https://www.sworldjournal.com/index.php/swj/article/view/swj31-01-013
DOI: 10.30888/2663-5712.2025-31-01-013

УДК 004.5

A CONCEPTUAL MODEL FOR BALANCE BENWEEN SECURITY AND USABILITY IN SOFTMARE

КОНЦЕПТУАЛЬНА МОДЕЛЬ ДЛЯ БАЛАНСУ МІЖ БЕЗПЕКОЮ ТА ЗРУЧНІСТЮ ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Krykhivskyi M.V. / Крихівський М.В.
c.t.s., assoc. prof. / к.т.н., доц.
ORCID: 0009-0000-3285-4308
Ivano-Frankivsk National Technical University of Oil and Gas,
Ivano-Frankivsk, Karpatska, 15, 76019
Івано-Франківський національний технічний університет нафти і газу,
м. Івано-Франківськ, вул. Карпатська, 15, 76019

Анотація. *В статті представлено концепцію динамічної моделі багаторівневої автентифікації (DMAA), яка пропонує інноваційний підхід до забезпечення безпеки користувачів у цифровому середовищі. Автор досліджує проблеми традиційних методів автентифікації, що часто вимагають компромісу між рівнем захисту та зручністю використання. Запропонована модель базується на поєднанні поведінкового аналізу користувача, контекстної оцінки ризиків, адаптивної багаторівневої перевірки та механізмів інтерактивного навчання для створення персоналізованої системи автентифікації.*

DMAA використовує нейронні мережі для аналізу поведінкових патернів, таких як динаміка введення пароля, характерні рухи миші та стиль взаємодії з інтерфейсом. На основі отриманих даних система формує детальний профіль користувача і застосовує алгоритми машинного навчання для виявлення аномалій, що можуть сигналізувати про потенційні загрози. Важливим аспектом моделі є контекстна оцінка ризиків, яка враховує змінні параметри, такі як місцезнаходження, тип пристрою, мережеві умови та час доби. Використання Байєсівських мереж і Марковських процесів дозволяє прогнозувати ймовірність загроз на основі аналізу послідовності дій користувача.

Особливістю моделі є персоналізований рівень захисту, який динамічно коригується залежно від оціненого рівня ризику. У разі виявлення аномальних дій або збільшення ймовірності загрози система може автоматично змінювати спосіб автентифікації, наприклад, переходячи від стандартного входу з паролем до багатофакторної автентифікації із залученням біометричних даних. Крім того, застосування генетичних алгоритмів дозволяє оптимізувати параметри безпеки для зменшення кількості хибних спрацьовувань.

DMAA також має механізм інтерактивного адаптивного навчання, що покращує точність розпізнавання користувачів на основі історичних даних. Це дозволяє системі ефективніше реагувати на зміну поведінки користувача, мінімізуючи ризики та підвищуючи загальний рівень захисту. Нечітка логіка використовується для аналізу ситуацій із невизначеними ризиками, що сприяє гнучкому підходу до автентифікації без надмірної жорсткості системи. Крім того, важливим компонентом є зворотний зв'язок із користувачем, який дозволяє інформувати його про потенційні загрози та рекомендувати додаткові заходи безпеки.

Запропонована динамічна модель багаторівневої автентифікації є значним кроком у розвитку систем захисту цифрових платформ, оскільки поєднує високий рівень безпеки з комфортною взаємодією користувача. Її впровадження дозволить значно зменшити ризики несанкціонованого доступу, зберігаючи водночас високу ефективність та зручність

використання. Ця модель буде корисною для розробників програмного забезпечення, спеціалістів із кібербезпеки та аналітиків UX-дизайну, які прагнуть створити більш захищені та гнучкі системи автентифікації.

Ключові слова: *інформаційна безпека, зручність програмного забезпечення, динамічна модель, автентифікація.*

Вступ.

Сучасні тенденції в кібербезпеці значно впливають на процес створення програмного забезпечення (ПЗ), яке має бути зручним та доступним для всіх користувачів (юзабіліті) та надавати простоту навігації, швидке завантаження сторінок, інтуїтивно зрозумілий інтерфейс. Тому виникають нові завдання, оскільки розробники прагнуть знайти баланс між захистом даних і зручністю використання.

Однією з ключових тенденцій є зростання використання штучного інтелекту (ШІ) для аналізу поведінки користувачів. Ці системи дозволяють виявляти аномалії в режимі реального часу, що може свідчити про потенційні загрози. Водночас, такі технології можуть адаптувати рівень безпеки залежно від поведінки користувача, знижуючи бар'єри для звичайних дій і посилюючи захист у разі підозрілої активності.

Іншою важливою тенденцією є впровадження багатофакторної автентифікації, яка стає стандартом для багатьох додатків. Хоча це підвищує рівень безпеки, водночас також можуть створюватись певні незручності для користувачів, якщо процес автентифікації не є інтуїтивно зрозумілим. Для вирішення цієї проблеми розробники активно працюють над спрощенням таких процесів, наприклад, через використання біометричних даних або одноразових кодів.

Зростання популярності хмарних технологій також впливає на кібербезпеку та юзабіліті. Хмарні сервіси забезпечують високий рівень захисту даних, але водночас вимагають від користувачів розуміння принципів безпечного доступу. Це стимулює розробку інтуїтивно зрозумілих інтерфейсів, які допомагають користувачам легко орієнтуватися в налаштуваннях безпеки.

Крім того, дедалі більше уваги приділяється захисту конфіденційності даних. Нові регуляторні вимоги, такі як GDPR, змушують компанії

впроваджувати прозорі механізми збору та обробки даних. Це впливає на дизайн додатків, оскільки користувачі повинні мати змогу легко керувати своїми даними, що вимагає створення зручних і зрозумілих інструментів.

Загалом, сучасні тенденції в кібербезпеці спрямовані на інтеграцію передових технологій, які забезпечують високий рівень захисту, не жертвуючи зручністю використання. Це створює нові виклики для розробників, але водночас відкриває можливості для інновацій у дизайні та функціональності додатків.

Основний текст.

Рекомендації щодо засобів контролю інформаційної безпеки, кібербезпеки та захисту конфіденційності надає міжнародний стандарт ISO/IEC 27002:2022 [1]. Його основною метою є допомога організаціям впроваджувати надійні механізми безпеки, які не лише захищають дані, але й сприяють зручності користувачів. Це особливо важливо у контексті розробки програмного забезпечення, де необхідно знайти баланс між строгими заходами кіберзахисту та комфортним користувацьким досвідом. Стандарт охоплює такі аспекти, як управління доступом, криптографія, безпека персоналу, реагування на інциденти та захист комунікацій.

Міжнародним стандартом, який визначає основні принципи зручності (юзабіліті) та його застосування в інтерактивних системах є ISO 9241-11:2018 Ергономіка взаємодії людина-система [2]. Він пояснює, що юзабіліті – це не просто характеристика продукту, а результат його використання в конкретному контексті. Стандарт надає визначення ключових термінів, таких як ефективність, продуктивність та задоволеність користувача, і пояснює, як ці фактори впливають на загальну якість взаємодії.

ISO 9241-11:2018 допомагає розробникам, дизайнерам та організаціям оцінювати юзабіліті своїх продуктів, враховуючи реальні умови використання. Він не містить конкретних методів розробки, але пропонує загальну концепцію, яка може бути застосована до різних типів систем, включаючи програмне забезпечення, веб-додатки та фізичні пристрої. Цей стандарт є важливим для забезпечення зручності користувачів, оскільки він дозволяє компаніям

створювати продукти, які не лише відповідають технічним вимогам, а й забезпечують комфортну та ефективну взаємодію. Він був підтверджений у 2023 році, що свідчить про його актуальність у сучасному цифровому середовищі.

Фундаментом для багатьох досліджень, що окреслює основні принципи впровадження заходів безпеки у життєвий цикл розробки інформаційних систем слугує робота [2]. Вона присвячена компонентам інформаційної безпеки життєвого циклу розробки системи (SDLC) Зокрема, розглядаються стратегії для зменшення ризиків, пов'язаних із загрозами, при цьому підкреслюється важливість інтеграції заходів безпеки ще на етапі формування вимог. Це дозволяє будувати системи, що відповідають жорстким вимогам безпеки, але розроблені з урахуванням зручності для користувачів і доступності.

Авторами роботи [3], що опублікована Національним інститутом стандартів і технологій (NIST), розглядається важливість інтеграції заходів безпеки на всіх етапах життєвого циклу розробки системи. Вони наголошують, що безпека повинна бути невід'ємною частиною процесу, починаючи з ініціації проєкту, аналізу вимог, проєктування, реалізації, тестування та експлуатації. Підкреслюється необхідність врахування ризиків та впровадження відповідних механізмів захисту ще на ранніх стадіях розробки, що дозволяє зменшити витрати на усунення вразливостей у майбутньому.

Документ також визначає ключові ролі та відповідальність учасників процесу, включаючи розробників, адміністраторів та керівників проєктів, які повинні забезпечувати відповідність системи вимогам безпеки. Особливу увагу приділено питанням управління ризиками, оцінці загроз та вибору відповідних заходів захисту. Робота містить рекомендації щодо застосування стандартів безпеки та методологій, які допомагають організаціям ефективно інтегрувати безпеку у свої процеси розробки.

У оглядовій статті [4] досліджені публікації про інтеграцію безпекових вимог в розробку програмного забезпечення Розглянуті методи або моделі, що придатні для інтеграції безпеки на всіх або деяких фазах життєвого циклу розробки програмного забезпечення, та досліджено, які з них найбільше

розглядаються або ігноруються. Автори зробили огляд для початку створення методології, яка інтегруватиме методи безпеки в гнучку розробку програмного забезпечення, що дозволить недосвідченим розробникам створювати більш безпечні програми. Вони виділяють новий безпечний життєвий цикл розробки програмного забезпечення (S-SDLC), який вирішує питання безпеки під час розробки програмного забезпечення; модель зрілості безпеки програмного забезпечення (SAMM), що є відкритою методологією, яка дозволяє реалізацію стратегії покращення безпеки програмного забезпечення; процес життєвого циклу розробки безпечного програмного забезпечення Макгроу (McGraw SDLC), який передбачає сім точок дотику; правильність за конструкцією (CbyC) є методологією, яка спрямована на мінімізацію рівня дефектів і підвищення стійкості до змін; модель ViewNext, що є гнучкою адаптацією S-SDLC, яка включає в себе найкращі методи безпеки з відомих моделей разом з іншими завданнями безпеки, заснованими на спіральній моделі, інтегровані в звичайні життєві цикли розробки програмного забезпечення; Microsoft SDL Agile, що є адаптація методології SDL (Security Development Lifecycle), яка зосереджена на інтеграції безпеки в кожну ітерацію процесу гнучкої розробки програмного забезпечення; модель зрілості безпеки Building Security In Maturity Model (BSIMM), яка використовується для опису практик і процесів провідними організаціями безпеки програмного забезпечення для розробки, вдосконалення та підтримки ефективних програм безпеки програмного забезпечення. BSIMM зосереджується на оцінці програм безпеки програмного забезпечення організацій шляхом вимірювання їх зрілості за 12 поширеними методами безпеки.

У дослідженні [5] розглядаються сценарії атак, які можуть вплинути на безпеку програмного забезпечення. Автор наголошує, що компанії повинні не лише впроваджувати DevSecOps, а й активно захищати свої конвеєри розробки від потенційних атак. Він в результаті аналізу загроз, пов’язаних з використанням DevSecOps, доводить, що сам факт впровадження DevSecOps не гарантує безпеку.

Досягнення балансу між кібербезпекою та юзабіліті вимагає комплексного підходу, що враховує як технічні, так і поведінкові аспекти взаємодії користувачів із системами. Одним із ключових підходів є використання адаптивної автентифікації, яка змінює рівень перевірки залежно від контексту.

У концептуальній моделі пропонується застосовувати кілька математичних моделей. **Динамічна модель багаторівневої автентифікації (DMAA):**

1. Поведінковий аналіз користувача

- Використання нейронних мереж для аналізу патернів поведінки (динаміка введення пароля, рухи миші, взаємодія з інтерфейсом).
- Машинне навчання для побудови профілю користувача та розпізнавання аномалій.
- Збір даних у режимі реального часу для аналізу стилю роботи користувача.

2. Контекстна оцінка ризиків

- Врахування факторів, таких як місцезнаходження, пристрій, мережеві умови, час доби.
- Байєсівські мережі для прогнозування ймовірності ризику.
- Використання Марковських процесів для аналізу послідовності дій користувача.

3. Персоналізований рівень захисту

- Динамічне коригування рівня автентифікації: від однофакторної до багатофакторної автентифікації залежно від рівня ризику.
- Використання біометричних даних (відбитки пальців, розпізнавання обличчя) при виявленні потенційної загрози.
- Генетичні алгоритми для оптимізації параметрів захисту.

4. Інтерактивна адаптація

- Система самонавчання та покращення точності на основі історичних даних.
- Використання нечіткої логіки для аналізу ситуацій з невизначеними ризиками.

- Зворотний зв'язок із користувачем (наприклад, повідомлення про потенційні загрози).

Ця модель дозволяє створити гнучку та адаптивну систему, яка враховує індивідуальні особливості, поточний контекст та динамічно налаштовує рівень захисту без надмірного ускладнення процесу автентифікації.

Висновки.

У дослідженні представлено концептуальну модель, яка спрямована на досягнення оптимального балансу між безпекою та зручністю програмного забезпечення. Вона враховує ключові аспекти взаємодії користувача з програмним забезпеченням, аналізує ризики та пропонує оптимізовані рішення для гармонійного поєднання безпекових заходів і зручності використання. Основні принципи моделі ґрунтуються на адаптивності та гнучкості, що дозволяє регулювати рівень захисту відповідно до потреб і контексту використання. Окрім цього, модель сприяє розробці інтуїтивно зрозумілих інтерфейсів і мінімізації бар'єрів у взаємодії користувача із захисними механізмами. Запропонований підхід може слугувати основою для подальших досліджень у сфері кібербезпеки та розробки програмних продуктів із більшою орієнтацією на баланс між захистом і зручністю. У перспективі це сприятиме підвищенню рівня довіри користувачів до програмного забезпечення, забезпечуючи його ефективність та безпеку без зайвого ускладнення.

Література.

1. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. URL: https://www.iso.org/standard/75652.html#lifecycle

2. ISO 9241-11:2018 Ergonomics of human-system interaction. URL: https://www.iso.org/standard/63500.html

3. Kissel R., Stine R., Scholl M., Rossman H., Fahlsing J., Gulick J. Security Considerations in the System Development Life Cycle. NIST, 2019. C. 44. URL: https://doi.org/10.6028/NIST.SP.800-64r2

4. Valdés-Rodríguez Y., Hochstetter-Diez J., Díaz-Arancibia J., Cadena-Martínez R. Towards the Integration of Security Practices in Agile Software Development: A Systematic Mapping Review. MDPI 13(7) 4578, 2023. URL: https://doi.org/10.3390/app13074578

5. Pecka N. S. Making Secure Software Insecure without Changing Its Code: The Possibilities and Impacts of Attacks on the DevOps Pipeline. Ph.D. Thesis, Iowa State University, Ames, IA, USA, 2022. URL: https://doi.org/10.48550/arXiv.2201.12879

Abstract. *The article presents the concept of a Dynamic Multi-Level Authentication Model (DMAA), which offers an innovative approach to ensuring user security in a digital environment. The author explores the challenges of traditional authentication methods, which often require a compromise between security levels and ease of use. The proposed model is based on a combination of user behavior analysis, contextual risk assessment, adaptive multi-level verification, and interactive learning mechanisms to create a personalized authentication system.*

DMAA utilizes neural networks to analyze behavioral patterns such as password entry dynamics, characteristic mouse movements, and interaction style with the interface. Based on the obtained data, the system creates a detailed user profile and applies machine learning algorithms to detect anomalies that may signal potential threats. An essential aspect of the model is contextual risk assessment, which considers variable parameters such as location, device type, network conditions, and time of day. The use of Bayesian networks and Markov processes enables the prediction of threat probability based on the analysis of the user's action sequence.

A distinctive feature of the model is its personalized security level, which dynamically adjusts based on the assessed risk level. If abnormal actions are detected or the probability of a threat increases, the system can automatically modify the authentication method, for example, shifting from standard password login to multi-factor authentication with biometric data. Additionally, the use of genetic algorithms helps optimize security parameters to reduce the number of false positives.

DMAA also features an interactive adaptive learning mechanism that enhances the accuracy of user recognition based on historical data. This enables the system to respond more effectively to changes in user behavior, minimizing risks and improving overall security levels. Fuzzy logic is used to analyze situations with uncertain risks, allowing for a flexible authentication approach without excessive system rigidity. Additionally, an important component is user feedback, which helps inform users about potential threats and recommends additional security measures.

The proposed dynamic multi-level authentication model represents a significant advancement in the protection of digital platforms, as it combines a high level of security with a seamless user experience. Its implementation will substantially reduce the risks of unauthorized access while maintaining high efficiency and usability. This model will be valuable for software developers, cybersecurity specialists, and UX design analysts striving to create more secure and flexible authentication systems.

Key words: *information security, software usability, dynamic model, authentication.*

Статья отправлена: 02.05.2025 г.