Сучасний стан наукових досліджень та технологій в промисловості. 2024. №1 (27)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

УДК 004.942
DOI: https://doi.org/10.30837/ITSSI.2024.27.067

І. Замрій, І. Шахматов

ПІДВИЩЕННЯ БЕЗПЕКИ ВЕБЗАСТОСУНКІВ З ДОПОМОГОЮ ІННОВАЦІЙНИХ ПАТЕРНІВ ІНТЕГРАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ

Зважаючи на сучасні виклики в забезпеченні безпеки цифрових операцій, особливо у сферах електронної комерції та фінансових транзакцій, **предметом вивчення** є розроблення спеціалізованої програмної бібліотеки, спрямованої на підвищення безпеки вебзастосунків. **Мета дослідження** полягає в розробленні програмної бібліотеки, що застосовує методи штучного інтелекту та машинного навчання для аналізу й підвищення рівня безпеки фінансових транзакцій. Використання цих передових технологій сприяє автоматизації виявлення потенційно шахрайських або ризикованих транзакцій, забезпечуючи цим більш високий рівень захисту користувачів. У статті вирішуються такі **завдання**: аналіз сучасних методів оброблення фінансових транзакцій та ідентифікації можливих загроз безпеці; розроблення *UML*-схеми класів бібліотеки з оброблення та аналізу фінансових транзакцій; тестування та валідація створеної моделі штучного інтелекту для оцінювання безпеки фінансових транзакцій на реальних фінансових даних. Визначено та застосовано **методи** машинного навчання за допомогою бібліотеки *scikit-learn* в *Python*, алгоритми якої здатні аналізувати великі обсяги інформації та виявляти потенційні ризики з високою точністю, що забезпечує ефективну інтеграцію технологій штучного інтелекту. У роботі досягнуто такі **результати**: визначено критерії оцінювання ризикованості фінансових транзакцій для ідентифікації потенційних ризиків; описано алгоритм роботи програми, що передбачає процедури визначення та класифікації ризиків транзакцій; запропоновано псевдокод, який ілюструє структуру класів і методів моделі, відкриваючи можливості для її адаптації та масштабування; розроблено методи генерації тестових даних, що відтворюють реалістичні сценарії фінансових транзакцій; проаналізовано результати для оцінювання ефективності розробленої моделі. **Висновки.** Результати дослідження та тестування дають змогу оцінити реакцію моделі на різноманітні дані та її ефективність у реальних умовах, оскільки в роботі наведено приклади оброблення різних типів транзакцій. Крім того, у дослідженні подано не лише розроблення та валідацію запропонованої моделі, але й перспективи її використання в більших масштабах, інтеграції з наявними вебзастосунками.

Ключові слова: штучний інтелект; безпека вебзастосунків; фінансові транзакції; машинне навчання; аналіз даних; виявлення шахрайства; *scikit-learn*.

Вступ

Завдяки стрімкому розвитку цифрових технологій, що проникають у кожен вимір нашого існування, забезпечення безпеки вебзастосунків та цифрових транзакцій стає першочерговим завданням. Цей процес супроводжується не тільки технологічними інноваціями, але й зростанням викликів, пов'язаних із захистом конфіденційної інформації та фінансових інтересів користувачів у цифровому просторі. Збільшення обсягів онлайн-операцій та їх різноманітності супроводжується зростанням випадків шахрайства та спроб проникнення в конфіденційні фінансові дані користувачів. Це вимагає від розробників створення ефективних інструментів для оцінювання та мінімізації ризиків у цифровому середовищі.

Сучасний стан цифрової економіки потребує не лише впровадження новітніх технологічних рішень, але й розроблення комплексних підходів до безпеки. Інтеграція методів штучного інтелекту (*AI*) та машинного навчання відкриває нові перспективи в боротьбі з кіберзагрозами, особливо в контексті їх розпізнавання та запобігання шахрайським діям в онлайн-транзакціях. Це дослідження спрямоване на створення інноваційного рішення, здатного ефективно виявляти порушення та запобігати потенційним загрозам у фінансовій сфері цифрових послуг.

Метою статті є розроблення ефективного інструменту, а саме програмної бібліотеки, для забезпечення безпеки фінансових даних, а також демонстрації значення технологій штучного інтелекту в розвитку цифрової економіки, наголошуючи на їх практичній значущості та потенціалі для вдосконалення повсякденного життя.

Проєкт оснований на використанні бібліотеки *scikit-learn* для *Python*, що є визнаною та широко застосовуваною в галузі машинного навчання. Це забезпечує інтеграцію перевірених і надійних

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2024. No. 1 (27)

алгоритмів *AI* в розроблювану бібліотеку, що гарантує її ефективність та надійність.

Робота спрямована на аналіз викликів у сфері безпеки фінансових транзакцій та демонстрацію, як упровадження інноваційних технологій машинного навчання може сприяти розв'язанню окреслених проблем. Розглядаються не лише технічні аспекти розроблення та імплементації моделі, але і її потенційне застосування в різних секторах, таких як електронна комерція, банківські послуги тощо, де безпека транзакцій є вирішальною.

Дослідження має на меті не лише запропонувати ефективний інструмент для захисту фінансових даних, а й зробити внесок у розвиток технологій штучного інтелекту, з огляду на їх практичну значущість і вплив на повсякденне життя.

Аналіз проблеми й наявних методів

Кіберфізична безпека в мережах Інтернету речей (*IoT*) стрімко розвивається, особливо з упровадженням технологій, таких як блокчейн та штучний інтелект (*AI*). Наголошується на важливості взаємної автентифікації між пристроями *IoT*, яка є основним елементом у підвищенні безпеки. Інтеграція блокчейну сприяє надійності валідації сесійних ключів, що є важливим для забезпечення цілісності інформації та зниження ризику несанкційного доступу. Також використання алгоритмів *AI* сприяє адаптивності систем до різноманітних атак, підвищуючи рівень безпеки *IoT*-екосистем. У сфері *IoT* важливою є не тільки імплементація наявних рішень безпеки, але й розроблення нових методів, особливо зважаючи на широкий спектр застосування – від сільського господарства до охорони здоров'я та технологій розумних будинків [1]. Це вимагає комплексного підходу, що поєднує традиційні механізми безпеки з інноваційними рішеннями, зокрема патернами інтеграції *AI*. Такі розробки відіграють важливу роль у виявленні та запобіганні потенційних загроз, а також у просуванні напрямів майбутніх досліджень у цій сфері.

Інтеграція *AI*, блокчейну та програмно-визначеної мережі (*SDN*) відіграє ключову роль у підвищенні безпеки кіберфізичних систем [2], особливо в контексті *IoT*. Це особливо актуально з огляду на сучасні виклики, такі як сумісність, енергоефективність та надійність безпеки в мережах *IoT*. У такому разі увага приділяється механізму автентифікації на основі довіри, що є ефективним для пристроїв *IoT* з обмеженими ресурсами. Такі інновації в безпеці *IoT* надихають на подальші дослідження у сфері впровадження *AI* для підвищення безпеки вебзастосунків [3].

Трансформаційний вплив *AI* на сферу кібербезпеки є надзвичайно значущим, особливо в контексті захисних стратегій. Інтеграція *AI* в заходи кібербезпеки не лише змінює підходи нападників, але й радикально підвищує ефективність оборонних механізмів. Цей процес передбачає аналіз і адаптацію до нових загроз, що постійно еволюціонують у кіберпросторі. Важливість *AI* полягає в його двозначному характері: з одного боку, він підвищує ефективність і масштабованість захисних механізмів, з іншого – відкриває нові можливості для кібератак. Особливо важливим є розуміння ролі *AI* в прогнозуванні загроз та протидії кібератакам, що зазнають постійних змін та ускладнень. Цей аспект є критичним у контексті підвищення безпеки вебзастосунків, де інноваційні патерни інтеграції *AI* можуть значно підсилити захисні можливості. Використання *AI* дає змогу не лише виявляти та нейтралізувати потенційні загрози, але й адаптуватися до постійно змінних тактик і методів нападників [4].

Вивчення впливу методів *AI* на кібербезпеку відкриває широкі перспективи для зміцнення захисту в сучасному кіберпросторі. Різноманітність методик *AI*, від розподілених до компактних, забезпечує гнучкість у виявленні, детектуванні та протидії кібератакам. Ці методи варіюються від складних алгоритмів машинного навчання до простіших, але ефективних рішень для конкретних викликів безпеки. Класифікація цих технік дає змогу глибше зрозуміти потенціал та обмеження *AI* у сфері кібербезпеки, а також визначити найбільш ефективні підходи для різних сценаріїв використання. Інноваційні патерни інтеграції *AI* у вебзастосунки можуть істотно підсилити здатність системи адаптуватися та реагувати на нові види кіберзагроз. Це передбачає розроблення та впровадження алгоритмів *AI*, здатних аналізувати та вчасно відповідати на підозрілі дії, що значно підвищує рівень безпеки вебзастосунків. Така інтеграція [5] є кроком вперед у захисті від кібератак, що постійно еволюціонують, та пропонує новітні рішення для підвищення рівня безпеки в цифровому світі.

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2024. №1 (27) ISSN 2524-2296 (online)

Виявлення кібератак у середовищі *IoT* вимагає застосування складних і ефективних методів, серед яких *AI* відіграє ключову роль. Систематичний огляд літератури виявляє, що техніки глибинного навчання та машинного навчання, такі як методи класифікації та аналізу інформації, зокрема машини опорних векторів (алгоритми, що аналізують дані для класифікації та регресійного аналізу) та випадкові ліси (ансамблеві методи для класифікації, регресії та інших завдань, що працюють шляхом створення множини рішення дерев під час навчання), є особливо ефективними у виявленні та відповіді на кіберзагрози в *IoT*. Ці методи демонструють високу точність та ефективне використання ресурсів, що є критично важливим для розроблення інтелектуальних систем виявлення вторгнень. Подібні висновки є особливо релевантними для розроблення інноваційних патернів інтеграції *AI* у вебзастосунки, де безпека є ключовим пріоритетом. Інтеграція цих методів у вебзастосунки дає змогу створити більш стійкі та адаптивні системи, здатні виявляти загрози та протистояти різноманітним формам кібератак. Особлива увага до розроблення розумних архітектурних рамок для систем інтелектуального виявлення вторгнень [6] наголошує на потребі постійно вдосконалювати методи виявлення загроз, зокрема ті, що стосуються вебзастосунків.

Глибокий аналіз методів *AI*, що використовуються для підвищення безпеки в пристроях *IoT*, відіграє ключову роль у розумінні зростання вразливості цих систем. З огляду на високу складність і збільшення кількості пристроїв *IoT* потреба в удосконаленні безпеки є нагальною. Нові методи та рамки, які використовують інтеграцію методів машинного навчання та глибинного навчання, мають значні можливості для захисту цих пристроїв. Розгляд різноманітних вразливостей *IoT* та обговорення потенційних рішень допомагає визначити ефективні стратегії безпеки. Ці методи та підходи є вкрай важливими для підвищення безпеки вебзастосунків. Використання інноваційних патернів інтеграції *AI* у вебзастосунках може значно підсилити здатність системи виявляти та протидіяти кіберзагрозам. Розроблення таких систем вимагає глибокого розуміння потенційних вразливостей і застосування передових технологій *AI* для створення більш безпечного цифрового середовища. Висвітлення цих аспектів у роботі [7] викликає необхідність інтеграції передових технологій *AI* у сфері веббезпеки, що стає все більш актуальним у сучасному цифровому світі.

Інтеграція *AI, IoT* та кіберфізичних систем (*CPS*) у моніторингу здоров'я відкриває нові перспективи в підвищенні безпеки та ефективності медичних систем. Використання *AI*-підсилених *IoT-CPS* для виявлення різноманітних захворювань з допомогою деяких сенсорів, що аналізують інформацію, застосовуючи алгоритми *AI*, є революційним підходом у сфері охорони здоров'я. Це дає змогу не тільки вчасно виявляти та лікувати хвороби, але й управляти великими обсягами медичних даних, підвищуючи точність та швидкість діагностики. Такий підхід має безпосереднє значення й для підвищення безпеки вебзастосунків. Інтеграція інноваційних патернів *AI* у вебзастосунки може суттєво підсилити здатність систем виявляти небезпеку та протидіяти кіберзагрозам. Це передбачає розроблення та впровадження складних алгоритмів *AI*, здатних аналізувати та вчасно реагувати на підозрілі дії, що підвищує загальний рівень безпеки вебзастосунків [8].

Спільне використання технологій *AI* та блокчейну в системах розумного дому на базі *IoT* відкриває нові можливості для підвищення їх безпеки та ефективності. Такі дослідження охоплюють різні виклики, з якими стикаються системи *IoT* розумного дому, зокрема вразливості до кібератак та проблеми приватності. Пропонуються інноваційні рішення, що використовують *AI* та блокчейн для захисту цих систем від зовнішніх загроз, забезпечуючи надійний та безпечний зв'язок між пристроями. Ці технології можуть бути також застосовані для підвищення безпеки вебзастосунків. Інтеграція інноваційних патернів *AI* у вебзастосунки допомагає створити більш стійкі та адаптивні системи, здатні виявляти ризики та протистояти кіберзагрозам. Використання блокчейну додатково забезпечує безпеку та прозорість у обробленні інформації, підвищуючи довіру та надійність вебзастосунків. Значення інтеграції сучасних технологій у сфері кібербезпеки є актуальним для вебзастосунків, особливо в контексті розумних систем дому [9].

Інтеграція *AI* та *IoT* у сфері охорони здоров'я, відома як *AIoT*, відкриває нові перспективи для покращення медичних послуг. Особливо наголошується на потенціалі *AIoT* у дистанційному моніторингу здоров'я та на управлінні хронічними захворюваннями, наприклад, діабетом і хворобою Паркінсона. Проте, разом з перевагами, виникають і значні виклики, зокрема щодо питань безпеки та

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2024. No. 1 (27)

конфіденційності медичних даних у *AIoT*-системах. Це потребує розроблення передових криптографічних рішень і стандартизації, щоб забезпечити належний захист інформації. Така інтеграція *AI* та *IoT* сприяє подальшим дослідженням щодо підвищення безпеки вебзастосунків з допомогою інноваційних патернів інтеграції *AI*. Подібні принципи можуть бути застосовані для підсилення безпеки вебзастосунків, особливо в секторах, де значний обсяг чутливої інформації вимагає надійного захисту. Застосування передових алгоритмів *AI* для аналізу, моніторингу та реагування на потенційні загрози може значно збільшити стійкість вебзастосунків до кібератак [10].

Детальний огляд впровадження "Зрозумілого штучного інтелекту" (XAI) у кібербезпеці відкриває нові перспективи для розуміння та використання *AI*. Особлива увага приділяється викликам, пов'язаним із проблематикою "чорної скриньки" *AI* у кібербезпеці, де рішення алгоритмів часто не прозорі. XAI пропонує способи, які роблять рішення *AI* більш зрозумілими та прозорими, що є критично важливим для побудови довіри та дотримання регулювань у цій галузі. Включення XAI у вебзастосунки дає змогу не тільки покращити захист від кіберзагроз, але й робить процеси прийняття рішень більш прозорими та зрозумілими для користувачів. Це може сприяти кращому розумінню та взаємодії користувачів із захисними механізмами, а також допомагає в розвитку більш стійких та довірених систем [11].

Інтеграція та майбутні тренди *AI* в комп'ютерних технологіях нового покоління відкривають широкі перспективи, особливо в контексті автономного обчислення. Автономія та продуктивність систем на великому масштабі можуть бути значно покращені за допомогою *AI*, але також виникає потреба в "Зрозумілому *AI*" (XAI) для забезпечення прозорості та зрозумілості цих процесів. Використання *AI* для автоматизації та оптимізації процесів у вебзастосунках може суттєво збільшити їх ефективність і безпеку. Зокрема застосування XAI дозволяє краще розуміти та контролювати, як *AI* приймає рішення в контексті веббезпеки, забезпечуючи більшу прозорість і довіру до цих систем. Результати цих досліджень [12] наголошують на важливості розвитку та інтеграції передових технологій *AI* для створення більш безпечних та ефективних вебзастосунків.

Усебічний аналіз інтеграції *AI* та блокчейну в бізнесі відкриває нові горизонти для розвитку цих технологій у різних секторах. Використовуючи бібліометрично-контентний підхід, дослідники детально вивчають злиття *AI* та блокчейну та їх застосування в таких галузях, як охорона здоров'я, безпечні транзакції, фінанси та ланцюги постачань. Виявлені тренди й кластери в поточних дослідженнях зосереджують увагу на те, як ці технології можуть доповнювати одна одну, покращуючи ефективність, прозорість та безпеку в бізнес-операціях. Інтеграція *AI* та блокчейну може відіграти значну роль у створенні більш безпечних, надійних і прозорих вебзастосунків. Особливо це стосується секторів, де важливий високий рівень інформації та фінансової безпеки. Використання *AI* для аналізу та передбачення потенційних загроз, а також упровадження блокчейну для забезпечення незмінності та прозорості даних дає змогу значно підвищити ефективність і безпеку вебсистем [13].

Застосування штучного інтелекту в системах планування ресурсів підприємства (*ERP*), особливо на хмарних платформах, відкриває нові можливості для підвищення ефективності та безпеки цих систем. Перспективи IT-фахівців щодо інтеграції *AI* та машинного навчання в ці системи є ключовими для розуміння потенціалу цих технологій. Різні аспекти, такі як виклики інтеграції *AI* в хмарні *ERP*-сервіси, необхідні ресурси для їх імплементації та кращі практики розроблення *AI*-моделей для таких систем, є важливими для успішного впровадження та використання. Застосування *AI* у вебзастосунках, зокрема на хмарних платформах, покращує їх ефективність, автоматизацію та безпеку. Інтеграція *AI* допомагає ефективно виявляти та протидіяти кіберзагрозам, оптимізувати процеси й забезпечити більш високий рівень захисту інформації [14].

Еволюція технологій у галузі охорони здоров'я, зокрема в контексті систематичного моніторингу здоров'я (*SHM*) за допомогою глибинного навчання та *AI*, пропонує нові можливості для поліпшення медичних послуг. Важливим аспектом є використання передових технологій промисловості 5.0 та *5G*, які дають змогу розробляти вартісно-ефективні сенсори для реального моніторингу здоров'я. Роль хмарних обчислень у цьому контексті також є значною, оскільки вони допомагають підвищити ефективність медичних послуг. Застосування зазначених технологій у вебзастосунках, зокрема у сфері охорони здоров'я, може значно покращити безпеку та адаптивність таких систем [15].

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2024. №1 (27) ISSN 2524-2296 (online)

Огляд етичних аспектів та інцидентів, пов'язаних з *AI*, важливий для розуміння як ключових сфер застосування *AI*, так і потенційних етичних проблем. З використанням інформації з бази даних інцидентів *AI* розглядаються різні сектори, де *AI* впливає на етичні питання, а саме на необхідність етичного проєктування та впровадження в системах *AI*. Особлива увага приділяється важливості регулювання *AI* та розробленню етичних настанов. Метою цього огляду є підвищення обізнаності про етичні виклики, пов'язані з *AI*, та необхідність інтеграції етичних міркувань у процес розроблення *AI*. Це має безпосередній зв'язок з підвищенням безпеки вебзастосунків завдяки інноваційним підходам до інтеграції *AI*. Знання про етичні проблеми та виклики в упровадженні *AI* сприяють створенню більш безпечних вебзастосунків, що відповідають етичним стандартам [16].

Інтеграція *AI* у хмарні технології відкриває нові можливості для підвищення безпеки вебзастосунків, зокрема у фінтех-секторі. *AI* ефективно використовується для виявлення аномалій, запобігання шахрайству, розвідки загроз та оцінювання ризиків, що значно підсилює захист інформації та фінансових операцій у хмарних фінтех-сервісах. Інноваційні патерни інтеграції *AI* дають змогу не тільки виявляти та нейтралізувати потенційні загрози, а й оптимізувати процеси, підвищуючи загальну ефективність систем. Розгляд реальних кейс-стаді, таких як *PayPal* та *Square*, демонструє, як застосування *AI* може значно покращити безпеку фінансових транзакцій. Проте існують певні виклики, пов'язані з упровадженням *AI*, зокрема йдеться про ризики помилкових спрацьовувань та вразливість до ворожих атак. Ці виклики потребують постійного вдосконалення технологій та методів інтеграції *AI* для забезпечення найвищого рівня безпеки [17].

Інноваційні патерни інтеграції *AI* відіграють важливу роль у підвищенні безпеки вебзастосунків, створюючи нові можливості для точного та ефективного оброблення даних. Особливо це важливо у сферах, де висока точність і надійність інформації є критичними. Використання мови програмування *Python* у дослідженнях охорони здоров'я наголошує на її важливості як надійного інструменту для розроблення високоточних медичних застосунків. Особлива увага приділяється алгоритмам машинного навчання, таким як логістична регресія та класифікатор випадкового лісу, що сприяють значному підвищенню точності діагностики серцевих захворювань. Цей підхід може бути адаптований і застосований у вебзастосунках для підсилення їх безпеки та надійності, забезпечуючи ефективні механізми захисту інформації та оптимізацію процесів її оброблення [18].

AI відіграє значну роль у підвищенні безпеки та ефективності онлайн-іспитів, пропонуючи інноваційні рішення для різних викликів, що виникають у сфері освіти. Особливо важливим є впровадження *AI* для дистанційної ідентифікації, що передбачає технології розпізнавання голосу та обличчя. Це значно покращує надійність і справедливість іспитів, зокрема під час вступу з-за кордону. *AI* також ефективно застосовується в системах оцінювання та в механізмах зворотного зв'язку, що робить освітній процес більш якісним. Однак ці технології несуть і певні виклики, наприклад, ризики шахрайства та підроблення особи в умовах онлайн-іспитів. Інноваційні патерни інтеграції *AI*, які розглядаються в дослідженні, пропонують ефективні рішення для протидії цим проблемам. Зокрема вони спрямовані на трансформацію процесу іспитів, підвищуючи їх безпеку та надійність, а також покращуючи загальний освітній досвід. Отже, *AI* відіграє вирішальну роль у модернізації освітнього процесу, забезпечуючи більшу безпеку та ефективність різного типу іспитів [19].

Інтеграція *AI* у різні технологічні сфери, наприклад Інтернет речей (*IoT*) та технології *5G*, відкриває нові горизонти для розвитку та покращення систем, як-от Смартгрід. Така інтеграція є ключовою для переходу від традиційних електромереж до більш передових, програмно-керованих мереж. Основна увага в цьому разі приділяється підвищенню ефективності та надійності з допомогою застосування інтелектуальних технологій. Упровадження *AI* для моніторингу та інтелектуального прийняття рішень може значно вдосконалити безпеку, швидкість оброблення інформації та надійність вебзастосунків. Еволюція та інтеграція *AI, IoT* та *5G*, зокрема в Смартгрід, показує величезний потенціал цих технологій і вказує на широкий спектр можливостей їх використання [20].

Застосування *AI* разом із технологією Інтернету речей (*IoT*) революціонізує сферу бібліотекарства, особливо в трьох ключових аспектах: розумне обслуговування, розумна стійкість та розумна безпека. Це перетворення традиційних бібліотек на розумні сприятиме підвищенню оперативної ефективності, управління ресурсами та безпеки.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2024. No. 1 (27)

Так, використання *AI* для моніторингу та аналізу інформації може виявляти потенційні загрози безпеці, покращуючи захист від несанкційного доступу або інших кібератак [21]. Цей перехід від традиційних методів до більш інноваційних, підкріплених *AI* та *IoT*, відкриває нові можливості для розвитку не тільки бібліотечних систем, а й вебзастосунків.

Опис проведених досліджень

У відповідь на сучасні виклики в забезпеченні безпеки цифрових операцій, особливо у сферах електронної комерції та фінансових транзакцій, це дослідження ініціює розроблення спеціалізованої бібліотеки.

Її мета – підвищення безпеки вебзастосунків із допомогою інтеграції алгоритмів штучного інтелекту. Запропонована модель і методологія спрямовані на детальне вивчення та розуміння процесів навчання *AI*, зокрема в контексті аналізу та управління ризиками.

Запропонований підхід оснований на розробленні інноваційної моделі для оцінювання ризиків транзакцій у вебзастосунках. Для цього використовується бібліотека *scikit-learn*, що пропонує широкий спектр алгоритмів машинного навчання. Ці алгоритми здатні аналізувати значні обсяги інформації та виявляти потенційні ризики з високою точністю.

Методологія дослідження охоплює кілька ключових етапів: починаючи з підготовки інформації до побудови та тестування моделі, завершуючи оцінюванням її ефективності. Особлива увага приділяється адаптації моделі до специфічних вимог безпеки вебзастосунків, що є критично важливим для їх надійної експлуатації.

Запропонована модель аналізу фінансових транзакцій спрямована на визначення їх потенційної ризикованості. Модель використовує комплексний набір характеристик транзакцій, зокрема географічне положення (країну проведення), суму платежу, час транзакції та тип платіжної картки, для оцінювання рівня безпеки кожної операції.

Ключовим компонентом дослідження є розроблена модель, що використовує комплексний підхід до оцінювання ризиків транзакцій. Ця модель інтегрує та аналізує різноманітні параметри, а саме: суму платежу, географічне положення, час транзакції та тип картки – для визначення загального ризику. Кожен параметр розглядається в контексті його впливу на рівень ризику, зважаючи на встановлені порогові значення та критерії. Наприклад, транзакції з великою сумою, що здійснюються в країнах із високим рівнем фінансових шахрайств, або транзакції, що відбуваються в нічний час, можуть бути оцінені як вищі за ризик.

Модель оцінює ризик транзакції за допомогою спеціальної функції, що інтегрує різні параметри, зокрема суму платежу, географічні фактори, час транзакції і тип картки. Загальний ризик транзакції, що первісно визначається сумуванням індивідуальних компонентів ризику (1), кожен з яких має діапазон від 0 до 1, підлягає нормалізації за допомогою спеціальної функції. Функція нормалізації адаптує сукупне значення так, щоб кінцева загальна оцінка ризику також була в межах діапазону від 0 до 1, незалежно від того, чи сума компонентів перевищує 1.

Загальний ризик транзакції:

$$Ризик = R_P(P) + R_C(C) + R_T(T) + R_K(K), \quad (1)$$

де $R_P(P)$ – це компонент ризику, що аналізує суму платежу, використовуючи логарифмічну функцію для відображення того, як ризик зростає пропорційно до збільшення суми. Визначення цього ризику формулюється як $R_P(P) = a * \log(P+1)$, де a – це коефіцієнт чутливості, що калібрує реакцію моделі на варіації суми платежу. Вихідне значення цього ризику приводиться до діапазону від 0 до 1, щоб забезпечити консистентність масштабування ризику в межах моделі;

$R_C(C)$ – компонент ризику, що оцінює географічні ризики, базуючись на системі вагових коефіцієнтів, що корелюють з історичним рівнем шахрайських дій, пов'язаних із певними країнами. Ці вагові коефіцієнти присвоюються кожній країні згідно з її репутацією у сфері фінансової безпеки: країни, що частіше асоціюються з фінансовими шахрайствами, отримують більш високі значення вагових коефіцієнтів. Унаслідок кінцевий географічний ризиковий компонент, $R_C(C)$, обчислюється таким чином, що його значення завжди залишається в межах від 0 до 1, забезпечуючи збалансований внесок у загальний ризик транзакції;

$R_T(T)$ – ризик, пов'язаний із часом проведення транзакції, з оцінками, що коливаються від 0 до 1. Для виокремлення періодів із підвищеним ризиком використовується гауссівський розподіл з огляду

Сучасний стан наукових досліджень та технологій в промисловості. 2024. №1 (27)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

на значення, що відповідають піковим годинам шахрайства. Формула може бути подана як $R_T(T) = b \times e^{-(T-\mu)^2/2\sigma^2}$, де T – час транзакції, b – множник або коефіцієнт масштабування для гауссівської функції. У контексті запропонованої моделі оцінювання ризику цей коефіцієнт визначає максимальне значення функції, тобто висоту "горба" гауссівського розподілу. Значення b може бути обране залежно від того, наскільки сильно час транзакції має впливати на загальний ризик, а μ та σ визначають години пікового ризику. Отже, функція $R_T(T)$ використовується для моделювання того, як час транзакції впливає на ризик. Час, близький до μ (час піку), дасть вищу оцінку ризику через цю експоненційну функцію, особливо якщо T дуже близько до μ. З іншого боку, час, що значно відрізняється від μ, дає меншу оцінку ризику;

$R_K(K)$ – ризик, асоційований з типом банківської картки, із значеннями, що змінюються від 0 до 1. Цей компонент ризику бере до уваги схильність різних типів карт до шахрайських операцій, присвоюючи вищі ризикові оцінки тим типам карток, що були частіше залучені в шахрайські справи. Використання цього складника дає змогу детально аналізувати ризик на основі предиктивної вартості типу картки, забезпечуючи важливий внесок у загальну оцінку ризику транзакції.

Загальний ризик транзакції порівнюється з установленим порогом безпеки, щоб визначити, чи є транзакція безпечною. Модель постійно адаптується та оновлюється з використанням нової інформації, забезпечуючи точність та актуальність оцінювання ризиків. Цей підхід допомагає не тільки оцінювати безпеку транзакцій у реальному часі, але й аналізувати історичні дані для виявлення тенденцій та вдосконалення моделі. Програмне відтворення розрахунку загального ризику подано на рис. 1.

```
components = [
    calculate_Rp(new_transaction['payment_amount']),
    calculate_Rc(new_transaction['country']),
    calculate_Rt(pd.to_datetime(new_transaction['payment_time']).hour),
    calculate_Rk(new_transaction['card_type'])
]

new_transaction['Risk'] = normalize_risk(components)
```

Рис. 1. Програмне відтворення розрахунку загального ризику

Транзакція вважається безпечною, якщо сумарний ризик залишається нижчим від установленого порогу безпеки, що вимірюється на шкалі від 0% до 100% (або від 0 до 1 в числовому виразі), де 0% відповідає абсолютній відсутності ризику, а 100% – максимальному ризику.

Застосування цієї моделі охоплює як оцінювання безпеки транзакцій у реальному часі, так і аналіз історичних даних. Її можна інтегрувати у фінансові та банківські системи для попередження та виявлення потенційних шахрайств, а також використовувати в дослідницьких та аналітичних цілях для вивчення тенденцій у фінансових операціях.

Для реалізації бібліотеки, спрямованої на підвищення безпеки вебзастосунків, розроблено алгоритм, оснований на використанні штучного інтелекту для аналізу фінансових транзакцій. Цей алгоритм структурований для оптимізації процесів виявлення та управління ризиками, з упровадженням інноваційних методів машинного навчання. На першому етапі алгоритму відбувається підготовка даних, під час якої система налаштована на оброблення реальних даних транзакцій, отриманих від адміністратора системи. Ці дані, що можуть містити атрибути, такі як географічне положення транзакції, сума, час проведення, тип картки та інші відповідні параметри, проходять процес очищення та нормалізації для забезпечення їх готовності до ефективного аналізу.

На наступному етапі кожна транзакція детально аналізується з використанням розробленої моделі *AI* (рис. 2). Аналізуються вказані параметри транзакції, зокрема різні ризикові фактори, такі як нестандартні суми, час проведення платежу, а також історичні дані про шахрайство в певних

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2024. No. 1 (27)

географічних локаціях. Кожна транзакція отримує оцінку ризику, і якщо ця оцінка перевищує встановлений поріг, транзакція визначається як потенційно небезпечна.

Рис. 2. Схематичне відображення етапів аналізу безпеки транзакцій

Після аналізу результати оброблення кожної транзакції зберігаються для подальшого використання. Інформація про кожну транзакцію, зокрема її параметри та оцінка безпеки, фіксується у форматі *JSON*, що сприяє зручному та ефективному зберіганню даних. Це дає змогу всебічно аналізувати тенденції у фінансових транзакціях, виявляти шахрайські схеми й забезпечувати додаткову інформацію для вдосконалення моделі. Аналітика, що базується на зібраних даних, допомагає виявити слабкі місця в системі та забезпечує інформацію для постійного оновлення алгоритму, збільшуючи його точність і надійність.

Запропонований алгоритм втілює сучасні підходи до застосування штучного інтелекту в аналізі фінансових даних, демонструючи, як інноваційні технології можуть удосконалювати процеси управління ризиками та підвищувати безпеку в цифровому світі. Використовуючи поєднання передових алгоритмів та ретельне оброблення інформації, система пропонує ефективний спосіб захисту від фінансових шахрайств і забезпечення безпеки користувачів вебзастосунків.

Детальний розгляд математичної моделі та алгоритму, що лежить в основі системи захисту вебзастосунків, веде до опису архітектури програмного забезпечення. Запропоновано *UML*-схему класів (рис. 3), яка ілюструє структуру бібліотеки для інтеграції штучного інтелекту в процес оброблення даних, що надходять через *POST*-запити у вебзастосунках.

Схема розподіляє систему на декілька ключових компонентів для підвищення модулярності та полегшення інтеграції. *DataLoader* відповідає за завантаження вхідної інформації, є початковим етапом оброблення даних, готуючи їх до подальшої передачі. *DataPreprocessor* виконує операції попереднього оброблення, зокрема перетворення інформації в *DataFrame*, логарифмічне перетворення, а також визначення географічних ризиків. *FeatureEncoder* застосовує кодування ознак, необхідне для алгоритмів машинного навчання, трансформуючи категоріальні дані для подальшого оброблення.

Сучасний стан наукових досліджень та технологій в промисловості. 2024. №1 (27)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

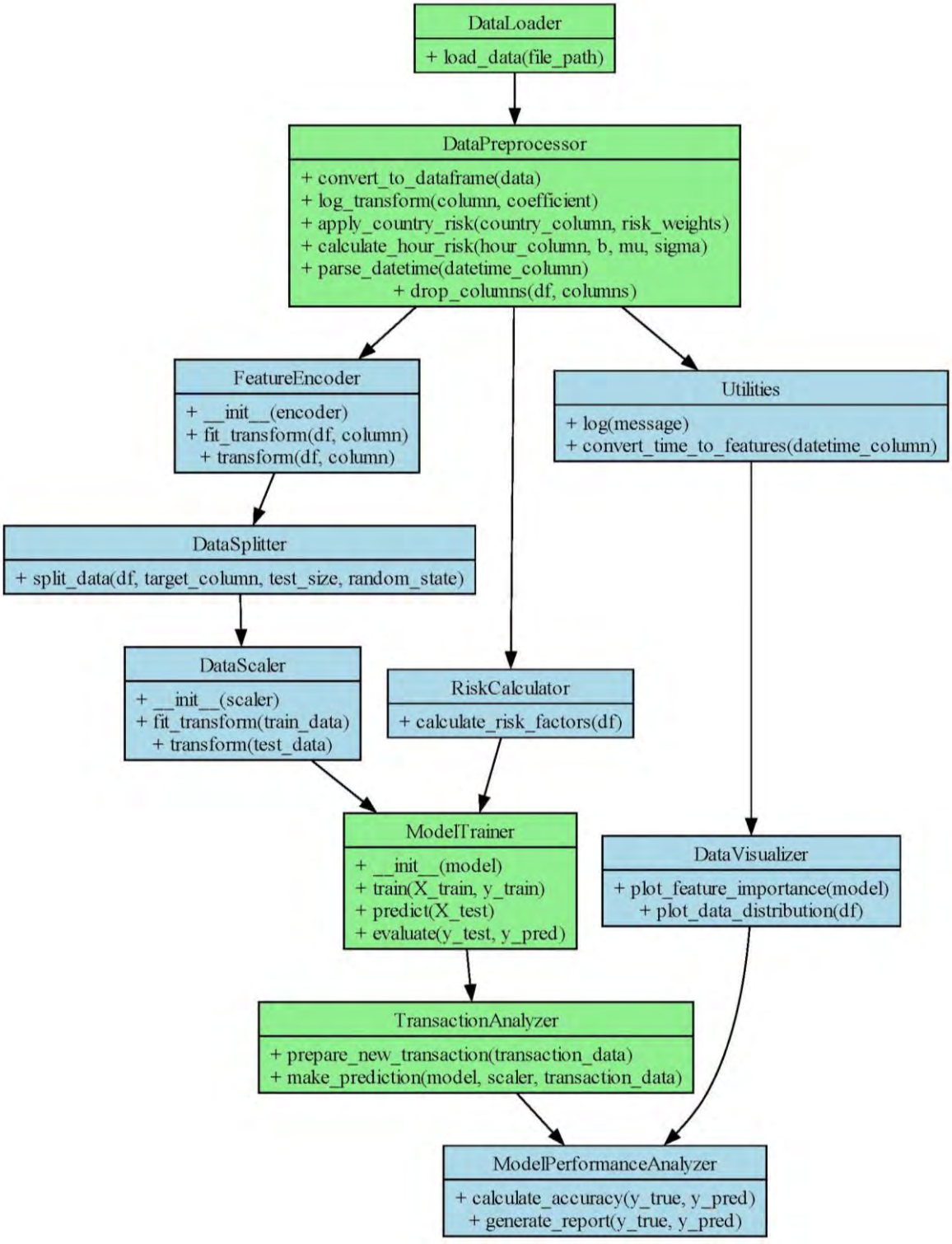

Рис. 3. *UML*-схема класів бібліотеки з оброблення та аналізу фінансових транзакцій

Компоненти *DataSplitter, DataScaler* і *ModelTrainer* забезпечують поділ даних на навчальні та тестові набори, їх нормалізацію, а також навчання та оцінювання моделі. *TransactionAnalyzer* спеціалізується на аналізі нових транзакцій, використовуючи навчену модель для визначення підозрілих чи безпечних транзакцій. *RiskCalculator* аналізує різні фактори ризику, пов'язані з даними транзакцій, зокрема оцінку ризику на основі географічного розташування.

Utilities надає допоміжні утиліти, такі як журналювання подій та конвертація часових

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2024. No. 1 (27)

міток. *ModelPerformanceAnalyzer* та *DataVisualizer* відіграють ключову роль у візуалізації даних та аналізі продуктивності моделі, допомагаючи краще розуміти та оптимізувати прийняття рішень.

Завдяки цій структурі бібліотека не тільки спрощує інтеграцію алгоритмів машинного навчання в застосунки, але й забезпечує гнучкість і розширюваність системи. Кожен клас має визначені відповідальності та взаємодіє з іншими, формуючи згуртовану систему, здатну ефективно обробляти та аналізувати великі обсяги транзакційних даних.

У межах дослідження для навчання та тестування моделі машинного навчання створено таблицю тестових даних (табл. 1), що містить декілька тисяч транзакцій і є важливою для розуміння аналізу та класифікації транзакцій моделлю. Таблиця має такі атрибути:

– країна, подана дволітерним кодом, важлива для визначення ризикованості транзакції, беручи до уваги різні рівні фінансових шахрайств у різних регіонах;

– сума платежу у валютних одиницях, критично важлива для ідентифікації нестандартних або підозрілих транзакцій;

– час платежу, зазначений у форматі "день.місяць.рік година:хвилина", може вказувати на підозрілу активність;

– тип картки (наприклад, *Visa, MasterCard, Amex*), де різні типи карток можуть мати різні рівні ризику;

– сайт покупки, доменне ім'я вебсайту, важливий індикатор, оскільки деякі сайти можуть бути причетними до шахрайських схем;

– інформація про клієнта, у цьому разі із значенням *'null'*, що вказує на відсутність конкретної інформації;

– безпека транзакції, булевий індикатор, що показує, чи вважається транзакція безпечною, використовується як цільова змінна для навчання моделі.

Таблиця 1. *Таблиця тестових даних*

Country	Payment Amount	Payment Time	Card Type	Purchase Site	Client Info	Transaction Safe
UG	418.57	09.04.2023 10:52	MasterCard	bowen-freeman.com	null	TRUE
UA	350000	29.05.2023 10:30	MasterCard	miller-kirby.com	null	TRUE
UA	3112.67	16.01.2023 11:18	Visa	nguyen-winters.com	null	FALSE
UA	4481.02	23.08.2023 6:46	MasterCard	garcia-vincent.biz	null	FALSE
UA	2988.13	21.10.2023 0:37	Visa	dunn.com	null	TRUE
NL	2202.47	24.04.2023 8:32	Visa	nelson-wallace.net	null	FALSE
NI	327.61	30.12.2023 12:33	Visa	yoder.net	null	TRUE
…	…	…	…	…	…	…

Ці тестові дані є основою для "навчання" моделі на реальних даних, даючи змогу з часом стати більш точною у визначенні ризикованих транзакцій. Репрезентативність даних забезпечує для моделі ефективне виявлення шахрайських дій у різних ситуаціях. Можливе розширення набору даних іншими атрибутами, такими як геолокація користувача, історія покупок, поведінкові фактори, може поліпшити здатність моделі до виявлення ризикованих патернів. Також важливо звертати увагу на якість даних, оскільки неповна, розмита або помилкова інформація здатна суттєво вплинути на точність моделі. Очищення даних, оброблення викидів і виправлення помилок є важливими кроками в підготовці набору даних для навчання.

Для детального опису результатів тестування та демонстрації роботи бібліотеки можна долучити два основні сценарії тестування. Перший сценарій демонструє, як бібліотека правильно ідентифікує безпечну транзакцію (рис. 4), а другий – як вона виявляє потенційно ризиковану транзакцію (рис. 5). У кожному сценарії можна навести конкретні приклади транзакцій, параметри, використані для аналізу, та висновки, до яких прийшла модель.

У сценарії ідентифікації безпечної транзакції параметри, такі як країна, сума, час, тип картки, демонструють, що модель визначила цю транзакцію як безпечну. Обґрунтуванням є те, що на основі заданих параметрів і навченої моделі транзакція не відповідає звичайним ознакам шахрайства.

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2024. №1 (27) ISSN 2524-2296 (online)

Рис. 4. Тестовий випадок № 1

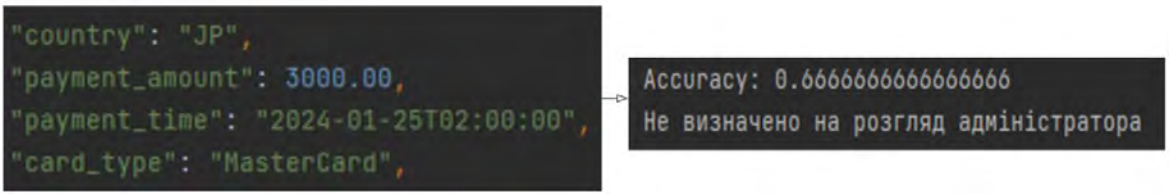

Рис. 5. Тестовий випадок № 2

У сценарії виявлення ризикованої транзакції параметри також містять країну, суму, час, тип картки. Модель визначила цю транзакцію як потенційно ризиковану, оскільки було виявлено декілька підозрілих факторів, наприклад незвичайно висока сума платежу та проведення транзакції в нічний час.

Результати тестування важливі для оцінювання точності та надійності моделі, виявлення потенційних сфер для поліпшення, а також демонстрації адаптованості моделі до різних умов і вимог, що є ключовим для її використання в реальних вебзастосунках.

У дослідженні проведено ґрунтовний аналіз та тестування розробленої моделі штучного інтелекту для оцінювання безпеки фінансових транзакцій у вебзастосунках. Результати тестування підтвердили здатність моделі ефективно ідентифікувати різні типи транзакцій, зокрема безпечні й потенційно ризиковані операції. Модель продемонструвала хорошу точність у виявленні шахрайських патернів, що є ключовим для захисту користувачів від фінансових втрат.

Висновки

У дослідженні запропоновано розроблення програмної бібліотеки, що використовує методи штучного інтелекту та машинного навчання для підвищення безпеки вебзастосунків, зокрема в контексті фінансових транзакцій. Основну увагу зосереджено на створенні моделі, здатної оцінювати ризикованість транзакцій на основі низки параметрів, зокрема країни проведення, суми платежу, часу й типу картки.

Робота демонструє, як інтеграція штучного інтелекту в системи оброблення транзакцій може суттєво підвищити їх безпеку, забезпечуючи автоматизоване виявлення потенційно ризикованих операцій. Використання бібліотеки *scikit-learn* для *Python* дало змогу впровадити перевірені та надійні алгоритми машинного навчання, що забезпечили високу точність і надійність розробленої моделі.

Запропоновано псевдокод, що описує потенційну структуру програми, зокрема класи та методи для аналізу транзакцій. Також розглянуто методи генерації тестових даних і наведено приклади тестових результатів, що демонструють роботу моделі в різних сценаріях.

Автори наголошують на важливості використання технологій штучного інтелекту в сучасних вебзастосунках та можливості їх застосування для підвищення безпеки. Подальші дослідження в цій сфері можуть бути спрямовані на розвиток більш складних моделей, здатних зважати на додаткові параметри та взаємозв'язки в даних, а також на інтеграцію моделі в реальні вебзастосунки для випробування її ефективності в реальних умовах.

Запропонована бібліотека робить вагомий внесок у розвиток методів штучного інтелекту та машинного навчання, демонструючи їх практичну значущість та ефективність у сфері захисту фінансових транзакцій і забезпечення безпеки користувачів у цифровому світі.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2024. No. 1 (27)

Список літератури

1. Attkan A., Ranga V. Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security. *Complex & Intelligent Systems*. 2022. Vol. 8. P. 3559–3591. DOI: https://doi.org/10.1007/s40747-022-00667-z
2. Sobchuk V., Zamrii I., Laptiev S. Ensuring Functional Stability of Technological Processes as Cyberphysical Systems Using Neural Networks. Lecture Notes in Networks and Systems. 2023. Vol. 536. P. 581–592. DOI: https://doi.org/10.1007/978-3-031-20141-7_53
3. Latif S., Xian Wen F., Iwendi C., Wang L.-l., Mohsin S., Han Z., Band S. AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. *Computer Communications*. 2022. Vol. 181. P. 274–283. DOI: https://doi.org/10.1016/j.comcom.2021.09.029
4. Bonfanti M. Artificial intelligence and the offense–defense balance in cyber security. *Cyber Security Politics; Socio-Technological Transformations and Political Fragmentation*. 2022. 1st Edition. P. 64–77. DOI: https://doi.org/10.4324/9781003110224-6
5. Naik B., Mehta A., Yagnik H., Shah M. The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review. *Complex & Intelligent Systems.* 2021. Vol. 8. P. 1763–1780. DOI: https://doi.org/10.1007/s40747-021-00494-8
6. Abdullahi M., Baashar Y., Alhussian H., Alwadain A., Aziz N., Capretz L., Abdulkadir S. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. *Electronics.* 2022. 11(2), 198. P. 2–27. DOI: https://doi.org/10.3390/electronics11020198
7. Ahanger T., Aljumah A., Atiquzzaman M. State-of-the-art survey of artificial intelligent techniques for IoT security. *Computer Networks.* 2022. Vol. 206. 108771 p. DOI: https://doi.org/10.1016/j.comnet.2022.108771
8. Ramasamy L., Khan F., Shah M., Prasad B., Iwendi C., Biamba C. Secure Smart Wearable Computing through Artificial Intelligence-Enabled Internet of Things and Cyber-Physical Systems for Health Monitoring. *Smart Healthcare Systems Based on the Internet of Things and Artificial Intelligence*. 2022. 22(3), 1076. P. 2–16. DOI: https://doi.org/10.3390/s22031076
9. Ghillani D. Deep Learning and Artificial Intelligence Framework to Improve the Cyber Security. *American Journal of Artificial Intelligence*. 2022. 11 p. DOI: https://doi.org/10.22541/au.166379475.54266021/v1
10. Pise A., Almuzaini K., Ahanger T., Farouk A., Pant K., Pareek P., Nuagah S. Enabling Artificial Intelligence of Things (AIoT) Healthcare Architectures and Listing Security Issues. *Computational Intelligence and Neuroscience*. 2022. Vol. 2022, Article ID 8421434, 14 p. DOI: https://doi.org/10.1155/2022/8421434
11. Zhang Z., Al Hamadi H., Damiani E., Yeun C. Y., Taher F. Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. *IEEE Access*. 2022. Vol. 10, P. 93104–93139. DOI: https://doi.org/10.1109/ACCESS.2022.3204051
12. Gill S., Xu M., Ottaviani C., Patros P., Bahsoon R., Shaghaghi A., Golec M., Stankovski V., Wu H., Abraham A., Singh M., Mehta H., Ghosh S., Baker T., Parlikad A., Lutfiyya H., Kanhere S., Sakellariou R., Dustdar S., Rana O., Uhlig S. AI for next generation computing: Emerging trends and future directions. *Internet of Things*. 2022. Vol. 19. 100514 p. DOI: https://doi.org/10.1016/j.iot.2022.100514
13. Kumar S., Lim W., Sivarajah U., Kaur J. Artificial Intelligence and Blockchain Integration in Business: Trends from a Bibliometric-Content Analysis. *Information Systems Frontiers.* 2023. Vol. 25. P. 871–896. DOI: https://doi.org/10.1007/s10796-022-10279-0
14. Yathiraju N. Investigating the use of an Artificial Intelligence Model in an ERP Cloud-Based System. *International Journal of Electrical, Electronics and Computers.* 2022. Vol. 7, Issue 2. P. 1–26. DOI: http://dx.doi.org/10.22161/eec.72.1
15. Sujith A., Sajja G., Mahalakshmi V., Nuhmani S., Prasanalakshmi B. Systematic review of smart health monitoring using deep learning and Artificial intelligence. *Neuroscience Informatics*. 2022. Vol. 2, Issue 3. 100028 p. DOI: https://doi.org/10.1016/j.neuri.2021.100028
16. Nasim S., Ali M., Kulsoom U. Artificial intelligence incidents & ethics: a narrative review. *Computer Science and Information Technology.* 2022. Vol. 2, No 2. P. 52–64. DOI: http://dx.doi.org/10.54489/ijtim.v2i2.80
17. Kunduru A. Artificial intelligence advantages in cloud fintech application security. *Central asian journal of mathematical theory and computer sciences*. 2023. Vol. 4, No. 8. P. 48–53 URL: https://cajmtcs.centralasianstudies.org/index.php/CAJMTCS/article/view/492
18. Chang V., Bhavani V., Xu A., Hossain M. An artificial intelligence model for heart disease detection using machine learning algorithms. *Healthcare Analytics*. 2022. Vol. 2. 100016 p. DOI: https://doi.org/10.1016/j.health.2022.100016
19. Babitha M., Sushama C., Gudivada V., Kazi K., Bandaru S. Trends of Artificial Intelligence for Online Exams in Education. *International Journal of Early Childhood Special Education*. 2022. 14(01). P. 2457–2463. URL: https://www.researchgate.net/publication/360513613_Trends_of_Artificial_Intelligence_for_Online_Exams_in_Education
20. Esenogho E., Djouani K., Kurien A. M. Integrating Artificial Intelligence Internet of Things and 5G for Next-Generation Smartgrid: A Survey of Trends Challenges and Prospect. *IEEE Access*. 2022. Vol. 10. P. 4794–4831. DOI: https://doi.org/10.1109/ACCESS.2022.3140595

Сучасний стан наукових досліджень та технологій в промисловості. 2024. №1 (27)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

21. Bi S., Wang C., Zhang J., Huang W., Wu B., Gong Y., Ni W. A Survey on Artificial Intelligence Aided Internet-of-Things Technologies in Emerging Smart Libraries. *AI-Aided Wireless Sensor Networks and Smart Cyber-Physical Systems*. 2022. No. 8. 2991 p. DOI: https://doi.org/10.3390/s22082991

References

1. Attkan, A., Ranga, V. (2022), "Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security", *Complex & Intelligent Systems*, Vol. 8, P. 3559–3591. DOI: https://doi.org/10.1007/s40747-022-00667-z
2. Sobchuk, V., Zamrii, I., Laptiev, S. (2023), "Ensuring Functional Stability of Technological Processes as Cyberphysical Systems Using Neural Networks", *Lecture Notes in Networks and Systems*, Vol. 536, P. 581–592. DOI: https://doi.org/10.1007/978-3-031-20141-7_53
3. Latif, S., Xian, Wen F., Iwendi, C., Wang, L.-l., Mohsin, S., Han, Z., Band, S. (2022), "AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems", *Computer Communications*, Vol. 181, P. 274–283. DOI: https://doi.org/10.1016/j.comcom.2021.09.029
4. Bonfanti, M. (2022), "Artificial intelligence and the offense–defense balance in cyber security", *Cyber Security Politics; Socio-Technological Transformations and Political Fragmentation*, 1st Edition, P. 64–77. DOI: https://doi.org/10.4324/9781003110224-6
5. Naik, B., Mehta, A., Yagnik, H., Shah, M. (2021), "The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review", *Complex & Intelligent Systems,* Vol. 8, P. 1763–1780. DOI: https://doi.org/10.1007/s40747-021-00494-8
6. Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L., Abdulkadir, S. (2022), "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review", *Electronics,* 11(2), 198, P. 2–27. DOI: https://doi.org/10.3390/electronics11020198
7. Ahanger, T., Aljumah, A., Atiquzzaman, M. (2022), "State-of-the-art survey of artificial intelligent techniques for IoT security", *Computer Networks,* Vol. 206, 108771 p. DOI: https://doi.org/10.1016/j.comnet.2022.108771
8. Ramasamy, L., Khan, F., Shah, M., Prasad, B., Iwendi, C., Biamba, C. (2022), "Secure Smart Wearable Computing through Artificial Intelligence-Enabled Internet of Things and Cyber-Physical Systems for Health Monitoring", *Smart Healthcare Systems Based on the Internet of Things and Artificial Intelligence*, 22(3), 1076. P. 2–16. DOI: https://doi.org/10.3390/s22031076
9. Ghillani, D. (2022), "Deep Learning and Artificial Intelligence Framework to Improve the Cyber Security", *American Journal of Artificial Intelligence*, 11 p. DOI: https://doi.org/10.22541/au.166379475.54266021/v1
10. Pise, A., Almuzaini, K., Ahanger, T., Farouk, A., Pant, K., Pareek, P., Nuagah, S. (2022), "Enabling Artificial Intelligence of Things (AIoT) Healthcare Architectures and Listing Security Issues", *Computational Intelligence and Neuroscience*, Vol. 2022, Article ID 8421434, 14 p. DOI: https://doi.org/10.1155/2022/8421434
11. Zhang, Z., Al Hamadi, H., Damiani, E., Yeun, C. Y., Taher, F. (2022), "Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research", *IEEE Access*, Vol. 10, P. 93104–93139. DOI: https://doi.org/10.1109/ACCESS.2022.3204051
12. Gill, S., Xu, M., Ottaviani, C., Patros, P., Bahsoon, R., Shaghaghi, A., Golec, M., Stankovski, V., Wu, H., Abraham, A., Singh, M., Mehta, H., Ghosh, S., Baker, T., Parlikad, A., Lutfiyya, H., Kanhere, S., Sakellariou, R., Dustdar, S., Rana, O., Uhlig, S. (2022), "AI for next generation computing: Emerging trends and future directions", *Internet of Things*, Vol. 19, 100514 p. DOI: https://doi.org/10.1016/j.iot.2022.100514
13. Kumar, S., Lim, W., Sivarajah, U., Kaur, J. (2023), "Artificial Intelligence and Blockchain Integration in Business: Trends from a Bibliometric-Content Analysis", *Information Systems Frontiers,* Vol. 25, P. 871–896. DOI: https://doi.org/10.1007/s10796-022-10279-0
14. Yathiraju, N. (2022), "Investigating the use of an Artificial Intelligence Model in an ERP Cloud-Based System", *International Journal of Electrical, Electronics and Computers,* Vol. 7, Issue 2, P. 1–26. DOI: http://dx.doi.org/10.22161/eec.72.1
15. Sujith, A., Sajja, G., Mahalakshmi, V., Nuhmani, S., Prasanalakshmi, B. (2022), "Systematic review of smart health monitoring using deep learning and Artificial intelligence", *Neuroscience Informatics*, Vol. 2, Issue 3, 100028 p. DOI: https://doi.org/10.1016/j.neuri.2021.100028
16. Nasim, S., Ali, M., Kulsoom, U. (2022), "Artificial intelligence incidents & ethics: a narrative review", *Computer Science and Information Technology,* Vol. 2, No 2, P. 52–64. DOI: http://dx.doi.org/10.54489/ijtim.v2i2.80
17. Kunduru, A. (2023), "Artificial intelligence advantages in cloud fintech application security", *Central asian journal of mathematical theory and computer sciences*, Vol. 4, No. 8, P. 48–53 URL: https://cajmtcs.centralasianstudies.org/index.php/CAJMTCS/article/view/492
18. Chang, V., Bhavani, V., Xu, A., Hossain, M. (2022), "An artificial intelligence model for heart disease detection using machine learning algorithms", *Healthcare Analytics*, Vol. 2, 100016 p. DOI: https://doi.org/10.1016/j.health.2022.100016
19. Babitha, M., Sushama, C., Gudivada, V., Kazi, K., Bandaru, S. (2022), "Trends of Artificial Intelligence for Online Exams in Education", *International Journal of Early Childhood Special Education*, 14(01), P. 2457–2463 URL: https://www.researchgate.net/publication/360513613_Trends_of_Artificial_Intelligence_for_Online_Exams_in_Education

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2024. No. 1 (27)*

20. Esenogho, E., Djouani, K., Kurien, A. (2022), "Integrating Artificial Intelligence Internet of Things and 5G for Next-Generation Smartgrid: A Survey of Trends Challenges and Prospect", *IEEE Access*, Vol. 10, P. 4794–4831. DOI: https://doi.org/10.1109/ACCESS.2022.3140595
21. Bi, S., Wang, C., Zhang, J., Huang, W., Wu, B., Gong, Y., Ni, W. (2022), "A Survey on Artificial Intelligence Aided Internet-of-Things Technologies in Emerging Smart Libraries", *AI-Aided Wireless Sensor Networks and Smart Cyber-Physical Systems*, No. 8, 2991 p. DOI: https://doi.org/10.3390/s22082991

Надійшла 28.02.2024

Відомості про авторів / About the Authors

Замрій Ірина Вікторівна – доктор технічних наук, доцент, Державний університет інформаційно-комунікаційних технологій, завідувач кафедри інженерії програмного забезпечення, Київ, Україна; e-mail: irinafraktal@gmail.com; ORCID ID: https://orcid.org/0000-0001-5681-1871

Шахматов Іван Олександрович – Державний університет інформаційно-комунікаційних технологій, аспірант кафедри інженерії програмного забезпечення, Київ, Україна; e-mail: ivan.shakhmatov@gmail.com; ORCID ID: https://orcid.org/0009-0004-9628-0365

Zamrii Iryna – Doctor of Sciences (Engineering), Associate Professor, State University of Information and Communication Technologies, Head at the Department of Software Engineering, Kyiv, Ukraine.

Shakhmatov Ivan – State University of Information and Communication Technologies, Postgraduate at the Department of Software Engineering, Kyiv, Ukraine.

ENHANCING THE SECURITY OF WEB APPLICATIONS THROUGH INNOVATIVE PATTERNS OF INTEGRATION OF ARTIFICIAL INTELLIGENCE

Ensuring the security of digital operations, especially in the areas of e-commerce and financial transactions, remains increasingly relevant. Therefore, **the subject** of research is the development of a specialized software library. This library aims to improve the security of web applications. **The purpose** of this study is to develop a software library that uses artificial intelligence and machine learning methods to analyze and improve the level of security of financial transactions. The use of these advanced technologies helps automate the detection of potentially fraudulent or risky transactions, thereby providing a higher level of user protection**.** The following **tasks** are solved in the article: analysis of modern methods of processing financial transactions and identification of possible security threats; development of a UML diagram of library classes for processing and analyzing financial transactions; testing and validation of the developed artificial intelligence model for assessing the security of financial transactions on real financial data. Machine learning **methods** were defined and applied using the scikit-learn library in Python, the algorithms of which are capable of analyzing large volumes of data and identifying potential risks with high accuracy. This ensures effective integration of artificial intelligence technologies. The following **results** were obtained in the work: the criteria for assessing the riskiness of financial transactions for the identification of potential risks are defined; the program operation algorithm is described, which includes procedures for determining and classifying transaction risks; pseudocode is presented, which illustrates the structure of classes and methods of the model, opening opportunities for its adaptation and scaling; methods of generating test data reproducing realistic scenarios of financial transactions have been developed; an analysis of the results was carried out to assess the effectiveness of the developed model. In **conclusion**, the results of research and testing allow us to evaluate the model's response to various data and its effectiveness in real conditions, as the work presents examples of processing various types of transactions. In addition, the study presents not only the development and validation of the developed model, but also the prospects of its use on a larger scale, integration with existing web applications.

Keywords: Artificial Intelligence; Web Application Security; Financial Transactions; Machine Learning; Data Analysis; Fraud Detection; scikit-learn.

Бібліографічні описи / Bibliographic descriptions

Замрій І. В., Шахматов І. О. Підвищення безпеки вебзастосунків з допомогою інноваційних патернів інтеграції штучного інтелекту. *Сучасний стан наукових досліджень та технологій в промисловості*. 2024. № 1 (27). С. 67–80. DOI: https://doi.org/10.30837/ITSSI.2024.27.067

Zamrii, I., Shakhmatov, I. (2024), "Enhancing the security of web applications through innovative patterns of integration of artificial intelligence", *Innovative Technologies and Scientific Solutions for Industries*, No. 1 (27), P. 67–80. DOI: https://doi.org/10.30837/ITSSI.2024.27.067