Розроблення структури інформаційної бази експертної системи виявлення інсайдерських кіберзагроз у банках*

Яровенко Ганна Миколаївна[1], Петренко Каріна Юріївна[2], Ульяновська Юлія Вікторівна[3], Небаба Наталія Олександрівна[4], Мормуль Микола Федорович[5]

Опубліковано	Секція	УДК
10.12.2023	Економіка	004.056

DOI: http://dx.doi.org/10.5281/zenodo.10350590

Анотація. Стійке зростання кіберзагроз у банківській сфері свідчить про те, що фінансові установи стають особливою мішенню для атак. Роль інсайдерів у цьому контексті стає небезпечною, оскільки їхні дії можуть виявитися ключовим чинником у спровокуванні та здійсненні кіберзагроз на фінансових платформах. Тому розробка експертної системи виявлення кіберзагроз внаслідок дій інсайдерів у банках є актуальним завданням в сьогоднішніх умовах. Загальна мета даного дослідження полягає в розробці інформаційної бази для формування ефективної експертної системи виявлення та протидії кіберзагрозам, ініціатором яких виступають працівники банківських установ. У статті охарактеризовано основні функції та компоненти експертної системи. Охарактеризовано компоненти інформаційної бази, такі як дані про користувачів, події та транзакції, моделі аномалій та машинне навчання, тощо. Авторами запропоновано їх структуру, базуючись на визначенні основних атрибутів. Було визначено дані про користувачів з урахуванням їх детального аналізу особистості та робочих аспектів працівників. Дані про події та транзакції сформульовано із зазначенням критичних моментів та можливих аномалій. Історію доступу та інформацію про конфігурацію системи визначено на основі інформації про авторизований і неавторизований доступ, зміни рівнів доступу та інших відомостей, тощо. Інформація про конфігурацію системи включає дані, які описують конфігурацію технічних аспектів.

* *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] д-рка. екон. наук, доцентка, доцентка кафедри економічної кібернетики Сумського державного університету, https://orcid.org/0000-0002-8760-6835
[2] магістрантка кафедри економічної кібернетики Сумського державного університету, https://orcid.org/0000-0002-1373-3428
[3] к.т.н., доцентка, завідувачка кафедри комп'ютерних наук та інженерії програмного забезпечення Університету митної справи та фінансів, https://orcid.org/0000-0001-5945-5251
[4]д-рка. екон. наук, доцентка, в.о. завідувачки кафедри економічного моделювання, обліку та статистики Дніпровського національного університету імені Олеся Гончара, https://orcid.org/0000-0003-1264-106X
[5] к.т.н., доцент, доцент кафедри комп'ютерних наук та інженерії програмного забезпечення Університету митної справи та фінансів

Структура інформації про поточний стан системи включає в себе дані про актуальний стан різних її компонентів та параметрів. Моделі аномалій та експертні знання визначено з урахуванням можливостей для виявлення аномалій. Перспектива розвитку структури інформаційної бази експертної системи для виявлення інсайдерських кіберзагроз вбачається у подальшому її удосконаленні та інтеграції з передовими технологіями, такими як штучний інтелект та аналітика в реальному часі.

Ключові слова: інсайдер, кіберзагроза, експертна система, інформаційна база, банк.

Development of the structure of the information base of the expert system for detecting insider cyber threats in banks

Annotation. The steady growth of cyber threats in the banking sector indicates that financial institutions are becoming a particular target for attacks. The role of insiders in this context becomes dangerous, as their actions can be a critical factor in provoking and executing cyber threats on financial platforms. Therefore, developing an expert system for detecting cyber threats due to the actions of insiders in banks is an urgent task in today's conditions. This study aims to develop an information base to form an effective expert system for detecting and countering cyber threats initiated by bank employees. The article describes the main functions and components of the expert system. The features of the information base, such as user data, events and transactions, anomaly models and machine learning, etc., are characterized. The authors proposed their structure based on the definition of the main attributes. User data was determined based on their detailed analysis of employees' personality and work aspects. Data about events and transactions is formulated with critical points and possible anomalies. Access history and system configuration information are determined based on information about authorized and unauthorized access, changes in access levels, and other information. System configuration information includes data that describes the configuration of technical aspects. The structure of information about the system's current state contains data about the current state of its various components and parameters. Anomaly models and expert knowledge are defined, considering the possibilities for detecting anomalies. The perspective of the development of the structure of the information base of the expert system for the detection of insider cyber threats is seen in its further improvement and integration with advanced technologies, such as artificial intelligence and real-time analytics.

Keywords: insider, cyber threat, expert system, information base, bank.

Вступ

За останнє десятиліття спостерігається зростання проблеми кіберзагроз в банківських установах, причиною яких стають інсайдери. Наприклад, в 2020 році компанія Verizon у своєму щорічному звіті про дослідження порушень (Verizon Data Breach Investigations Report) вказала, що інсайдерські загрози становили приблизно 30% всіх кіберінцидентів. Звіт Insider Threat Report 2020 вказує, що середні втрати від інсайдерських загроз для фінансових установ становили близько 5.8 мільйонів доларів у 2020 році. Дані цифри свідчать про серйозність цієї проблеми для банків. Поява кіберзагроз, ініційованих інсайдерами у банках, може мати коріння в кількох чинниках. Перш за все, працівники банків мають доступ до критично важливої інформації, що робить їх привабливими цілями для зловмисників. Мотивацією для інсайдерів може бути фінансова вигода, використовуючи свій доступ для особистої користі або торгівлі конфіденційною інформацією. Неадекватні заходи безпеки та несприятлива корпоративна культура можуть створювати умови, в яких інсайдери відчуваються менш підданими виявленню та покаранню за свої дії. Внутрішні конфлікти та невдоволеність

теж можуть впливати на дії працівників. Споживання наркотиків або алкоголю, а також соціальний інжиніринг та недоліки в системах безпеки можуть сприяти виникненню інсайдерських загроз.

Протидія кіберзагрозам, ініційованим інсайдерами в банках, визначається кількома ключовими аспектами. По-перше, це фінансові втрати, які можуть виникнути в результаті крадіжок коштів, фінансових маніпуляцій або зловживання привілеями. Другий аспект полягає в порушенні конфіденційності та можливому витоку конфіденційної інформації, що може спричинити втрату репутації та порушення законів про конфіденційність. Третій аспект стосується загроз інформаційній безпеці, які можуть включати атаки на інформаційні системи та мережі. Порушення внутрішнього порядку та регуляторних вимог також може виникнути через дії інсайдерів, призводячи до штрафів та судових справ. У зв'язку з цим виникає необхідність в створенні експертної системи для виявлення кіберзагроз від дій інсайдерів.

Така система забезпечить раннє виявлення аномалій та автоматизовану обробку великого обсягу даних, що є критичним у банківському середовищі. Застосування технологій машинного навчання дозволить системі навчатися на основі історичних даних та адаптуватися до нових видів загроз. Експертна система також забезпечить постійний моніторинг та можливість швидкого реагування на потенційні загрози, а її використання дозволить постійно вдосконалювати систему в залежності від змін у кіберзагрозах та інсайдерських методах. Для надійної та ефективної роботи експертної системи, що протидіє діям інсайдерів у банківському середовищі, критично важливим є розроблення структури інформаційного забезпечення. Воно повинно включати можливості для виявлення аномалій, систематичного моніторингу дій користувачів, аналізу транзакцій та поведінки користувачів, попередження та реагування, тощо. Саме тому в даній статті буде запропоновано структуру інформаційної бази експертної системи виявлення кіберзагроз в результаті дій інсайдерів у банках.

Аналіз останніх досліджень і публікацій. Тема ідентифікації інсайдерських кіберзагроз у банках є актуальною та практично значущою. Але її вузька направленість та специфіка роблять її не дуже популярною у наукових колах. Це пов’язано з високим рівнем комерційної таємниці, яку банки накладають на сферу кіберзахисту. Не дивлячись на це, слід відмітити деякі наукові дослідження, які в деякій мірі стосуються окресленої проблеми. Джарра О. М. А., Аюб М. А., Джарарве Й. запропонували експертну систему на основі штучного інтелекту, яка спрямована на виявлення хмарних інсайдерських атак [1]. Кунц М., Хаммер М., Фукс Л., Неттер М., Пернул Г. провели дослідження літератури для виявлення тенденцій корпоративної ідентифікації користувачів [2]. Амірі-Заранді М., Каріміпур Х., Дара Р. А. розробили науково-методичний підхід виявлення внутрішніх загроз, який забезпечує виконання вимог конфіденційності і зрозумілості [3]. В рамках удосконалення системи виявлення вторгнень Муярт М., Медейрос Мачадо Г., Джун Ж.-Ю. розглянули умовну табличну генеративну змагальну мережу з гіперпараметрами, оптимізованими за допомогою деревоподібної оцінки Парзена [4]. Сінгх І. та Джиндал Р. запропонували рішення для аналізу поведінки користувачів на основі фактору довіри, яке базується на використанні послідовного аналізу шаблонів для систем виявлення вторгнень у бази даних [5].

Заслуговує на увагу кластер досліджень, які стосуються розробки систем протидії інсайдерським кіберзагрозам на основі методів машинного навчання. Д'Амбросіо Н., Перроне Г., Романо С.П. присвятили своє дослідження вивченню розширення байєсівських мереж не тільки для виявлення кіберзагроз, але й для ідентифікації тих, ініціатором яких є інсайдери [6]. Атту Х., Мохі-еддін М., Геззаз А., Бенкіран С., Азрур М., Алабдултіф А., Альмусаллам Н. запропонували підхід для знаходження внутрішніх вразливостей, який базується на застосуванні нейронної мережі радіальної базисної

функції та випадкового лісу [7]. Го Г.-М., Бу С.-Ж., Чо С.-Б. побудували глибоку метричну нейронну мережу зі стратегічним алгоритмом вибірки, яка визначає міру подібності між запитами користувачів – інсайдерів та їх відповідними ролями в системі [8]. Джиндал Р. та Сінгх І. розробили метод для системи виявлення вторгнень у базу даних, побудований на основі частого послідовного аналізу шаблонів і модифікованого метаевристичного гібридного кластеризування алгоритму оптимізації Gray Wolf і Whale [9]. Брахма А. та Паніграхі С. змоделювали поведінку ролей користувачів на основі нейронної мережі з теорії адаптивного резонансу, що дозволяє виявляти внутрішні загрози організацій [10].

Не дивлячись на вагомий науковий внесок щодо вирішення проблеми виявлення кіберзагроз в різних сферах економіки, не вирішеними залишаються питання побудови експертної системи для ідентифікації інсайдерських кіберзагроз саме у банках, а також розробки її компонентів, одним з яких є інформаційне забезпечення. Виходячи з окреслення даної проблематики, було сформовано основну ціль даного дослідження.

Мета статті полягає у розробленні структури інформаційної бази експертної системи виявлення кіберзагроз в результаті дій інсайдерів у банках.

Результати

Експертна система виявлення кіберзагроз в результаті дій інсайдерів у банках - це інформаційна система, яка використовується для виявлення та аналізу можливих загроз безпеці в межах банківського середовища, зумовлених внутрішніми (інсайдерськими) діями працівників. Інсайдери - це особи, які мають авторизований доступ до внутрішньої інформації та ресурсів організації, і вони можуть використовувати свій доступ для шкідливих або несанкціонованих дій. Експертні системи в цьому контексті використовують штучний інтелект для аналізу великої кількості даних та виявлення аномалій, які можуть свідчити про потенційні загрози безпеці. Основні функції експертної системи включають:

- моніторинг активності. Система виявляє незвичайні патерни або активності в системі, які можуть бути підозрілими;
- аналіз доступу. Перевірка та аналіз авторизацій та доступів працівників до різних ресурсів банку;
- виявлення аномалій. Система використовує алгоритми машинного навчання для виявлення аномалій в поведінці працівників чи використанні ресурсів;
- інтеграція з іншими системами безпеки. Взаємодія з іншими системами безпеки (наприклад, системами виявлення вторгнень) для отримання повної карти загроз;
- генерація тривог. Система може автоматично генерувати тривоги або повідомлення для операторів безпеки при виявленні потенційних загроз;
- ідентифікація ризикових патернів. Використання експертних знань для ідентифікації та аналізу патернів, які можуть свідчити про інсайдерські загрози.

Експертні системи такого роду допомагають банкам ефективно виявляти, відстежувати та вирішувати потенційні кіберзагрози, пов'язані з діями внутрішніх користувачів, зменшуючи ризики витоку інформації та інших безпекових проблем. Вони можуть складатися з різних компонентів, які спільно працюють для ефективного виявлення та відповіді на потенційні загрози безпеці. Основні компоненти такої системи включають:

- систему моніторингу та аудиту, яка відслідковує активності та події в банківській інфраструктурі, включаючи доступ до ресурсів, транзакції, зміни в правах доступу та інші події;

- модуль виявлення аномалій, який використовує алгоритми машинного навчання та аналізу даних для виявлення незвичайних патернів, що можуть свідчити про потенційні загрози з боку інсайдерів;
- базу даних та сховище інформації, яке зберігає інформацію про користувачів, ресурси, транзакції та інші дані, що використовуються для аналізу та виявлення аномалій;
- експертні правила та база знань, які включають в себе правила та експертні знання про типові патерни поведінки користувачів та інсайдерські загрози;
- модуль ідентифікації та аутентифікації, який відповідає за перевірку та аутентифікацію користувачів, а також контроль доступу до різних ресурсів;
- систему генерації тривог, що виробляє тривоги та повідомлення для операторів безпеки або інших відповідальних осіб при виявленні потенційних загроз;
- модуль відповідей та контрзаходів, який забезпечує автоматичні або рекомендації щодо контрзаходів та відповіді на виявлені загрози;
- інтеграцію з іншими системами безпеки, такими як системи виявлення вторгнень, для отримання повної картини безпекового стану;
- інтерфейс для адміністраторів та аналітиків, який забезпечує користувачам інтерфейс для налаштування системи, аналізу результатів та вживання заходів.

Ці компоненти спільно працюють, щоб створити комплексну систему, яка дозволяє ефективно виявляти, аналізувати та реагувати на кіберзагрози, пов'язані з інсайдерською діяльністю в банках.

Інформаційне забезпечення банківської експертної системи виявлення кіберзагроз в результаті дій інсайдерів - це сукупність ресурсів, процедур та технологій, які використовуються для забезпечення конфіденційності, цілісності та доступності інформації, що обробляється системою. Це включає в себе різноманітні заходи та засоби для захисту інформації від несанкціонованого доступу, втрати, викриття чи зміни. Ключовим аспектом інформаційного забезпечення банківської експертної системи виявлення кіберзагроз в результаті дій інсайдерів є інформаційна база, яка представляє собою сукупність даних, знань, та ресурсів, які система використовує для виявлення та аналізу потенційних кіберзагроз, пов'язаних з інсайдерською діяльністю в банку. Ця інформаційна база служить основою для прийняття рішень та виявлення аномалій у поведінці користувачів та системи. Ключовими складовими інформаційної бази є:

- дані про користувачів, які включають в себе інформацію про ідентифікацію та атрибути користувачів, їхні облікові записи, ролі, рівень доступу та історію взаємодії з системою;
- дані про події та транзакції, які включають інформацію про всі події, транзакції та інші активності, які відбуваються в банківській системі, з врахуванням даних про час, місце та особливості кожної події;
- історія доступу, яка надає деталі про те, які користувачі мали доступ до певних ресурсів, часи та обсяги цього доступу;
- інформація про конфігурацію системи, що представляє собою дані про налаштування системи, включаючи параметри безпеки, версії програмного забезпечення та конфігураційні параметри;
- експертні знання та правила, тобто знання, яке вбудоване в систему, включаючи експертні правила та алгоритми, розроблені для виявлення аномалій та потенційних загроз;
- моделі аномалій та машинного навчання, що представляють собою моделі, побудовані на основі машинного навчання, які використовуються для виявлення незвичайних патернів та аномалій в поведінці користувачів чи системи;

– інформація про поточний стан системи, яка включає дані про стан різних компонентів системи, враховуючи поточні тривоги, відомості про підключені пристрої та інші параметри безпеки.

Інформаційна база допомагає експертній системі аналізувати, виявляти аномалії та реагувати на можливі кіберзагрози в реальному часі. Використання різноманітних даних та знань дозволяє системі ефективно оцінювати ризики та приймати інформовані рішення щодо безпеки.

Структура даних про користувачів в банківській експертній системі виявлення кіберзагроз може включати різноманітні елементи, які дозволяють ідентифікувати, атрибутізувати та відстежувати активності користувачів. Тут є деякі загальні елементи, які можуть бути частиною такої структури:

1. «Ідентифікатор користувача» – унікальний код або номер, який ідентифікує конкретного користувача в системі. Це може бути логін, ID або інша унікальна мітка;
2. «Ім'я та прізвище» – особисті дані про користувача, які можуть включати його ім'я та прізвище для легшої ідентифікації;
3. «Облікові дані» – інформація, пов'язана з обліковим записом користувача, така як пароль, методи аутентифікації та інші параметри безпеки;
4. «Роль користувача» вказує на те, яку роль в системі виконує користувач. Наприклад, чи є він адміністратором, оператором чи звичайним користувачем;
5. «Рівень доступу» визначає, до яких ресурсів, функцій чи даних має доступ користувач. Це може бути виражено числовим рівнем чи категорією;
6. «Історія входів» – інформація про те, коли та де користувач увійшов в систему, включаючи дати та місця входу;
7. «Доступ до ресурсів» – інформація про те, до яких конкретних ресурсів або об'єктів в системі має доступ користувач. Це може бути деталізовано для кожного окремого ресурсу;
8. «Статус облікового запису» вказує на стан облікового запису, наприклад, чи він активний, заблокований або призупинений;
9. «Дані про діяльність» – інформація про активності користувача в системі, така як взаємодія з додатками, внесення змін або інші дії.

Така структура даних про користувачів дозволяє системі експертного виявлення кіберзагроз ефективно аналізувати та виявляти незвичайні патерни або аномалії, що можуть вказувати на потенційні загрози безпеці. Збереження і моніторинг цих даних допомагає створити повну картину активності користувачів у системі.

Структура даних про події та транзакції в банківській експертній системі виявлення кіберзагроз повинна містити інформацію про різноманітні дії та події, що відбуваються в системі. Ці дані важливі для виявлення аномалій та потенційних загроз безпеці. Основні елементи структури можуть включати:

1. «Ідентифікатор події/транзакції» – унікальний код або номер, який ідентифікує конкретну подію чи транзакцію в системі;
2. «Дата та час» – інформацію про точний момент часу, коли відбулася подія чи транзакція;
3. «Користувачі» – інформація про користувачів, які брали участь у події чи здійснили транзакцію, включаючи їхні ідентифікатори;
4. «Тип події/транзакції» – категорія або класифікація, яка вказує на характер події чи транзакції (наприклад, вхід в систему, зміна даних, фінансова транзакція тощо);
5. «Опис події/транзакції» – деталізований опис того, що саме відбулося під час події чи транзакції;

6. «Ресурси» – інформація про ресурси, до яких було звернено під час події чи транзакції (наприклад, файли, бази даних, мережеві ресурси);
7. «Результат» – інформація про результат чи стан системи після виконання події чи транзакції;
8. «Місце події» – дані про локацію, де відбулася подія чи здійснилася транзакція (наприклад, IP-адреса, фізичне розташування);
9. «Параметри транзакції» – у випадку, якщо це транзакція, то сюди входять інші параметри, що стосуються конкретної операції (наприклад, сума переказу, тип операції);
10. «Інформація про безпеку» – записи щодо заходів безпеки, взятих під час події чи транзакції (наприклад, вірусні сканування, перевірка аутентифікації);
11. «Контекст історії» – зв'язок події чи транзакції з попередніми подіями та контекстом історії.

Ця структура даних допомагає експертній системі аналізувати та відстежувати події, розглядати їх у відповідному контексті та виявляти аномалії, які можуть бути індикаторами можливих загроз безпеці в банківському середовищі.

Історія доступу в контексті банківської експертної системи виявлення кіберзагроз – це відображення того, які користувачі мали доступ до різних ресурсів системи, коли цей доступ відбувався, та яким чином він був здійснений. Історія доступу включає в себе інформацію про авторизований і неавторизований доступ, зміни рівнів доступу та інші відомості, які можуть бути важливими для виявлення незвичайних патернів та потенційних кіберзагроз. Структура історії доступу може містити наступні елементи:

1. «Ідентифікатор доступу» – унікальний код або номер, що ідентифікує конкретний випадок доступу;
2. «Ідентифікатор користувача» – унікальний ідентифікатор користувача, який отримав доступ;
3. «Дата та час доступу» – інформація про точний момент часу, коли відбувався доступ;
4. «Ресурс» – інформація про ресурс, до якого було звернено (наприклад, файл, база даних, додаток);
5. «Тип доступу» вказує, чи був доступ авторизований чи неавторизований. Також може вказувати на тип доступу (наприклад, читання, запис, виконання);
6. «Результат» – інформація про результат випадку доступу, наприклад, чи був успішним, чи спричинив помилку;
7. «Місце доступу» – дані про локацію, з якої був здійснений доступ (наприклад, IP-адреса, фізичне розташування);
8. «Деталі доступу» – додаткові відомості про сам доступ, такі як тип пристрою, використовувані агенти, параметри запиту тощо;
9. «Інша метадані» – додаткова інформація, яка може бути корисною для аналізу, така як ідентифікатор сесії, номер транзакції, тощо.

Історія доступу надає адміністраторам та системам безпеки повний огляд того, яким чином користувачі взаємодіють з системою, і дозволяє вчасно виявляти аномальні або підозрілі дії, що може свідчити про потенційні загрози безпеці.

Інформація про конфігурацію системи включає в себе дані, які описують конфігурацію технічних аспектів системи, такі як параметри, налаштування, версії програмного забезпечення та інші важливі параметри, які визначають спосіб функціонування системи. Ця інформація важлива для забезпечення стабільності та безпеки системи. Структура об'єкту бази даних "Інформація про конфігурацію системи" може включати наступні елементи:

1. «Ідентифікатор конфігурації» – унікальний код або номер, що ідентифікує конкретну конфігурацію системи;
2. «Дата та час збереження конфігурації» – інформація про той час, коли була збережена інформація про конфігурацію;
3. «Інформація про операційну систему» – версія операційної системи, тип архітектури, патчі та оновлення;
4. «Інформація про апаратне забезпечення» – деталі про апаратні компоненти, такі як процесор, обсяг оперативної пам'яті, жорсткий диск та інші пристрої;
5. «Версії програмного забезпечення» – інформація про версії встановленого програмного забезпечення, включаючи операційну систему, антивірусні програми, файєрволи та інші додатки;
6. «Налаштування безпеки» – параметри та налаштування безпеки, такі як правила файєрволу, антивірусні налаштування та інші заходи безпеки;
7. «Параметри мережі» – інформація про мережеві налаштування, включаючи IP-адресу, маску підмережі, шлюз, DNS-сервери та інші параметри мережі;
8. «Ліцензійна інформація» – інформація про ліцензійні ключі та терміни дії ліцензій для встановлених програм;
9. «Інші конфігураційні параметри» – додаткові параметри та конфігураційні налаштування, які можуть бути важливими для конкретної системи.

Ця інформація про конфігурацію системи допомагає забезпечити контроль над станом та функціональністю системи, а також сприяє вчасному виявленню змін, які можуть вказувати на потенційні проблеми або загрози.

Інформація про поточний стан системи включає в себе дані про актуальний стан різних компонентів та параметрів, що характеризують працездатність системи в реальному часі. Ця інформація важлива для моніторингу та виявлення аномалій або проблем в роботі системи. Структура об'єкта бази даних (БД) "Інформація про поточний стан системи" може включати такі елементи:

1. «Дата та час останнього оновлення» – інформація про час, коли були отримані та оновлені дані про поточний стан системи;
2. «Статус системи» – індикатор, який вказує на загальний стан системи, такий як "працює нормально", "проблеми", "відновлення", тощо;
3. «Використання ресурсів» – дані про використання ресурсів, такі як CPU, RAM, дисковий простір та інші аспекти апаратної потужності;
4. «Стан мережі» – інформація про стан мережі, включаючи доступність, пропускну здатність, пінги та інші параметри;
5. «Активні процеси» – перелік активних процесів та їхні властивості, такі як ідентифікатори, використання ресурсів та інші;
6. «Стан служб та додатків» – інформація про стан важливих служб та додатків, їхні версії, час їхньої роботи та інші параметри;
7. «Інформація про події» – записи про останні події та активності в системі, такі як запуск процесів, помилки та інші важливі події;
8. «Стан безпеки» – інформація про поточний стан заходів безпеки, включаючи антивірусний захист, стан брандмауера та інші аспекти;
9. «Підключені пристрої» – інформація про пристрої, які підключені до системи, такі як USB-пристрої, мережеві пристрої та інші;
10. «Інші параметри» – додаткові параметри та станові показники, які можуть бути важливими для конкретної системи.

Ця структура даних дозволяє ефективно відстежувати та аналізувати поточний стан системи, що є важливим для забезпечення її стабільності та безпеки.

Найважливішим компонентом інформаційної бази банківської експертної системи виявлення кіберзагроз в результаті дій інсайдерів є моделі аномалій. Вони використовуються для виявлення аномалій або незвичайних патернів в даних, наприклад, для виявлення підозрілих транзакцій чи несанкціонованого доступу. Структура об'єкту "Моделі аномалій виявлення кіберзагроз в результаті дій інсайдерів" може містити наступні ключові елементи:

- таблиця "Моделі аномалій" містить інформацію про різні моделі аномалій, які використовуються в системі для аналізу та виявлення невідповідностей та аномальних зразків в користувацькому поведінці чи системних діях. Така таблиця дозволяє ефективно управляти різними моделями аномалій, їхніми характеристиками та використанням у системі виявлення кіберзагроз;
- таблиця "Виявлені аномалії" містить інформацію про аномальні події, які були виявлені системою на основі моделей аномалій. Ця таблиця дозволяє системі зберігати та відстежувати інформацію про кожну виявлену аномалію, а також асоціювати її з конкретним користувачем, дією та моделлю аномалій, яка використовувалася для виявлення. Це важливо для подальшого аналізу, вдосконалення моделей та прийняття відповідних заходів безпеки;
- таблиця "Параметри моделі" дозволяє зберігати налаштування кожної моделі, що може включати в себе різні параметри, які визначають її поведінку. Ця таблиця важлива для динамічного управління параметрами моделей, що може бути корисним під час настройки та оптимізації системи виявлення аномалій. Зміни в параметрах можуть бути внесені під час експлуатації системи для покращення її ефективності та адаптації до змін в оточенні.

Елемент бази даних "Експертні знання та правила" для банківської експертної системи виявлення кіберзагроз в результаті дій інсайдерів може включати в себе різноманітні компоненти для зберігання експертних знань, правил і відомостей, які використовуються для аналізу та класифікації подій. Нижче подано ключові елементи, які можуть бути включені в такий об'єкт бази даних:

- таблиця "Експертні знання" містить інформацію про експертні знання, які використовуються для аналізу подій та виявлення аномалій. Вона дозволяє системі зберігати та організовувати експертні знання, які використовуються для визначення нормального та аномального поведінки в банківській експертній системі. Інформація в цій таблиці може бути використана для визначення експертних правил та алгоритмів виявлення кіберзагроз;
- таблиця "Правила виявлення" містить інформацію про правила виявлення, які визначають, як система аналізує події та визначає їх як аномальні чи небезпечні. Вона надає можливість експертній системі визначати, які події або дії вважаються аномальними чи потенційно загрозливими, а також які заходи повинні бути прийняті при виявленні таких аномалій;
- таблиця "Історія виявлень" служить для відстеження історії виявлених аномалій та подій в системі. Вона забезпечує зберігання історії аномалій та виявлених подій, що є важливим для подальшого аналізу, статистики та вдосконалення експертних моделей системи виявлення кіберзагроз.

Висновки

Розробка структури інформаційної бази для експертної системи виявлення кіберзагроз внаслідок дій інсайдерів у банках є надзвичайно важливим завданням в контексті зростаючого обсягу кіберзагроз та потенційно серйозних наслідків для банківської сфери. Ця система повинна виявляти та відвертати загрози, забезпечуючи високий рівень безпеки та довіри. У даному дослідженні було надано інформацію про

компоненти, структури та елементи, які складають інформаційну базу експертної системи. Важливо враховувати, що інформаційна база включає в себе такі компоненти, як інформація про користувачів, події та транзакції, експертні знання та правила, а також моделі аномалій для застосування машинного навчання.

Структура даних про користувачів передбачає детальний аналіз особистих та робочих аспектів працівників банку, враховуючи їхні повноваження та історію доступу. Дані про події та транзакції включають історію фінансових операцій, доступ до конфіденційної інформації та інші аспекти, що можуть слугувати підставою для виявлення аномалій. Інформаційна база також враховує історію доступу та поточний стан системи, надаючи можливість для ефективного моніторингу та виявлення незвичайної активності. Інформаційна база також включає дані про конфігурацію системи, що дозволяє ефективно взаємодіяти з різними компонентами та забезпечувати стабільність системи.

Одним із ключових аспектів є використання моделей аномалій та машинного навчання для виявлення та аналізу незвичайної активності. Ці моделі вбудовуються в інформаційну базу, навчаючись на основі історичних даних та виявляючи нові патерни та загрози. Таблиці, такі як "Моделі аномалій", "Виявлені аномалії", "Параметри моделі", "Експертні знання", "Правила виявлення" та "Історія виявлень", створюють структуровану основу для зберігання та аналізу даних, що сприяє ефективному функціонуванню експертної системи.

Важливість протидії кіберзагрозам ініційованим інсайдерами у банках виявляється через можливі наслідки, такі як фінансові втрати, порушення конфіденційності даних, репутаційні ризики та загрози економічній та національній безпеці. Розробка ефективної експертної системи та відповідної інформаційної бази для неї є критичною для забезпечення стійкості та надійності банківської сфери перед різноманітними кіберзагрозами.

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. URL: https://doi.org/10.1504/ijics.2017.082840
2. Analyzing Recent Trends in Enterprise Identity Management / M. Kunz et al. 2014 25th International Workshop on Database and Expert Systems Applications (DEXA), Munich, Germany, 1–5 September 2014. 2014. URL: https://doi.org/10.1109/dexa.2014.62
3. Amiri-Zarandi M., Karimipour H., Dara R. A. A federated and explainable approach for insider threat detection in IoT. Internet of Things. 2023. P. 100965. URL: https://doi.org/10.1016/j.iot.2023.100965
4. Mouyart M., Medeiros Machado G., Jun J.-Y. A Multi-Agent Intrusion Detection System Optimized by a Deep Reinforcement Learning Approach with a Dataset Enlarged Using a Generative Model to Reduce the Bias Effect. Journal of Sensor and Actuator Networks. 2023. Vol. 12, no. 5. P. 68. URL: https://doi.org/10.3390/jsan12050068
5. Singh I., Jindal R. Trust factor-based analysis of user behavior using sequential pattern mining for detecting intrusive transactions in databases. The Journal of Supercomputing. 2023. URL: https://doi.org/10.1007/s11227-023-05090-w.
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. URL: https://doi.org/10.1016/j.cose.2023.103410
7. Towards an Intelligent Intrusion Detection System to Detect Malicious Activities in Cloud Computing / H. Attou et al. Applied Sciences. 2023. Vol. 13, no. 17. P. 9588. URL: https://doi.org/10.3390/app13179588

8. Go G.-M., Bu S.-J., Cho S.-B. Insider attack detection in database with deep metric neural network with Monte Carlo sampling. Logic Journal of the IGPL. 2022. URL: https://doi.org/10.1093/jigpal/jzac007
9. Jindal R., Singh I. Detecting malicious transactions in database using hybrid metaheuristic clustering and frequent sequential pattern mining. Cluster Computing. 2022. URL: https://doi.org/10.1007/s10586-022-03622-2
10. Brahma A., Panigrahi S. Role-Based Profiling Using Fuzzy Adaptive Resonance Theory for Securing Database Systems. International Journal of Applied Metaheuristic Computing. 2021. Vol. 12, no. 2. P. 36–48. URL: https://doi.org/10.4018/ijamc.2021040103.