

1. Fang, K., Zhao, J., Li, X., et al. Quantum NETwork: from theory to practice. *Sci. China Inf.* 2023. Sci. 66, 180509
2. Gyongyosi, Laszlo and Imre, Sandor Advances Quantum Internet. *Association for Computing Machinery*. 2022. № 8. С. 52–63
3. Koudia, S., A. S. Cacciapuoti, K. Simonov and M. Caleffi How Deep the Theory of Quantum Communications Goes: Superadditivity, Superactivation and Causal Activation. *IEEE Communications Surveys & Tutorials*. 2022. № 4. С. 1926-1956
4. M. Caleffi, K. Simonov and A. S. Cacciapuoti, Beyond Shannon Limits: Quantum Communications Through Quantum Paths. *IEEE Journal on Selected Areas in Communications*. 2023. № 8. С. 2707-2724
5. Остапов С.Е., Добровольський Ю.Г. Квантова інформатика та квантові обчислення. *Чернівці ЧНУ*. 2021. 99 с.

## **РОЛЬ СУЧАСНИХ СИСТЕМ МОНІТОРИНГУ У ПРОТИДІІ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ**

**Прокопенко О. С.**

*доктор філософії, начальник науково-дослідної лабораторії  
навчально-наукового центру стратегічних комунікацій  
у сфері забезпечення національної безпеки та оборони  
Національного університету оборони України*

**Лашин Я. О.**

*науковий співробітник  
навчально-наукового центру стратегічних комунікацій  
у сфері забезпечення національної безпеки та оборони  
Національного університету оборони України*

**Сівоха І. М.**

*науковий співробітник  
навчально-наукового центру стратегічних комунікацій  
у сфері забезпечення національної безпеки та оборони  
Національного університету оборони України*

У сучасному світі інформаційний простір став важливим елементом суспільного життя та міжнародних відносин. Зростаюча кількість даних, що поширюються через інтернет та соціальні мережі, призвела до збільшення інформаційних загроз, таких як фейкові новини, кібератаки та інші форми дезінформації. У зв'язку з цим, розробка та застосування сучасних систем моніторингу інформаційного простору стали невід'ємною складовою боротьби з інформаційними загрозами.

Інформаційні загрози можуть мати серйозні наслідки для державної безпеки, суспільства та економіки. Фейкові новини, розповсюджені швидко та масштабно, можуть викликати паніку серед населення, спричинити розкол у суспільстві, вплинути на політичні процеси тощо.

Для ефективної протидії інформаційним загрозам необхідно мати системи моніторингу, які здатні відстежувати, аналізувати та реагувати на негативні

тенденції в інформаційному середовищі. Сучасні системи моніторингу інформаційного простору використовуються для виявлення та аналізу інформації з різних джерел, включаючи соціальні мережі, новинні сайти, форуми та інші. Ці системи дозволяють виявляти незвичні або підозрілі дії в мережі та аналізувати їх для виявлення можливих загроз [1, с. 11–12; 2, с. 175–177].

Одним із головних завдань систем моніторингу інформаційного простору є виявлення фейкових новин та дезінформації. Системи моніторингу використовують технології аналізу текстів та мовлення, що дозволяє виявляти недостовірну, маніпулятивну або шкідливу інформацію.

Також системи моніторингу дозволяють аналізувати активність у соціальних мережах, що є важливим аспектом в протидії фейковим новинам та дезінформації.

Окрім того, системи моніторингу інформаційного простору дозволяють виявляти тенденції та тренди в інформаційному просторі та прогнозувати можливі ризики. Такі можливості дозволяють виявляти та запобігати можливим загрозам, впливаючи на ситуацію заздалегідь [1, с. 13–14; 2, с. 180–182].

Інформаційні системи моніторингу забезпечують збір, аналіз та обробку великого обсягу даних з метою виявлення небажаних активностей та загроз.

Основні технології які використовують системи моніторингу інформаційного простору:

Штучний інтелект (AI) та машинне навчання (ML): Використання AI та ML дозволяє автоматизувати процес виявлення та аналізу небажаних активностей в інформаційному просторі. Системи можуть навчитися розпізнавати патерни та аномалії, що допомагає виявляти загрози швидше та ефективніше.

Біг-дата (Big Data) та аналітика: Завдяки розвитку технологій збирання та збереження великого обсягу даних, стає можливим проводити глибокий аналіз інформації для виявлення складних зв'язків та трендів. Це допомагає виявляти нові загрози та реагувати на них швидше.

Аналіз текстів та мовлення: Системи моніторингу використовують технології аналізу текстів та мовлення, що дозволяє виявляти недостовірну, маніпулятивну або шкідливу інформацію.

Візуалізація даних: Використання візуалізації даних дозволяє користувачам більш зрозуміло та ефективно аналізувати інформацію.

Одним з прикладів використання моніторингу у протидії інформаційним загрозам є використання моніторингу фейків та російської дезінформації в українських онлайн-медіа. Український інформаційний простір зазнає значного впливу дезінформації, особливо в умовах війни. У цьому контексті моніторинг фейків та дезінформації може допомогти виявити та запобігти їх поширенню[3].

Отже, моніторинг інформаційного простору є важливим інструментом для протидії інформаційним загрозам. Використання сучасних систем моніторингу дозволяє збирати, аналізувати та обробляти великі обсяги даних для виявлення небажаних активностей та загроз. Основні технології в цій галузі включають: використання штучного інтелекту, аналітику великих даних та візуалізацію отриманих даних. Ці технології роблять моніторинг інформаційного простору ефективнішим та допомагають виявляти та аналізувати негативні тенденції у

поширенні інформації, що дозволяє забезпечити більшу довіру до інформації та захистити суспільство від можливих наслідків дезінформації та інших інформаційних загроз.

#### ЛІТЕРАТУРА

1. Любовець Г. В., Король В. Г. Аналіз підходів до моніторингу інформаційного простору в Україні. *Держава та регіони. Серія: Соціальні комунікації*. 2015. №3. С. 10–16. - URL: [http://nbuv.gov.ua/UJRN/drsk\\_2015\\_3\\_4](http://nbuv.gov.ua/UJRN/drsk_2015_3_4) (дата звернення: 19.08.2023).
2. Тищенко В. С., Мужанова Т. М. Дезінформація і фейкові новини: ознаки та методи виявлення в мережі інтернет. Електронне фахове наукове видання «*Кібербезпека: освіта, наука, техніка*» 2022. 2(18), 175–186. <https://doi.org/10.28925/2663-4023.2022.18.175186> (дата звернення: 19.08.2023).
3. Методологія моніторингу фейків та російської дезінформації в українських онлайн-медіа. *Інститут масової інформації*. URL: <https://imi.org.ua/monitorings/metodolohiia-monitorynhu-feyktiv-ta-rosiys-koi-dezinformatsii-v-ukrains-kykh-onlayn-media-i28321> (дата звернення: 19.08.2023).

### МОДЕЛЬ УПРАВЛІННЯ ПРОГРАМНИМИ ПРОЕКТАМИ

**Рейда О. М.**

*кандидат технічних наук,*

*доцент кафедри програмного забезпечення*

*Вінницького національного технічного університету*

Цілі, функції та інструменти проектного менеджменту у сукупності формують модель управління програмним проектом.

Відповідно до визначення Інститутом управління проектами США (Project Management Institute — PMI) управління проектами це методологія організації, планування, управління, координації трудових, фінансових і матеріально-технічних ресурсів впродовж проектного циклу, що спрямована на ефективне досягнення мети проекту.[1]

Розрізняють такі схеми управління проектом: «базова», «розширеного управління», «повного управління».

«Базова» система управління проектом передбачає, що керівником проекту є представник замовника, який не несе фінансової відповідальності за ухвалені рішення. Керівник проекту забезпечує координацію і управління ходом розробки і реалізації проекту.

Характерною рисою системи «розширеного управління» є відповідальність за проект керівника в межах фіксованого бюджету, який забезпечує управління і координацію процесів проекту. Відповідальність покладається на керівника проекту в межах контрактних умов.

Система «повного управління» базується на залучені до управління проектом спеціалізованих груп або компаній, які несуть повну відповідальність перед замовником за виконання проекту.