Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U000521

Особливі позначки: відкрита

Дата реєстрації: 10-03-2026

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Глазунов Андрій Сергійович
2. Andrii S. Hlazunov

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 122

Назва наукової спеціальності: Комп'ютерні науки

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Інформаційні технології

Дата захисту: 16-04-2026

Спеціальність за освітою: Комп'ютерні науки та інформаційні технології

Місце роботи здобувача: Національний університет біоресурсів і природокористування України

Код за ЄДРПОУ: 00493706

Місцезнаходження: вул. Героїв Оборони, Київ, 03041, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 185

Повне найменування юридичної особи: Національний університет біоресурсів і природокористування України

Код за ЄДРПОУ: 00493706

Місцезнаходження: вул. Героїв Оборони, Київ, 03041, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Національний університет біоресурсів і природокористування України

Код за ЄДРПОУ: 00493706

Місцезнаходження: вул. Героїв Оборони, Київ, 03041, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 50.37.23, 20.56.01, 20.56.02, 20.56.03

Тема дисертації:

1. Комп'ютерні баєсівські моделі виявлення інсайдерів у хмарних сервісах
2. Computer Bayesian Models for Detecting Insiders in Cloud Services

Реферат:

1. У дисертації представлено результати досліджень, які спрямовані на розв'язання актуального наукового завдання створення моделі інтелектуальної системи виявлення інсайдерських загроз у хмарних сервісах на основі модифікованої баєсівської мережі. Запропоноване рішення 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. Стрімке впровадження хмарних сервісів у головні галузі економіки та державного управління – фінанси, охорону здоров'я, логістику, енергетику, освіту тощо зумовило необхідність ефективного управління ризиками інформаційної безпеки, зокрема тими, що пов'язані з інсайдерськими загрозами. 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. Саме інсайдерські загрози сьогодні визнаються одними з найнебезпечніших і найменш контрольованих форм атак на інформаційну безпеку хмарних середовищ. Актуальність дослідження зумовлена потребою у створенні 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. Для реалізації мети дослідження 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. Вперше розроблено модифіковану модель баєсівської мережі для виявлення інсайдерських загроз у хмарних сервісах інформаційних систем. На відміну від наявних рішень, модель включає спеціалізовані вузли для врахування дій осіб, які займають керівні посади, і моделює ризики шахрайської поведінки з боку такого персоналу. Модель враховує цифрові сліди, які формуються під час взаємодії користувача з хмарними застосунками, 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. Удосконалено метод виявлення несанкціонованого доступу до хмарних сервісів шляхом впровадження адаптивної баєсівської мережі з функціональністю прогнозування інсайдерських загроз. Відмінністю даного підходу є врахування не лише поточних індикаторів загрози, але і їхніх взаємозалежностей у часі, що дозволяє виявляти загрозу на ранніх стадіях та своєчасно запобігати порушенням. Запропоновано уточнену процедуру побудови оптимальних послідовних баєсівських правил, які дозволяють адаптувати порогові значення оцінювання ризику залежно від контексту дій. Такий підхід базується на мінімізації апостеріорного ризику і дозволяє приймати виважені рішення щодо безпеки в умовах багатокритеріальної невизначеності.

2. The dissertation presents the results of research aimed at solving the urgent scientific problem of creating a model of an intelligent system for detecting insider threats in cloud services based on a modified Bayesian network. The proposed solution is of significant importance for the development of information technologies, as it enables the consideration of behavioral, technical, and organizational indicators, as well as scenarios of fraudulent actions by managerial personnel. The obtained results have been implemented in the form of a prototype decision support system, which makes it possible to integrate the model into information security tools for cloud systems. The rapid implementation of cloud services (CS) in the main sectors of the economy and public administration – finance, healthcare, logistics, energy, education, etc. – has created the need for effective management of information security (IS) risks, particularly those associated with insider threats. Although cloud computing (CC) provides high flexibility, scalability, and speed of data processing, it simultaneously complicates the control of user behavior and contributes to an increased likelihood of security breaches by internal subjects of access. Insider threats are now recognized as among the most dangerous and least controllable forms of attacks on the information security of cloud environments.The relevance of the research is determined by the need to create improved probabilistic models and methods for detecting insider threats in cloud environments that combine analytical rigour, adaptability to user behaviour scenarios, and the possibility of implementation in practical cyber defence systems. To achieve the research goal, a modified Bayesian network model for detecting insider threats in

cloud services was developed. It differs in its structure, which includes nodes for assessing fraudulent actions of managerial personnel, and in its ability to take into account digital traces generated in the process of interaction with the cloud infrastructure. A procedure for constructing optimal sequential Bayesian rules has been studied and implemented, enabling the assessment of the probability of an information security violation even before an incident occurs, taking into account causal and nonlinear dependencies between risks. The use of technical, behavioral, and organizational indicators in the tasks of forecasting insider activity has been substantiated. The results have also been implemented in software form as a prototype decision support system for information security specialists, which provides interactive interaction with an analyst, visualization of results, and support for making informed decisions regarding internal (insider) threats. For the first time, a modified Bayesian network model for detecting insider threats in cloud services of information systems has been developed. Unlike existing solutions, the model includes specialized nodes for taking into account the actions of individuals in managerial positions and models the risks of fraudulent behavior by such personnel. The model takes into account digital traces generated during user interaction with cloud applications, which makes it possible to assess the probability of internal threats before an actual violation occurs. The structure of the developed model includes a description of prior and posterior probabilities for key technical, behavioral, and organizational indicators, providing deeper causal modeling of threat situations under conditions of incomplete information. The method for detecting unauthorized access to cloud services has been improved by introducing an adaptive Bayesian network with functionality for forecasting insider threats. The distinctive feature of this approach is that it takes into account not only current threat indicators but also their interdependencies over time, enabling threats to be detected at early stages and violations to be prevented in a timely manner. A refined procedure has been proposed for constructing optimal sequential Bayesian rules, which allows the adaptation of threshold values for risk assessment depending on the context of actions. This approach is based on minimizing posterior risk and enables well-grounded security decisions to be made under conditions of multi-criteria uncertainty.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- 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.
- Глазунов А. С. Огляд та аналіз досліджень з проблематики інформаційної безпеки хмарних інфраструктур. Інформаційні технології та суспільство. 2024. № 1 (12). С. 38–45.
- Глазунов А. С. Байєсівські правила прогнозування несанкціонованого доступу внутрішнього порушника до публічних сервісів компанії. Наука і техніка сьогодні. 2025. № 1 (42).
- Глазунов А., Гуржій А. Метод раннього виявлення інсайдерів у хмарних середовищах. Технічна інженерія. 2025. № 2 (96). С. 90–94.

Наукова (науково-технічна) продукція: програмні продукти, програмно-технологічна документація

Соціально-економічна спрямованість: забезпечення промисловості чи населення новим видом інформаційно-комунікаційних послуг

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Гуржій Андрій Миколайович

2. Andrii M. Hurzhii

Кваліфікація: д. т. н., професор, 05.03.01

Ідентифікатор ORCID ID: 0000-0002-2797-5831

Додаткова інформація:

Повне найменування юридичної особи: Національний університет біоресурсів і природокористування України

Код за ЄДРПОУ: 00493706

Місцезнаходження: вул. Героїв Оборони, Київ, 03041, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Євсєєв Сергій Петрович

2. Serhii P. Yevsieiev

Кваліфікація: д. т. н., професор, 21.05.01

Ідентифікатор ORCID ID: 0000-0003-1647-6444

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Лащевська Наталія Олександрівна

2. Nataliia O. Lashchevska

Кваліфікація: к. т. н., доц., 05.12.17

Ідентифікатор ORCID ID: 0000-0003-2148-115X

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Криворучко Олена Володимирівна
2. Olena V. Kryvoruchko

Кваліфікація: д. т. н., професор, 05.13.22

Ідентифікатор ORCID ID: 0000-0002-7661-9227

Додаткова інформація:

Повне найменування юридичної особи: Національний університет біоресурсів і природокористування України

Код за ЄДРПОУ: 00493706

Місцезнаходження: вул. Героїв Оборони, Київ, 03041, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Шкарупило Вадим Вікторович
2. Vadym V. Shkarupylo

Кваліфікація: д. т. н., доц., 05.13.05

Ідентифікатор ORCID ID: 0000-0002-0523-8910

Додаткова інформація: https://www.scopus.com/authid/detail.uri?authorId=57189326576

Повне найменування юридичної особи: Національний університет біоресурсів і природокористування України

Код за ЄДРПОУ: 00493706

Місцезнаходження: вул. Героїв Оборони, Київ, 03041, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Лахно Валерій Анатолійович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Лахно Валерій Анатолійович
Відповідальний за підготовку облікових документів	Боярчук Сергій Васильович
Реєстратор	Юрченко Тетяна Анатоліївна
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна