ЗАТВЕРДЖУЮ
Проректор з наукової роботи
та інноваційної діяльності
Національного університету біоресурсів
і природокористування України
доктор сільськогосподарських наук,
професор
_____ Оксана ТОНХА
«___» _____ 2026 р.

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації
Глазунова Андрія Сергійовича
на тему: **«Комп'ютерні баєсівські моделі виявлення інсайдерів у хмарних сервісах»**,
поданої на здобуття ступеня доктора філософії
зі спеціальності **122 «Комп'ютерні науки»**
галузі знань **12 «Інформаційні технології»**

Витяг з протоколу № 1 фахового семінару кафедри інформаційних систем і технологій факультету інформаційних технологій Національного університету біоресурсів і природокористування України від «05» лютого 2026 року.

Присутні члени фахового семінару кафедри інформаційних систем і технологій факультету інформаційних технологій Національного університету біоресурсів і природокористування України: О. Є. Коваленко, професор кафедри комп'ютерних систем, мереж та кібербезпеки, доктор технічних наук, професор, гарант освітньо-наукової програми «Інформаційні технології», голова фахового семінару; І. М. Болбот, декан факультету інформаційних технологій, доктор технічних наук, професор; Б. Л. Голуб, завідувач кафедри комп'ютерних наук, кандидат технічних наук, доцент; А. М. Гуржій, професор кафедри інформаційних систем і технологій, доктор технічних наук, професор, науковий керівник; Н. А. Клименко, доцент кафедри економічної кібернетики, кандидат економічних наук, доцент; В. М. Кравченко, професор кафедри економічної кібернетики, доктор економічних наук, доцент; О. В. Криворучко, професор кафедри комп'ютерних систем, мереж та кібербезпеки, доктор технічних наук, професор, експертка; О. Г. Кузьмінська, професор кафедри інформаційних систем і технологій, доктор педагогічних наук, професор; В. А. Лахно, професор кафедри комп'ютерних систем, мереж та кібербезпеки, доктор технічних наук, професор; С. М. Мамченко, професор кафедри комп'ютерних систем, мереж та кібербезпеки, доктор педагогічних наук, професор; М. В. Мокрієв, доцент кафедри інформаційних систем і технологій, кандидат економічних наук, доцент; В. М. Смолій, професор кафедри інформаційних систем і технологій, доктор технічних наук, професор; М. З. Швиденко, завідувач кафедри інформаційних систем і технологій, кандидат економічних наук, доцент; Т. В. Волошина, доцент кафедри інформаційних систем і технологій, кандидат педагогічних наук, доцент; В. В. Шкарупило, професор кафедри комп'ютерних систем, мереж та кібербезпеки, доктор технічних наук, доцент, експерт; Т. А. Вакалюк, завідувачка кафедри інженерії програмного забезпечення Державного університету «Житомирська політехніка», доктор педагогічних наук, професор; Є. А. Лавров, професор кафедри інформаційних технологій Сумського державного університету, доктор технічних наук, професор.

Інші присутні на засіданні фахового семінару кафедри інформаційних систем і технологій факультету інформаційних технологій Національного університету біоресурсів і природокористування України: А. С. Глазунов, здобувач ступеня доктора філософії.

Порядок денний: обговорення основних наукових результатів дисертації **Глазунова Андрія Сергійовича** на тему: **«Комп'ютерні баєсівські моделі виявлення інсайдерів у хмарних сервісах»**, поданої на здобуття ступеня доктора філософії зі спеціальності 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології».

Тему дисертації затверджено (протокол № 11 від 20 червня 2022 року) та уточнено (протокол № 6 від «17» лютого 2025 року) вченою радою факультету інформаційних технологій Національного університету біоресурсів і природокористування України.

Дисертацію виконано на кафедрі інформаційних систем і технологій факультету інформаційних технологій Національного університету біоресурсів і природокористування України.

Науковий керівник: доктор технічних наук, професор **Гуржій Андрій Миколайович**, професор кафедри інформаційних систем і технологій Національного університету біоресурсів і природокористування України.

Слухали: доповідь здобувача А. С. Глазунова про основні положення дисертації. Здобувач представив основні результати дослідження, розкрив зміст, мету та науково-практичну значущість дисертації. У доповіді обґрунтовано актуальність теми, що підтверджується стрімким впровадженням хмарних сервісів у найважливіші сфери діяльності як держав, так й окремих компаній (фінанси, охорона здоров'я, логістика, енергетика, освіта та державне управління тощо) і обумовлює необхідність ефективного управління ризиками інформаційної безпеки, пов'язаних з інсайдерськими загрозами. Метою дисертації визначено підвищення ефективності 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.

У науковій новизні підкреслено, що 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.

Методологічну основу дослідження становлять аналітичні, математичні, статистичні та програмні методи. Аналітичні методи використано для огляду та систематизації наукових підходів до забезпечення інформаційної безпеки хмарних сервісів. Методи теорії ймовірностей та баєсівської статистики – для побудови і навчання баєсівських мереж та визначення апостеріорних ймовірностей гіпотез щодо наявності інсайдерської загрози. Методи багатоальтернативної послідовної перевірки гіпотез – для формалізації процедури виявлення несанкціонованого доступу на основі накопичення даних, з урахуванням змінних порогових значень і ризику прийняття хибного рішення. Методи математичної оптимізації – для мінімізації апостеріорного ризику в процедурі прийняття рішень для забезпечення інформаційної безпеки хмарних сервісів. Методи валідації програмної реалізації для тестування моделі на синтетичних даних, що містять ознаки минулих інцидентів, згенерованих на основі типових сценаріїв поведінки інсайдерів та візуалізація результатів для перевірки якості класифікації співробітників за рівнем ризику.

Основні результати роботи полягають у тому, що було розроблено модифіковану модель баєсівської мережі для виявлення інсайдерських загроз у хмарних сервісах, яка відрізняється своєю структурою, що включає вузли для оцінювання шахрайських дій керівного персоналу, та здатністю враховувати цифрові сліди, сформовані в процесі взаємодії з хмарною інфраструктурою. Досліджено й реалізовано процедуру побудови оптимальних послідовних баєсівських правил, яка дає змогу оцінювати ймовірність порушення інформаційної безпеки ще до настання інциденту, з урахуванням причинно-наслідкових і нелінійних залежностей між ризиками й обґрунтовано використання технічних, поведінкових та організаційних індикаторів у задачах прогнозування інсайдерської

активності. А також програмно реалізовано у вигляді прототипу системи підтримки прийняття рішень для фахівців з інформаційної безпеки, яка забезпечує інтерактивну взаємодію з аналітиком, візуалізацію результатів і підтримку ухвалення обґрунтованих рішень щодо внутрішніх (інсайдерських) загроз.

Практичне значення результатів дослідження полягає у тому, що виконано розроблення і тестування мережі Баєса для моделювання внутрішнього порушника безпеки або інсайдера за допомогою програмного забезпечення GeNIe/SMILE, а також алгоритмічної мови Python. Показано, що використання програмного забезпечення для баєсівського мережного моделювання і аналізу даних дає змогу зручно та ефективно будувати й аналізувати баєсівські мережі, роблячи процес моделювання і аналізу більш точним та інформативним. Спроєктовано і апробовано на рівні прототипу варіант системи підтримки прийняття рішень для виявлення внутрішніх порушників та інсайдерів у компаніях, що використовують хмарний сервіс, в якому віконні елементи забезпечують зручний та інтуїтивно зрозумілий інтерфейс для введення даних, і співробітнику відділу безпеки буде легше вводити значення для кожного фактора окремо, що поліпшує загальне сприйняття системи. Окрім того, покрокове заповнення даних для кожного співробітника дає можливість збирати інформацію поступово, що зменшує ймовірність помилок і полегшує процес введення даних. На синтетичному наборі даних продемонстровані результати навчання такої баєсівської мережі, а також результати роботи системи підтримки прийняття рішень у вигляді гістограми для порівняння ймовірності інсайдерської загрози для кожного співробітника. Проведено апробацію технології на реальних даних компанії ТОВ «Інфобіт», що підтвердило її ефективність і достовірність результатів.

Здобувачеві було поставлено 13 запитань, на які він надав обґрунтовані відповіді та пояснення.

Виступили:

Науковий керівник – доктор технічних наук, професор А. М. Гуржій відзначив актуальність і затребуваність теми дисертаційного дослідження в контексті того, що хмарні сервіси активно використовують для оптимізації виробничих процесів, керування фінансами, опрацювання медичних даних, організації освітнього процесу, автоматизації торгівлі, оптимізації логістики тощо та інформаційна безпека хмарних сервісів є невід'ємним елементом для успішного ведення бізнесу, забезпечуючи захист даних, безперервність бізнес-процесів, відповідність нормативним вимогам та довіру клієнтів. У своєму виступі він наголосив, що у дисертації представлено результати проведених здобувачем досліджень, які спрямовані на розв'язання актуального наукового завдання створення моделі інтелектуальної системи виявлення інсайдерських загроз у хмарних сервісах на основі модифікованої баєсівської мережі. Було підкреслено, що А. С. Глазуновим запропоновано рішення, яке має істотне значення для розвитку інформаційних технологій, оскільки забезпечує врахування поведінкових, технічних і організаційних індикаторів, а також сценаріїв шахрайських дій з боку керівного персоналу, а отримані результати реалізовано у вигляді прототипу системи підтримки прийняття рішень, що дозволяє інтегрувати модель у засоби інформаційної безпеки хмарних систем.

Науковий керівник зазначив, що А. С. Глазунов у роботі над виконанням дослідження проявив глибокі теоретичні знання у сфері функціонування систем забезпечення інформаційної безпеки у хмарних середовищах інформаційних систем, а також продемонстрував сформовані компетентності у математичному моделюванні та практичному застосуванню методів та алгоритмів для побудови локальних баєсівських мереж та багато-альтернативної послідовної перевірки гіпотез для аналізу поведінкових та системних даних, отриманих із засобів кібербезпеки (SIEM, DLP, IDS/IPS тощо).

Гуржій А. М. підкреслив, що наукове дослідження має чітко виражену наукову новизну, яка полягає у розробленні модифікованої моделі баєсівської мережі для виявлення інсайдерських загроз у хмарних сервісах інформаційних систем, що включає спеціалізовані вузли для врахування дій осіб, які займають керівні посади, моделює ризики шахрайської поведінки з боку такого персоналу, враховує цифрові сліди користувачів хмарних застосунків,

що дозволяє оцінювати ймовірність внутрішніх загроз до моменту фактичного порушення. Структура розробленої моделі включає опис апріорних і апостеріорних ймовірностей для вирішальних технічних, поведінкових та організаційних індикаторів, що забезпечує глибше причинно-наслідкове моделювання ситуацій загрози в умовах неповної інформації.

Окремо відзначено практичну цінність результатів, підтверджену їх апробацією та впровадженням у компанії ТОВ «Інфобіт», де реалізоване практичне впровадження програмного забезпечення, та у навчальному процесі студентів факультету інформаційних технологій Національного університету біоресурсів і природокористування України.

Гуржій А. М. також зазначив, що здобувач повною мірою виконав освітньо-наукову програму «Інформаційні технології», успішно опанував навчальні дисципліни, продемонстрував високий рівень аналітичного мислення, самостійності, відповідальності та працелюбності під час виконання наукової роботи. У процесі підготовки дисертації здобувач проявив ініціативність, здатність до міждисциплінарного наукового пошуку, уміння формулювати складні наукові завдання, аргументовано обґрунтовувати отримані результати та ефективно презентувати їх на наукових семінарах і конференціях. Отримані результати дисертаційного дослідження, включно з теоретичними положеннями, практичними рекомендаціями та висновками, отримано автором самостійно.

Експерти:

Криворучко О. В., доктор технічних наук, професор, відзначила високий науково-технічний рівень дисертації, її системність, логічність викладу та цілісність проведеного дослідження. Було підкреслено, що хоча хмарні обчислення забезпечують високу гнучкість, масштабованість і швидкість опрацювання даних, вони водночас ускладнюють контроль за поведінкою користувачів і сприяють зростанню ймовірності порушень безпеки з боку внутрішніх суб’єктів доступу. Експерт зазначила, що переважна більшість досліджень зосереджена на виявленні зовнішніх загроз або типових інцидентів інформаційної безпеки без врахування специфіки високорівневих інсайдерських сценаріїв, зокрема з боку керівного складу, водночас інсайдерські загрози сьогодні визнаються одними з найнебезпечніших і найменш контрольованих форм атак на інформаційну безпеку хмарних середовищ. Тому актуальність теми дослідження зумовлена потребою у створенні вдосконалених імовірнісних моделей та методів для виявлення інсайдерських загроз у хмарних середовищах.

Серед сильних сторін дослідження експерт відзначила доведену наукову новизну дослідження та застосовану методологічну базу дослідження. Зокрема, експерт наголосила, що в дисертації вперше розроблено модифіковану модель баєсівської мережі для виявлення інсайдерських загроз у хмарних сервісах інформаційних систем, удосконалено метод виявлення несанкціонованого доступу до хмарних сервісів шляхом впровадження адаптивної баєсівської мережі з функціональністю прогнозування інсайдерських загроз, запропоновано уточнену процедуру побудови оптимальних послідовних баєсівських правил, які дозволяють адаптувати порогові значення оцінювання ризику залежно від контексту дій, дістав подальшого розвитку метод щодо раннього виявлення інсайдерів у хмарному середовищі, який базується на інтеграції технічних, поведінкових і організаційних індикаторів у межах баєсівської моделі.

Криворучко О. В. відзначила високу прикладну значущість отриманих результатів, що підтверджується їх апробацією та впровадженням у діяльність бізнес-компанії. Підкреслено практичне значення дисертаційного дослідження, що 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.

Водночас, експерт висловив низку зауважень. Зокрема, було вказано на необхідності розширення набору та послідовності ключових слів дослідження, уточнення назви розділу 3 та його підрозділів з метою стандартизації використовуваної у дисертації термінології. Крім того, рекомендовано уточнити терміни «угнута функція», «угнутість функції», структурувати

загальні висновки у відповідності до результатів наукової новизни, вказано на описки та стилістичні огріхи на с. 66, 94–95, 107 та інших, помилки у підписах рисунків. Експертка також вказала низку побажань, що спрямовані на підвищення наукової обґрунтованості та практичної значущості дослідження.

На основі проведеного аналізу дисертації експерткою запропоновано дати їй загальну позитивну оцінку, як такій, що відповідає вимогам 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, та рекомендувати дисертацію для подання до розгляду та захисту у разовій спеціалізованій вченій раді на здобуття ступеня доктора філософії зі спеціальності 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології».

Шкарупило В. В., доктор технічних наук, доцент, позитивно оцінив дисертацію здобувача та підтвердив, що вона відповідає всім вимогам до досліджень на здобуття ступеня доктора філософії зі спеціальності 122 «Комп'ютерні науки». У експертному висновку відзначено високий рівень наукової обґрунтованості, актуальності та завершеності проведеного дослідження, достатню кількість і належну якість наукових публікацій за темою дисертації, що відображають основні результати роботи. Наголошено на теоретичній і практичній значущості отриманих результатів, їх відповідності сучасним тенденціям розвитку інформаційних технологій та вимогам до інформаційної безпеки.

Експерт підкреслив, що дисертація містить доведені положення наукової новизни, є самостійним, завершеним науковим дослідженням, виконаним із дотриманням принципів академічної доброчесності, без ознак запозичень і порушень наукової етики. Окремо експерт відзначив практичний результат, зокрема програмну реалізація моделі, яка здійснена за допомогою середовища GeNIe/SMILE та мови програмування Python, що дозволяє забезпечити модульність, масштабованість та інтеграцію з типовими інструментами кіберзахисту, такими як SIEM, DLP, IDS/IPS. У моделі реалізовано вузли, які описують як технічні й поведінкові ознаки активності користувачів, так і фактори, пов'язані з організаційним контекстом і управлінськими повноваженнями. Створено прототип системи підтримки прийняття рішень, адаптований для використання фахівцями підрозділів інформаційної безпеки. Система підтримки прийняття рішення 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.

Також відзначено чітку логічну структуру роботи, послідовність викладення матеріалу, аргументованість висновків і належний рівень методичного та програмного забезпечення дослідження. Зазначено, що отримані результати є обґрунтованими, достовірними та можуть бути використані у практиці закладів вищої освіти для підвищення ефективності виявлення та прогнозування інсайдерських загроз у хмарних сервісах інформаційних систем.

Серед зауважень експертом зазначено, що у частині опису наукової новизни, у формулюванні проведеного удосконалення методу раннього виявлення інсайдерів в організаціях зазначається відмінність від відомих підходів, але доречно, стверджувати стосовно відмінності від відомих методів або альтернативних рішень. Експерт звернув увагу на назву підрозділу 3.2, зокрема, у частині: «Розробка і тестування» – формулювання є некоректним, так як тестування є етапом процесу розроблення. Рекомендовано формулювання: «Проєктування, реалізація і тестування…». Експерт висловив низку рекомендацій щодо рисунків та їх назв, зокрема, на рис. 3.20 блок-схему краще подавати як діаграму дій. Експерт порекомендував замінити формулювання «актуального наукового завдання» на «актуальну наукову задачу» на с. 2, та звернув увагу на інші наявні стилістичні і граматичні помилки. Наприклад, на с. 27 (і далі) назву таблиці 1.2 слід подавати з абзацного відступу; с. 39 – перелік посилань «[73, 74, 75, 76, 77, 78]» подавати з використанням дефісу; розділи подавати з нового рядка (наприклад, розділ 2); після номерів підрозділів крапку не ставити (наприклад, підрозділ 2.1 на с. 65 і далі); с. 72 і далі – у нумерованих списках

з дужками після елементів має слідувати крапка з комою, після заключного елементу – крапка, речення починати з малої літери; с. 149 – таблиця займає більше аркуша – доречно винести в додатки.

На основі проведеного аналізу дисертації експертом запропоновано дати їй загальну позитивну оцінку, як такій, що відповідає вимогам 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, та рекомендувати дисертацію для подання до розгляду та захисту у разовій спеціалізованій вченій раді на здобуття ступеня доктора філософії зі спеціальності 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології».

В обговоренні результатів дисертації взяли участь: доктор технічних наук, професор І. М. Болбот; доктор технічних наук, професор О. Є. Коваленко; доктор технічних наук, професор В. А. Лахно; доктор економічних наук, доцент В. М. Кравченко; доктор технічних наук, професор В. М. Смолій; доктор технічних наук, професор С. М. Мамченко, кандидат економічних наук, доцент М. З. Швиденко; кандидат технічних наук, доцент Б. Л. Голуб.

Виступаючі зазначили, що дисертація А. С. Глазунова виконана на важливу тему, робота містить значну кількість нових наукових даних, має наукову новизну, актуальність, важливе теоретичне та практичне значення, відповідає 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.

Було підтримано пропозицію експертів про рекомендацію дисертації А. С. Глазунова для подання до розгляду та захисту у разовій спеціалізованій вченій раді на здобуття ступеня доктора філософії зі спеціальності 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології».

Постановили: заслухавши та обговоривши дисертацію **Глазунова Андрія Сергійовича** на тему: **«Комп'ютерні баєсівські моделі виявлення інсайдерів у хмарних сервісах»**, члени фахового семінару кафедри інформаційних систем і технологій факультету інформаційних технологій Національного університету біоресурсів і природокористування України ухвалили:

1. Актуальність теми дисертації. Дисертацію присвячено розробленню інформаційної технології освітньої аналітики на основі методів інтелектуального аналізу даних. Стрімке впровадження хмарних сервісів у найважливіші сфери діяльності як держав, так й окремих компаній (фінанси, охорона здоров'я, логістика, енергетика, освіта та державне управління тощо) обумовлює необхідність ефективного управління ризиками інформаційної безпеки, пов'язаних з інсайдерськими загрозами. Хоча хмарні обчислення забезпечують гнучкість, масштабованість та оперативність обробки даних, але одночасно ускладнюють контроль над користувацькою поведінкою, сприяючи зростанню ризику порушень із середини організації. Саме інсайдерські загрози визнані фахівцями одними з найбільш прихованих і складно виявлюваних типів атак на інформаційну безпеку хмарних середовищ. Протягом останніх десятиліть низка дослідників активно займалася проблематикою захисту хмарних обчислень та дослідженням ефективності хмарних сервісів у різних галузях. Паралельно розвивалися підходи до аналізу користувацької поведінки за допомогою методів штучного інтелекту й машинного навчання, серед яких помітне місце займають баєсівські мережі, здійснювалися дослідження щодо локальних баєсівських мереж для кібербезпеки. Попри це, значна частина існуючих рішень фокусується на зовнішніх загрозах або типових сценаріях, що не враховують специфіку високорівневих інсайдерських дій, зокрема з боку

керівного персоналу. Крім того, у більшості моделей недостатньо формалізовано зв'язок між цифровими слідами в хмарних сервісах, поведінковими індикаторами та оцінкою ризику. Таким чином, актуальність теми дисертаційного дослідження зумовлена потребою у створенні удосконалених методів та моделей виявлення інсайдерських загроз у хмарних сервісах.

2. Зв'язок теми дисертації з державними програмами, науковими напрямами Університету та кафедри. Дисертаційне дослідження виконано відповідно до пріоритетного тематичного напряму «Інформаційні та комунікаційні технології», затвердженого постановою Кабінету Міністрів України від 30.04.2024 № 476, а також у межах реалізації завдань Стратегії кібербезпеки України (Указ Президента України № 447/2021) та Концепції Державної цільової науково-технічної програми з використання технологій штучного інтелекту (Розпорядження КМУ № 320-р від 13.04.2024), що спрямовані на посилення захисту інформаційних ресурсів у хмарних сервісах від внутрішніх загроз». Робота виконувалася 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). Тема дисертації повністю відповідає науковим напрямам факультету інформаційних технологій та кафедри інформаційних систем і технологій, узгоджується із загальною дослідницькою стратегією Університету, спрямованою на цифрову трансформацію освітньої діяльності та використання сучасних інформаційних технологій в освітньому процесі.

3. Особистий внесок здобувача в отриманні наукових результатів та вирішенні конкретного наукового завдання. У процесі виконання дисертаційного дослідження всі основні результати, положення та висновки отримано автором самостійно. Здобувачем самостійно проведено пошук, аналіз і систематизацію наукових, методичних та інформаційних джерел, що стосуються тематики дослідження. Самостійно розроблено модифіковану модель баєсівської мережі, яка враховує як технічні та поведінкові індикатори користувачів, так і загрози шахрайських дій осіб, що обіймають керівні посади. Здобувачем удосконалено метод виявлення несанкціонованого доступу до хмарних сервісів шляхом розроблення оптимального послідовного баєсівського правила. Здобувачем особисто розроблено прототип системи підтримки прийняття рішень у системах інформаційної безпеки для виявлення інсайдерських загроз. Усі етапи дослідження від теоретичного обґрунтування до практичної реалізації та апробації результатів виконано без залучення сторонніх розробок. Інтерпретацію результатів, формулювання висновків і практичних рекомендацій здійснено під науковим консультуванням керівника, при цьому всі основні положення дисертації, що виносяться на захист, є самостійним науковим здобутком здобувача. Особистий внесок у публікаціях, виконаних у співавторстві, чітко визначено у списку наукових праць.

4. Достовірність і обґрунтованість отриманих результатів і запропонованих автором рішень, висновків, рекомендацій. Результати дисертаційного дослідження здобувача є достовірними, відтворюваними та науково обґрунтованими, що забезпечено належним методичним рівнем проведеного аналізу та використанням сучасного науково-технічного інструментарію. У процесі роботи застосовано аналітичні методи – для огляду та систематизації наукових підходів до забезпечення інформаційної безпеки хмарних сервісів; методи теорії ймовірностей та баєсівської статистики – для побудови і навчання баєсівських мереж та визначення апостеріорних ймовірностей гіпотез щодо наявності інсайдерської загрози; методи багатоальтернативної послідовної перевірки гіпотез – для формалізації процедури виявлення несанкціонованого доступу на основі накопичення даних, з урахуванням змінних порогових значень і ризику прийняття хибного рішення; методи математичної оптимізації – для мінімізації апостеріорного ризику в процедурі прийняття рішень для забезпечення інформаційної безпеки хмарних сервісів; програмні методи та інструменти – для створення прототипу баєсівської мережі та візуалізації графової структури моделі та для реалізації функцій обчислення ймовірностей інсайдерської

загрози із подальшим відображенням результатів у вигляді гістограм; методи валідації програмної реалізації – для тестування моделі на синтетичних даних, що містять ознаки минулих інцидентів, згенерованих на основі типових сценаріїв поведінки інсайдерів та візуалізація результатів для перевірки якості класифікації співробітників за рівнем ризику.

Достовірність висновків підтверджено результатами експериментального дослідження розроблених моделей на синтетичних даних, зокрема, у ході апробації встановлено, що розроблена інформаційна технологія забезпечує високу прогностичну здатність.

5. Наукова новизна основних результатів дослідження. Наукова новизна дисертації здобувача полягає у тому, що 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.

Зазначені елементи новизни демонструють, що дисертація містить оригінальні наукові результати.

6. Практична цінність результатів дослідження та їх впровадження. Практична цінність результатів роботи полягає у створенні, програмній реалізації та апробації моделі модифікованої баєсівської мережі, що призначена для виявлення інсайдерських загроз у хмарних сервісах організацій. Програмно реалізовано алгоритмічну процедуру побудови оптимальних послідовних баєсівських правил для прогнозування несанкціонованого доступу, що дозволяє здійснювати поетапну оцінку рівня загрози на основі порівняння апостеріорних ймовірностей гіпотез із гнучкими пороговими значеннями. У цій процедурі враховано вартість помилкових рішень (як хибнопозитивних, так і хибнонегативних) та змінну критичність етапів прийняття рішень, що забезпечує гнучкість налаштування до конкретних організаційних вимог. Розроблено програмну реалізацію баєсівської мережі з використанням середовища GeNIe/SMILE та мови Python, яка підтримує обробку поведінкових і системних ознак, отриманих із засобів контролю безпеки (SIEM, DLP, IDS/IPS). У програмному застосунку враховано спеціалізовані вузли, що дозволяють моделювати не лише типові сценарії інсайдерської активності, а й шахрайські дії на керівних рівнях управління.

7. Перелік наукових праць, які відображають основні результати дисертації. Основні положення виконаного А. С. Глазуновим дослідження опубліковано у 6 наукових працях, з яких 4 статті у наукових виданнях, включених до Переліку наукових фахових видань України, 2 тези наукових доповідей.

Статті у наукових виданнях,
включених до Переліку наукових фахових видань України

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

2. Глазунов А. С. Огляд та аналіз досліджень з проблематики інформаційної безпеки хмарних інфраструктур. Інформаційні технології та суспільство. 2024. № 1 (12). С. 38–45.

3. Глазунов А. С. Байєсівські правила прогнозування несанкціонованого доступу внутрішнього порушника до публічних сервісів компанії. Наука і техніка сьогодні. 2025. № 1 (42).

4. **Глазунов А.**, Гуржій А. Метод раннього виявлення інсайдерів у хмарних середовищах. Технічна інженерія. 2025. № 2 (96). С. 90–94. *(Глазуновим А. С. обґрунтовано вдосконалений метод раннього виявлення інсайдерів у хмарних середовища, формалізовано і змодельована ймовірність шахрайських дій. Гуржієм А. М. здійснено наукове консультування щодо методології ймовірнісного моделювання, постановка задачі за темою публікації та сформульовано перспективи подальшого впровадження запропонованого методу у системи підтримки прийняття рішень в інформаційній безпеці)*.

Тези наукових доповідей

5. **Глазунов А. С.**, Гуржій А. М. Оптимізація навчального порталу Moodle за допомогою Amazon Web Services. Інформаційні технології: економіка, техніка, освіта ‘2023: Міжнародна науково-практична конференція молодих вчених, м. Київ, 26–27 жовтень 2023 року: тези доповіді. Київ, 2024. С. 75–77. *(Глазуновим А. М. вивчено оптимізацію навчального порталу Moodle за допомогою Amazon Web Services. Гуржієм А. М. проведено консультації)*.

6. Глазунов А. С., Матієвський В. В. Порівняльний аналіз управління ідентифікацією та доступом основних хмарних постачальників. Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні '2024: XII Міжнародна науково-практична конференція, м. Київ, 21–22 листопада 2024 року: тези доповіді. Київ, 2024. С. 103–107. *(Глазуновим А. М. здійснено порівняльний аналіз управління ідентифікацією та доступом основних хмарних постачальників. Матвієвським В. В. проведено консультації)*.

8. Апробація основних результатів дослідження. Основні наукові положення, результати та висновки дисертаційного дослідження А. С. Глазунова пройшли апробацію на: Міжнародній науково-практичній конференції молодих вчених «Інформаційні технології: економіка, техніка, освіта ‘2023» (м. Київ, 2023 р.); XII Міжнародній науково-практичній конференції «Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні '2024» (м. Київ, 2024 р.).

Ухвалили:

Дисертація здобувача ступеня доктора філософії Глазунова Андрія Сергійовича на тему: «Комп’ютерні баєсівські моделі виявлення інсайдерів у хмарних сервісах» є завершеною кваліфікаційною науковою працею, спрямованою на вирішення актуального наукового завдання створення моделі інтелектуальної системи виявлення інсайдерських загроз у хмарних сервісах на основі модифікованої баєсівської мережі, має теоретичну й практичну значущість для посилення захисту інформаційних ресурсів у хмарних сервісах від внутрішніх загроз та становить істотне значення для галузі знань 12 «Інформаційні технології».

Дисертація відповідає 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.

З урахуванням наукової зрілості та професійних якостей здобувача Глазунова Андрія Сергійовича дисертація на тему: «Комп'ютерні баєсівські моделі виявлення інсайдерів у хмарних сервісах» рекомендується для подання до розгляду та захисту у разовій спеціалізованій вченій раді на здобуття ступеня доктора філософії зі спеціальності 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології».

Рішення прийнято одноголосно.

Головуючий на засіданні фахового семінару
кафедри інформаційних систем і технологій
факультету інформаційних технологій
Національного університету біоресурсів
і природокористування України
професор кафедри комп'ютерних систем,
мереж та кібербезпеки,
доктор технічних наук, професор **Олексій КОВАЛЕНКО**

Експерти:
Професор кафедри комп'ютерних систем,
мереж та кібербезпеки
Національного університету біоресурсів
і природокористування України,
доктор технічних наук, доцент **Вадим ШКАРУПИЛО**

Професор кафедри комп'ютерних систем,
мереж та кібербезпеки
Національного університету біоресурсів
і природокористування України,
доктор технічних наук, професор **Олена КРИВОРУЧКО**

Відповідальний за атестацію здобувачів
вищої освіти ступеня доктора філософії **Сергій БОЯРЧУК**