ВІДГУК

офіційного опонента
завідувача кафедри комп'ютерної інженерії
Державного університету інформаційно-комунікаційних технологій,
кандидата технічних наук, доцента **ЛАЩЕВСЬКОЇ Наталії Олександрівни**
на дисертацію **ГЛАЗУНОВА Андрія Сергійовича**
на тему: **«Комп'ютерні баєсівські моделі виявлення інсайдерів у хмарних сервісах»**,
подану на здобуття ступеня доктора філософії
за спеціальністю 122 «Комп'ютерні науки»

Актуальність теми дослідження. Парадигма «Zero Trust» (нульової довіри) вимагає перегляду підходів до внутрішнього моніторингу в хмарах. Статичні правила доступу виявилися безсилими перед легітимними діями привілейованих користувачів, які діють зі зловмисними намірами. Актуальність роботи А. С. Глазунова підтверджується необхідністю створення інтелектуальних агентів моніторингу, які здатні виявляти не окремі факти порушень, а складні поведінкові шаблони інсайдерів, що використовують специфіку хмарної інфраструктури для приховування своїх дій.

Зв'язок роботи з науковими програмами, планами і темами. Робота виконана в рамках наукової тематики Національного університету біоресурсів і природокористування України «Стратегія цифрової трансформації економіки України як інструменту забезпечення соціально-економічного розвитку та національної безпеки» (номер державної реєстрації 0121U110194).

Тематика дисертації безпосередньо корелює з державними ініціативами у сфері високих технологій, зокрема з Концепцією розвитку штучного інтелекту в Україні (розпорядження КМУ від 13.04.2024 № 320-р) та пріоритетами ІКТ-сектору (постанова КМУ № 476). Роботу спрямовано на виконання стратегічних завдань із кіберзахисту (Указ Президента № 447/2021), що передбачають розроблення інтелектуальних моделей для протидії внутрішнім загрозам у розподілених хмарних середовищах.

Наукова новизна одержаних результатів дослідження. Здобувачем *вперше:* розроблено модифіковану модель баєсівської 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 баєсівської 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 баєсівських 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 одержаних результатів дослідження. Практичне значення одержаних результатів полягає у розробленні та програмному втіленні моделі на основі модифікованої баєсівської мережі, адаптованої для моніторингу інсайдерських ризиків у хмарній інфраструктурі. Головним прикладним елементом є алгоритмізація послідовних баєсівських правил. Це дозволяє прогнозувати несанкціоновану активність внутрішніх порушників інформаційної безпеки. Система забезпечує багатокритеріальну оцінку загроз через зіставлення апостеріорних ймовірностей із варіативними порогами чутливості, враховуючи при цьому ймовірнісні витрати на хибні спрацювання. Завдяки використанню мови Python та бібліотек GeNIe/SMILE, створене рішення легко інтегрується з існуючими засобами захисту (SIEM, DLP), дозволяючи моделювати загрози з боку привілейованих користувачів та топменеджменту.

Сформульовані рекомендації щодо впровадження баєсівських моделей у хмарні сервіси підтверджені актом про впровадження, що вказує на реальне практичне значення отриманих результатів. Результати дисертаційного дослідження А. С. Глазунова також впроваджені у освітній процес, зокрема, розроблене програмне забезпечення впроваджено у ТОВ «Інфобіт», та у навчальні курси факультету інформаційних технологій Національного університету біоресурсів і природокористування України.

Структура дисертації, достовірність та обґрунтованість наукових положень, висновків та рекомендацій. Дисертація А. С. Глазунова характеризується логічною послідовністю викладу та цілісністю структури. Робота складається з анотації, вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків.

Вступ містить чітке обґрунтування актуальності, визначення об’єкта, предмета та методів дослідження. Розділ 1 присвячено аналітичному огляду сучасних хмарних моделей та критичному аналізу існуючих засобів захисту, що дозволило автору ідентифікувати прогалину у виявленні інсайдерських загроз. Розділ 2 фокусується на розробленні теоретичного підґрунтя – модифікованої баєсівської мережі, інтегрованої з організаційними та технічними індикаторами. Розділ 3 містить алгоритмічну реалізацію послідовних баєсівських правил та результати експериментальної апробації створеного прототипу системи підтримки прийняття рішень.

Висновки дисертації А. С. Глазунова узагальнюють результати комплексного інтелектуального дослідження методів виявлення інсайдерських загроз у хмарних сервісах. Автор послідовно виклав ключові положення, що охопили аналіз вразливостей хмарних інфраструктур, формалізацію технічних та поведінкових індикаторів, розроблення модифікованої моделі баєсівської мережі та впровадження оптимальних послідовних правил перевірки гіпотез для мінімізації ризиків інформаційної безпеки. Висновками підтверджено ефективністю застосування імовірнісного підходу для моделювання дій привілейованих користувачів, зокрема керівного складу, що має критичне прогностичне значення для сучасних систем кіберзахисту. У висновках підкреслено роль адаптивного коригування порогових значень ризику у підвищенні стійкості хмарних систем до складних внутрішніх атак. Висновки є змістовним та переконливим підсумком дисертації. Висновки структуровані у логічній послідовності, що полегшує їх сприйняття, мають вагоме значення для розвитку комп’ютерних наук, інтелектуального аналізу даних та формування стратегій безпечного функціонування цифрової інфраструктури України в умовах глобальної цифровізації.

Список використаних джерел (с. 163–179) містить 153 посилання, з них латиницею 131 джерело. Представлена література є сучасною та відповідає напряму дослідження дисертації. Загальний обсяг роботи становить 190 сторінок. Матеріал ілюстровано 11 таблицями та 37 рисунками. Дисертація доповнена трьома додатками. Вони представлені фрагментом прикладу таблиці з результатами навчання мережі Байєса для виявлення внутрішніх порушників та/або інсайдерів у компанії, актом впровадження результатів досліджень у виробництво та довідкою впровадження результатів дисертації у навчальний процес.

Загальний обсяг дисертації та співвідношення між її частинами відповідають встановленим вимогам для кваліфікаційних праць рівня доктора філософії.

Дослідження демонструє завершений цикл наукової роботи: від обґрунтування проблеми до програмної реалізації та впровадження. Дисертація характеризується концептуальною цілісністю, оскільки поєднує технічні аспекти з поведінковими

та організаційними факторами, відповідністю обраного методологічного апарату та якісною інженерною реалізацією.

Достовірність отриманих результатів не викликає сумнівів і підтверджується фундаментальною базою, зокрема, теорії ймовірностей, математичної статистики та баєсівського висновку. Використання апарату послідовного аналізу Вальда забезпечує математичну надійність процедур прийняття рішень. Використані методи інтелектуального аналізу даних та баєсівського моделювання адекватно відповідають поставленим задачам. Процес навчання мережі (визначення умовних ймовірностей CPD) проведено із застосуванням статистично значущих вибірок. Використання професійного середовища моделювання GeNIe/SMILE у поєднанні з мовою програмування Python дозволило уникнути обчислювальних помилок та забезпечило високу точність ітераційних розрахунків апостеріорних ймовірностей.

Мова та стиль викладення результатів. Дисертація А. С. Глазунова виконана державною мовою і є цілісною сукупністю наукових положень, представлених до публічного захисту. Робота характеризується високим ступенем завершеності, логічною структурованістю та чітко вираженим особистим внеском автора у розв’язання поставленого завдання. Виклад матеріалу відзначається лаконічністю, професійним володінням термінологією та дотриманням методологічних стандартів технічних наук. Належне оформлення ілюстративного матеріалу та відповідність підсумкових результатів сформульованій меті свідчать про високу якість підготовки рукопису. За змістом, тематикою та отриманими результатами дисертація повністю відповідає профілю спеціальності 122 «Комп’ютерні науки» галузі знань 12 «Інформаційні технології».

Повнота викладення результатів дослідження в наукових публікаціях, зарахованих за темою дисертації, відсутність порушення академічної доброчесності. Результати дисертації пройшли достатню апробацію у фаховому середовищі, що підтверджує наукову цінність та актуальність отриманих даних. Основні теоретичні та практичні положення дослідження висвітлено у 6 наукових працях, з яких 4 статті у наукових виданнях, включених до Переліку наукових фахових видань України, 2 тези наукових доповідей. Рецензування представлених робіт, висновків та рекомендацій підтверджує їхню повну відповідність темі дисертації. Дослідження виконано з суворим дотриманням принципів академічної доброчесності та етичних норм наукової спільноти.

Окремі дискусійні питання і зауваження щодо дисертації. При загальній позитивній оцінці змісту та результатів дисертаційного дослідження, вважаю за доцільне висловити низку зауважень та пропозицій для наукової дискусії:

1. У другому розділі автор використовує баєсівську мережу для оцінки ризиків, проте в роботі недостатньо деталізовано методику первинного визначення апріорних ймовірностей

для вузлів, що описують «людський фактор». Необхідно уточнити, наскільки чутливою є модель до суб'єктивізму експертних оцінок на етапі ініціалізації мережі.

2. Хмарні сервіси генерують величезні масиви лог-файлів (Big Data). З тексту дисертації не цілком зрозуміло, як саме реалізована оптимізація обчислювальної складності алгоритму при збільшенні кількості вузлів мережі та чи здатна запропонована модель працювати в режимі реального часу (Real-time processing) без значних затримок у прийнятті рішень.

3. У проблематиці представленого дослідження часто виникає проблема «холодного старту». Запропонована методика базується на аналізі цифрових слідів. Виникає питання щодо ефективності моделі для нових співробітників або при переході організації на нові хмарні додатки, коли історичних даних (навчальної вибірки) для побудови адекватного поведінкового профілю недостатньо.

4. Оскільки інсайдерами часто виступають технічно грамотні фахівці або керівники, чи розглядалася в роботі можливість навмисного спотворення інсайдером своїх «цифрових слідів» з метою поступового «привчування» баєсівської мережі до аномальної поведінки як до нормальної?

5. Автор пропонує прототип системи підтримки прийняття рішень, реалізований на Python. Проте в роботі варто було б більше уваги приділити архітектурним аспектам інтеграції цієї системи з промисловими платформами (наприклад, через API до систем класу SIEM або Microsoft Azure Sentinel), що підвищило б практичну цінність дослідження.

6. Використання організаційних та поведінкових індикаторів для моніторингу керівного складу може межувати з питаннями приватності. Було б доцільно почути думку автора щодо компромісу між глибиною моніторингу та дотриманням політик конфіденційності (наприклад, вимог GDPR).

Висновки про відповідність дисертації встановленим вимогам. На основі аналізу дисертації А. С. Глазунова можна стверджувати, що автор виконав кваліфікаційну роботу високого рівня, спрямовану на посилення кібербезпеки хмарних ресурсів від внутрішніх загроз. Розроблена баєсівська модель та алгоритмічні рішення становлять суттєвий внесок у прикладну науку в межах спеціальності 122 «Комп'ютерні науки» галузі 12 «Інформаційні технології». Робота характеризується повнотою висвітлення результатів у фахових виданнях та повною відповідністю принципам академічної доброчесності. Усе вищезазначене дозволяє зробити висновок, що дисертація цілком відповідає чинним вимогам наказу Міністерства освіти і науки України № 40 від 12 січня 2017 року «Про затвердження вимог до оформлення дисертації», Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України № 44

від 12 січня 2022 року, а її автор Глазунов Андрій Сергійович заслуговує на присудження ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології».

Офіційний опонент завідувач кафедри комп'ютерної інженерії Державного університету інформаційно-комунікаційних технологій, кандидат технічних наук, доцент Наталія ЛАЩЕВСЬКА