УДК 004.056:004.056.5:004.056.2
DOI https://doi.org/10.36994/2788-5518-2024-02-08-04

МЕТОД ЗАХИСТУ ІНФОРМАЦІЇ НА МОБІЛЬНИХ ПРИСТРОЯХ НА ОСНОВІ АДАПТИВНОЇ ПОВЕДІНКОВОЇ МОДЕЛІ

Бровченко Є. М., *Відкритий міжнародний університет розвитку людини «Україна», Інститут комп'ютерних технологій, Київ, Україна. https://orcid.org/0000-0002-1416-0385, yebrovchenko@hotmail.com*

Самарай В. П., *к.т.н., с.н.с., доцент, Відкритий міжнародний університет розвитку людини «Україна», Інститут комп'ютерних технологій, Київ, Україна. https://orcid.org/0000-0003-4419-1366, samaraj@ukr.net*

Анотація. *Стаття присвячена проблемі захисту неструктурованої інформації на мобільних пристроях на основі адаптивної поведінкової моделі. Досліджено сучасні виклики інформаційної безпеки, що виникають у зв'язку з активним використанням мобільних пристроїв у цифровому середовищі. Запропоновано новий підхід до захисту даних, що включає машинне навчання, поведінкову аналітику та адаптивні механізми ідентифікації загроз. Використання штучного інтелекту та поведінкових моделей безпеки сприяє вдосконаленню механізмів ідентифікації загроз та адаптивного реагування на можливі ризики. Розглянуто основні методи, такі як багатофакторна автентифікація, криптографічні алгоритми, блокчейн та квантово-стійке шифрування, які забезпечують комплексний рівень безпеки. Проведені експериментальні дослідження продемонстрували ефективність адаптивного підходу у виявленні та попередженні потенційних загроз для інформаційної безпеки. Методи захисту інформації засновувалися на засадах інтеграційного машинного навчання, математичних моделей прогнозування загроз, алгоритмів шифрування та багатофакторної автентифікації. Аспекти захисту: моніторинг, адаптація, прогнозування загроз, прийняття рішень, шифрування та біометрична автентифікація. Кожен етап включає підхід із використанням формул і відповідних алгоритмів. Отримані результати підтверджують, що впровадження інноваційних моделей захисту дозволяє підвищити рівень кібербезпеки мобільних пристроїв, зменшуючи ризики несанкціонованого доступу до конфіденційної інформації. Використання адаптивних моделей дозволить ефективно виявляти загрози та реагувати на аномальну поведінку користувачів у реальному часі. Блокчейн та квантово-стійке шифрування сприятимуть підвищенню безпеки даних, а концепція «приватності за замовчуванням» гарантуватиме інтеграцію кібербезпеки на всіх етапах розробки. Комплексний підхід, що поєднує технологічні рішення, підвищення обізнаності користувачів та нормативне регулювання, стане ключем до ефективного захисту мобільної інформації.*

Ключові слова: *мобільні пристрої, захист інформації, неструктурована інформація, кібербезпека, поведінкова аналітика, машинне навчання, багатофакторна автентифікація.*

ADAPTIVE BEHAVIORAL MODEL-BASED METHOD FOR INFORMATION PROTECTION ON MOBILE DEVICES

Evgen Brovchenko, *Open International University of Human Development "Ukraine", Kyiv, Ukraine. https://orcid.org/0000-0002-1416-0385, yebrovchenko@hotmail.com*

Valery Samarai, *Ph.D. in Technical Sciences, Senior Research Fellow, Associate Professor, Open International University of Human Development "Ukraine", Kyiv, Ukraine. https://orcid.org/0000-0003-4419-1366, samaraj@ukr.net*

Abstract. *This paper addresses the issue of protecting unstructured information on mobile devices based on an adaptive behavioral model. The increasing role of mobile devices in digital ecosystems necessitates the development of advanced security solutions that ensure data integrity, confidentiality, and resilience to cyber threats. The research focuses on modern cybersecurity challenges arising from the widespread use of mobile devices, including data breaches, unauthorized access, phishing attacks, and malware exploitation. The study explores an innovative approach that integrates behavioral analytics, machine learning, and adaptive threat identification mechanisms to enhance security measures. Key methods such as multi-factor authentication (MFA), cryptographic algorithms, blockchain, and quantum-resistant encryption are examined to establish a comprehensive security framework. Experimental research was conducted using various mobile security scenarios, including different levels of threat exposure, data transmission security, and real-time behavioral monitoring. The results demonstrated that adaptive behavioral models significantly improve the detection and mitigation of cyber threats, dynamically adjusting security policies*

based on user interactions and environmental conditions. By leveraging artificial intelligence and behavioral biometrics, this approach enhances authentication accuracy, reduces the risk of unauthorized access, and strengthens protection against evolving cyberattacks. The study findings highlight the importance of combining advanced encryption techniques with behavioral-based security mechanisms to create a proactive cybersecurity strategy. Implementing adaptive security models enables mobile devices to function as secure elements within digital infrastructures, ensuring both user convenience and high-level protection. The proposed methodology contributes to the ongoing development of intelligent mobile security systems, offering effective solutions for safeguarding sensitive information in an increasingly connected world.

Key words: *mobile devices, information security, unstructured data protection, cybersecurity, behavioral analytics, machine learning, multi-factor authentication.*

Вступ

Інтенсивний розвиток сучасних інформаційних технологій вимагає впровадження інноваційних рішень із захисту даних. При цьому безпека інформації на мобільних пристроях стає критично важливою з урахуванням їх ключової ролі і в приватному житті, і в професійній діяльності людей.

Використання штучного інтелекту та поведінкових моделей безпеки сприяє вдосконаленню механізмів ідентифікації загроз та адаптивного реагування на можливі ризики. Мобільні пристрої – вже не просто засоби комунікації, а складові частини інформаційних екосистем, що зберігають значні обсяги конфіденційних даних. У майбутньому інтеграція між користувачем та пристроєм стане ще більш динамічною, що підвищить вимоги до ефективності захисних механізмів. З огляду на постійний розвиток кіберзагроз та непередбачуваність атак перед фахівцями стоїть завдання розробки гнучких, адаптивних методів захисту, що можуть автоматично аналізувати поведінкові характеристики користувачів, визначати аномальні дії та застосовувати відповідні контрзаходи. Запровадження адаптивної поведінкової моделі безпеки дозволяє створити проактивний підхід до захисту даних, що забезпечує не лише виявлення загроз у реальному часі, а й їхнє прогнозування на основі аналізу поведінки користувача та змін у його середовищі. Таким чином, мобільні пристрої мають бути розглянуті не лише як частина цифрової екосистеми, а й як динамічні елементи, що інтегрують передові засоби інформаційної безпеки.

Безпека неструктурованих даних, що зберігаються на мобільних пристроях, є ключовим аспектом кіберзахисту [3; 8]. Такі дані включають текстові файли, електронну пошту, мультимедійний контент (фотографії, відео, аудіозаписи) та інші інформаційні об'єкти, що можуть бути вразливими до несанкціонованого доступу. Основні загрози для інформаційної безпеки мобільних пристроїв включають ризик втрати або крадіжки пристрою [7], експлуатацію вразливостей операційної системи [9] та додатків, недостатній рівень шифрування, слабкі паролі та нехтування принципами кібергігієни [4; 6; 10]. Запровадження адаптивних поведінкових моделей безпеки дозволяє ефективніше протидіяти цим загрозам, аналізуючи звички користувача та виявляючи аномальну активність [2]. Такий підхід дає змогу в режимі реального часу адаптувати механізми захисту залежно від контексту використання пристрою, рівня ризику та зовнішніх факторів. Водночас сучасні архітектурні рішення безпеки не завжди враховують необхідність гнучкої інтеграції з адаптивними методами захисту [7], що може створювати додаткові виклики з погляду продуктивності та економічної ефективності впровадження.

Аналіз сфери кібербезпеки та результати досліджень у галузі поведінкової аналітики, адаптивних систем автентифікації [1; 2], методів шифрування даних на мобільних пристроях [3; 7], а також сучасних підходів до виявлення аномалій [6; 8] підкреслюють важливість захисту інформації та зростаючий попит на надійні рішення для захисту інформаційних систем і мобільних пристроїв. Захист інформації є комплексним завданням: від етапу розробки до контролю під час експлуатації, включаючи інформаційну обізнаність і відповідальність кінцевого користувача [9]. Кібербезпека переходить на новий рівень, де лише комплексний підхід здатен забезпечити ефективні рішення [10; 11].

Аналіз останніх досліджень і публікацій

Аналіз особливостей використання мобільних пристроїв як у особистих, так і корпоративних цілях дає змогу виокремити ключові тенденції та методи, що застосовуються для адаптивного захисту інформації [2]. Основою такої системи є біометричний доступ [1]. Постійний розвиток у сфері біометрії сприяє підвищенню точності та надійності цих технологій. Додатково важливим компонентом інформаційного захисту є шифрування, яке вдосконалюється завдяки новітнім алгоритмам та методам безпечного зберігання ключів [6]. Серед актуальних рішень для мобільних пристроїв варто відзначити використання віртуальних приватних мереж (VPN), які, однак, не завжди ефективно застосовуються користувачами через складність налаштування або недостатню обізнаність [8]. Окрему увагу слід приділити захисту від шкідливого програмного забезпечення та вірусних загроз. Фахівці з кібербезпеки безперервно аналізують нові загрози, такі як фітингові атаки, експлойти нульового дня, мобільні троянські програми тощо [4], та розробляють ефективні методи їх виявлення й нейтралізації [5; 7; 10]. Таким чином, адаптивний захист інформації на мобільних пристроях базується на комбінації біометричної автентифікації, сучасних методів шифрування, VPN-технологій та антивірусного захисту, що разом забезпечують високий рівень безпеки та конфіденційності даних.

Аналіз систем захисту інформації на мобільних пристроях дозволяє виділити основні тенденції у розвитку загроз згідно з [4], виявити ключові вразливості [5], а також оцінити ефективність сучасних методів захисту даних від несанкціонованого доступу [6] та атак зловмисників [7; 10]. Хоча різноманітність методів та рівень інтеграції можуть ускладнити користування для кінцевого користувача, це дозволяє ефективно протистояти зловмисникам.

У табл. 1 наведено результати аналізу порушень на мобільних пристроях за десять років у 2014–2023 рр. на основі даних з [2; 3; 4; 9; 10].

Таблиця 1

Динаміки порушень у системах захисту інформації на мобільних пристроях на основі аналітичного аналізу (2014–2023 рр.)

Рік	Кількість інцидентів	Кількість постраждалих (млн)	Приблизний розмір втрат (млн $)	Основні причини
2014	50	20	10	Витік даних через незахищені додатки
2015	70	30	15	Викрадення даних, слабкі паролі
2016	90	100	50	Атаки через фішинг, ненадійні мережі
2017	120	200	200	Витік даних у результаті зламу
2018	150	300	300	Атаки через публічні Wi-Fi мережі
2019	200	500	400	Використання шкідливих додатків
2020	250	600	600	Порушення через віддалену роботу
2021	300	800	1,000	Підвищена активність кібератак
2022	350	1,200	1,500	Недостатня безпека додатків
2023	400	1,500	2,000	Зростання використання мобільних пристроїв

Аналіз даних таблиці 1 дозволяє виокремити ключові тенденції у порушеннях захисту неструктурованої інформації на мобільних пристроях за останнє десятиліття.

З 2014 по 2023 рік спостерігається стійкий ріст кількості інцидентів, що свідчить про зростаючі загрози. За цей період кількість випадків зросла з 50 до 400, що вказує на підвищений інтерес зловмисників до мобільних пристроїв. Число постраждалих користувачів також збільшується. У 2014 році кількість постраждалих становила 20 млн осіб, а до 2023 року досягла 1,5 млрд, що вказує на зростаючу масштабність порушень. Втрати від витоків даних мають зростаючу тенденцію. Якщо у 2014 році втрати становили 10 млн доларів, то у 2023 році ця сума досягла 2 млрд доларів, що свідчить про значні фінансові наслідки порушень для бізнесу та економіки. Причини витоків даних еволюціонують: на початку основними проблемами були незахищені додатки та слабкі паролі, однак з часом головними загрозами стали фішинг-атаки, ненадійні мережі та шкідливі додатки. Це свідчить про те, що зловмисники адаптуються до нових умов, що вимагає постійного вдосконалення заходів безпеки. Значний сплеск інцидентів у 2020 році пов'язаний із переходом на віддалену роботу під час пандемії COVID-19, що показує, що зміни у технологіях і форматі роботи можуть суттєво впливати на безпеку даних, потребуючи адаптації стратегій захисту.

Таким чином, питання захисту неструктурованої інформації на мобільних пристроях стає дедалі актуальнішим через зростання кількості загроз. Це зумовлює необхідність впровадження сучасних технологій безпеки. Для ефективного захисту слід застосовувати комплексний підхід, який включає передові криптографічні методи, адаптивні механізми безпеки та дотримання міжнародних стандартів. Такий підхід дозволить мінімізувати ризики витоку даних та підвищити рівень захисту мобільних платформ у сучасному цифровому середовищі.

Методи захисту інформації: прогнозування загроз, шифрування та біометрична автентифікація.

У нашому випадку методи захисту інформації засновувалися на засадах інтеграційного машинного навчання, математичних моделей прогнозування загроз, алгоритмів шифрування та багатофакторної автентифікації. Аспекти захисту: моніторинг, адаптація, прогнозування загроз, прийняття рішень, шифрування та біометрична автентифікація. Кожен етап включає підхід із використанням формул і відповідних алгоритмів.

На першому етапі застосовувався метод адаптивного моніторингу стану системи, який передбачає, що моніторинг є основою адаптації, тому що зміна стану системи впливає на реакцію системи захисту. Математично така методологія набуває такого алгоритмічного вигляду:

Стан системи описується вектором (1.1.):

$$S(t) = \left[s1(t), s2(t), \ldots, sn\ (t) \right], \tag{1.1}$$

де $s1(t), s2(t), ..., sn(t)$ – параметри, що характеризують певний аспект (активність мережі, стан програмного забезпечення, місцезнаходження тощо);

На оптимізаційному рівні для прогнозування загроз застосовувалися засади машинного навчання, зокрема метод рекурентних нейронних мереж (RNN), для прогнозування виникнення потенційних атак. У цьому разі прогнозування можливості появи загроз розраховувалось згідно з (1.2):

$$h_t = f\left(W_x x_t + W_h h_{t-1} + b\right), \tag{1.2}$$

де h_t – приховані стани в момент часу t; x_t – вхідні дані про стан системи, W_x, W_h – ваги мережі, b – зсув.

Натомість прогноз активації загрози реалізувався згідно з виразом (1.3):

$$y_{t+1} = g\left(W_o h_t + b_0\right), \tag{1.3}$$

де y_{t+1} – прогнозовані загрози, g – активаційна функція.

На другому етапі проводились дослідження на базі застосування засад методу прийняття рішень, у відповідності до якого передбачається, що на основі моніторингу системи адаптивна система захисту повинна приймати рішення щодо вжиття певних заходів безпеки. Згідно із вищевказаним методом оптимізаційна задача прийняття рішень формується як вираз (1.4.):

$$\mathrm{A}^*(t) = \arg\min_{A} \mathrm{E}\left[C(\mathrm{A}, \mathrm{M}(t), \mathrm{Z}(t))\right], \tag{1.4}$$

де A – набір можливих дій, $C(\mathrm{A}, \mathrm{M}(t), \mathrm{Z}(t))$ – функція вартості виконання дії A при поточному стані системи $\mathrm{M}(t)$ і загрозах $\mathrm{Z}(t)$.

На третьому етапі досліджувалась адаптація, яка є основним складником системи, котра дозволяє захисту пристосовуватися до змін середовища та загроз. Математично механізм адаптації можна описати таким чином:

– Адаптація рівня шифрування залежно від загроз (1.5):

$$E_{enc}(t) = f(\mathrm{Z}(t)), \tag{1.5}$$

де $E_{enc}(t)$ – рівень шифрування в момент часу t, a $f(\mathrm{Z}(t))$ – функція, що визначає ступінь шифрування залежно від загроз.

– Адаптація доступу до ресурсів (1.6.):

$$P_{access(t)} = \mathrm{g}(\mathrm{M}(\mathrm{t})), \tag{1.6}$$

де $P_{access(t)}(t)$ – ймовірність доступу до певного ресурсу, яка залежить від поточного стану системи $\mathrm{M}(\mathrm{t})$.

Адаптивна зміна ключа шифрування залежно від часу має вигляд виразу (1.7):

$$\mathrm{K}(t) = h(\mathrm{Z}(t)), \tag{1.7}$$

де $h(\mathrm{Z}(t))$ – функція зміни ключа залежно від рівня загроз.

Використання мультифакторного шифрування математично можна записати у вигляді виразу (1.8.):

$$C = \mathrm{E}(\mathrm{M}, \mathrm{K}_1(t), \mathrm{K}_2(t), ..., \mathrm{K}_n(t)), \tag{1.8}$$

де $\mathrm{K}_1(t), \mathrm{K}_2(t), ..., \mathrm{K}_n(t)$ – набір ключів, що змінюються залежно від стану системи.

На четвертому етапі досліджень застосовувалися засади методу біометричної автентифікації.

– Імовірність успішної автентифікації через біометрію (1.9):

$$\mathrm{P}_{auth}(\mathrm{B}, t) = \frac{1}{1 + e^{-\theta \cdot (\mathrm{B} - \mathrm{B}_{th})}}, \tag{1.9}$$

де B – біометричний параметр (відбиток пальця, обличчя тощо), B_{th} – порогове значення, а θ – коефіцієнт чутливості.

$$\mathrm{P}_{auth}(\mathrm{B}, t) = \frac{1}{1 + e^{-\theta \cdot (\mathrm{B} - \mathrm{B}_{th})}}, \tag{1.9.}$$

де B – біометричний параметр (відбиток пальця, обличчя тощо), B_{th} – порогове значення, а θ – коефіцієнт чутливості.

З огляду на те, що прогнозування загроз є важливою частиною адаптивної системи і становить суттєву різноманітність загроз під час проведення досліджень вирішено додатково застосовувати ще декілька моделей прогнозування, використовується машинне навчання для прогнозування можливих атак, а саме:

Модель на основі логістичної регресії для прогнозування ймовірності загрози (1.10):

$$\mathrm{P}(\mathrm{Z}|\mathrm{M}(t)) = \frac{1}{1+e^{-\beta_0-\sum_{i=1}^{n}\beta_i s_i(t)}}, \quad (1.10)$$

де $\beta_0, \beta_1, ..., \beta_n$ – параметри моделі.

– Використання адаптованих рекурентних нейронних мереж для довгострокового прогнозування (1.11):

$$h_t = \sigma(W_h h_{t-1} + W_x X_t), \quad (1.11)$$

де h_t – приховані стани мережі, X_t – вхідні дані (стан системи), W_h та W_x – ваги мережі.

У такому випадку передбачається використання машинного навчання (ML), котре дозволяє значно покращити точність прогнозування, що зменшує час на реакцію системи безпеки і дозволяє виявляти потенційні атаки.

Далі наведемо математичний опис застосованого в дослідженні методу багатофакторної автентифікації (MFA), який застосовували для вищого рівня безпеки шляхом використання кількох незалежних методів для підтвердження особи користувача.

У відповідності до MFA модель успішної автентифікації визначає ймовірність успішної автентифікації P_{auth} через n -факторну систему автентифікації (1.12):

$$P_{auth}(t) = \prod_{i-1}^{n} \mathrm{P}_i(t), \quad (1.12)$$

де $\mathrm{P}_i(t)$ – ймовірність успішної автентифікації для кожного з n факторів.

Також у MFA застосовується модель для кожного фактора.

Загальна ймовірність успішної атаки розраховується згідно з (1.13):

$$P_{attack}(t) = 1 - P_{auth}(t), \quad (1.13)$$

що демонструє, як збільшення кількості факторів значно зменшує ймовірність успішної атаки.

На п'ятому етапі в рамках дослідження передбачалося також застосувати засади методів на базі використання блокчейн-технологій. Наведемо математичний опис використання блокчейн-технологій.

Збереження даних у блоках: кожен блок містить хеш попереднього блоку і нові дані (1.14):

$$H(B_i) = Hash(B_{i-1,} M_1), \quad (1.14)$$

де $H(B_i)$ – хеш блоку $B_{i,} B_{i-1}$ – попередній блок, а M_i – нові дані.

У межах дослідження в нашому випадку очікується, що запропоновані рішення, такі як багатофакторна автентифікація, прогнозування загроз з використанням ML, квантово-стійкі алгоритми та блокчейн, забезпечують значне підвищення рівня захисту інформації на мобільних пристроях.

Виконання досліджень

Дослідження проводилося на основі моделювання сценаріїв із різними рівнями загроз та використанням захисних механізмів, таких як багатофакторна автентифікація, VPN, апаратне шифрування та прогнозування загроз на базі машинного навчання. Залучено 10 мобільних пристроїв у кейс-менеджмент системі, що працювали з неструктурованими даними (документи, зображення, відео).

Сценарії дослідження:

– Сценарій 1: Низький рівень загрози, звичайна передача даних без прогнозування загроз.

– Сценарій 2: Середній рівень загрози, використання VPN для захисту передачі даних.

– Сценарій 3: Високий рівень загрози, активація машинного навчання для прогнозування загроз і автоматичне посилення шифрування та доступу.

– Сценарій 4: Виявлення атаки «людина посередині» під час передачі даних, динамічна реакція та оновлення ключів VPN.

– Сценарій 5: Підключення через незахищену мережу, автоматичне блокування доступу до даних.

Основними параметрами оцінювання стали швидкість передачі даних, час автентифікації, реакція системи на загрози та споживання ресурсів пристрою. В ході експериментів встановлено, що впровадження адаптивного поведінкового підходу дозволяє ефективніше прогнозувати загрози та динамічно змінювати рівень захисту, забезпечуючи баланс між безпекою та продуктивністю мобільного пристрою.

На рис. 1 представлено результати дослідження захисту інформації на мобільних пристроях згідно зі сценаріями.

З графіків на рис. 1 видно, що:

– швидкість передачі даних (Мбіт/с) зменшується зі збільшенням рівня загроз;

– час автентифікації (с) зростає у складніших сценаріях безпеки;

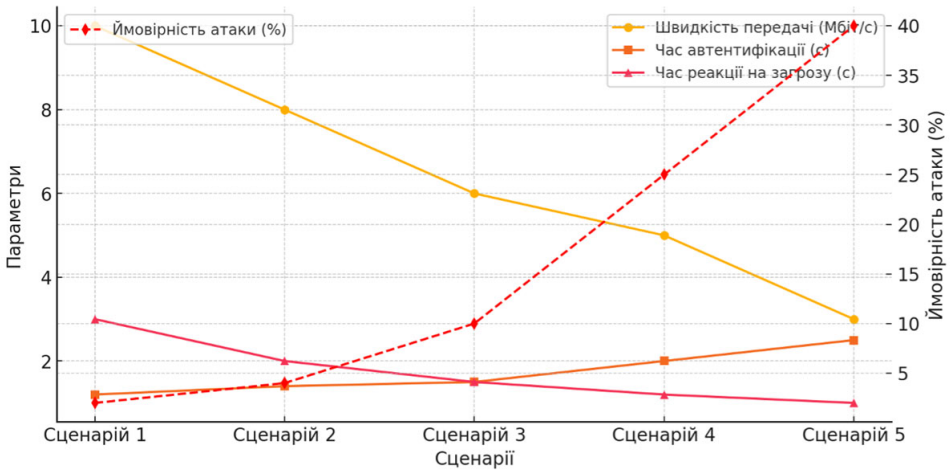

Рис. 1. Сценарії захисту на мобільних пристроях

– час реакції на загрозу (с) зменшується у випадках активного захисту;
– ймовірність атаки (%) значно зростає у сценаріях з вищим рівнем загроз.

Результати

У ході дослідження розроблено та апробовано методи захисту інформації на мобільних пристроях на основі адаптивної поведінкової моделі. Дослідження підтвердило ефективність поєднання алгоритмів машинного навчання, математичних моделей прогнозування загроз, криптографічних методів та багатофакторної автентифікації.

Запропонований підхід включає аналіз поведінки користувачів (UBA), що дозволяє відстежувати та аналізувати шаблони взаємодії з мобільними пристроями. Виявлення аномалій у реальному часі забезпечує ідентифікацію потенційних загроз через застосування алгоритмів кластеризації, нейронних мереж та статистичних методів.

Розроблені контекстно-залежні політики безпеки дозволяють адаптувати протоколи захисту залежно від умов використання пристрою, таких як місцезнаходження, мережеве середовище та час доступу. Впровадження адаптивних механізмів автентифікації на основі поведінкових біометричних характеристик, зокрема динаміки набору тексту та сенсорних даних, сприяє безперервному контролю автентичності користувачів.

Дослідження продемонструвало, що застосування моделей машинного навчання, таких як рекурентні нейронні мережі (RNN) та LSTM, підвищує точність прогнозування загроз та дозволяє виявляти потенційно небезпечні дії ще до їх реалізації.

Результати експериментального аналізу показали, що запропонований метод забезпечує високий рівень безпеки мобільних пристроїв, дозволяючи системам динамічно адаптуватися до змін у поведінці користувачів та ефективно запобігати потенційним загрозам.

Обговорення

Основними перевагами методу є підвищена точність і надійність автентифікації, а також можливість раннього виявлення загроз. Водночас серед викликів залишається необхідність оптимізації обчислювальних ресурсів та зменшення хибнопозитивних спрацьовувань.

Перспективи подальших досліджень

Подальші дослідження зосереджені на вдосконаленні адаптивної поведінкової моделі шляхом інтеграції глибокого навчання та розширення набору поведінкових параметрів. Також перспективним є оптимізація алгоритмів шифрування для мобільних пристроїв і впровадження контекстно-орієнтованих механізмів безпеки.

Висновки

Результати дослідження показали, що адаптивний захист є перспективним підходом у захисті мобільних пристроїв. Він передбачає застосування заходів захисту, що змінюються залежно від динамічного контексту користувача і його середовища, наприклад, залежно від локації, часу доби, стану пристрою та специфіки взаємодії. Майбутнє захисту інформації на мобільних пристроях залежатиме від інтеграції штучного інтелекту, машинного навчання та вдосконалення біометричної автентифікації. Використання адаптивних моделей дозволить ефективно виявляти загрози та реагувати на аномальну поведінку користувачів у реальному часі. Блокчейн та квантово-стійке шифрування сприятимуть підвищенню безпеки даних, а концепція «приватності за замовчуванням» гарантуватиме інтеграцію кібербезпеки на всіх етапах розробки. Комплексний підхід, що поєднує технологічні рішення, підвищення обізнаності користувачів та нормативне регулювання, стане ключем до ефективного захисту мобільної інформації.

Література

1. Брегін Ю. І. Системи біометричної аутентифікації особи для мобільних пристроїв : автореф. ELARTU – Інституційний репозиторій ТНТУ імені Івана Пулюя. 2018. URL: http://elartu.tntu.edu.ua/handle/lib/23585.

2. Бровченко Є. М. Адаптивний захист інформації на мобільному пристрої. 2023 International Conference on Innovative Solutions in Software Engineering (ICISSE), Vasyl Stefanyk Precarpathian National University, Ivano-Frankivsk, Ukraine, Nov. 29–30, 2023, pp. 8–24. DOI: https://doi.org/10.5281/zenodo.10397356.

3. Карпачев І. І. Інформаційна технологія забезпечення функціональної безпеки мобільних пристроїв : автореф. дис. ... канд. техн. наук : 05.13.06. Чернігів. Електронний архів Чернігівського національного технологічного університету (IRChNUT). 2021. URL: http://ir.stu.cn.ua/123456789/24245.

4. Метик А. В., Сєвєрінов О. В. Аналіз загроз безпеки в системах безконтактної передачі даних. *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління :* тези доповідей XI міжнародної науково-технічної конференції, 8–9 квітня 2021 р. ВА ЗС АР; НТУ «ХПІ»; НАУ, ДП «ПДПРОНДІАВІАПРОМ»; УмЖ. Електронний архів відкритого доступу Харківського національного університету радіоелектроніки. 2021. URL: https://openarchive.nure.ua/handle/document/15762.

5. Мороз А. С., Петренко О. Є. Засоби захисту інформації на основі нейронних мереж. *Проблеми інформатизації* : тези доповідей VIII Міжнародної науково-технічної конференції, 26–27.11.2020. НТУ «ХПІ». Електронний архів відкритого доступу Харківського національного університету радіоелектроніки. 2020. URL: http://openarchive.nure.ua/handle/document/14291.

6. Dharminder C., Anushaa S. S., Naundhini S., & Durgarao M. S. P. A novel post-quantum piekert's reconciliation-based forward secure authentication key agreement for mobile devices. *Communication and intelligent systems*, 2023. Pp. 101–110. Springer Nature Singapore. https://doi.org/10.1007/978-981-99-2100-3_9.

7. Kret T. Approaches to threat modeling in the creation of a comprehensive information security system for a multi-level intelligent control systems. *Computer Systems and Network*, 2024. 6(1), 81–88. https://doi.org/10.23939/csn2024.01.081.

8. Mobile devices. Encyclopedia of education and information technologies. Springer International Publishing. 2020. 1160 p. https://doi.org/10.1007/978-3-030-10576-1_300442.

9. Retracted: Infrastructure smart service system based on big data information system. *Mobile Information Systems*, 2022, 1. https://doi.org/10.1155/2022/9879217.

10. Yang, Y., Huang X., Guo Y., & Sun J. S. Dynamic multi-level privilege control in behavior-based implicit authentication systems leveraging mobile devices. 2020 IEEE 17th International conference on mobile ad hoc and sensor systems (MASS). IEEE. 2020. https://doi.org/10.1109/mass50613.2020.00037.

References

1. Brehin, Yu. I. (2018). Biometric person authentication systems for mobile devices: Thesis Abstract. ELARTU – Institutional repository of TNTU named after Ivan Pulyuy. Retrieved from: http://elartu.tntu.edu.ua/handle/lib/23585.

2. Brovchenko, E. M. (2023). "Adaptive information protection on a mobile device," 2023 International Conference on Innovative Solutions in Software Engineering (ICISSE). Vasyl Stefanyk Precarpathian National University, Ivano-Frankivsk, Ukraine, Nov. 29–30, 2023, pp. 8–24. https://doi.org/10.5281/zenodo.10397356.

3. Karpachev, I. I. (2021). Information technology for ensuring functional security of mobile devices: candidate's thesis. Chernihiv. Electronic archive of the Chernihiv National University of Technology (IRChNUT). Retrieved from: http://ir.stu.cn.ua/123456789/24245.

4. Metik, A. V., & Severinov, O. V. (2021). Analysis of security threats in contactless data transmission systems. *Suchasni napryamy rozvytku informatsiyno-komunikatsiynyh tehnologiy ta zasobiv upravlinnya*: tezy dopovidey XI mizhnarodnoyi naukovo-tehnicnoyi konferentciyi, 8–9 kvitnya 2021 r. VA ZS AR; NTU "KhPI"; NAU, SE "PDPRONDIAVIAPROM"; UmJ. Electronic archive of the Kharkiv National University of Radioelectronics. Retrieved from: https://openarchive.nure.ua/handle/document/15762.

5. Moroz, A. S., & Petrenko, O. E. (2020). Features of information protection based on neural measurements: Thesis, NTU "KhPI". Electronic archive of the Kharkiv National University of Radioelectronics. Retrieved from: http://openarchive.nure.ua/handle/document/14291.

6. Dharminder, C., Anushaa, S. S., Naundhini, S., & Durgarao, M. S. P. (2023). A novel post-quantum piekert's reconciliation-based forward secure authentication key agreement for mobile devices. Communication and intelligent systems. Pp. 101–110. Springer Nature Singapore. https://doi.org/10.1007/978-981-99-2100-3_9.

7. Kret, T. (2024). Approaches to threat modeling in the creation of a comprehensive information security system for a multi-level intelligent control systems. *Computer Systems and Network*, 6(1), 81–88. https://doi.org/10.23939/csn2024.01.081.

8. Mobile devices. (2020). Encyclopedia of education and information technologies. 1160 p. Springer International Publishing. https://doi.org/10.1007/978-3-030-10576-1_300442.

9. Retracted: Infrastructure smart service system based on big data information system. *Mobile Information Systems*, 2022, 1. https://doi.org/10.1155/2022/9879217.

10. Yang, Y., Huang, X., Guo, Y., & Sun, J. S. (2020). Dynamic multi-level privilege control in behavior-based implicit authentication systems leveraging mobile devices. 2020 IEEE 17th International conference on mobile ad hoc and sensor systems (MASS). IEEE. https://doi.org/10.1109/mass50613.2020.00037.