комплексному підходу, який поєднав державну політику, медіаграмотність, активність громадянського суспільства та волонтерські ініціативи.

Державні структури, такі як Центр стратегічних комунікацій, своєчасно спростовували фейки та надавали громадянам достовірну інформацію, мінімізуючи паніку. Водночас широкомасштабна волонтерська діяльність, культурні події, ініціативи психологічної допомоги та взаємодопомога у громадах формували відчуття єдності та підтримки, що значно підвищувало стійкість населення. Особливо ефективною виявилася робота державних і громадських платформ, таких як StopFake, гарячі лінії психологічної підтримки, інформаційні кампанії з медіаграмотності, а також ініціативи з розвитку критичного мислення серед молоді. Ці заходи дозволили не лише нейтралізувати вплив дезінформації, а й підвищити готовність суспільства до спільних дій у кризових умовах.

Український досвід показує, що психологічна стійкість населення є не лише результатом індивідуальної витримки, а й комплексним ефектом координації держави, медіа, громадських організацій і самих громадян. Стійке суспільство стало важливою складовою національної оборони, рівнозначною армії чи кіберзахисту, і слугує прикладом для інших держав, що опинилися під інформаційним тиском та агресією.

Психологічна стійкість – це не лише риса особистості, а стратегічний ресурс держави. Вона формує інформаційний щит, який захищає суспільство від паніки, фейків і маніпуляцій. Формування цієї стійкості потребує спільних зусиль держави, освіти, медіа та кожного громадянина. У війні за свідомість людей перемагає не той, хто має більше інформації, а той, хто здатен мислити критично й залишатися внутрішньо сильним..

Література

1. Національна рада України з питань телебачення і радіомовлення. *Протидія дезінформації в умовах війни, українське законодавство та роль медіа.* URL: https://webportal.nrada.gov.ua/protydiya-dezinformatsiyi-v-umovah-vijny-ukrayinske-zakonodavstvo-ta-rol-media/ (дата звернення: 11.11.2025).

2. Корольова Н.Д., Матохнюк Л.О., Таран А.А. Психологічна стійкість молоді в умовах військової агресії. *Вісник Донецького національного університету імені Василя Стуса. Серія Психологічні науки*. 2025. Вип. 2(5). С. 72–79. DOI: 10.31558/2786-8745.2024.2(5).8.

3. StopFake.org. URL: https://www.stopfake.org/uk/ (дата звернення: 11.11.2025).

4. Ласкова-Ярмоленко А., Слинькова Т. Медіаграмотність в системі освіти: вимоги сучасності у сфері соціальної комунікації. *Педагогічні інновації: ідеї, реалії, перспективи*. 2024. Том 1. № 32 (2024). С 100–105. DOI: 10.32405/2413-4139-2024-1(32)-100-105.

5. Центр стратегічних комунікацій. URL: https://spravdi.gov.ua/ (дата звернення: 11.11.2025).

УДК 004.056.5:004.738.5

КОНЦЕПТУАЛЬНА МОДЕЛЬ МІНІМІЗАЦІЇ ВИТОКІВ ДАНИХ У КОРПОРАТИВНОМУ СЕРЕДОВИЩІ НА ОСНОВІ ПРИНЦИПІВ ZERO TRUST АРХІТЕКТУРИ

Анастасія СОРОКА, Валентина ЯЩУК, Валерія БАЛАЦЬКА
Львівський державний університет безпеки життєдіяльності

Анотація. *Запропоновано концептуальну модель мінімізації витоків даних у корпоративному середовищі, засновану на принципах архітектури Zero Trust. Проаналізовано обмеження традиційних периметрових моделей безпеки та обґрунтовано необхідність переходу до динамічної системи довіри, де кожна взаємодія перевіряється у режимі реального часу. Визначено три базові рівні моделі — ідентифікаційно-контрольний, сегментаційно-політичний і моніторингово-аналітичний. Показано, що реалізація Zero Trust-підходу дає змогу зменшити ризики витоків даних і підвищити рівень кіберстійкості корпоративної інфраструктури.*

Ключові слова: *Zero Trust, кібербезпека, витік даних, корпоративне середовище, мікросегментація, політики доступу, кіберстійкість.*

Abstract. *A conceptual model for minimizing data leaks in a corporate environment is proposed, based on the principles of the Zero Trust architecture. The limitations of traditional perimeter security models are analyzed and the need to transition to a dynamic trust system is justified, where each interaction is checked in real time. Three basic levels of the model are identified - identification and control, segmentation and policy, and monitoring and analysis. It is shown that the implementation of the Zero Trust approach allows you to reduce the risks of data leaks and increase the level of cyber resilience of corporate infrastructure.*

Keywords: *Zero Trust, cybersecurity, data leakage, corporate environment, microsegmentation, access policies, cyber resilience.*

У сучасному корпоративному середовищі, що характеризується високим рівнем цифровізації бізнес-процесів, використанням хмарних сервісів та зростанням кількості віддалених користувачів, питання забезпечення конфіденційності й цілісності даних набуває стратегічного значення. Традиційні периметрові моделі захисту більше не відповідають сучасним викликам, адже межі корпоративних мереж стають розмитими, а дані циркулюють між внутрішніми й зовнішніми середовищами. У цих умовах особливого значення набуває архітектура Zero Trust (ZTA), побудована на принципі «ніколи не довіряй, завжди перевіряй». Концепція передбачає відмову від довіри за замовчуванням, застосування постійної автентифікації користувачів і пристроїв, а також мінімізацію рівня доступу відповідно до контексту ризику.

Метою даного дослідження є розроблення концептуальної моделі мінімізації витоків даних у корпоративному середовищі на основі принципів Zero Trust, що поєднує ідентифікаційні, політичні та аналітичні механізми безпеки в єдину динамічну систему управління довірою.

Запропонована концептуальна модель мінімізації витоків даних у корпоративному середовищі базується на трирівневій архітектурі, що інтегрує принципи Zero Trust із сучасними технологіями ідентифікації, сегментації та аналітичного моніторингу. Така багаторівнева структура забезпечує комплексне покриття основних етапів життєвого циклу даних — від доступу до виявлення та реагування на інциденти — і спрямована на усунення довіри за замовчуванням у будь-яких взаємодіях між користувачами, пристроями та сервісами.

Ідентифікаційно-контрольний рівень виконує функції автентифікації, авторизації та перевірки цілісності взаємодій у реальному часі. У межах цього рівня передбачено впровадження багатофакторної автентифікації (MFA), що поєднує щонайменше два незалежні фактори — знання (пароль), володіння (токен, мобільний пристрій) та біометричний параметр (відбиток пальця, розпізнавання обличчя). Додатково застосовується поведінкова аналітика, яка аналізує шаблони активності користувача (час входу, місце, тип пристрою, характер дій) для формування динамічної оцінки ризику. Система контекстного доступу приймає рішення про дозвіл чи блокування операції з урахуванням поточних умов — геолокації, статусу пристрою, рівня загрози в мережі. Таким чином, доступ до даних здійснюється лише за умови відповідності всім політикам безпеки, що значно знижує ризик компрометації облікових записів та внутрішніх загроз.

Сегментаційно-політичний рівень забезпечує просторову і логічну ізоляцію інформаційних потоків у межах корпоративної інфраструктури. Ключовим механізмом є мікросегментація, що передбачає поділ мережі на ізольовані домени з мінімально необхідними маршрутами взаємодії між ними. Такий підхід запобігає горизонтальному переміщенню зловмисників після первинного проникнення. Для керування доступом використовуються контекстно-залежні політики, зокрема RBAC (Role-Based Access Control) — доступ на основі ролей користувачів, ABAC (Attribute-Based Access Control) — доступ, що враховує динамічні атрибути (місце, час, пристрій, рівень ризику), та Risk-Based Access, який автоматично адаптує рівень доступу залежно від оціненого ризику конкретної сесії. Усі політики реалізують принцип найменших привілеїв (Least Privilege), згідно з яким користувач або процес отримує лише ті права, які необхідні для виконання конкретних завдань. Це мінімізує наслідки можливих витоків та обмежує масштаб потенційних інцидентів.

Моніторингово-аналітичний рівень виконує функції спостереження, виявлення аномалій і реагування на загрози. Центральним елементом цьо-

го рівня є системи управління інформаційною безпекою (SIEM), які здійснюють кореляційний аналіз подій із різних джерел — серверів, робочих станцій, мережевого обладнання, хмарних сервісів. Для підвищення точності детекції застосовуються алгоритми машинного навчання та штучного інтелекту, які здатні самостійно формувати профілі нормальної поведінки системи та виявляти відхилення, що можуть свідчити про витік або спробу несанкціонованого доступу. Також впроваджується механізм адаптивного реагування, який дозволяє автоматично змінювати політики доступу, ізолювати підозрілі вузли або активувати процедури інцидент-респонсу в режимі реального часу.

Загалом, взаємодія трьох рівнів забезпечує замкнений цикл безпеки, де автентифікація, сегментація та моніторинг утворюють самопідсилювальну систему динамічного контролю довіри. Така архітектура дозволяє не лише мінімізувати ризики витоків даних, а й формує основу для побудови адаптивної кіберстійкої корпоративної екосистеми, здатної ефективно функціонувати в умовах постійної еволюції цифрових загроз. Інтеграція цих рівнів у єдину архітектуру дозволяє реалізувати динамічну модель довіри, яка зменшує ризик несанкціонованого доступу, внутрішніх порушень і компрометації облікових даних. За результатами аналітичного моделювання доведено, що застосування Zero Trust-підходу може знизити ймовірність витоку даних на 70–80% у порівнянні з традиційними стратегіями захисту.

Запровадження Zero Trust-архітектури у корпоративному середовищі є ефективним кроком до формування проактивної системи безпеки, орієнтованої на мінімізацію ризиків витоків даних і підвищення кіберстійкості організації. Подальші дослідження доцільно спрямувати на створення інтегрованих моделей Zero Trust для мультихмарних середовищ та розроблення алгоритмів автоматичного управління політиками довіри у динамічних цифрових екосистемах.

Література

1. Kindervag, J. (2010). Build security into your network’s DNA: The Zero Trust network architecture. Forrester Research.

2. Ящук В.І., Івануса А.І., Маслова Н.О., Ткачук Р.Л., Брич Т.Б. Концептуалізація інтегративного використання баз даних вразливостей у контексті системного менеджменту інформаційної безпеки // Вісник Львівського державного університету безпеки життєдіяльності. – 2025. – Т. 31. – С. 59–61

3. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST SP 800-207). National Institute of Standards and Technology.

4. Scarfone, K., & Jansen, W. (2021). Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security (NIST SP 800-46 Rev. 2). National Institute of Standards and Technology