ВІДГУК
офіційного опонента
завідувача кафедри кібербезпеки
Національного технічного університету «Харківський політехнічний інститут»,
доктора технічних наук, професора **ЄВСЄЄВА Сергія Петровича**
на дисертацію **ГЛАЗУНОВА Андрія Сергійовича**
на тему: **«Комп'ютерні баєсівської моделі виявлення інсайдерів у хмарних сервісах»**,
подану на здобуття ступеня доктора філософії
за спеціальністю 122 «Комп'ютерні науки»

Актуальність теми дисертації

Актуальність теми зумовлена зростаючим протиріччям між зростанням обсягів конфіденційних даних у хмарних сховищах та обмеженими можливостями наявних засобів захисту щодо виявлення складних інсайдерських атак, особливо тих, що здійснюються особами з високим рівнем повноважень. Впровадження інтелектуальних моделей на основі модифікованих баєсівських мереж дозволяє формалізувати невизначеність поведінкових чинників та забезпечити перехід до систем превентивного моніторингу, що є пріоритетним завданням сучасної галузі комп'ютерних наук.

Наукова новизна одержаних результатів.

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 урахування 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

Практичне значення результатів 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. 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. Результати дисертаційного дослідження А. С. Глазунова впровадженням у ТОВ «Інфобіт», де реалізоване практичне впровадження програмного забезпечення, та у навчальному процесі студентів факультету інформаційних технологій Національного університету біоресурсів і природокористування України.

Мова та стиль викладення дисертації

Мова та стиль викладення матеріалів роботи дозволяє зрозуміти суть розроблених наукових положень та одержаних практичних результатів. Дисертація відповідає вимогам, які висуваються до її оформлення, відповідно до Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), що затверджений постановою Кабінету Міністрів України від 12 січня 2022 року № 44 (зі змінами), й Вимог до оформлення дисертації, затверджених наказом Міністерства освіти і науки України від 12 січня 2017 року № 40. У цілому зміст дисертації викладено послідовно та логічно.

Достовірність та обґрунтованість наукових положень, висновків та рекомендацій, сформульованих в дисертаційній роботі

Дисертаційні дослідження присвячено створенню вдосконалених імовірнісних моделей та методів для виявлення інсайдерських загроз у хмарних середовищах, які б поєднували

аналітичну строгість, адаптивність до сценаріїв поведінки користувачів і можливість впровадження в практичні системи кіберзахисту. Розв'язання даної задачі дозволяє підвищити ефективність виявлення та прогнозування інсайдерських загроз у хмарних сервісах інформаційних систем шляхом розроблення математично обґрунтованого методу та моделі на основі послідовних баєсівських правил, побудови локальних баєсівських мереж та використання методів інтелектуального аналізу даних.

Достовірність наукових положень, висновків і рекомендацій підтверджується узгодженістю теоретичних досліджень з результатами імітаційного моделювання, практичною імплементацією розроблених моделей і методів, результатами експериментів, які узгоджуються з даними відомих досліджень.

Повнота оприлюднення результатів дисертації

Основні результати дисертації опубліковано у 6 наукових працях, з яких 4 статті у наукових виданнях, включених до категорії «Б» Переліку наукових фахових видань України, 2 тези наукових доповідей. Основний внесок за обсягом у матеріалах публікацій належить здобувачу.

Загальна характеристика структури та змісту дисертації

У дисертації А. С. Глазунова проведено всебічний огляд та аналіз використання хмарних обчислень і сервісів, проблеми забезпечення їх інформаційної безпеки. У **вступі** обґрунтовано актуальність теми дисертації, визначено мету і завдання, предмет та об'єкт дослідження, зазначено методи дослідження, відображено наукову новизну і практичне значення одержаних результатів.

У **першому розділі** автор проводить ґрунтовний аналіз сучасного стану ринку хмарних послуг (SaaS, PaaS, IaaS) та специфіки їх впровадження в критичні галузі економіки, у результаті якого визначено, що попри технологічні переваги, хмарні архітектури мають вразливі місця, пов'язані з розмиттям периметра безпеки. Проведено порівняльний огляд існуючих підходів машинного навчання. Автор обґрунтовує, що традиційні методи часто не враховують контекст поведінки внутрішніх користувачів, що створює підґрунтя для використання імовірнісних моделей.

Другий розділ присвячено теоретичному обґрунтуванню застосування мереж Байєса та машинного навчання для виявлення внутрішніх загроз у бізнес-процесах, заснованих на хмарних сервісах. Розроблено концептуальну модель раннього виявлення інсайдерів. Автор акцентує увагу на тому, що баєсівські мережі дозволяють інтегрувати різнорідні дані: від технічних логів (SIEM) до організаційних чинників. Описано логіку врахування «цифрових слідів» та специфіку моніторингу привілейованих користувачів, що є ключовою відмінністю роботи від існуючих аналогів.

Третій розділ є ядром практичної та математичної реалізації дослідження. Розроблено та протестовано алгоритмічну процедуру багатоальтернативної послідовної перевірки гіпотез. Вона дозволяє системі накопичувати докази підозрілої поведінки та приймати рішення про блокування або попередження лише при досягненні певного порогу імовірності, мінімізуючи ризик помилки. Описано створення прототипу СППР (на Python та GeNIe/ SMILE). Наведено результати тестування на синтетичних сценаріях, що імітують дії реальних інсайдерів (наприклад, витік даних керівником у неробочий час). Візуалізація результатів у формі графових структур та гістограм підтверджує працездатність моделі.

Загальні висновки дисертації узгоджуються з метою і завданнями дослідження. Отримані результати характеризуються науковою новизною та практичною цінністю, обґрунтовані теоретично та підтверджені експериментальними дослідженнями. У цілому, дисертація А. С. Глазунова є завершеним науковим дослідженням, яке містить теоретичні розробки та відповідні їм експериментальні перевірки.

Зауваження щодо змісту дисертації

1. У першому розділі дисертації (табл. 1.2, с. 30–33) наведено результати досліджень використання різних хмарних сервісів за галузями. Але не зрозуміло, чому автор не використовує оцінку хмарних сервісів об’єктів критичної інфраструктури, а також не зрозуміло, чому автор оцінює одну складову безпеки – інформаційну безпеку, не враховуючи інші – кібербезпеку та безпеку інформації.

2. У підрозділі 1.2 проводиться аналіз досліджень проблематики забезпечення інформаційної безпеки хмарних інфраструктур (с. 35–41, табл. 1.3, 1.4) але не зрозуміло, чому не визначені комплексування цільових (змішаних) атак на хмарні сервіси з методами соціальної інженерії. Також бажано було б навести класифікацію інсайдерів з урахуванням їх фінансових, обчислювальних можливостей, мети тощо.

3. На с. 53–54 (табл. 1.5) наведено результати порівняльного аналізу переваг та недоліків різних методів машинного навчання, які потенційно можна використовувати у системах інформаційної безпеки хмарних сервісів, з якої не зрозуміло, чому саме Мережі Байєса автором вибрано як кращий варіант побудови моделей виявлення інсайдерів у хмарних сервісах.

4. У розділі 2 дисертації автор використовує апріорні ймовірності для налаштування вузлів баєсівської мережі. Проте не зрозуміло, яким саме чином здійснюється первинне оцінювання цих імовірностей, чи на основі експертних оцінок, чи на основі статистичних даних минулих інцидентів, або шляхом автоматичного навчання на лог-файлах конкретної організації. Також не зрозуміло, чому у підрозділі 2.1 автор проводить аналіз методів та моделей інсайдерської загрози.

5. У підрозділі 2.2 дисертації запропоновано математичний опис оголошення базового набору показників інформаційної безпеки для хмарного сервісу (вираз 2.1), в якому є множина метрик інформаційної безпеки хмарного сервісу, але які метрики не вказано. Формула 2.2 визначає список метрик відповідно до стандартів інформаційної безпеки та рекомендованих практик для кожного конкретного хмарного сервісу, але не зрозуміло, на яких міжнародних регуляторах базується цей список. Запропонована модифікована баєсівська мережа містить значну кількість вузлів, але при цьому не зрозуміло, як її можливо масштабувати збільшенні кількості користувачів до десятків тисяч і чи не виникає критичних затримок у прийнятті рішень.

6. У дисертації автор пропонує власну процедуру перевірки гіпотез (с. 90–100, підрозділ 3.1), але при цьому не зрозуміло наскільки ці процедури корелюють з нормативними міжнародними регуляторами, наприклад ISO/IEC 27035–2024.

7. У підрозділі 3.2 дисертації проводиться верифікація запропонованого підходу, але за результатами не зрозуміло на скільки/або у скільки підвищується рівень виявлення інсайдерів у хмарних сервісах.

Вказані зауваження і недоліки не впливають на загальну позитивну оцінку виконаного дисертаційного дослідження та не зменшують його наукову новизну та практичну значущість і не знижують загального позитивного сприйняття проведеного обсягу досліджень.

Загальний висновок щодо дисертації

На основі критичного вивчення дисертації та праць здобувача, які опубліковано за темою дисертації, об’єктивно встановлено:

– дисертація Глазунова Андрія Сергійовича відповідає чинним вимогам, які встановлені Порядком підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженим постановою Кабінету Міністрів України від 23 березня 2016 року № 261 (зі змінами), та Порядком присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженим постановою Кабінету Міністрів України від 12 січня 2022 року № 44 (зі змінами);

– використання чужих наукових результатів без посилань на авторів у дисертації не виявлено, що свідчить про особистий внесок здобувача в науку;

– дисертація Глазунова Андрія Сергійовича є завершеною науковою працею, в якій отримано нові науково обґрунтовані результати, які дозволяють підвищити ефективність виявлення та прогнозування інсайдерських загроз у хмарних сервісах інформаційних систем;

– автор дисертації Глазунов Андрій Сергійович заслуговує на присудження ступеня доктора філософії в галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп’ютерні науки».

Офіційний опонент завідувач кафедри кібербезпеки Національного технічного університету «Харківський політехнічний інститут», доктор технічних наук, професор, Лауреат національної премії імені Бориса Патона Сергій ЄВСЄЄВ