УДК 004.056:159.923.2
DOI: https://doi.org/ 10.17721/3041-2323.2024.263-285

Валентина ПЛЕСКАЧ[1], д-р екон. наук, проф.
ORCID ID: 0000-0003-0552-0972
e-mail: v_pleskach@ukr.net

Ірма ШИЛЕЙКЕНЕ[2], д-р техн. наук, доц.
ORCID ID: 0000-0002-1185-0970
e-mail: irma.sileikiene@vilniustech.lt

Романас ТУМАСОНІС[3], д-р техн. наук, доц.
ORCID ID: 0000-0002-8921-0674
e-mail: r.tumasonis@eif.viko.lt

Євгеній ТОПОЛЬСЬКОВ[1], канд. техн. наук, доц.
ORCID ID: 0000-0001-5587-3069
e-mail: y.topolskov@knu.ua

[1]Київський національний університет
імені Тараса Шевченка, Київ, Україна
[2]Вільнюський технічний університет,
Вільнюс, Литва
[3]Вільнюський університет прикладних наук
Вільнюс, Литва

АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЦИФРОВИХ РІШЕНЬ ДЛЯ БОРОТЬБИ З ПРОКРАСТИНАЦІЄЮ

Розглянуто різні системи безпеки, моделювання загроз і методи управління ризиками. Охоплюючи важливі аспекти безпеки, такі як автентифікація, конфіденційність даних, керування сеансами та відповідність міжнародним законодавчим актам, зокрема і GDPR, дослідження не лише відображає потенційні вразливості, виявлені за допомогою моделювання загроз, але і створює потужну основу для практичного впровадження функцій безпеки. Цей комплексний підхід гарантує, що прототип не лише функціональний, але й захищений від різних загроз кібербезпеці.

Ключові слова: ***інформаційна безпека, інфраструктура безпеки, вимоги до безпеки, заходи безпеки, управління ризиками.***

Вступ

Інтеграція технологій у повсякденне життя значно підвищила персональну та професійну продуктивність. Однак ця цифрова експансія також поставила користувачів перед складними викликами кібербезпеки. Програми, розроблені для підвищення продуктивності, особливо вразливі, оскільки вони часто керують великими обсягами конфіденційних даних, що робить їх основними цілями для кіберзагроз. У цьому контексті інформаційна безпека має першочергове значення, захищаючи від витоку даних, несанкціонованого доступу й інших загроз, які підривають конфіденційність і довіру користувачів. Отже, надійні заходи інформаційної безпеки є фундаментальними для збереження конфіденційності, цілісності та доступності даних.

Сучасні кіберзагрози стають дедалі складнішими через кілька головних факторів, зокрема, ускладнення методів атак, використання штучного інтелекту (ШІ), атаки на ланцюжки постачання, міжнародну кіберзлочинність, підвищену анонімність зловмисників, а головне, через новітні тенденції у розвитку новітніх технологій (Rajasekharaiah, et al., 2020) тощо. Враховуючи складність сучасних кіберзагроз, які тепер охоплюють такі передові тактики, як соціальна інженерія, програми-вимагачі та складні атаки зловмисного програмного забезпечення, цифрові рішення вимагають надійних і комплексних протоколів безпеки, а також здатності адаптуватися до швидко змінюваного ландшафту кіберризиків. Крім того, міжнародний масштаб розгортання цифрових застосунків вимагає дотримання різних законів про захист даних, таких як GDPR (EU General Data Protection Regulation, 2018) і CCPA. Це складне середовище свідчить про необхідність постійного вдосконалення стратегій безпеки для підтримки довіри користувачів і забезпечення цілісності персональних даних.

Отже, перетин рішень інформаційної безпеки та розроблення спеціалізованих програмних застосунків є важливою сферою вивчення та застосування.

Ця робота має на меті подолати розрив між розробленням застосунків і надійними практиками кібербезпеки, гарантуючи, що цифрові рішення не тільки ефективні у розв'язанні проблем поведінки людей, таких як зволікання, але й захищені від поточних і

потенційних майбутніх кіберзагроз. Тому мета цієї роботи – проаналізувати наявні межі цифрової безпеки, щоб оцінити їхню застосовність до продуктивних програм, особливо тих, які призначені для боротьби з прокрастинацією; розробити вимоги безпеки, тобто сформулювати конкретні стратегії безпеки, призначені для захисту цифрових рішень як від поточних, так і від нових кіберзагроз; застосувати ці заходи безпеки у готовому прототипному рішенні й оцінити їхню ефективність через систематичне тестування, удосконалюючи підхід на основі емпіричних результатів і відгуків користувачів.

Результати

Технологічний прогрес запропонував унікальні рішення проблем, серед яких прокрастинація є складною проблемою, що впливає на продуктивність і добробут людей. З появою цифрових рішень для розв'язання цієї проблеми неможливо переоцінити важливість упровадження надійних заходів безпеки інформації. Розроблення застосунків, призначених для пом'якшення прокрастинації через модифікацію поведінки, підкреслює необхідність гарантувати, що ці рішення не лише виконують цільове призначення, але й захищають дані та конфіденційність користувачів.

Інформаційна безпека – це практика захисту цифрових активів, таких як дані, мережі, системи та пристрої, від несанкціонованого доступу, використання, розголошення, порушення, модифікації або знищення. Вона охоплює ряд практик, технологій і процесів, призначених для захисту цифрової інформації та забезпечення конфіденційності, цілісності та доступності критично важливих ресурсів (NIST, 2012; Khidzir et al., 2018).

Важливість ISM у сучасному цифровому середовищі є багатогранною, вона стосується необхідності захисту від кіберзагроз, дотримання нормативних вимог, пом'якшення економічних і соціальних наслідків, забезпечення безпечної цифрової трансформації та підвищення довіри користувачів. Оскільки цифровий ландшафт продовжує розвиватися, роль ISM буде тільки зростати, акцентуючи на необхідності постійних інвестицій у практику, технології та навички інформаційної безпеки.

Інформаційна безпека складається з кількох ключових принципів, кожен з яких виконує окрему роль у боротьбі зі складними

загрозами та вразливими місцями в цифровому середовищі. Ці принципи охоплюють *конфіденційність, цілісність і доступність*.

Конфіденційність гарантує, що конфіденційна інформація доступна лише авторизованим особам і захищена від тих, хто не має до неї доступу. У цифрових рішеннях, особливо тих, що керують персональною продуктивністю, конфіденційність може бути забезпечена за допомогою шифрування, безпечних методів автентифікації користувачів і жорсткого контролю доступу (Al-Janabi, & Al-Shourbaji, 2021). Наприклад, цифровий затосунок, призначений для боротьби з прокрастинацією, може зберігати дані користувача, пов'язані з персональними цілями та повсякденною діяльністю, які мають бути доступні лише для користувача. Прототип буде використовувати криптографічні хеш-функції, включаючи "солоні" хеші для підвищення безпеки збережених облікових даних. "Солоні" хеші запобігають ефективному використанню зловмисниками заздалегідь обчислених таблиць для злому паролів, що значно підвищує рівень безпеки застосунку (Daisie Team, 2023). Забезпечення конфіденційності має першорядне значення не лише для довіри користувачів, але і для довіри до програми та довгострокової життєздатності. Користувачі довіряють програмним застосункам свої дані, очікуючи, що їхня інформація оброблятиметься з максимальною обачністю. Порушення конфіденційності може призвести до втрати довіри користувачів, юридичних наслідків і потенційної шкоди особам, чиї дані можуть бути розкриті. Досягнення конфіденційності вимагає комплексного підходу, що охоплює, як технічні заходи, так і організаційну політику. Методи забезпечення конфіденційності охоплюють шифрування, механізми контролю доступу та політики класифікації даних, які визначають рівні секретності, та заходи, необхідні для захисту кожного рівня класифікації.

У програмних застосунках, спрямованих на зволікання, цілісність даних є основою довіри користувачів і ефективності затосунків. Цілісність означає впевненість у тому, що інформація захищена від несанкціонованої зміни чи видалення, і що вона точно відображає оригінальний вміст, створений, переданий або збережений користувачем. Цей принцип гарантує, що дані, представлені й оброблені як користувачами, так і алгоритмами застосун-

ків, залишаються коректними стосовно першоджерел, незаплямованими корупцією чи несанкціонованими маніпуляціями. Механізми захисту цілісності охоплюють криптографічні хеш-функції, цифрові підписи та системи контролю версій. Ці заходи допомагають виявити несанкціоновані зміни, запобігти фальсифікації даних і гарантують, що дані залишаються послідовними, точними та дійсними протягом усього життєвого циклу.

Доступність має вирішальне значення для функціональності та надійності цифрових рішень. Забезпечення доступності продуктивних застосунків передбачає комплексну стратегію, яка охоплює резервування, відмовостійкість, регулярне обслуговування, планування аварійного відновлення, балансування навантаження та ретельний моніторинг. Для програм, націлених на зміну поведінки, зокрема прокрастинації, безперервна доступність тісно пов'язана зі здатністю програми ефективно підтримувати користувачів у досягненні їхніх цілей. Перебої в обслуговуванні не тільки перешкоджають прогресу користувача, але також можуть викликати розчарування та знижувати мотивацію, підриваючи мету програми.

Огляд поширених загроз безпеці. Сфера кібербезпеки безперервно розвивається, з виникненням у цьому процесі низки різноманітних і складних загроз. Ці загрози, від зловмисного програмного забезпечення до складних атак на відмову в обслуговуванні, ставлять під загрозу конфіденційність, цілісність і доступність цифрових даних.

Зловмисне програмне забезпечення становить значну загрозу, охоплюючи різні форми шкідливого програмного забезпечення, такі як віруси, хробаки та трояни. Віруси, наприклад, можуть розмножуватися та поширюватися мережами, пошкоджуючи дані та порушуючи роботу. Черви діють так само, але не потребують людських дій для розмноження, що робить їх особливо шкідливими. Трояни маскуються під законне програмне забезпечення, створюючи бекдори в безпеці, щоб сприяти подальшій незаконній діяльності. Кожен тип шкідливого програмного забезпечення може завдати великої шкоди комп'ютерним системам, скомпрометувавши як персональні, так і корпоративні дані.

Фішингові атаки використовують соціальну інженерію, щоб змусити користувачів розкрити конфіденційну інформацію. Ці атаки зазвичай відбуваються через електронну пошту, де зловмисники видають себе за діючі інституції, щоб спонукати жертв до введення персональних даних на шахрайських вебсайтах. Фішинг особливо небезпечний, оскільки він використовує вразливість людини, оминаючи багато технічних засобів захисту.

Програми-вимагачі – це певний тип шкідливого програмного забезпечення, що шифрує файли-жертви, вимагаючи плату за відновлення доступу. Ці атаки безпосередньо впливають на доступність даних і можуть призупинити бізнес-операції, що призведе до значних фінансових втрат і підриву довіри серед користувачів.

Атаки на відмову в обслуговуванні (DoS) і розподілені атаки на відмову в обслуговуванні (DDoS) порушують роботу сервісів, перевантажуючи системи потоком трафіка. DoS-атаки походять з одного джерела, тоді як DDoS-атаки поширюються на численні скомпрометовані пристрої. Ці атаки спрямовані на те, щоб зробити вебсайти та онлайн-сервіси непрацездатними, спричиняючи збої в роботі та підриваючи довіру до репутації.

Вразливості системи безпеки та їхні наслідки для продуктивних програм. Еволюція ландшафту загроз кібербезпеці також створює значні проблеми для продуктивних програм, як основних інструментів, що підтримують і персональну продуктивність, і ефективність організації. Ці програми, що охоплюють широкий спектр комунікаційних платформ для інструментів управління проєктами, слугують сховищами для величезних обсягів конфіденційних даних, що робить їх основними цілями для кіберзагроз.

Коли зловмисники маніпулюють запитами SQL, щоб отримати неавторизований доступ або змінити базу даних, наслідки можуть бути серйозними. Цей тип уразливості не тільки призводить до витоку даних, але й підриває довіру користувачів і може призвести до значних юридичних і фінансових наслідків відповідно до законів про захист даних, таких як GDPR.

Крім того, уразливості, які дозволяють зловмисникам упроваджувати шкідливі сценарії на вебсторінки, наражають користувачів на ризик крадіжки конфіденційної інформації, наприклад маркерів сеансу. У середовищах, де програми пропонують функції спільної

роботи, такі порушення безпеки можуть підірвати довіру до платформи та зменшити впевненість користувачів у безпеці їхніх даних.

Проблеми із процесами автентифікації також викликають занепокоєння. Неадекватні механізми автентифікації забезпечують легкі точки входу для зловмисників, що призводить до несанкціонованого доступу та потенційного витікання даних. Наслідки виходять за межі цілісності даних, впливаючи на доступ користувачів і загальну надійність програми. Ці збої особливо шкідливі для застосунків, які щодня покладаються на персональне керування та продуктивність, безпосередньо впливаючи на задоволеність користувачів і довіру.

Розкриття конфіденційних даних через незахищені API або недосконалі методи шифрування може привернути значну увагу регуляторів, що призведе до великих штрафів і шкоди репутації організації. Крім того, збої в роботі через такі атаки, як DDoS, не лише погіршують якість обслуговування, але також можуть призвести до значних простоїв, розчаровуючи користувачів і ставлячи під загрозу ефективність програми.

Щоб розв'язати ці проблеми, критично важливо застосувати підхід безпеки протягом усього життєвого циклу розроблення програми. Запроваджуючи жорстке тестування, перевірку відповідності та навчання користувачів, розробники можуть зменшити ризики та посилити систему безпеки своїх програм. Ця проактивна позиція щодо безпеки не лише захищає від певних уразливостей, але й підвищує довіру користувачів і дотримання міжнародних стандартів і правил стосовно інформаційної безпеки.

Управління ризиками в ISM. Розглянемо методологічні підходи щодо оцінювання ризиків. Оцінювання ризиків є фундаментальним аспектом керування інформаційною безпекою, що забезпечує систематичний процес виявлення вразливостей і оцінювання ризиків, пов'язаних із потенційними загрозами безпеці. Методологічні підходи щодо оцінювання ризиків, які використовують саме для оцінки ризиків, можуть дуже відрізнятися, кожен зі своїм підходом до кількісної оцінки й управління ризиками.

Оцінки ризиків зазвичай поділяють на два типи: якісні та кількісні. Якісні оцінки зосереджено на суб'єктивному аналізі впливу та ймовірності ризиків на основі експертної думки та знань га-

лузі. Цей тип часто приводить до пріоритезації ризиків за такими шкалами, як низький, середній або високий. З іншого боку, кількісні оцінки спрямовано на присвоєння числових значень ризикам, обчислення потенційних наслідків у фінансовому вираженні або інших вимірних одиницях. Такий підхід може забезпечити об'єктивнішу основу для порівняння ризиків і розподілу ресурсів.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) – оцінка критичних операційних загроз, активів і вразливостей**)**, розроблена Університетом Карнегі – Меллона, є інфраструктурою, яка зосереджена на організаційних ризиках і методах безпеки, що особливо підходить для великих організацій, які прагнуть об'єднати бізнес-цілі зі стратегіями безпеки на основі ризиків (Cisco, n. d.).

FAIR (факторний аналіз інформаційного ризику) – це методологія кількісної оцінки ризику, яка допомагає організаціям зрозуміти, проаналізувати та кількісно оцінити інформаційний ризик у фінансовому контексті, що є корисним для прийняття обґрунтованих рішень щодо інвестицій у безпеку та пріоритетів управління ризиками.

Risk IT Framework розроблено ISACA для ризиків, пов'язаних з IT, Risk IT Framework надає підприємствам вичерпний посібник із визначення, управління IT-ризиками, що допомагає організаціям узгодити управління вказаними ризиками із загальним управлінням ризиками підприємства.

Адаптація цих методологій до цифрових рішень передбачає врахування конкретних характеристик і вимог програми. Наприклад, цифровий інструмент, призначений для боротьби з прокрастинацією, може використовувати OCTAVE для оцінювання організаційних ризиків, пов'язаних із безпекою даних користувачів і доступністю системи. FAIR можна використовувати для кількісної оцінки фінансових наслідків можливих порушень або простоїв, що допоможе прийняти рішення про те, на чому зосередити зусилля з безпеки. Структура Risk IT може керувати загальною структурою управління ризиками, забезпечуючи систематичне управління всіма IT-ризиками відповідно до стратегічних цілей програми (Tucker, 2018).

Виявлення, визначення пріоритетів і пом'якшення ризиків. Ефективне управління ризиками в цифрових застосунках вимагає ідентифікації, пріоритезації ризиків і впровадження відповідних стратегій пом'якшення. Цей інтегрований підхід гарантує, що найкритичніші ризики розглядаються за допомогою ефективних рішень для захисту програми та її користувачів.

Першим кроком в управлінні ризиками є визначення потенційних ризиків, що передбачає ретельний аналіз усієї екосистеми цифрової програми, включаючи компоненти програмного забезпечення, взаємодію користувачів, потоки даних і зовнішню інтеграцію. Такі методи, як мозковий штурм, інтерв'ю з експертами та використання автоматизованих інструментів, можуть допомогти виявити потенційні вразливості. Для цифрових затосунків, спрямованих на боротьбу з прокрастинацією, ризики можуть охоплювати несанкціонований доступ до даних користувача, витікання даних або перерви в обслуговуванні, які можуть завадити підвищенню продуктивності користувачів.

Після визначення ризиків їх установлюють за пріоритетом на основі потенційного впливу на програму та ймовірності їх виникнення. Такі інструменти, як матриці ризиків і SWOT-аналіз, допомагають оцінювати ризики, щоб зосередити ресурси й увагу на найбільш значущих загрозах. Пріоритезація враховує фактори, впливу, вимоги дотримання нормативів і експлуатаційну критичність.

Наступним важливим кроком є впровадження стратегій пом'якшення цих ризиків. Уникнення ризиків може бути застосовано для усунення загроз, наприклад, вибір безпечніших альтернатив у технології або перепроєктування вразливих компонентів системи. Там, де ризиків неможливо повністю уникнути, стратегії зменшення є вирішальними та можуть охоплювати застосування розширених заходів безпеки, таких як шифрування, контроль доступу та дотримання методів безпечного кодування. У сценаріях, коли ризиками неможливо керувати всередині країни, ефективною може бути передача їх через страхування або аутсорсинг стороннім постачальникам зі спеціалізованим досвідом безпеки. Прийняття ризику розглядають для менш критичних ризиків, де вартість пом'якшення перевищує потенційний вплив. Невід'ємною частиною цих стратегій є впровадження надійних профілак-

тичних, детективних і коригувальних заходів. Запобіжні заходи призначені для запобігання інцидентам безпеки, детективні засоби контролю – для ідентифікації і реагування на інциденти, коли вони відбуваються, і коригувальні засоби керування – для відновлення після інцидентів і відновлення нормальної роботи. Постійний моніторинг і регулярний перегляд цих засобів контролю є важливими для забезпечення їхньої ефективності та коригування відповідно до нових загроз і потреб бізнесу.

Міжнародні стандарти безпеки. Встановлені межі забезпечують вичерпні вказівки та найкращі практики для встановлення, впровадження, підтримки та постійного вдосконалення інформаційної безпеки.

ISO/IEC 27001 є одним із найпоширеніших міжнародних стандартів для систем управління інформаційною безпекою (ISMS), який описує системний підхід до управління конфіденційною інформацією компанії, щоб вона залишалася в безпеці. Він охоплює людей, процеси та IT-системи через застосування процесу управління ризиками. Цей стандарт особливо корисний для організацій, яким необхідно продемонструвати свою відданість інформаційній безпеці клієнтам або регуляторним органам через формальну сертифікацію (ISO/IEC, 2022).

NIST Cybersecurity Framework розроблено Національним інститутом стандартів і технологій у Сполучених Штатах. Фреймворк використовують в усьому світі для покращення кібербезпеки в різних галузях. Він надає структуру вказівок щодо комп'ютерної безпеки для організацій, які хочуть оцінити та покращити свою здатність запобігати, виявляти та реагувати на кіберінциденти. NIST Framework є гнучким і може бути адаптований до конкретних потреб окремих організацій, незалежно від їхнього розміру чи сектору (NIST, 2019).

COBIT – це структура для керування IT, розроблена ISACA, яку створено як допоміжний інструмент для менеджерів і яка дозволяє подолати розрив між технічними проблемами, бізнес-ризиками та вимогами до контролю. Принципи й інструменти COBIT спрямовано на забезпечення цілісного підходу до управління IT і зосереджено на максимізації цінності інформації шляхом узгодження IT-процесів із бізнес-цілями.

Інтеграцію встановлених меж і стандартів ISM у цифрові рішення, спрямовано на боротьбу з прокрастинацією, підвищення продуктивності, має вирішальне значення для забезпечення надійної безпеки за підтримки функціонального й орієнтованого на користувача дизайну. Ці інфраструктури забезпечують структурований підхід до захисту конфіденційних даних користувачів і підтримки цілісності застосунків, які обробляють персональні дані продуктивності.

Програми, призначені для керування прокрастинацією, часто збирають деталізовані дані про звички користувачів, уподобання та моделі продуктивності. Дотримання таких стандартів, як ISO/IEC 27001 і NIST Cybersecurity Framework, допомагає гарантувати, що ці дані обробляються безпечно та відповідально. Ці норми містять вказівки щодо впровадження комплексних заходів захисту даних, які поважають конфіденційність користувачів і одночасно запобігають несанкціонованому доступу та витіканню даних (ISO/IEC, 2022).

Довіра є наріжним каменем програм, орієнтованих на особисту продуктивність, оскільки користувачі мають бути впевнені, що їхні конфіденційні дані в надійних руках. Відповідність загальновизнаним стандартам безпеки демонструє прихильність до захисту даних, що може стати суттєвим фактором у сприйнятті та збереженні даних користувачами. Наприклад, узгодження із GDPR та іншими нормативними актами щодо конфіденційності не тільки відповідає вимогам законодавства, але й позиціонує програму як надійну.

Цифрові рішення для прокрастинації мають бути гнучкими та реагувати на зміни в поведінці користувачів і технологічний прогрес. Фреймворки, такі як COBIT, можуть допомогти розробникам керувати IT-ризиками, які можуть вплинути на продуктивність і безпеку програми. До них належать ризики, пов'язані з оновленням програмного забезпечення, інтеграцією з іншими програмами або новими кіберзагрозами. Структурований процес управління ризиками дозволяє розробникам завчасно виявляти потенційні вразливості та відповідно адаптувати свої стратегії безпеки (Hussain, 2022).

Програми для керування прокрастинацією виграють від постійного вдосконалення підходу до безпеки, що передбачає регулярні аудити безпеки, цикли зворотного зв'язку з користувачами й оновлення політик безпеки як частину керування життєвим циклом, передбаченого такими міжнародними стандартами, як ISO/IEC 27001. Постійне вдосконалення допомагає гарантувати, що програма адаптується до нових проблем безпеки й очікувань користувачів, зберігаючи її ефективність і конкурентну перевагу.

Оцінка інфраструктур безпеки має важливе значення для визначення їхньої придатності для виконання унікальних вимог і викликів застосунків, що борються з прокрастинацією (Kuzminykh et al., 2021). У табл. 1 розглянуто ефективність і застосовність установлених структур у контексті вказаних програм, з огляду на такі фактори, як комплексність, гнучкість і узгодженість із нормативними вимогами.

Конфіденційність і захист даних. Закони про захист даних відіграють вирішальну роль у захисті персональної інформації, особливо для програм, які збирають і обробляють дані користувачів, щоб керувати такими поведінками, як прокрастинація. Розуміння цих правил важливе для забезпечення дотримання законодавства та захисту конфіденційності користувачів. Порівняльну характеристику різних підходів щодо захисту інформації подано у табл. 1.

Таблиця 1

Порівняння фреймворків

Документ	**Зона фокусування**	**Ключові характеристики**	**Застосовність до програм, які борються з прокрастинацією**
ISO/IEC 27001	Комплексна СУІБ	Системний підхід, управління ризиками, здійснення контролю	Високий – універсальний для всіх типів програм

Закінчення табл. 1

Документ	Зона фокусування	Ключові характеристики	Застосовність до програм, які борються з прокрастинацією
NIST Кібербезпека	Управління ризиками кібербезпеки	Основні функції (ідентифікація, захист, виявлення, реагування, відновлення), адаптовані до потреб організації	Середній – ідеально підходить для застосунків критичної інфраструктури
COBIT	Управління IT	Узгоджує IT з бізнес-цілями, забезпечує відповідність, оптимізує ресурси	Низький – більше підходить для управління IT підприємства
PCI DSS	Безпека даних платіжної картки	Безпечне оброблення даних, надійний контроль доступу, безпека мережевої інфраструктури	Середній – необхідний для застосунків, що обробляють платежі
GDPR	Захист даних і конфіденційність	Права суб'єктів даних, принципи захисту даних, відповідність нормативним вимогам	Високий – обов'язковий для застосунків, якими користуються жителі ЄС

Закон Каліфорнії про конфіденційність споживачів (CCPA) дає жителям Каліфорнії право знати, які персональні дані про них збирають, чи продають чи розкривають. Він також надає право заперечувати продаж персональних даних і право доступу до їхніх даних. Для програм, зосереджених на продуктивності та

зволіканні, які можуть збирати детальні дані про дії користувачів, відповідність передбачає впровадження процесів для ефективного та прозорого керування запитами на доступ до даних користувачів (California Legislative Information, 2018).

Залежно від характеру застосунку для керування прокрастинацією можуть також застосовувати інші нормативи. Наприклад, застосунки, які об'єднують аспекти відстеження стану здоров'я чи психічного благополуччя, можуть відповідати Закону США про перенесення та підзвітність медичного страхування (HIPAA), який захищає конфіденційну інформацію про здоров'я пацієнтів від розголошення без згоди або відома пацієнта. Розробники також повинні бути в курсі нових законів в інших регіонах, як-от LGPD у Бразилії чи запропонований в Індії законопроєкт про захист персональних даних, які вводять додаткові вимоги до відповідності та можуть вплинути на глобальну діяльність.

Є законодавство, що пов'язане з регулюванням оброблення персональних даних у Сінгапурі, відповідно до Personal Data Protection Act (PDPA), яке визначає вимоги й практичні підходи до анонімізації даних із метою запобігання повторній ідентифікації осіб під час їх збору, використання чи поширення (Personal Data Protection Commission Singapore, PDPC, 2018).

Відповідність цифровим рішенням. Програми, призначені для керування прокрастинацією, часто збирають і аналізують велику кількість персональних даних, щоб надавати індивідуальні поради та відстежувати прогрес користувача. Конфіденційність цих даних і потенційні наслідки їхнього неправильного використання роблять надійний захист даних фундаментальною вимогою для цих цифрових рішень.

Програми для керування прокрастинацією зазвичай збирають дані, які користувачі вважають конфіденційними, як-от: відомості про особисті цілі, розпорядок дня та моделі поведінки. Ці дані можуть розповісти багато про спосіб життя, здоров'я та психологічний стан людини. Тому захист цієї інформації є юридичним зобов'язанням згідно з такими законами, як GDPR і CCPA, а також важливим аспектом підтримки довіри користувачів. Будь-яке порушення, яке призведе до несанкціонованого доступу, може

мати серйозні наслідки, завдаючи шкоди довірі користувачів і репутації програми.

Користувачі цифрових інструментів продуктивності мають високі очікування щодо конфіденційності та безпеки своїх даних. Вони вірять, що ці програми не лише допомагають їм ефективніше керувати своїм часом, але й захищають особисту інформацію, якою вони діляться. Невиконання вказаних очікувань може призвести до втрати довіри, втрати користувачів і серйозної шкоди репутації.

Специфічний характер даних, зібраних застосунками для керування зволіканнями, збільшує їхній ризик, що робить їх потенційними цілями для кіберзагроз, таких як витікання даних або несанкціонований доступ. Ці ризики є не лише технічними, а і юридичними й етичними, оскільки неправильне поводження з особистими даними може призвести до значних юридичних наслідків відповідно до таких законів, як GDPR або CCPA.

Недотримання законів про захист даних може призвести до великих штрафів і судових позовів. Крім фінансових наслідків, невідповідність може підірвати довіру користувачів, вплинувши на товарний вигляд і довгострокову життєздатність програми. Наприклад, порушення конфіденційності даних користувача може призвести до зниження активності користувачів, що негативно вплине на загальну ефективність програми в управлінні прокрастинацією.

Стратегії відповідності. Забезпечення відповідності законам про захист даних має вирішальне значення для програм, які допомагають користувачам справлятися з прокрастинацією. Ці закони не лише захищають користувачів, але і зміцнюють довіру та підвищують довіру до цифрових рішень.

Цифрові рішення, спрямовані на боротьбу із зволіканням, повинні застосовувати підхід до мінімізації даних, збираючи лише необхідну інформацію, необхідну для їхньої функціональності. Обмежуючи збір даних основними елементами, такими як налаштування користувача чи розклади завдань, ці програми можуть мінімізувати потенційний вплив витікання даних і несанкціонованого доступу.

Крім того, впровадження надійних механізмів отримання згоди користувачів має першочергове значення для забезпечення дотримання правил конфіденційності. Програми для боротьби із зволіканням мають отримати чітку згоду користувачів перед тим, як збирати, обробляти чи ділитися їхніми даними. Прозоре оприлюднення методів використання даних і чіткі параметри дозволу / відмови дають користувачам змогу приймати обґрунтовані рішення щодо використання даних, зміцнюючи довіру та підзвітність.

Включення принципів конфіденційності у процес розроблення є невід'ємною частиною створення орієнтованих на конфіденційність рішень для боротьби з прокрастинацією. Впроваджуючи питання конфіденційності на кожному етапі проєктування та розроблення продукту, від ідеї концепції до розгортання, розробники можуть завчасно вирішувати ризики конфіденційності та вразливості. Функції підвищення конфіденційності, такі як наскрізне шифрування та методи анонімізації, повинні мати пріоритет, щоб захистити дані користувача від несанкціонованого доступу та зловживання.

Постійний моніторинг відповідності й аудит є важливими компонентами ефективної стратегії конфіденційності та захисту даних. Розробники застосунків, які борються із зволіканням, повинні встановити внутрішні процеси для регулярного оцінювання дотримання відповідних нормативних актів, проведення оцінювання впливу на конфіденційність і ведення комплексних журналів аудиту. Зовнішні аудити, проведені незалежними сторонніми оцінювачами, можуть забезпечити додаткову перевірку зусиль із дотримання вимог, демонструючи прихильність до прозорості та підзвітності.

Вимоги до безпеки для цифрового рішення, що запобігає зволіканню. У цьому дослідженні викладено вимоги безпеки для прототипу мобільного застосунку, призначеного для боротьби з проблемою прокрастинації через гейміфікацію та керування завданнями. Вимоги безпеки структуровані таким способом, щоб забезпечити комплексний підхід до захисту програми від початку до розгортання й експлуатації. Забезпечена стандартом перевірки безпеки мобільних застосунків OWASP (MASVS) програма узгод-

жується зі всесвітньо визнаними найкращими практиками, розробленими спеціально для мобільного середовища.

Архітектура, дизайн і моделювання загроз. Концепцію прототипу розроблено так, щоб залучати користувачів за допомогою динамічного інтерфейсу, який допомагає ефективно керувати завданнями, заохочуючи прогрес за допомогою гейміфікованих елементів (Hajrić et al., 2020). Як прототип, спрямований на демонстрацію потенційних функціональних можливостей і стратегій безпеки, він містить найкращі практики в архітектурі програмного забезпечення та безпеки мобільних застосунків.

На рис. 1 зображено вимоги безпеки для прототипу мобільного застосунку, розробленого для боротьби з проблемою прокрастинації за допомогою гейміфікації та управління завданнями.

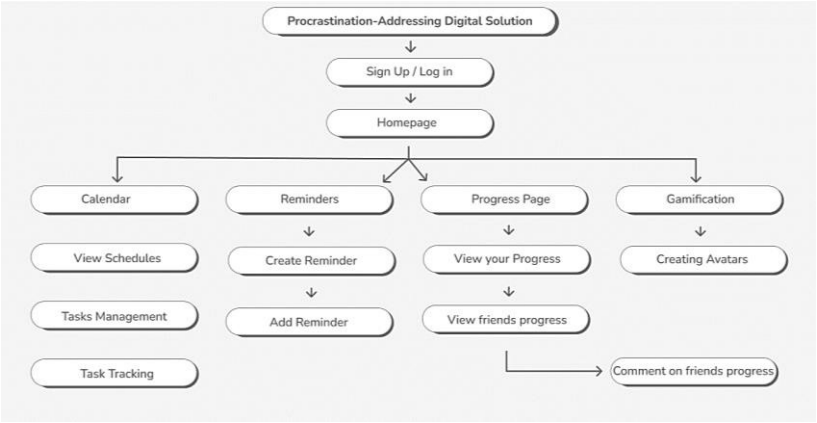

Рис. 1. *Архітектура мобільного застосунку*

Архітектура цифрового рішення охоплює кілька рівнів, кожен з яких виконує окремі функції, одночасно сприяючи загальній безпеці та зручності використання програми. На рівні презентації використання таких фреймворків, як React Native або Flutter, забезпечує чутливий і привабливий інтерфейс користувача на різних мобільних платформах. Цей рівень ретельно розроблено для оброблення введених даних користувачами, відображення інфор-

мації, пов'язаної із завданнями, та керування інтерактивними елементами з акцентом на зручності та доступності.

Під рівнем презентації розміщено рівень бізнес-логіки, де розташовано основні функції програми. Цей рівень обробляє запити користувачів, керує даними завдань і організовує функції гейміфікації, щоб стимулювати залучення користувачів і продуктивність. Рівень бізнес-логіки, розміщений на захищеній хмаровій платформі, використовує власні хмарові сервіси та найкращі практики для забезпечення масштабованості, надійності та стійкості до потенційних загроз безпеці.

Рівень зберігання даних, розташований в основі архітектури, відповідає за постійне зберігання даних користувача, інформації, пов'язаної із завданнями, і налаштувань програми. Використовуючи рішення із зашифрованою базою даних, цей рівень використовує галузеві стандартні алгоритми шифрування та механізми контролю доступу для захисту конфіденційних даних від несанкціонованого доступу та зловмисного втручання. Крім того, перевірки цілісності даних і заходи надлишковості впроваджують для зменшення ризику пошкодження або втрати даних.

Дискусія і висновки

Аспекти інформаційної безпеки є важливими для забезпечення ефективності, надійності й етичності цифрових рішень для боротьби з прокрастинацією, і захисту користувачів від кіберзагроз і неправомірного використання їхніх даних. Передусім, це конфіденційність персональних даних, безпека поведінкових даних, захист від кіберзагроз, цілісність даних, автентифікація та авторизація, етика використання персональних даних, правове регулювання та відповідність міжнародним стандартам тощо.

Програми для боротьби з прокрастинацією часто збирають персональну інформацію користувачів, включаючи звички, розпорядок дня, цілі, продуктивність і психологічні дані. Захист цих даних є критично важливим для збереження конфіденційності. Якщо дані будуть скомпрометовані чи потраплять у руки сторонніх осіб, це може призвести до серйозних наслідків, включаючи шахрайство чи порушення приватності користувачів. Цифрові рішення для боротьби з прокрастинацією часто аналізують поведінкові патерни користувача, щоб надавати персоналізовані рекомен-

дації. Дані про поведінку можуть бути надзвичайно чутливими, і їхній захист важливий для уникнення маніпуляцій або експлуатації цієї інформації для шахрайських цілей. Цифрові платформи можуть стати мішенню для кіберзлочинців, які можуть використовувати їх для фішингу, атак на ланцюжки постачання або розповсюдження шкідливого програмного забезпечення. Ненадійні рішення можуть стати вразливими, що не лише ставить під загрозу користувачів, а й підриває довіру до таких інструментів. Для ефективної боротьби з прокрастинацією користувачам важливо отримувати точні та достовірні дані про свій прогрес. Якщо система належно не захищена, то дані можуть бути спотворені чи втратити свою цілісність через хакерські атаки або технічні помилки, що знижує ефективність рішення. Багато рішень для боротьби з прокрастинацією дозволяють користувачам синхронізувати їхні облікові записи з іншими сервісами чи зберігати дані у хмарі. Без належних методів автентифікації та авторизації (напр., багатофакторної автентифікації) може виникнути ризик несанкціонованого доступу до важливої інформації. Рішення для боротьби з прокрастинацією можуть збирати багато даних про користувачів, і важливо, щоб ці дані використовувалися етично. Забезпечення того, щоб цифрові інструменти відповідали вимогам інформаційної безпеки й етичним стандартам, допоможе запобігти їхньому використанню для маніпуляцій чи отримання прибутку за рахунок користувачів. Цифрові рішення мають відповідати законам про захист даних, таким як GDPR у Європі чи CCPA у США. Недотримання цих стандартів може призвести до юридичних проблем, штрафів і втрати довіри з боку користувачів.

Список використаних джерел

Al-Janabi, S., & Al-Shourbaji, I. (2021). Information Security Requirement: The Relationship Between Confidentiality, Integrity and Availability in Digital Social Media. In *Information Security Theory and Practice* (pp. 289–305). Springer.

California Legislative Information. (2018). *Civil Code - CIV.* https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Cisco. (2017). *Securing Cisco IP Telephony Networks.* Cisco Press. https://www.ciscopress.com/articles/article.asp?p=2803867&seqNum=4

Daisie Team. (2023). *Cryptography for Mobile App Security: 5 Ways.* Daisie. https://blog.daisie.com/cryptography-for-mobile-app-security-5-ways/

EU General Data Protection Regulation (GDPR). (2018). http://www.privacy-regulation.eu/en/

Hajrić, A., Smaka, T., Baraković, S., & Baraković Husić, J. (2020). Methods, methodologies, and tools for threat modeling with case study. *Telfor Journal,* 12(1).

Hussain, O. K. (2022). *The process of risk management needs to evolve with the changing technology in the digital world.* Springer Nature.

International Organization for Standardization. (2022). *Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2022).* https://www.iso.org/standard/27001

Khidzir, N. Z., Daud, K. A. M., Ismail, A. R., Ghani, M. S. A. A., & Ibrahim, M. A. H. (2018). Information Security Requirement: The Relationship Between Cybersecurity Risk Confidentiality, Integrity and Availability in Digital Social Media. In *Regional Conference on Science, Technology and Social Sciences (RCSTSS 2016)* (pp. 229–237). Springer, Singapore.

Kollnig, K., Binns, R., Van Kleek, M., Lyngs, U., Zhao, J., Tinsman, C., & Shadbolt, N. (2021). Before and after GDPR: Tracking in mobile apps. *Internet Policy Review,* 10(4).

OWASP. (2024). *Mobile Application Security Verification Standard (MASVS) (Version 2.1.0) [OWASP MASVS].* https://mas.owasp.org/MASVS

OWASP. (2021). *Mobile App Cryptography. OWASP Mobile Application Security Testing Guide (MASTG).* OWASP Mobile Security Testing Guide Release | OWASP Foundation.

Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). Information Security Risk Assessment. *Encyclopedia,* 1, 602–617. https://doi.org/10.3390/encyclopedia1030050

Lambert, T. (2023). *Personal Data Protection in Mobile Apps: Best Practices and Guidelines.* https://pdtn.org/personal-data-protection-in-mobile-apps/

National Institute of Standards and Technology. (2024). *NIST Cybersecurity Framework.* https://www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0

NIST. (2012). *Guide for conducting risk assessments (NIST SP 800-30 R1).* NIST Special Publication, 800-30 Revision 1.

Personal Data Protection Commission Singapore (PDPC). (2018). *Guide to Basic Data Anonymisation Techniques.* https://iapp.org/resources/article/guide-to-basic-data-anonymization-techniques/

Rajasekharaiah, K. M. et al., 2020. Cyber Security Challenges and its Emerging Trends on Latest Technologies. *IOP Conference Series: Materials Science and Engineering,* 981, 022062.

Rouland, Q., Hamid, B., & Jaskolka, J. (2021). Specification, detection, and treatment of STRIDE threats for software components: Modeling, formal methods, and tool support. *Journal of Systems Architecture,* 117, 102073.

Tucker, B. (2021). *OCTAVE® FORTE and FAIR Connect Cyber Risk Practitioners with the Boardroom.* https://insights.sei.cmu.edu/blog/octave-forte-and-fair-connect-cyber-risk-practitioners-with-the-boardroom/

Thakur, M. (2024). Cyber Security Threats and Countermeasures in Digital Age. *Journal of Applied Science and Education (JASE),* 4(1), 1–20.

Van der Ham, J. (2021). Toward a Better Understanding of "Cybersecurity." *Digital Threats: Research and Practice,* 2(3), Article 18.

References

Al-Janabi, S., & Al-Shourbaji, I. (2021). Information Security Requirement: The Relationship Between Confidentiality, Integrity and Availability in Digital Social Media. In *Information Security Theory and Practice* (pp. 289–305). Springer.

California Legislative Information. (2018). *Civil Code - CIV.* https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Cisco. (2017). *Securing Cisco IP Telephony Networks*. Cisco Press. https://www.ciscopress.com/articles/article.asp?p=2803867&seqNum=4

Daisie Team. (2023). *Cryptography for Mobile App Security: 5 Ways*. Daisie. https://blog.daisie.com/cryptography-for-mobile-app-security-5-ways/

EU General Data Protection Regulation (GDPR). (2018). http://www.privacy-regulation.eu/en/

Hajrić, A., Smaka, T., Baraković, S., & Baraković Husić, J. (2020). Methods, methodologies, and tools for threat modeling with case study. *Telfor Journal,* 12(1).

Hussain, O. K. (2022). *The process of risk management needs to evolve with the changing technology in the digital world.* Springer Nature.

International Organization for Standardization. (2022). *Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2022).* https://www.iso.org/standard/27001

Khidzir, N. Z., Daud, K. A. M., Ismail, A. R., Ghani, M. S. A. A., & Ibrahim, M. A. H. (2018). Information Security Requirement: The Relationship Between Cybersecurity Risk Confidentiality, Integrity and Availability in Digital Social Media. In *Regional Conference on Science, Technology and Social Sciences (RCSTSS 2016)* (pp. 229–237). Springer, Singapore.

Kollnig, K., Binns, R., Van Kleek, M., Lyngs, U., Zhao, J., Tinsman, C., & Shadbolt, N. (2021). Before and after GDPR: Tracking in mobile apps. *Internet Policy Review,* 10(4).

OWASP. (2024). *Mobile Application Security Verification Standard (MASVS) (Version 2.1.0) [OWASP MASVS].* https://mas.owasp.org/MASVS

OWASP. (2021). *Mobile App Cryptography. OWASP Mobile Application Security Testing Guide (MASTG).* OWASP Mobile Security Testing Guide Release | OWASP Foundation.

Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). Information Security Risk Assessment. *Encyclopedia,* 1, 602–617. https://doi.org/10.3390/encyclopedia1030050

Lambert, T. (2023). *Personal Data Protection in Mobile Apps: Best Practices and Guidelines.* https://pdtn.org/personal-data-protection-in-mobile-apps/

National Institute of Standards and Technology. (2024). *NIST Cybersecurity Framework.* https://www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0

NIST. (2012). *Guide for conducting risk assessments (NIST SP 800-30 R1).* NIST Special Publication, 800-30 Revision 1.

Personal Data Protection Commission Singapore (PDPC). (2018). *Guide to Basic Data Anonymisation Techniques.* https://iapp.org/resources/article/guide-to-basic-data-anonymization-techniques/

Rajasekharaiah, K. M. et al., 2020. Cyber Security Challenges and its Emerging Trends on Latest Technologies. *IOP Conference Series: Materials Science and Engineering,* 981, 022062.

Rouland, Q., Hamid, B., & Jaskolka, J. (2021). Specification, detection, and treatment of STRIDE threats for software components: Modeling, formal methods, and tool support. *Journal of Systems Architecture,* 117, 102073.

Tucker, B. (2021). *OCTAVE® FORTE and FAIR Connect Cyber Risk Practitioners with the Boardroom.* https://insights.sei.cmu.edu/blog/octave-forte-and-fair-connect-cyber-risk-practitioners-with-the-boardroom/

Thakur, M. (2024). Cyber Security Threats and Countermeasures in Digital Age. *Journal of Applied Science and Education (JASE),* 4(1), 1–20.

Van der Ham, J. (2021). Toward a Better Understanding of "Cybersecurity." *Digital Threats: Research and Practice,* 2(3), Article 18.

Отримано редакцією журналу / Received: 17.09.24
Прорецензовано / Revised: 27.09.24
Схвалено до друку / Accepted: 01.10.24

Valentyna PLESKACH[1], DSc (Econ.), Prof.
ORCID ID: 0000-0003-0552-0972
e-mail: valentyna.pleskach@knu.ua

Irma ŠILEIKIENĖ[2], DSc (Engin.), Assoc. Prof.
ORCID ID: 0000-0002-1185-0970
e-mail: irma.sileikiene@vilniustech.lt

Romanas TUMASONIS[3], DSc (Engin.), Assoc. Prof.
ORCID ID: 0000-0002-8921-0674
e-mail: r.tumasonis@eif.viko.lt

Yevhenii TOPOLSKOV[1], PhD(Engin.), Assoc. Prof.
ORCID ID: 0000-0001-5587-3069
e-mail: y.topolskov@knu.ua

[1]Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
[2]Vilnius Technical University, Vilnius, Lithuania
[3]Vilnius University of Applied Sciences, Vilnius, Lithuania

INFORMATION SECURITY ASPECTS FOR DIGITAL SOLUTIONS TO COMBAT PROCRASTINATION

This paper explores various security frameworks, threat modeling, and risk management techniques, the assignment provided a thorough theoretical backdrop against which practical security measures can be developed and implemented. Covering critical aspects of security such as authentication, data privacy, session management, and compliance with legal standards like GDPR, the work not only addressed potential vulnerabilities identified through threat modeling but also set a solid framework for implementing these security features practically. This comprehensive approach ensures that the prototype is not only functional but also secure from various cybersecurity threats. Moreover, it showcased how security and functionality can be balanced

effectively, paving the way for potential future development and real-world application of the prototype.

Keywords: ***information security, security frameworks, security requirements, security measures, risk management.***

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.