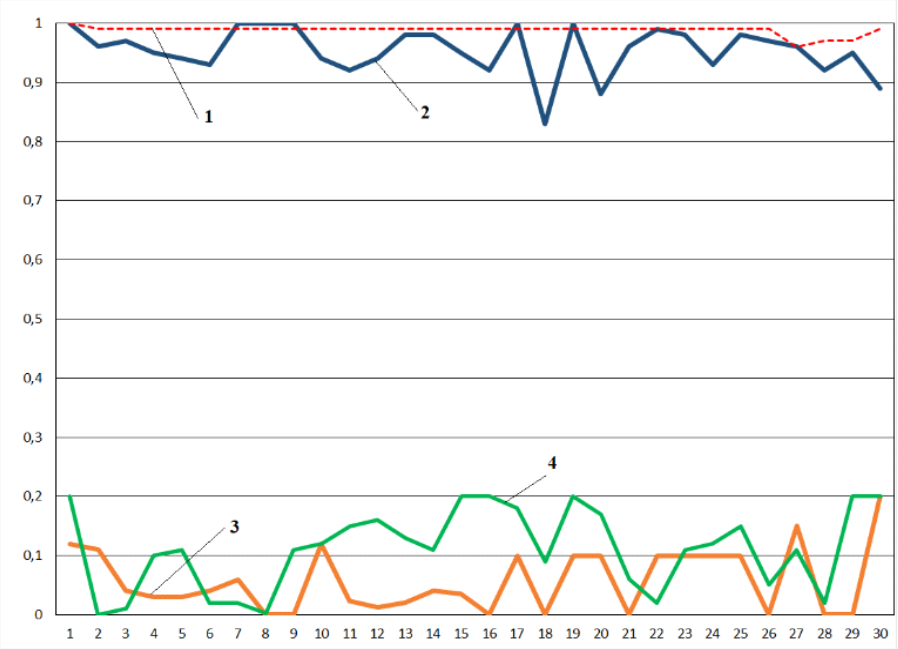

Рис. 3. Імовірність коректного визначення та трактування шахрайських дій на керівних посадах компанії, яка використовує хмарні сервіси (похибки 1-го та другого 2-го роду) для мережі Байєса, які навчалися за допомогою різних алгоритмів.

РС та ЕМ алгоритми показали хороші результати навчання для складеної мережі Байєса. У середньому обидва алгоритми дозволяють із 90–93% точністю чітко визначати виявлення внутрішнього порушника ІБ. Однак, у даній серії обчислювальних експериментів, ЕМ алгоритм показав вищі результати.

Таким чином, у даному підрозділі роботи на конкретному прикладі розглянуто метод виявлення внутрішніх порушників ІБ на основі використання байєсівських мереж. Приклад може бути масштабований і інші ситуації, пов'язані з виявленням внутрішніх порушників. Однак оскільки робота формування бази знань, що включає і мережу Байєса для кожної потенційно небезпечної ситуації є досить трудомісткою, то необхідно в процесі розробки бази знань наповнити її досить великою кількістю байєсівських мереж для всіх ситуацій, які раніше були перераховані в даній статті.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Сьогодні, хмарні сервіси стали невід'ємною частиною корпоративних процесів, вони забезпечують гнучкість і масштабованість, доступність та надійність, а також безліч механізмів забезпечення безперервної роботи систем, що відповідно покращує роботу бізнесу і не тільки. Для розпізнавання внутрішніх загроз, включаючи загрози від інсайдерів, компанії використовують різні механізми та інструменти.

Розглянуто приклад використання байєсівських мереж для виявлення внутрішніх порушників (інсайдерів) ІБ компанії, яка використовує хмарні сервіси у своїх бізнес-

процесах. Приклад може бути масштабований під інші ситуації, пов'язані з виявленням внутрішніх порушників. Однак, оскільки робота формування бази знань, що включає мережі Байєса для кожної потенційно небезпечної ситуації, є досить трудомісткою, то необхідно в процесі розробки бази знань наповнити її досить великою кількістю байєсівських мереж для всіх ситуацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Novaes Neto, N., Madnick, S., de Paula, M. G., & Malara Borges, N. (2020). *A case study of the capital one data breach.* http://dx.doi.org/10.2139/ssrn.3542567
2. Bodie, M. T. (2022). The Law of Employee Data: Privacy, Property, Governance. *Ind. Lj*, *97*.
3. Microsoft: Lapsus$ Used Employee Account to Steal Source Code. (n. d.). https://threatpost.com/microsoft-lapsus-compromised-one-employees-account/179048/
4. Verizon confirms data of 6 million customers was leaked. (n. d.). 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
5. Tesla sues ex-employee for hacking, theft, and leaking to the press. (n. d.). https://www.theverge.com/2018/6/20/17484030/tesla-sues-employee-hacking-theft-leaking
6. Nearly 7 Million Dropbox Passwords Have Been Hacked. (n. d.). https://www.businessinsider.com/dropbox-hacked-2014-10
7. NASA says was hacked 13 times last year. (n. d.). https://www.reuters.com/article/us-nasa-cyberattack-idUKTRE8211G320120303/
8. Agrafiotis, I., Erola, A., Goldsmith, M., & Creese, S. (2016). A tripwire grammar for insider threat detection. *In Proc. of the 8th ACM CCS International Workshop on Managing Insider Security Threats (MIST'16),* 105–108.
9. Agrafiotis, I., Nurse, J. R., Buckley, O., Legg, P., Creese, S., & Goldsmith, M. (2015). Identifying attack patterns for insider threat detection. *Computer Fraud & Security, 2015(7),* 9–17.
10. Eberle, W., Graves, J., & Holder, L. (2010). Insider threat detection using a graph-based approach. *Journal of Applied Security Research, 6(1),* 32–81.
11. Cappelli, D. M., Moore, A. P., & 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*.
12. Brdiczka, O., Liu, J., Price, B., Shen, J., Patil, A., Chow, R., Bart, E., & Ducheneaut, N. (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),* 142–149.
13. Bishop, M., & Gates, C. (2008). 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)*.
14. Нечипуренко, К. О. (б. д.). *Способи виявлення інсайдерів на підприємстві. актуальні проблеми кібербезпеки.*
15. Lewellen, T., Moore, A. P., Cappelli, D. M., Trzeciak, R. F., Spooner, D., & Weiland, R. M. (2012). Spotlight on: Insider threat from trusted business partners. version 2: Updated and revised. *Technical report, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University*.
16. Weiland, R. M., Moore, A. P., Cappelli, D. M., Trzeciak, R. F., & Spooner D. (2010). Spotlight on: Insider threat from trusted business partners. *CERT Program*.
17. Згуровський, М. З., Бідюк, П. І., Терентьєв, О. М., & Просянкіна-Жарова, Т. І. (2015). *Байєсівські мережі в системах підтримки прийняття рішень*. ТОВ «Видавниче Підприємство «Едельвейс».
18. Бідюк, П. І., Терентьєв, О. М., & Коновалюк, М. М. (2010). Байєсівські мережі в технологіях інтелектуального аналізу даних. *Наукові праці [Чорноморського державного університету імені Петра Могили]. Сер.: Комп'ютерні технології, 134(121),* 6–16.
19. Шевченко, С. М., Жданова, Ю. Д., Складанний, П. М., & Бойко, С. В. (2022). Інсайдери та інсайдерська інформація: суть, загрози, діяльність та правова відповідальність. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 15(3),* 175–185.
20. Akhmetov, B., Akhanova, M., Lakhno, V., Ydyryshbayeva, M., Yagaliyeva, B., Baiganova, A., & Tashimova, A. (2021). Application of bayesian networks in the decision support system during the analysis of cyber threats. *Journal of Theoretical and Applied Information Technology, 99(4),* 884–893.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023

Andrii Hlazunov
Postgraduate student, Specialty 122 Computer Science
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID: 0009-0003-8631-8430
glasgarick2013@gmail.com

DEVELOPMENT OF BAYESIAN NETWORKS FOR A DECISION SUPPORT SYSTEM DURING INTERNAL CYBER THREATS ANALYSIS

Abstract. Today, cloud computing has become an important technological paradigm that has become widely implemented in the activities of modern organizations, including in Ukraine. The transition to cloud services (CS) allows companies to increase efficiency, flexibility and competitiveness, as well as to optimize operational costs and risks related to information security (IS). Cloud technologies ensure the availability, scalability and reliability of corporate software applications and systems, which contributes to their widespread use in the modern business environment. At the same time, the use of CS creates new challenges and threats to IS, among which internal violators occupy a prominent place. Internal IS threats can pose the greatest danger to companies. These can be both intentional actions by disloyal employees and unintentional mistakes by honest employees. Insider attackers can have direct access to sensitive information and systems, making it difficult to detect and counter these threats. Effective internal threat risk management requires a comprehensive approach that includes technical, organizational, and personnel security measures. This work is an attempt to develop a method for early detection of such violators based on the application of Bayesian networks. The classification of internal intruders proposed in the study and the identified indicators of their activity constitute a new approach to the analysis and detection of IS threats in the cloud environment. The implementation of the learning model in Python and GeNIe Modeler demonstrates the possibility of creating effective intrusion detection tools that can complement existing DLP systems. The use of modern development and modeling tools makes this work relevant and innovative in the field of protecting cloud services from internal information security threats. Further research involves detailing the proposed method, as well as the analysis of other mathematical approaches that can be used to solve the task, with an assessment of the results of their application.

Keywords: cloud services; informational security; internal violators; Bayes network.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Novaes Neto, N., Madnick, S., de Paula, M. G., & Malara Borges, N. (2020). *A case study of the capital one data breach.* http://dx.doi.org/10.2139/ssrn.3542567
2. Bodie, M. T. (2022). The Law of Employee Data: Privacy, Property, Governance. *Ind. Lj, 97.*
3. Microsoft: Lapsus$ Used Employee Account to Steal Source Code. (n. d.). https://threatpost.com/microsoft-lapsus-compromised-one-employees-account/179048/
4. Verizon confirms data of 6 million customers was leaked. (n. d.). 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
5. Tesla sues ex-employee for hacking, theft, and leaking to the press. (n. d.). https://www.theverge.com/2018/6/20/17484030/tesla-sues-employee-hacking-theft-leaking
6. Nearly 7 Million Dropbox Passwords Have Been Hacked. (n. d.). https://www.businessinsider.com/dropbox-hacked-2014-10
7. NASA says was hacked 13 times last year. (n. d.). https://www.reuters.com/article/us-nasa-cyberattack-idUKTRE8211G320120303/
8. Agrafiotis, I., Erola, A., Goldsmith, M., & Creese, S. (2016). A tripwire grammar for insider threat detection. *In Proc. of the 8th ACM CCS International Workshop on Managing Insider Security Threats (MIST'16),* 105–108.
9. Agrafiotis, I., Nurse, J. R., Buckley, O., Legg, P., Creese, S., & Goldsmith, M. (2015). Identifying attack patterns for insider threat detection. *Computer Fraud & Security, 2015(7),* 9–17.

10. Eberle, W., Graves, J., & Holder, L. (2010). Insider threat detection using a graph-based approach. *Journal of Applied Security Research, 6(1),* 32–81.
11. Cappelli, D. M., Moore, A. P., & 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*.
12. Brdiczka, O., Liu, J., Price, B., Shen, J., Patil, A., Chow, R., Bart, E., & Ducheneaut, N. (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),* 142–149.
13. Bishop, M., & Gates, C. (2008). 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)*.
14. Nechipurenko, K.O. (n. d.). *Ways to identify insiders in the enterprise. topical issues of cybersecurity.*
15. Lewellen, T., Moore, A. P., Cappelli, D. M., Trzeciak, R. F., Spooner, D., & Weiland, R. M. (2012). Spotlight on: Insider threat from trusted business partners. version 2: Updated and revised. *Technical report, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University*.
16. Weiland, R. M., Moore, A. P., Cappelli, D. M., Trzeciak, R. F., & Spooner D. (2010). Spotlight on: Insider threat from trusted business partners. *CERT Program*.
17. Zgurovsky, M. Z., Bidyuk, P. I., Terentyev, O. M., & Prosyankina-Zharova, T. I. (2015). Bayesian networks in decision support systems. *Edelweiss Publishing House LLC.*
18. Bidyuk, P. I., Terentyev, O. M., & Konovaluk, M. M. (2010). Bayesian networks in data mining technologies. *Scientific works [of the Petro Mohyla Black Sea State University]. Ser: Computer Technologies, 134(121),* 6–16.
19. Shevchenko, S. M., Zhdanova, Y. D., Skladanny, P. M., & Boyko, S. V. (2022). Insiders and insider information: essence, threats, activities and legal responsibility. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology", 15(3),* 175-185.
20. Akhmetov, B., Akhanova, M., Lakhno, V., Ydyryshbayeva, M., Yagaliyeva, B., Baiganova, A., & Tashimova, A. (2021). Application of bayesian networks in the decision support system during the analysis of cyber threats. *Journal of Theoretical and Applied Information Technology, 99(4),* 884–893.