Ганна М. Яровенко[1], Лариса П. Перхун[2], Наталія О. Небаба[3], Ольга Ф. Булгакова[4], Вікторія В. Костенко[5]

РОЗРОБКА МОДЕЛІ ФОРМАЛІЗАЦІЇ ПРОЦЕСУ ВИЯВЛЕННЯ ІНСАЙДЕРСЬКИХ КІБЕРЗАГРОЗ У БАНКАХ: ОНТОЛОГІЧНИЙ ПІДХІД

Стаття присвячена розробці онтологічної моделі формалізації процесу виявлення інсайдерських кіберзагроз для банківських установ. Було визначено загальні вимоги та критерії, елементи та етапи побудови даної моделі. В рамках реалізації моделі було запропоновано структуру класів, відносин між ними, характеристику правил та обмежень, станів об'єктів, часові та просторові аспекти, а також аспекти аутентифікації, контролю доступу, шифрування та інших напрямків кібербезпеки.

В сучасних реаліях постійно зростаючих кіберзагроз, розробка ефективних засобів їх виявлення та протидії стає критичною задачею для забезпечення кібербезпеки банківських систем. Специфіка банківської діяльності, де чутлива фінансова інформація знаходиться під постійним ризиком, робить цю проблему особливо актуальною. Особливо це відчувається при вирішенні завдань, пов'язаних із зловживанням довіри внутрішніми користувачами, тому виявлення інсайдерських загроз стає значним викликом для банків. Складність їх виявлення обумовлена рядом чинників, таких як внутрішні привілеї осіб, які мають доступ до конфіденційної інформації, а також різноманітні трафіки та способи вторгнення. Тому метою даної статті визначено створення моделі для формалізації процесу виявлення інсайдерських кіберзагроз у банках на основі онтологічного підходу. Розробка онтологічної моделі спрямована на аналіз та стандартизацію знань про інсайдерські загрози, щоб покращити можливості їхнього вчасного виявлення та зменшити час реакції на події безпеки. Застосування такого підходу дозволяє систематизувати та стандартизувати знання про інсайдерські загрози, визначаючи взаємозв'язки між різними концепціями та об'єктами в цьому контексті. В рамках реалізації мети дослідження було визначено загальні вимоги та критерії, елементи та етапи побудови онтологічної моделі формалізації процесу виявлення інсайдерських кіберзагроз у банках. Було запропоновано структуру класів, відносин між ними, характеристику правил та обмежень, станів об'єктів, часові та просторові аспекти, а також аспекти аутентифікації, контролю доступу, шифрування та інших напрямків кібербезпеки. Розроблена модель покликана вирішувати проблеми ідентифікації, аналізу та реагування на інсайдерські загрози у банківській сфері, сприяючи підвищенню рівня кібербезпеки та відповідальності в цьому важливому секторі.

Ключові слова: *банк, інсайдер, кіберзагроза, онтологічний підхід, формалізація.*

Табл. 6. Літ. 10.

DOI: 10.32752/1993-6788-2023-1-268-71-83

Ganna M. Yarovenko, Larisa P. Perkhun, Natalia A. Nebaba, Olha F. Bulhakova, Victoria V. Kostenko

DEVELOPMENT OF A MODEL FOR THE FORMALIZATION OF THE PROCESS OF DETECTING INSIDER CYBER THREATS IN BANKS: AN ONTOLOGICAL APPROACH

The article is devoted to developing an ontological model of the formalization of detecting insider cyber threats for banking institutions. This model's general requirements and criteria, ele-

[1] Sumy State University. Ukraine.
[2] Sumy State University. Ukraine.
[3] Oles Honchar Dnipro National University. Ukraine.
[4] University of Customs and Finance. Ukraine.
[5] University of Customs and Finance. Ukraine.

ments and stages of construction were defined. As part of the model implementation, the structure of classes, relationships between them, characteristics of rules and restrictions, states of objects, temporal and spatial aspects, and aspects of authentication, access control, encryption and other areas of cyber security were proposed.

In the modern realities of constantly growing cyber threats, developing effective means of their detection and countermeasures becomes a critical task for ensuring the cyber security of banking systems. The specificity of banking, where sensitive financial information is at constant risk, makes this problem particularly relevant. This is especially felt when solving tasks related to abuse of trust by internal users, so identifying insider threats becomes a significant challenge for banks. The difficulty of their detection is determined by several factors, such as the internal privileges of individuals with access to confidential information, as well as various traffic and intrusion methods. Therefore, this article aims to create a model for formalising the process of detecting insider cyber threats in banks based on an ontological approach. The development of an ontological model seeks to analyse and standardise knowledge about insider threats to improve the possibilities of their timely detection and reduce the reaction time to security events. Applying such an approach allows us to systematise and standardise knowledge about insider threats, defining relationships between concepts and objects in this context. As part of the research goal, the general requirements and criteria, elements and stages of building an ontological model of the formalisation of the process of detecting insider cyber threats in banks were determined. The structure of classes, relationships between them, characterisation of rules and restrictions, states of objects, temporal and spatial aspects, and aspects of authentication, access control, encryption and other areas of cyber security were proposed. The developed model is designed to solve the problems of identification, analysis and response to insider threats in the banking sector, contributing to increasing cyber security and responsibility in this crucial sector.

Keywords: *bank, insider, cyber threat, ontological approach, formalization.*
Peer-reviewed, approved and placed: *13.10.2023.*

Постановка проблеми. Інсайдерські кіберзагрози представляють собою загрози для кібербезпеки, які виникають внаслідок дій осіб, що мають легальний доступ до інформаційних систем та даних в організації чи компанії. Ці особи можуть бути співробітниками, партнерами чи іншими особами, які мають привілеї доступу. Інсайдерські загрози можуть включати навмисні або неумисні дії, що становлять ризик для конфіденційності, цілісності та доступності інформації. Інсайдерські атаки можуть приймати різні форми, такі як неправомірний доступ до конфіденційної інформації, витік даних, зловживання привілеями або навіть умисні дії, спрямовані на завдання шкоди організації. Одним із аспектів інсайдерських загроз є те, що ці особи вже перебувають всередині об'єкта атаки, що може робити виявлення та запобігання таким загрозам більш складним завданням порівняно з зовнішніми атаками.

Проблема боротьби з інсайдерськими кіберзагрозами у банках полягає в тому, що вони виникають через дії осіб з легальним доступом до систем та інформації у банку. Це може включати зловживання довіри або неправомірне використання повноважень, призводячи до втрати конфіденційної інформації, фінансових збитків та системних ризиків. Сутність проблеми також включає соціальну інженерію, атаки, що використовують маніпулювання людьми для отримання конфіденційної інформації. Працівники банку можуть стати жертвами фішингу, обману чи інших

соціально-інженерних методів, що може відкрити доступ до важливих ресурсів. Неадекватність управління правами доступу також є проблемою, де проблеми з управлінням можуть призвести до надання зайвих або непотрібних прав користувачам. Недостатня або надмірна аутентифікація та авторизація може відкривати можливості для інсайдерських атак. Брак ефективних систем моніторингу та аудиту ускладнює виявлення незвичайної чи підозрілої активності. Відсутність реакції на надто розгалужену або аномальну активність може зробити інсайдерські атаки важкими для виявлення.

Актуальність теми підтримується зростанням інсайдерських загроз, фінансовими наслідками, регуляторними вимогами та зростанням обсягів даних у банківському секторі, що підвищує ризик витоку та зловживання інформацією. Загальна архітектура та моделювання інсайдерських загроз стає критичною для ефективного виявлення та запобігання інсайдерським атакам. Для боротьби з інсайдерськими кіберзагрозами необхідні ефективні стратегії управління доступом, моніторингу активності користувачів та застосування технологій, що спрямовані на розпізнавання аномалій та запобігання невірному використанню привілеїв. В якості такої стратегії є необхідність формалізації процесу виявлення інсайдерських кіберзагроз, що дозволить чітко розуміти, як формувати інформаційне забезпечення систем кіберзахисту. Застосування онтологічного підходу з цією метою сприятиме розробці якісної структури концепцій, об'єктів, відносин, та правил в даній предметній області.

Аналіз останніх досліджень і публікацій. Тема виявлення та протидії інсайдерських кіберзагроз є мало дослідженою в наукових публікаціях. Це пов'язано із специфікою предметної області, а також з тими обмеженнями, які накладає банківський сектор на їх розробки, особливо в частині інформаційних технологій та кібербезпеки. Але зазначена проблема на сьогоднішній день й продовжує залишатися невирішеною, що пов'язано із стрімким зростання комп'ютеризації та інформатизації багатьох процесів, а також доступністю інструментів кіберзлочинів для пересічних користувачів.

Так, Афак С. А., Узма С., Ясмін Г. вивчали проблему кіберризиків у контексті цифрової економіки та виділили одним із значущих вплив інсайдерських груп, що найбільше відчувається у сфері охорони здоров'я, харчовій промисловості та сільському господарстві [1]. Слід відмітити внесок Мішри Ш., який запропонував техніку кібербезпеки на основі штучного інтелекту для класифікації проблем кібератак у фінансовому секторі [2]. Рауф У., Мохсен Ф. та Вей З. розглянули набори для даних, які можна використовувати для ідентифікації атрибутів бази даних внутрішніх загроз, ініціаторами яких є працівники компаній [3]. Грін М. Л. та Дозьє П. провели дослідження щодо виявлення людських факторів кіберзагроз, які дозволяють виявляти індивідуальні, культурні та технологічні впливи [4].

Переважна кількість досліджень стосується застосування методів машинного навчання для виявлення та протидії інсайдерських кіберзагроз. Так, Аль-Фава'ре М., Аль-Файюмі М., Нашван С., Фрайхат С. запропонували модель глибокої нейронної мережі у комбінації з аналізом основних

компонент для виявлення кіберзагроз [5]. Мамун М. та Ши К. розробили базову модель виявлення аномальної поведінки користувачів інформаційної системи на основі нейронної мережі довгострокової пам'яті (LSTM) [6]. Хоча засоби машинного навчання є потужним інструментарієм для виявлення аномалій в системі, але Скотт Дж. та Кіобе М. зробили висновок, що вони не забезпечують в повній мірі потреби кіберзахисту, оскільки не враховують аспекти людської поведінки [7].

При дослідженні такої серйозної проблеми, як інсайдерські кіберзагрози, треба до її вирішення підходити комплексно. Застосування онтологічного підходу є одним з потенційних напрямків. Цей метод має свою специфіку, оскільки застосовується в системній інженерії та для розпізнавання текстів. Але не слід його не дооцінювати для використання при побудови систем кіберзахисту. Так, Санчес-Зас К., Вільягра В. А., Вега-Барбас М., Ларріва-Ново Х., Морено Дж. І., Беррокаль Дж. запропонували онтологію для опису різних типів аномалій для підвищення ефективності управління кіберризиками [8]. Дора Дж. Р., Глучи Л., Немога К. створили онтологію для вирішення проблеми вразливостей баз даних SQL [9]. Хуанг К.К., Хуанг П.Ю., Куо Ю.Р., Вонг Г.В., Хуанг Ю.Т., Сунь Ю.С., Чен М.К. запропонували основу для розробки онтології для розуміння тактики кіберзлочинців [10].

Не дивлячись на значний науковий доробок, невирішеним залишається питання формалізації процесу виявлення інсайдерських кіберзагроз саме для банківських установ, для реалізації якого доцільно застосувати підхід побудови онтологій. Саме вирішенню даного питання й буде присвячене дане дослідження.

Мета дослідження полягає у розробленні моделі формалізації процесу виявлення інсайдерських кіберзагроз у банках із застосуванням онтологічного підходу.

Основні результати дослідження. Онтологічна модель формалізації процесу виявлення інсайдерських кіберзагроз у банках – це структурований опис та репрезентація концепцій, об'єктів, відносин, та правил в даній предметній області, яка дозволяє систематизувати та узгоджувати знання про інсайдерські загрози в контексті банківської безпеки. Ця модель використовується для формалізації та стандартизації розуміння експертами та системами конкретних аспектів, пов'язаних із виявленням інсайдерських загроз у банківському секторі. Такий опис робить можливим розуміння та обробку інформації комп'ютерами, що дозволяє їм ефективно взаємодіяти з даними в певній області. Онтологія використовується для створення формалізованих моделей предметних областей, які полегшують обробку та обмін інформацією між системами. Такі онтології можуть використовуватися в різних галузях, таких як веб-пошук, інтелектуальні системи, обробка природної мови та інші області, де важлива концептуальна ясність та узгодженість в розумінні термінів і відносин.

Створення онтології для формалізації моделі виявлення інсайдерських кіберзагроз у банках вимагає врахування конкретних особливостей банківської галузі та кіберзахисту. Ось деякі загальні вимоги та критерії для побудови такої онтології:

- ретельний аналіз особливостей банківської діяльності, процесів та інфраструктури, та визначення основних аспектів, які піддаються ризику внаслідок інсайдерських загроз;
- створення чітких визначень термінів, пов'язаних із загрозами та вразливостями, та здійснення їх узгодження з загальноприйнятими стандартами та визначеннями;
- розробка сценаріїв, які описують можливі дії інсайдерів, та визначення можливих шляхів атак та їхніх етапів;
- ідентифікація важливих атрибутів, що визначають стан систем та ідентифікацію загроз, та включення тих, які дозволяють виявляти аномальні або підозрілі дії;
- узгодженість інтеграції даних онтології з існуючими системами та стандартами в галузі кіберзахисту;
- визначення алгоритмів та правил для виявлення аномалій та інсайдерських дій, та розробка механізмів кореляції даних для визначення складних взаємозв'язків;
- створення системи класифікації для об'єктів та подій, пов'язаних із загрозами, та визначення метаданих для опису різних елементів онтології;
- розгляд можливостей включення динамічних аспектів та визначення зміни стану системи під час атаки;
- створення онтології таким чином, щоб вона була відкритою для розширення новими знаннями та даними.

Ці критерії допоможуть забезпечити створення ефективної та потужної онтології для виявлення інсайдерських кіберзагроз у банках. Розробка онтологічної моделі включає кілька ключових етапів:

1. визначення конкретної області банківської безпеки, на яку буде спрямована онтологічна модель, обсягу та мети моделі;
2. детальний аналіз різних бізнес-процесів банку, ідентифікація потенційних загроз в рамках цих процесів та врахування особливостей банківської галузі та її ризиків;
3. встановлення основних понять, які визначають предметну область (інсайдер, кіберзагроза, банківський процес і т. д.) та визначення відносин між цими поняттями;
4. створення онтологічних класів для представлення об'єктів і понять, таких як користувачі, системи, процеси тощо, а також визначення властивостей для класів, які вказують на їхні характеристики та взаємозв'язки;
5. впорядкування класів в ієрархію, щоб відображати спільні абстракції та специфікації, та забезпечення логічної та чіткої структури;
6. перевірка і узгодження моделі з існуючими стандартами безпеки та кіберзахисту з використанням відомих онтологічних мов чи стандартів, таких як OWL (Web Ontology Language) або RDF (Resource Description Framework);
7. визначення властивостей для опису стану об'єктів та систем, та врахування часових та просторових аспектів стану;
8. формулювання правил, які обмежують допустимі взаємодії між об'єктами в системі, а також визначення умов, за яких може виникнути інсайдерська загроза;

9. проведення тестів для перевірки коректності та ефективності моделі та здійснення валідації моделі на реальних чи симульованих даних;

10. підтримка гнучкості та здатності до оновлення моделі для включення нових загроз та висновків із досліджень;

11. розробка документації, яка пояснює структуру, правила та використання онтології, а також забезпечення ефективної комунікації між розробниками та користувачами онтології.

Ці етапи допомагають створити ефективну та гнучку онтологічну модель, що сприяє покращенню кібербезпеки в цій галузі.

Онтологічна модель формалізації процесу виявлення інсайдерських кіберзагроз у банках може включати в себе такі елементи:

- основні класи об'єктів та концепцій в галузі банківської безпеки, наприклад, "Інсайдер", "Користувач", "Система", "Транзакція" та інші;
- властивості класів, які вказують на їхні характеристики та атрибути. Наприклад, для класу "Інсайдер" може бути властивість "Рівень доступу";
- встановлення взаємозв'язків між класами. Наприклад, відносини між "Інсайдером" та "Транзакцією" можуть вказувати на можливість інсайдера впливати на фінансові операції;
- формалізація правил та обмежень, які визначають допустимі взаємодії між об'єктами та стан системи;
- визначення стану об'єктів та системи в різний час. Це важливо для виявлення аномалій та змін стану, що можуть свідчити про інсайдерські загрози;
- узгодження часових та просторових аспектів для визначення моменту виявлення та географічного розташування інсайдера;
- врахування інших аспектів безпеки, таких як методи аутентифікації, контроль доступу, шифрування тощо.

Класи онтологічної моделі представляють об'єкти, концепції та аспекти, що важливі для формалізації процесу виявлення інсайдерських кіберзагроз у банках. Нижче наведено детальний огляд можливих класів для такої моделі (Таблиця 1).

Класи і їхні властивості взаємодіють між собою через визначені відносини, що дозволяє створити комплексну модель для виявлення інсайдерських кіберзагроз у банках. Також відносини визначають структуру та взаємодії між класами. При цьому важливо враховувати конкретні особливості банківської галузі та взаємодії між різними сутностями та подіями. Нижче наведено детальний огляд можливих відносин, які можуть існувати в такій моделі (Таблиця 2).

Таблиця 1. **Потенційні класи та їх властивості в онтологічній моделі формалізації процесу виявлення інсайдерських кіберзагроз у банках,** *складено авторами*

Назва класу	Характеристика класу	Властивості класу
Інсайдер	Описує особу, яка має легальний доступ до систем банку, але використовує цей доступ нелегально або шкідливо	Ім'я, роль в банку, рівень доступу тощо
Користувач	Загальний клас, що описує будь-якого користувача системи, включаючи інсайдерів та легітимних користувачів	Ім'я, ідентифікатор, роль, рівень доступу
Транзакція	Визначає операції або обміни даними, які відбуваються в банківській системі	Сума, тип транзакції, дата та час
Система	Представляє інформаційну та технічну інфраструктуру банку	Версія ПЗ, типи баз даних, технічні параметри
Аномалія	Описує будь-які незвичайні події або стани, які можуть свідчити про можливу інсайдерську загрозу	Час виявлення, характер аномалії, ступінь загрози
Заходи безпеки	Визначає заходи та політики, які застосовуються для запобігання та виявлення інсайдерських кіберзагроз	Тип заходу, термін дії, область застосування
Вразливість	Описує слабкі місця в системі, які можуть бути використані інсайдерами для здійснення атак	Опис вразливості, рівень критичності
Правила виявлення	Визначає правила та алгоритми для виявлення аномальних дій чи поведінки, які можуть свідчити про інсайдерську загрозу	Тип правила, умови виявлення
Запитання безпеки	Описує запитання, які можуть бути використані для перевірки легітимності користувача в процесі взаємодії з системою	Тип запитання, область застосування

Таблиця 2. **Потенційні відносини між класами в онтологічній моделі формалізації процесу виявлення інсайдерських кіберзагроз у банках,** *складено авторами*

Назва відносин	Класи, між якими встановлюються відносини	Значення відносин
Має доступ	"Інсайдер" та "Система"	Визначає, які інсайдери мають доступ до конкретних систем в банку
Здійснює транзакцію	"Інсайдер" та "Транзакція"	Показує, на які транзакції можуть впливати інсайдери
Використовує правило виявлення	"Інсайдер" та "Правила виявлення"	Вказує, які правила виявлення використовуються для виявлення інсайдерської діяльності
Застосовує заходи безпеки	"Інсайдер" та "Заходи безпеки"	Показує, які заходи безпеки застосовуються для запобігання інсайдерським загрозам
Виявляє аномалію	"Система" та "Аномалія"	Показує, які аномалії в системі можуть свідчити про інсайдерські дії
Має рівень доступу	"Користувач" та "Система"	Визначає, які користувачі мають певний рівень доступу до системи
Взаємодіє з вразливістю	"Інсайдер" та "Вразливість"	Вказує, які вразливості можуть бути використані інсайдером для атаки
Здійснює запитання безпеки	"Користувач" та "Запитання безпеки"	Показує, які запитання безпеки використовуються для перевірки легітимності користувача

Правила та обмеження в онтологічній моделі для формалізації процесу виявлення інсайдерських кіберзагроз у банках визначають умови, обмеження та норми, які регулюють взаємодію між різними класами та об'єктами в системі. В таблиці 3 представлено детальний огляд можливих правил та обмежень.

Таблиця 3. **Правила та обмеження онтологічної моделі формалізації процесу виявлення інсайдерських кіберзагроз у банках,** *складено авторами*

Назва правила / обмеження	Опис правила / обмеження	Приклад правила / обмеження
Правила виявлення	Визначає умови та методи виявлення інсайдерських дій в системі	Якщо користувач проводить несподівано велику кількість транзакцій протягом короткого періоду, то система визначає це як потенційно підозрілу активність
Обмеження рівня доступу	Визначає, які ресурси та функціонал доступні різним рівням користувачів або систем	Інсайдерам обмежено доступ до критичних фінансових операцій
Аудит та логування	Визначає правила збору та зберігання журналів подій для аналізу та виявлення аномалій	Усі спроби доступу до конфіденційної інформації записуються в системному журналі
Обмеження використання заходів безпеки	Визначає обов'язкове використання конкретних заходів безпеки, таких як двофакторна аутентифікація чи шифрування	Усі користувачі повинні пройти двофакторну аутентифікацію для доступу до фінансових систем
Часові обмеження	Визначає правила та обмеження для доступу до системи в певні періоди часу	Користувачі з підозрілою активністю можуть бути обмежені в доступі під час некритичних годин
Обмеження аномалій	Визначає, які аномалії вважати нормальними та які є підозрілими	Пересилання великої кількості конфіденційної інформації на зовнішні адреси може викликати попередження
Обмеження вразливостей	Визначає правила для зменшення вразливостей системи та даних	Всі важливі патчі та оновлення мають бути встановлені в системі протягом певного періоду
Автоматичне реагування	Визначає автоматичні дії, які слід вжити у випадку виявлення підозрілої активності	Автоматична блокування акаунту при підозрілій аутентифікації

Визначені правила та обмеження взаємодіють у складі системи виявлення інсайдерських кіберзагроз, забезпечуючи безпеку та виявлення потенційно небезпечних дій у банківському середовищі.

Стан об'єктів в онтологічній моделі формалізації процесу виявлення інсайдерських кіберзагроз у банках відображає поточний статус та характеристики різних об'єктів в системі. Детальний огляд можливих аспектів стану об'єктів в такій моделі представлено в таблиці 4.

Стан об'єктів може змінюватися в залежності від дій та подій в системі. Моніторинг та аналіз цих станів допомагає виявляти аномалії та потенційні загрози для банківської безпеки.

Часові та просторові аспекти визначають контекст виявлення інсайдерських кіберзагроз у банках та допомагають покращити ефективність системи безпеки. Їх характеристику запропоновано у таблиці 5.

Таблиця 4. **Характеристика станів об'єктів в онтологічній моделі формалізації процесу виявлення інсайдерських кіберзагроз у банках,** *складено авторами*

Назва стану	Опис стану	Приклади властивостей
Інсайдер	Вказує на поточний статус інсайдера в системі, його активності та легітимності	– Рівень доступу (високий, середній, низький) – Стан легітимності (підозрілий, нормальний)
Користувач	Відображає стан та активність користувачів в системі банку	– Остання активність – Статус облікового запису (активний, заблокований) – Історія вхідних та вихідних транзакцій
Транзакція	Визначає поточний статус та характеристики фінансових транзакцій	– Сума транзакції – Час та дата проведення – Статус (успішна, відхилена, в очікуванні)
Система	Вказує на стан технічної інфраструктури та інформаційних систем банку	– Версія програмного забезпечення – Доступність системи – Статус безпеки (захищена, під загрозою)
Аномалія	Показує, чи виникла аномалія та як це може вплинути на безпеку системи	– Час виявлення – Тип аномалії (вихід за межі норми, атака, несподівана активність)
Заходи безпеки	Вказує на поточний статус застосованих заходів безпеки в системі	– Термін дії заходу безпеки – Активність (включений, виключений)
Вразливість	Показує ступінь небезпеки та статус виправлення вразливостей в системі	– Рівень критичності вразливості. – Дата патчу чи виправлення
Правила виявлення	Вказує на стан та ефективність правил для виявлення інсайдерських загроз	– Частота виявлення підозрілих подій. – Ступінь впевненості виявлення

Таблиця 5. **Часові та просторові аспекти в онтологічній моделі формалізації процесу виявлення інсайдерських кіберзагроз у банках,** *складено авторами*

Назва аспекту	Опис аспекту	Приклад аспект
Часові аспекти		
Час виявлення аномалій	Визначає, як швидко система може виявити аномалії та підозрілі активності	Певні аномалії можуть бути виявлені тільки після виявлення взірців поведінки протягом тривалого часу
Часові обмеження для заходів безпеки	Визначає, наскільки тривалим є застосування певних заходів безпеки та чи вони мають термін дії	Ліміти на період дії аутентифікаційних токенів для користувачів
Часові маркери та тайм-штампи транзакцій	Використовується для фіксації часу та порядку подій, щоб легше визначити хронологію та послідовність транзакцій	Кожна транзакція має тайм-штамп, який вказує час її виконання
Часові проміжки для аналізу поведінки	Визначає інтервали часу, протягом яких аналізується поведінка користувачів для виявлення аномалій	Система аналізує активність користувачів протягом останніх 30 днів
Просторові аспекти		
Географічне розташування користувачів	Визначає, з яких місць користувачі можуть отримувати доступ до системи та чи є це типовим для їхньої поведінки	Виявлення доступу із незвичайних географічних областей для конкретного користувача

Закінчення табл. 5

Назва аспекту	Опис аспекту	Приклад аспект
Мережева топологія	Визначає, як об'єкти взаємодіють у мережевому середовищі та чи є це відповідно до типової поведінки	Виявлення незвичайних мережевих з'єднань, які можуть свідчити про атаку або нелегітимний доступ
Локації фізичних об'єктів	Визначає, де розташовані фізичні об'єкти, такі як сервери та дата-центри, та як це впливає на їх безпеку	Забезпечення фізичної безпеки дата-центрів для уникнення фізичних атак
Топологія систем та їхній зв'язок	Визначає, які системи взаємодіють між собою та як це впливає на загальну безпеку	Виявлення непередбачених з'єднань між системами, які можуть бути використані для атаки
Локації вразливостей	Визначає, де знаходяться вразливості в системі та як це впливає на потенційні загрози	Виявлення вразливостей у важливих компонентах системи та їх негайне виправлення

Поза часовими та просторовими аспектами, існує ряд інших важливих аспектів безпеки в онтологічній моделі для виявлення інсайдерських кіберзагроз у банках. Вони враховують важливі методи та стратегії для забезпечення безпеки в банківському секторі, щоб ефективно виявляти інсайдерські кіберзагрози. Їх характеристику наведено у таблиці 6.

Висновки та перспективи подальших досліджень. Вирішення проблеми побудови онтологічної моделі для формалізації процесу виявлення інсайдерських кіберзагроз у банках є критичним завданням у сучасному контексті кібербезпеки. Онтологічні моделі стають важливим інструментом для представлення знань та взаємозв'язків в складних системах, таких як інформаційні технології банківських установ. Успішне вирішення цієї проблеми передбачає ретельне проектування та розробку онтологічної моделі, яка враховує специфіку банківського сектору. Моделювання процесів виявлення інсайдерських кіберзагроз є необхідним для адекватного відображення всіх можливих сценаріїв та взаємодій між різними елементами системи. Онтологічна модель повинна бути тісно пов'язана з бізнес-процесами та стратегіями банку. Вона повинна відображати не тільки технічні аспекти, але й брати до уваги правила та регуляції, яким підлягає банк. Онтологічна модель повинна бути здатною інтегруватися з існуючими системами без втрати ефективності та швидкості виявлення кіберзагроз, враховувати вимоги до безпеки та захисту конфіденційної інформації, забезпечуючи високий рівень захисту від несанкціонованого доступу, бути гнучкою та легко адаптовуватися до змін в банківському середовищі, включаючи технологічні оновлення та зміни в законодавстві.

Запропонована у статті онтологічна модель формалізації процесу виявлення інсайдерських кіберзагроз у банках враховує всі ключові аспекти виявлення загроз, забезпечуючи узгодженість з бізнес-процесами та інтеграцію з існуючими системами. Результат опису елементів онтологічної моделі демонструє необхідність та доцільність впровадження комплексного підходу до виявлення та протидії інсайдерським кіберзагрозам у банківському секторі. Важливим завданням є не тільки побудова самої моделі, але й постійна підтримка та оптимізація її функціональності. Це вимагає командної

роботи експертів із кібербезпеки, фахівців з області банківського бізнесу та інженерів знань, щоб забезпечити повноту та ефективність онтологічної моделі в контексті виявлення інсайдерських кіберзагроз.

Таблиця 6. **Характеристика інших аспектів в онтологічній моделі формалізації процесу виявлення інсайдерських кіберзагроз у банках,** *складено авторами*

Назва аспекту	Опис аспекту	Приклад аспекту
Методи аутентифікації		
Однофакторна аутентифікація	Використання одного засобу аутентифікації, такого як пароль чи біометричні дані	Введення пароля для входу в банківський обліковий запис
Двофакторна аутентифікація	Використання двох різних методів аутентифікації для підтвердження ідентичності користувача	Комбінація пароля та одноразового коду, отриманого через SMS
Мультифакторна аутентифікація	Використання трьох чи більше факторів для підтвердження ідентичності	Пароль, відбиток пальця та RFID-карта
Контроль доступу		
Рівні доступу	Визначення рівнів доступу до різних ресурсів залежно від ролі користувача	Адміністратори мають повний доступ, клієнти — обмежений
Контроль прав доступу	Встановлення обмежень на доступ до конкретних операцій чи даних	Користувачі можуть переглядати баланс, але не мати права на внесення змін
Логічний та фізичний контроль	Забезпечення доступу до інформації як логічно, так і фізично	Фізичний доступ до серверних приміщень обмежений картками доступу
Шифрування		
Шифрування даних в спокої	Захист інформації в непередбачуваному стані, коли вона не використовується	Зберігання паролів у зашифрованому вигляді в базі даних
Шифрування даних в русі	Захист інформації під час передачі по мережі чи інших комунікаційних каналах	Використання протоколу HTTPS для зашифрованого обміну даними між клієнтом і сервером
Шифрування сховища	Захист інформації в базі даних чи інших сховищах даних	Зашифроване зберігання конфіденційних клієнтських даних
Інші аспекти безпеки		
Захист від атак	Включає в себе заходи для виявлення та запобігання різним видам кібератак, таким як DDoS атаки чи SQL-ін'єкції	Використання систем виявлення вторгнень (IDS) та витончених механізмів фільтрації трафіку
Захист від витоків інформації	Запобігання витокам конфіденційної інформації внаслідок атак або помилок	Використання Data Loss Prevention (DLP) систем
Автоматизоване виявлення інсайдерських загроз	Використання аналітики та систем виявлення аномалій для ідентифікації підозрілої активності	Моніторинг надмірного доступу до конфіденційних даних

Подальше дослідження проблеми побудови онтологічної моделі для формалізації процесу виявлення інсайдерських кіберзагроз у банках має за

мету розширення її функціональності та адаптацію до зростаючих викликів у сфері кібербезпеки. Важливим аспектом є врахування ширшого контексту дій інсайдерів, включаючи внутрішні та зовнішні чинники, які можуть впливати на їхню активність. Загалом, подальше дослідження має ставити за мету розробку більш сучасних та ефективних стратегій виявлення та протидії інсайдерським кіберзагрозам, а також адаптацію моделі до змін в кіберландшафті та вимогам банківського сектора.

Робота виконана в рамках держбюджетної науково-дослідної роботи 0121U109559 «Національна безпека через конвергенцію систем фінансового моніторингу та кібербезпеки: інтелектуальне моделювання механізмів регулювання фінансового ринку».

1. Afaq S. A., Uzma S., Yasmeen G. The Critical Impact of Cyber Threats on Digital Economy. In Advances in Cyberology and the Advent of the Next-Gen Information Revolution. IGI Global. 2023. P. 86-108. https://doi.org/10.4018/978-1-6684-8133-2.ch005

2. Mishra S. Exploring the Impact of AI-Based Cyber Security Financial Sector Management. Applied Sciences. 2023. № 13(10). Art. number 5875. DOI: 10.3390/app13105875

3. Rauf U., Mohsen F., Wei Z. A Taxonomic Classification of Insider Threats: Existing Techniques, Future Directions & Recommendations. Journal of Cyber Security and Mobility. 2023. № 12(2). P. 221-252. https://doi.org/10.13052/jcsm2245-1439.1225

4. Green M. L., Dozier P. Understanding Human Factors of Cybersecurity: Drivers of Insider Threats. In 2023 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE, 2023. P. 111-116. https://doi.org/10.1109/CSR57506.2023.10224926

5. Al-Fawa'reh M., Al-Fayoumi M., Nashwan S., Fraihat S. Cyber threat intelligence using PCA-DNN model to detect abnormal network behavior. Egyptian Informatics Journal. 2022. № 23(2). P. 173-185. https://doi.org/10.1016/j.eij.2021.12.001

6. Mamun M., Shi K. DeepTaskAPT: insider apt detection using task-tree based deep learning. In 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE. 2021. P. 693-700. https://doi.org/10.1109/TrustCom53373.2021.00102

7. Scott J., Kyobe M. Trends in cybersecurity management issues related to human behaviour and machine learning. In 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET). IEEE. 2021. P. 1-8. https://doi.org/10.1109/ICECET52533.2021.9698626

8. Sбnchez-Zas C., Villagrб V. A., Vega-Barbas M., Larriva-Novo X., Moreno J. I., Berrocal J. Ontology-based approach to real-time risk management and cyber-situational awareness. Future Generation Computer Systems. 2023. №141. P. 462-472. https://doi.org/10.1016/j.future.2022.12.006

9. Dora J. R., Hluchэ L., Nemoga K. Ontology for Blind SQL Injection. Computing and Informatics. 2023. № 42(2). P. 480-500. https://doi.org/10.31577/cai_2023_2_480

10. Huang C. C., Huang P. Y., Kuo Y. R., Wong G. W., Huang Y. T., Sun Y. S., Chen M. C. Building Cybersecurity Ontology for Understanding and Reasoning Adversary Tactics and Techniques. In 2022 IEEE International Conference on Big Data (Big Data). IEEE. 2022. P. 4266-4274 https://doi.org/10.1109/BigData55660.2022.10021134

---

1. Afaq S. A., Uzma S., Yasmeen G. (2023). The Critical Impact of Cyber Threats on Digital Economy. In Advances in Cyberology and the Advent of the Next-Gen Information Revolution (pp. 86-108). IGI Global. DOI: 10.4018/978-1-6684-8133-2.ch005

2. Mishra S. (2023). Exploring the Impact of AI-Based Cyber Security Financial Sector Management. Applied Sciences. Vol. 13(10). Art. number 5875. DOI: 10.3390/app13105875

3. Rauf U., Mohsen F., Wei Z. (2023). A Taxonomic Classification of Insider Threats: Existing Techniques, Future Directions & Recommendations. Journal of Cyber Security and Mobility. Vol. 12(2). pp. 221-252. DOI: 10.13052/jcsm2245-1439.1225

4. Green M. L., Dozier P. (2023, July). Understanding Human Factors of Cybersecurity: Drivers of Insider Threats. In 2023 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 111-116). IEEE. DOI: 10.1109/CSR57506.2023.10224926

5. Al-Fawa'reh M., Al-Fayoumi M., Nashwan S., Fraihat S. (2022). Cyber threat intelligence using PCA-DNN model to detect abnormal network behavior. Egyptian Informatics Journal. Vol. 23(2). pp. 173-185. DOI: 10.1016/j.eij.2021.12.001

6. Mamun M., Shi K. (2021, October). DeepTaskAPT: insider apt detection using task-tree based deep learning. In 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (pp. 693-700). IEEE. DOI: 10.1109/TrustCom53373.2021.00102

7. Scott J., Kyobe M. (2021, December). Trends in cybersecurity management issues related to human behaviour and machine learning. In 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1-8). IEEE. DOI: 10.1109/ICECET52533.2021.9698626

8. Sбnchez-Zas C., Villagrб V. A., Vega-Barbas M., Larriva-Novo X., Moreno J. I., Berrocal J. (2023). Ontology-based approach to real-time risk management and cyber-situational awareness. Future Generation Computer Systems. Vol. 141. pp. 462-472. DOI: 10.1016/j.future.2022.12.006

9. Dora J. R., Hluchэ L., Nemoga K. (2023). Ontology for Blind SQL Injection. Computing and Informatics. Vol. 42(2). pp. 480-500. DOI: 10.31577/cai_2023_2_480

10. Huang C. C., Huang P. Y., Kuo Y. R., Wong G. W., Huang Y. T., Sun Y. S., Chen M. C. (2022, December). Building Cybersecurity Ontology for Understanding and Reasoning Adversary Tactics and Techniques. In 2022 IEEE International Conference on Big Data (Big Data) (pp. 4266-4274). IEEE. DOI: 10.1109/BigData55660.2022.10021134