DOI: https://doi.org/10.32782/2524-0072/2023-57-130

УДК 336.71:330.46: 330.47

КОНЦЕПЦІЯ СТВОРЕННЯ ЕКСПЕРТНОЇ СИСТЕМИ РАННЬОЇ ДІАГНОСТИКИ СИГНАЛІВ ПІДОЗРІЛОЇ ДІЯЛЬНОСТІ СПІВРОБІТНИКІВ ФІНАНСОВОЇ УСТАНОВИ[1]

THE CONCEPT OF CREATING AN EXPERT SYSTEM FOR EARLY DIAGNOSTIC SIGNALS OF SUSPICIOUS ACTIVITIES OF FINANCIAL INSTITUTION EMPLOYEES

Яровенко Ганна Миколаївна
докторка економічних наук, доцентка,
Сумський державний університет
ORCID: https://orcid.org/0000-0002-8760-6835

Yarovenko Hanna
Sumy State University

Стаття присвячена концепції створення експертної системи для ранньої діагностики сигналів підозрілої діяльності співробітників фінансових установ. В роботі аргументовано актуальність цього напрямку в сучасному світі, де фінансові організації стикаються з різноманітними ризиками та викликами. Огляд літератури виявив недостатній рівень наукових досліджень з даної проблеми, що пов'язано обмеженнями публічного доступу та розголосу комерційної таємниці щодо кібербезпеки фінансових установ. Розробка експертної системи вимагає комплексного підходу та урахування різноманітних факторів, які впливають на фінансовий сектор, а також включають особливості поведінки інсайдерів. Стаття надає докладний огляд концепції, яка базується на десяти ключових етапах розробки експертної системи. Перший етап пов'язаний з визначенням мети та областю застосування та включає в себе основні цілі та завдання системи, функції, користувачів, вимоги та обмеження. На другому реалізується збір вхідних даних, який базується на їх форматі, структурі, джерелах, валідації, конфіденційності, тощо. Підготовка та очищення даних має на увазі процедури роботи з даними, необхідними для роботи експертної системи. Етап вибору технологій передбачає використання різних інструментів та середовищ програмування, які забезпечать ефективність та надійність експертної системи. Етап розробки моделей є найбільш складним, оскільки він є ключовим для виявлення підозрілої діяльності інсайдерів і потребує постійне вдосконалення на основі нових даних та розширення їхньої функціональності. Етап машинного навчання та тренування моделей описує відповідні процедури та вимагає постійного навчання системи та адаптації до нових видів загроз. Інтеграція з передовими технологіями машинного навчання та розширена обробка природної мови є необхідним етапом розробки експертної системи, оскільки дозволяє отримувати інформацію з різних підсистем корпоративної системи фінансової установи. Етап тестування та валідації гарантуватиме коректність роботи експертної системи. Впровадження та моніторинг є етапом реалізації експертної системи у життєдіяльність фінансової установи. Навчання та адаптація дозволяє системі бути динамічною та адаптуватися до внутрішніх та зовнішніх умов.

Ключові слова: діагностика, експертна система, інсайдер, кібершахрайство, фінансова установа.

The article is devoted to creating an expert system for early diagnosis of employees' suspicious activity in financial institutions. The work argues the relevance of this direction in the modern world, where financial organizations face various risks and challenges. The literature review revealed insufficient scientific research on this problem due to restrictions on public access and disclosure of commercial secrets regarding the cyber security of financial institutions. Developing an expert system requires a comprehensive approach and consideration of various factors that affect the financial sector, as well as including the specifics of insider behaviour. The article provides a detailed overview of the concept based on ten key stages of developing an expert system. The first stage is related to defining the purpose and scope and includes the main goals and objectives of the system, functions, users, requirements and limitations. The second implements input data collection based on their format, structure, sources, validation,

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

confidentiality, etc. Data preparation and cleaning refers to procedures for working with data necessary to operate an expert system. The technology selection stage involves using various tools and programming environments to ensure the expert system's efficiency and reliability. The model development stage is the most difficult, as it is critical to detecting suspicious insider activity and requires constant improvement based on new data and expanding their functionality. The machine learning and model training set describes the relevant procedures and requires regular system training and adaptation to new threats. Integration with advanced machine learning technologies and natural language processing is necessary for developing an expert system, as it allows obtaining information from various subsystems of the corporate system in a financial institution. The testing and validation stage will guarantee the correctness of the expert system. Implementation and monitoring are stages of the expert system's implementation in a financial institution's life. Learning and adaptation allow the system to be dynamic and adapt to internal and external conditions.

Keywords: diagnostics, expert system, insider, cyber fraud, financial institution.

Постановка проблеми. Проблема, пов'язана з підозрілою діяльністю співробітників фінансової установи, представляє собою серйозний виклик для фінансового сектору та загрожує як фінансовій стійкості, так і довірі громадськості до цих установ. Однією з ключових аспектів цієї проблеми є можливість внутрішньої загрози та фінансового маніпулювання з боку власних співробітників. Підозріла діяльність співробітників може включати в себе різноманітні аспекти, такі як незаконні фінансові транзакції, використання конфіденційної інформації для особистої вигоди, або сприяння здійсненню шахрайства чи відмиванню грошей. Ці дії можуть призвести до значних втрат для фінансових установ, порушення законодавства та негативно вплинути на репутацію установи в очах клієнтів та громадськості.

Одним із викликів є виявлення такої підозрілої діяльності, оскільки співробітники можуть використовувати внутрішні знання та доступ до систем для того, щоб уникати виявлення. Потрібні ефективні механізми моніторингу та аналізу фінансових операцій, які дозволяють виявити неправомірну діяльність та уникнути втрат. Крім того, проблема підозрілої діяльності співробітників підкреслює важливість вдосконалення систем внутрішнього контролю, перевірок та балансів для зменшення можливості виникнення конфлікту інтересів та зловживання повноважень. Враховуючи динаміку фінансового сектору та зростання кількості та складності фінансових операцій, вирішення проблеми підозрілої діяльності співробітників вимагає інноваційних та ефективних стратегій, які б забезпечили надійний контроль та захист фінансових інтересів установи. Розробка та впровадження експертної системи в сфері ранньої діагностики сигналів підозрілої діяльності співробітників фінансової установи може суттєво поліпшити процес виявлення та реагування на потенційні загрози. Експертна система, базуючись на сучасних технологіях машинного навчання та аналітики даних, вноситиме значний внесок у підвищення безпеки та ефективності фінансових операцій.

По-перше, така система дозволить аналізувати великий обсяг структурованих та неструктурованих даних, таких як фінансові транзакції, інформація про доступ до систем, а також внутрішні та зовнішні сигнали, що можуть свідчити про підозрілу діяльність. Алгоритми машинного навчання дозволять системі виявляти патерни та аномалії, що можуть залишитися непоміченими при традиційних методах аудиту. По-друге, система буде здатна автоматично класифікувати та оцінювати рівень ризику для кожної виявленої аномалії чи сигналу. Це дозволить працівникам фінансової установи швидко реагувати на найбільш критичні ситуації та вживати необхідні заходи для запобігання можливим фінансовим втратам чи неправомірним діям. По-третє, розроблена система буде постійно навчатися та адаптуватися до нових векторів загроз та шаблонів підозрілої діяльності. Це означає, що система буде вдосконалюватися в часі, враховуючи зміни в фінансовому середовищі та еволюцію методів здійснення фінансових злочинів. По-четверте, впровадження експертної системи спростить процес виявлення та співробітництва з іншими інформаційними системами в установі. Це дозволить розширити область виявлення підозрілої діяльності та забезпечити комплексний підхід до безпеки.

Розробка та впровадження експертної системи в контексті ранньої діагностики підозрілої діяльності співробітників фінансової установи веде до підвищення ефективності, точності та оперативності виявлення потенційних ризиків, сприяючи загальному підвищенню безпеки та надійності в фінансовому секторі.

Аналіз останніх досліджень і публікацій. Тема ранньої діагностики сигналів підозрілої діяльності інсайдерів фінансових установ є практично значущою, оскільки дана проблема може вирішуватися тільки постфактум. Також важко виявити мотивацію співробітників щодо реалізації ними злочинних намірів та передбачити ті способи і інструменти, які будуть використані в процесі реалізації кібершахрайств. Тому на цю сферу накладаються суттєві обмеження щодо надання даних у відкритий доступ. Відповідно результатом цього є недостатня кількість публікацій.

На запит ключових слів «експертна система» та «інсайдер» база даних Скопус надала всього 57 документів, публікація яких відбувалася протягом 1990–2023 років, що свідчить про специфіку даного дослідження. Серед них слід відмітити наступні роботи. Джарра О. М. А., Аюб М. А., Джарарве Й. працювали над розробкою експертної системи для виявлення хмарних інсайдерських атак, яку було побудовано на основі штучного інтелекту [1]. Дханья Д., Катір І., Кучіпуді Р., Тамараі І. та Кумар Е. Р. запропонували модель експертної системи виявлення вторгнень, яка використовує нечітку логіку у режимі реального часу [2]. Прадеші К.В. та Каннан А. дослідили можливості інтелектуального вибору функцій на основі правил і класифікації для виявлення DoS атак у хмарі, але ж питання інсайдерських кібершахрайств вони не розглядали при цьому [3]. Рауф У., Мохсен Ф. та Вей З. запропонували структури даних для ідентифікації атрибутів бази даних, створеної для виявлення кіберзагроз, джерелом яких виступають співробітники підприємств нефінансової сфери [4].

Для вирішення проблеми ідентифікації інсайдерських кіберзагроз пропонується використання різних методів. Так, Чен Р. К., Ченг К. Ф. та Сє К. К. обґрунтували можливості застосування нейронної мережі та правила нечіткої теорії адаптивного резонансу для виявлення вторгнень у безпеку даних державних установ [5]. Д'Амбросіо Н., Перроне Г. та Романо С.П. розробили методику ідентифікації внутрішніх кіберзагроз на основі байєсівських нейронних мереж [6]. Дасс М., Кеннаді Дж. та Поттер В. Д. розкритикували можливості штучного інтелекту для виявлення вторгнень та запропонували навчальну систему на основі дошки, яка керується автономними агентами та має можливість онлайн-навчання [7].

Заслуговують на окрему увагу дослідження, супутні для вирішення поставленої проблеми. Алеман-Меза Б., Бернс П., Евенсон М., Паланісвамі Д. та Шет А. запропонували онтологічний підхід до системи, яка дозволяє досліджувати документи, пов’язані з внутрішніми кіберзагрозами [8]. Шеффер Е., Шафі С., Майр А. та Франке Дж. обґрунтовують перспективи застосування конфігураторів знань для розробки експертних систем, що дозволить економити кошти на їх створення [9]. Кунц М., Хаммер М., Фукс Л., Неттер М. та Пернул Г. дослідили тренди у створенні та організації менеджменту ідентифікації в різних компаніях та відмітили наявність стагнації у процесах керування привілейованими користувачами [10].

Не дивлячись на існування певних напрацювань, невирішеними залишаються багато питань, в тому числі й створення експертної системи діагностики діяльності інсайдерів саме фінансових установ. Вирішенню даного питання й буде присвячене це дослідження.

Мета статті полягає у розробленні концепції створення експертної системи, яка дозволить проводити ранню діагностику сигналів підозрілої діяльності співробітників фінансової установи.

Виклад основного матеріалу дослідження. Експертна система ранньої діагностики сигналів підозрілої діяльності співробітників фінансової установи – це інформаційна система, яка використовується для автоматичного виявлення та аналізу ненормальної чи потенційно аферистської діяльності серед працівників фінансових організацій. Ця система зазвичай базується на використанні штучного інтелекту, методів машинного навчання та аналізу великих обсягів даних. Основні функції експертних систем ранньої діагностики включають:

1) моніторинг активності, коли система автоматично відстежує та аналізує активність працівників в системі фінансової установи, враховуючи різноманітні параметри, такі як доступ до конфіденційної інформації, частота та обсяг фінансових транзакцій тощо;

2) виявлення аномалій, коли система використовує алгоритми аналізу аномалій для виявлення невластивих патернів чи незвичайних змін в поведінці працівників, що можуть вказувати на підозрілу діяльність;

3) аналіз внутрішніх та зовнішніх факторів, коли система враховує як внутрішні фактори, пов'язані зі змінами в робочій поведінці працівників, так і зовнішні фактори, такі

як зміни в економічному середовищі або в законодавстві;

4) створення алертів і звітів. Якщо система виявляє підозрілу активність, вона може генерувати автоматичні алерти та створювати звіти для відповідальних осіб чи служб безпеки;

5) машинне навчання, коли експертна система може використовувати методи машинного навчання для постійного вдосконалення своїх алгоритмів та адаптації до нових викликів та змін в середовищі.

Експертні системи допомагають фінансовим установам запобігти фінансовим шахрайствам, неправомірним трансакціям та іншим видам злочинності, забезпечуючи ефективний контроль та безпеку в їхніх операціях.

Створення експертної системи ранньої діагностики сигналів підозрілої діяльності співробітників фінансової установи – це складний процес. Її концепція базується на реалізації наступних етапів: визначення мети та області застосування; збір вихідних даних; підготовка та очищення даних; вибір технологій; розробка моделі; машинне навчання та тренування моделі; інтеграція з іншими системами; тестування та валідація; впровадження та моніторинг; навчання та адаптація.

Етап *«Визначення мети та області застосування»* є фундаментальним для успішного створення експертної системи, оскільки від нього залежить далі вибір технологій, розробка функціоналу та оцінка ефективності системи. На цьому етапі визначається суть та напрямок системи. Основними аспектами цього етапу є:

– основні цілі та завдання системи повинні бути чітко визначені. Наприклад, основною метою може бути виявлення та запобігання фінансовим аферам, недобросовісній діяльності, витокам конфіденційної інформації або порушенням внутрішніх правил установи;

– ретельний аналіз того, як система буде використовуватися в конкретному контексті фінансової установи. Це включає вивчення поточних процесів, ідентифікацію слабких місць, визначення основних викликів та потреб користувачів;

– визначення того, які функції системи будуть реалізовані для досягнення мети. Це може включати в себе моніторинг фінансових транзакцій, аналіз доступу до конфіденційної інформації, виявлення аномалій у поведінці співробітників та інші аспекти;

– визначення групи користувачів, які будуть взаємодіяти з системою. Це можуть бути аналітики фінансового відділу, служба безпеки, адміністратори системи та інші фахівці;

– розгляд вимог та обмежень, пов'язаних із використанням системи, включаючи законодавчі норми, політики безпеки, етичні стандарти та інші аспекти, що можуть впливати на функціонування системи;

– взаємодія з керівництвом фінансової установи та іншими зацікавленими сторонами для забезпечення відповідності мети системи стратегічним цілям організації.

На етапі *«Збір вихідних даних»* здійснюється збір необхідних даних, які будуть використовуватися для аналізу та прийняття рішень, оскільки точність та повнота зібраних даних суттєво впливають на ефективність та точність експертної системи в подальшому. Основні аспекти цього етапу включають:

– визначення джерел, з яких можна отримати необхідні дані. Це може включати бази даних фінансової установи, системи моніторингу транзакцій, логи доступу, індивідуальні профілі співробітників, а також зовнішні джерела інформації;

– визначення того, як часто збирати дані та який обсяг інформації необхідний для забезпечення ефективної роботи системи. Це може бути залежно від специфіки діяльності фінансової установи та потреб системи;

– визначення форматів та структури даних, що будуть збиратися. Різні джерела можуть надавати дані у різних форматах, тому важливо забезпечити їхню сумісність для подальшого аналізу;

– розробку механізмів забезпечення конфіденційності та захисту даних. Особливо важливо при роботі з фінансовою інформацією та особистими даними співробітників;

– виконання процедур валідації та очищення даних для виявлення та коригування можливих помилок, викидів чи неправильних значень;

– забезпечення можливості інтеграції з існуючими інформаційними системами фінансової установи для забезпечення єдиної точки доступу до даних;

– створення документації, яка описує характеристики та особливості зібраних даних. Це сприяє зрозумінню та ефективному використанню інформації;

– розробку механізмів для відстеження та управління змінами в джерелах даних, щоб система була завжди актуальною.

Етап *«Підготовка та очищення даних»* є важливим для того, щоб забезпечити якість та

достовірність даних, які використовуються в системі, і підготувати їх для подальшого використання в алгоритмах машинного навчання чи інших методах аналізу. На цьому етапі проводяться різні операції з обробки та підготовки даних для подальшого використання в аналізі та тренуванні моделей. Основними аспектами цього етапу є:

– виявлення та коригування помилок, викидів, аномалій або відсутніх значень в даних. Це може включати в себе заміну втрачених значень, вилучення аномальних або викидів, а також корекцію помилкових даних;

– розгляд методів для заповнення втрачених або відсутніх значень в даних. Це важливо для підтримання повноти та достовірності даних під час аналізу;

– приведення даних до стандартних форматів та одиничних шкал для уникнення спотворень у вагомості різних атрибутів під час аналізу;

– процес перетворення категоріальних даних у числовий формат, що є придатним для використання в алгоритмах машинного навчання;

– відбір та вилучення зайвих атрибутів, які не несуть корисної інформації для вирішення конкретної задачі. Це може покращити ефективність моделі та зменшити обсяг обробки даних;

– створення нових ознак на основі існуючих даних, щоб покращити розуміння та виявлення залежностей в даних;

– забезпечення балансування класів, особливо в задачах класифікації, де може бути нерівноважна кількість прикладів різних класів;

– збереження очищених та оброблених даних у відповідному форматі для подальшого використання під час тренування та валідації моделей.

На етапі *«Вибір технологій»* слід враховувати специфіку завдань, ресурсні обмеження, технічні вимоги та величину організації. Найкращий підхід – використовувати технології, які найбільше відповідають конкретним потребам та дозволяють забезпечити ефективність та надійність експертної системи. Правильний вибір технологій може значно вплинути на ефективність, продуктивність та масштабованість системи. Основні аспекти цього етапу включають:

– вибір мов програмування, які найкраще підходять для реалізації системи. Python, Java, або R часто використовуються у сфері машинного навчання та аналітики даних;

– вибір бази даних для зберігання та керування даними. Для великих обсягів даних може бути корисними NoSQL бази даних, такі як MongoDB чи Cassandra;

– використання відомих фреймворків для машинного навчання, таких як TensorFlow, PyTorch або scikit-learn;

– вибір інструментів для очищення, обробки та аналізу даних, таких як Pandas, NumPy або Apache Spark;

– використання інструментів для візуалізації результатів та подання зрозумілої інформації, таких як Matplotlib, Seaborn або Tableau;

– використання систем керування версіями, таких як Git, для ефективного співпраці в робочій групі та відслідковування змін в коді;

– вибір інструментів для забезпечення безпеки даних та зменшення ризиків витоку конфіденційної інформації;

– використання інтегрованих середовищ розробки та інструментів тестування для забезпечення надійності та високої якості коду;

– розгляд використання хмарних сервісів для забезпечення масштабованості та доступності системи, таких як Amazon AWS, Microsoft Azure чи Google Cloud;

– розробка інтерфейсів та механізмів для ефективної інтеграції з існуючими інформаційними системами фінансової установи.

«Розробка моделі» – це ітеративний процес, що може вимагати декількох етапів налаштування та оптимізації для досягнення найкращих результатів. На цьому етапі будується алгоритм або модель, яка виявлятиме аномалії та підозрілі патерни на основі навчання на наявних даних. Важливо постійно вдосконалювати модель і реагувати на зміни в даних та середовищі. Основні аспекти розробки моделі включають:

– конкретне формулювання завдань, які модель повинна вирішити. Це може включати виявлення аномалій у фінансових транзакціях, моніторинг доступу до конфіденційної інформації та інші завдання, пов'язані з ранньою діагностикою підозрілої діяльності співробітників;

– визначення методів, які будуть використовуватися для розробки моделі. Це може включати методи машинного навчання (наприклад, класифікація, кластеризація), статистичні методи або глибинне навчання;

– визначення ознак, які будуть використовуватися для навчання моделі. Це може включати фінансові показники, характе-

ристики доступу, історію транзакцій та інші відомості;

– використання навчального набору даних для навчання моделі. Підбір оптимальних параметрів та архітектури моделі для досягнення високої точності та надійності;

– тестування моделі на тестовому наборі даних для оцінки її ефективності та генералізації на нові дані;

– оптимізація моделі для забезпечення кращої продуктивності, швидкодії та низького ризику перенавчання;

– інтеграція розробленої моделі в загальну архітектуру експертної системи та її взаємодія з іншими компонентами;

– перенесення розробленої моделі в робоче середовище. Це включає в себе встановлення необхідних компонентів, налаштування та перевірку правильності функціонування;

– встановлення механізмів для постійного навчання моделі на нових даних, щоб вона була адаптивною та ефективною у мінливому середовищі;

– створення системи моніторингу для виявлення аномалій в роботі моделі та надання технічної підтримки для вирішення можливих проблем.

«Машинне навчання та тренування моделі» – це ітеративний процес, який може включати кілька циклів оптимізації та покращення. На цьому етапі використовуються алгоритми та методи, які дозволяють моделі "вивчати" закономірності в даних та здатність робити прогнози або класифікації на нових даних. Даний етап включає:

– формалізацію задачі, яку модель повинна вирішити. Це може бути класифікація (визначення категорії), регресія (прогнозування числового значення), кластеризація (групування) або інше;

– визначення конкретного алгоритму машинного навчання, який найкраще підходить для вирішення визначених завдань. Це може бути алгоритм класифікації, регресії, кластеризації або ансамблеві методи;

– визначення функції, яка оцінює різницю між прогнозованими та фактичними значеннями. Ця функція визначає, як модель «навчається» та адаптується до даних;

– розділення доступних даних на тренувальний та валідаційний набори для ефективного тренування та оцінки ефективності моделі;

– подачу тренувальних даних у модель для того, щоб вона вивчала внутрішні закономірності та параметри, що дозволяють їй робити прогнози на нових даних;

– налаштування параметрів моделі для досягнення максимальної точності та уникнення перенавчання;

– оцінку ефективності моделі на валідаційному та тестовому наборах даних для перевірки її здатності генералізуватися на нові дані;

– забезпечення механізмів для постійного навчання моделі на нових даних, що дозволяє їй адаптуватися до змін у середовищі;

– аналіз результатів та визначення, наскільки ефективно модель вирішує визначені завдання;

– впровадження навченої моделі в робоче середовище для використання в реальних умовах.

«Інтеграція з іншими системами» в контексті експертної системи ранньої діагностики сигналів підозрілої діяльності означає забезпечення взаємодії та обміну даними з існуючими інформаційними системами в організації. Інтеграція з іншими системами вимагає дбайливого підходу та співпраці між різними відділами та командами в організації. Правильна інтеграція допомагає забезпечити взаємодію систем та максимально використовувати корисність експертної системи у фінансовому середовищі. Основні аспекти інтеграції включають:

– ретельний аналіз існуючих інформаційних систем у фінансовій установі. Визначення структури даних, форматів зберігання, інтерфейсів та потреб в інформації;

– визначення ключових точок, де може відбуватися обмін даними між експертною системою та існуючими системами. Це може бути обмін даними через API, бази даних, файлові системи тощо;

– створення програмних інтерфейсів для ефективного обміну даними між експертною системою та іншими системами;

– забезпечення стандартизації форматів даних, які використовуються в обміні між системами. Це сприяє уніфікації та зменшенню конфліктів при обміні інформацією;

– розробку механізмів автоматичного обміну даними між системами для забезпечення оперативності та актуальності інформації;

– впровадження механізмів безпеки для захисту конфіденційності та цілісності обмінюваних даних. Використання шифрування, автентифікації та авторизації;

– розробку систем моніторингу та логування для відстеження обміну даними та виявлення можливих проблем або помилок;

– проведення тестів інтеграції для перевірки правильності та ефективності обміну даними між системами;

– розробку механізмів резервного копіювання та відновлення даних для забезпечення безпеки та надійності обміну;

– розробку документації та надання інструкцій для користувачів та технічної підтримки для вирішення питань та проблем, пов'язаних з інтеграцією.

«Тестування та валідація» допомагає гарантувати, що система працює ефективно та відповідає вимогам та очікуванням користувачів. Цей процес спрямований на перевірку правильності та ефективності роботи системи перед впровадженням в реальне середовище. Тестування та валідація включають:

– використання тренувальних даних для навчання моделі та валідаційних даних для оцінки її ефективності. Тренувальні дані використовуються для налаштування параметрів, а тестові дані – для оцінки загальної продуктивності та генералізації;

– розробку стратегій тестування, включаючи модульне тестування (тестування окремих компонентів), інтеграційне тестування (взаємодія компонентів), та системне тестування (повна система);

– визначення тестових випадків для перевірки функціональності системи, а також негативних сценаріїв для визначення, як система реагує на неправильні дані чи ситуації;

– оцінку точності та вірогідності результатів системи порівняно з валідованими даними. Це включає оцінку чутливості (дії на справжні позитиви) та специфічності (уникнення хибно-позитивних результатів);

– вимірювання часу відповіді системи на різні запити та завдання для забезпечення відповідності встановленим вимогам;

– тестування системи на стійкість до штучних втручань чи атак. Це важливо для забезпечення безпеки та надійності системи;

– визначення, наскільки добре модель генералізує знання та може застосовуватися до нових, реальних сценаріїв;

– використання реальних даних для валідації продуктивності та ефективності системи у реальних умовах;

– фіксацію результатів тестів та валідації у вигляді документації для подальшого використання та аналізу;

– виправлення помилок, що були виявлені під час тестів, та оптимізація системи для підвищення її ефективності та надійності.

«Впровадження та моніторинг» включає в себе впровадження системи в реальне виробниче середовище та постійний моніторинг її роботи. Успішне проведення цього етапу допомагає забезпечити надійність та ефективність системи в реальному виробничому середовищі. Його основні аспекти включають:

– розробку детального плану впровадження, включаючи часові рамки, відповідальність та послідовність дій. Впровадження може бути поетапним для зменшення впливу на робочий процес;

– забезпечення необхідних ресурсів та інфраструктури для роботи системи, включаючи обладнання, мережу, бази даних та інші ресурси;

– встановлення та конфігурування всіх компонентів системи відповідно до розробленого плану. Це включає встановлення програмного забезпечення, налаштування параметрів та забезпечення взаємодії з існуючими системами;

– проведення тренінгів та навчання для персоналу, який буде взаємодіяти з системою. Це допомагає забезпечити ефективне використання та розуміння системи;

– проведення тестів та випробувань системи в реальних умовах для визначення її продуктивності, ефективності та взаємодії з реальними даними;

– запуск системи в робочому режимі та постійний моніторинг її роботи. Аналіз результатів та виявлення будь-яких аномалій чи проблем;

– встановлення механізмів для постійного навчання моделі на нових даних для забезпечення її актуальності та адаптивності;

– впровадження оновлень та покращень системи відповідно до змін у вимогах, технологічному середовищі та зміни в бізнес-процесах;

– постійну перевірку та оновлення механізмів безпеки системи для забезпечення захисту від потенційних загроз;

– ведення документації та створення звітів про роботу системи. Це включає в себе відслідковування виявлених проблем, виконані оновлення та результати моніторингу.

«Навчання та адаптація» є процесами, які дозволяють системі залишатися реактивною та ефективною в змінних умовах, а також надавати користувачам актуальні та надійні результати. Цей етап передбачає постійне удосконалення системи на основі нових даних, досвіду її використання та змін в середовищі. Навчання та адаптація це:

– постійний збір нових даних для системи. Це може включати як нові дані щодо активності користувачів чи фінансових транзакцій, так і дані про нові типи загроз або аномальні події;

– використання нових даних для оновлення моделі системи. Це може включати періодичне перетренування моделі для врахування нових закономірностей та змін у середовищі;

– додавання нових функціональних можливостей або алгоритмів на основі виявлених потреб користувачів чи нових вимог. Це може включати вдосконалення системи для виявлення нових видів загроз чи покращення точності прогнозів;

– постійна оптимізація параметрів системи для досягнення максимальної точності та ефективності. Це може вимагати регулярного перегляду та налаштування параметрів;

– виявлення та виправлення помилок чи невірних висновків системи. Постійне вдосконалення алгоритмів для зменшення хибно-позитивних та хибно-негативних результатів;

– вивчення та аналіз використання системи користувачами. Виявлення шляхів покращення інтерфейсу та функціоналу для забезпечення більшої зручності та задоволення користувачів;

– постійна адаптація системи до змін в зовнішньому середовищі, таких як нові технології, правила чи законодавство. Це дозволяє системі залишатися актуальною та ефективною;

– аналіз та оновлення заходів безпеки системи для виявлення та захисту від нових загроз;

– використання зворотного зв'язку від користувачів та експертів для удосконалення системи та виправлення слабких місць;

– забезпечення регулярних оновлень програмного забезпечення та моделей системи для усунення помилок, виявлення нових можливостей та підтримки сучасних стандартів.

Висновки. Концепція створення експертної системи ранньої діагностики сигналів підозрілої діяльності співробітників фінансової установи є актуальним та стратегічно важливим напрямком в сучасному світі, де фінансові організації стикаються з різноманітними ризиками та викликами. Розробка такої експертної системи вимагає комплексного підходу та врахування різноманітних факторів, які впливають на фінансовий сектор. Зазначена концепція є складною та багатоетапною задачею, яка вимагає комплексного підходу, використання сучасних технологій та урахування специфіки фінансового сектору. Її реалізація може призвести до покращення безпеки та довіри в фінансовому секторі, а також зниження ризиків фінансових злочинів та неправомірних дій.

Концепція створення експертної системи ранньої діагностики сигналів підозрілої діяльності співробітників фінансової установи базується на основних етапах розробки такої системи. Починаючи з визначення мети та області застосування, процес включає в себе збір та очищення вихідних даних, вибір технологій, розробку та навчання моделі, інтеграцію з іншими системами, тестування та валідацію, впровадження та моніторинг, а також постійне навчання та адаптацію. Цей комплексний підхід дозволяє створити ефективну систему, яка забезпечує вчасне виявлення та реагування на потенційно підозрілу діяльність, сприяючи підвищенню безпеки та надійності фінансових операцій у відповідній установі.

Запропонована у статті концепція має значний потенціал для подальшого розвитку та вдосконалення експертної системи. Ключовим кроком в цьому напрямку є постійне вдосконалення моделей на основі нових даних та розширення їхньої функціональності. Подальша інтеграція з передовими технологіями машинного навчання, розширена обробка природної мови та аналітичні методи можуть значно підвищити точність та швидкість реакції системи. Однією з ключових перспектив є також удосконалення механізмів виявлення аномалій та реагування на нові види загроз, враховуючи зміни в сучасних фінансових схемах та технологічних вирішеннях. Навчання системи на основі зворотного зв'язку від користувачів та експертів також може допомогти виявити та виправити недоліки, що виникають у реальних умовах використання. Забезпечення високого рівня безпеки та конфіденційності є іншим важливим аспектом розвитку. Запровадження та оновлення заходів забезпечення інформаційної безпеки дозволить експертній системі ефективно функціонувати в умовах зростаючого обсягу кіберзагроз. Підвищення взаємодії та інтеграції системи з іншими інформаційними системами у фінансовому секторі також може забезпечити більш комплексний та зручний підхід до виявлення та аналізу підозрілих сигналів.

Загалом, динаміка розвитку цієї концепції полягає у поєднанні сучасних технологій, аналітичних методів та постійного навчання, щоб забезпечити ефективну та надійну реакцію на ризики та підозрілі дії у фінансовому секторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Jarrah O. M. A., Ayoub M. A., Jararweh Y. Hierarchical detection of insider attacks in cloud computing systems. *International Journal of Information and Computer Security*. 2017. Vol. 9, no. 1/2. P. 85. DOI: https://doi.org/10.1504/ijics.2017.082840

2. Dhanya D., Kathir I., Kuchipudi R., Thamarai I., Kumar E. R. Intrusion detection system using soft computing techniques in 5G communication systems. In *Artificial Intelligence, Blockchain, Computing and Security Volume 1*. CRC Press, 2023. P. 574–579.

3. Pradeepthi K. V., Kannan A. Cloud Attack Detection with Intelligent Rules. *KSII Transactions on Internet & Information Systems*. 2015. Vol. 9(10). P. 4204–4222. DOI: https://doi.org/10.3837/tiis.2015.10.025

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

5. Chen R. C., Cheng K. F., Hsieh C. C. Using Fuzzy Neural Networks and rule heuristics for anomaly intrusion detection on database connection. In *2008 International Conference on Machine Learning and Cybernetics*. IEEE. 2008. Vol. 6. P. 3607–3612. DOI: https://doi.org/10.1109/ICMLC.2008.4621030

6. D'Ambrosio N., Perrone G., Romano S. P. Including Insider Threats into Risk Management through Bayesian Threat Graph Networks. *Computers & Security.* 2023. P. 103410. DOI: https://doi.org/10.1016/j.cose.2023.103410

7. Dass M., Cannady J., Potter W. D. A blackboard-based learning intrusion detection system: a new approach. In *Chung, P.W.H., Hinde, C., Ali, M. (eds) Developments in Applied Artificial Intelligence. IEA/AIE 2003. Lecture Notes in Computer Science, vol 2718.* Springer, Berlin, Heidelberg. 2003. P. 385–390. DOI: https://doi.org/10.1007/3-540-45034-3_39

8. Aleman-Meza B., Burns P., Eavenson M., Palaniswami D., Sheth A. An ontological approach to the document access problem of insider threat. In *Kantor, P., et al. Intelligence and Security Informatics. ISI 2005. Lecture Notes in Computer Science, vol 3495*. Springer, Berlin, Heidelberg. 2005. P. 486–491. DOI: https://doi.org/10.1007/11427995_47

9. Schäffer E., Shafiee S., Mayr A., Franke J. A strategic approach to improve the development of use-oriented knowledge-based engineering configurators (KBEC). *Procedia CIRP*. 2021. Vol. 96. P. 219–224. DOI: https://doi.org/10.1016/j.procir.2021.01.078

10. Kunz M., Hummer M., Fuchs L., Netter M., Pernul G. Analyzing recent trends in enterprise identity management. In *2014 25th international workshop on database and expert systems applications*. IEEE. 2014. P. 273–277. DOI: https://doi.org/10.1109/DEXA.2014.62

REFERENCES:

1. Jarrah, O. M. A., Ayoub, M. A., & Jararweh, Y. (2017). Hierarchical detection of insider attacks in cloud computing systems. *International Journal of Information and Computer Security*, *9*(1/2), 85. DOI: https://doi.org/10.1504/ijics.2017.082840

2. Dhanya, D., Kathir, I., Kuchipudi, R., Thamarai, I., & Kumar, E. R. (2023). Intrusion detection system using soft computing techniques in 5G communication systems. In *Artificial Intelligence, Blockchain, Computing and Security Volume 1*. (pp. 574–579). CRC Press.

3. Pradeepthi, K. V., & Kannan, A. (2015). Cloud Attack Detection with Intelligent Rules. *KSII Transactions on Internet & Information Systems*, *9*(10), 4204–4222. DOI: https://doi.org/10.3837/tiis.2015.10.025

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

5. Chen, R. C., Cheng, K. F., & Hsieh, C. C. (2008). Using Fuzzy Neural Networks and rule heuristics for anomaly intrusion detection on database connection. In *2008 International Conference on Machine Learning and Cybernetics*. (Vol. 6., pp. 3607–3612.). IEEE. DOI: https://doi.org/10.1109/ICMLC.2008.4621030

6. D'Ambrosio, N., Perrone, G., & Romano, S. P. (2023). Including Insider Threats into Risk Management through Bayesian Threat Graph Networks. *Computers & Security,* 103410. DOI: https://doi.org/10.1016/j.cose.2023.103410

7. Dass, M., Cannady, J., & Potter, W. D. (2003). A blackboard-based learning intrusion detection system: a new approach. In *Chung, P.W.H., Hinde, C., Ali, M. (eds) Developments in Applied Artificial Intelligence. IEA/AIE 2003. Lecture Notes in Computer Science, vol 2718.* (pp. 385–390). Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-45034-3_39

8. Aleman-Meza, B., Burns, P., Eavenson, M., Palaniswami, D., & Sheth, A. (2005). An ontological approach to the document access problem of insider threat. In *Kantor, P., et al. Intelligence and Security Informatics. ISI 2005.*

Lecture Notes in Computer Science, vol 3495. (pp. 486–491). Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/11427995_47

9. Schäffer, E., Shafiee, S., Mayr, A., & Franke, J. (2021). A strategic approach to improve the development of use-oriented knowledge-based engineering configurators (KBEC). *Procedia CIRP*, *96*, 219–224. DOI: https://doi.org/10.1016/j.procir.2021.01.078

10. Kunz, M., Hummer, M., Fuchs, L., Netter, M., & Pernul, G. (2014, September). Analyzing recent trends in enterprise identity management. In *2014 25th international workshop on database and expert systems applications*. (pp. 273–277). IEEE. DOI: https://doi.org/10.1109/DEXA.2014.62