СЕКЦІЯ 3. ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

ІЄРАРХІЧНА МОДЕЛЬ РОЛЕЙ У CRM-СИСТЕМАХ / HIERARCHICAL ROLE MODEL IN CRM-SYSTEMS

Демидов М.[1], Бабенко Ю.[1], Бабенко М.[2] / Demydov M.[1], Babenko Y.[1], Babenko M.[2]
[1]Київський національний університет імені Тараса Шевченка / Taras Shevchenko National University of Kyiv
04116, Київ, вул. Богдана Гаврилишина, 24, факультет інформаційних технологій, кафедра кібербезпеки та захисту інформації
[2]Дніпровський державний технічний університет / Dniprovsky State Technical University
51918, м. Кам'янське, вул. Дніпробудівська, 2, факультет комп'ютерних технологій та енергетики, кафедра програмного забезпечення систем
E-mail: maksimdemidov05@gmail.com, yurii.babenko@knu.ua, mvbab130973@gmail.com

The growing adoption of CRM systems increases the need for effective user access control mechanisms. This paper analyzes the hierarchical role-based access control (RBAC) model in the context of CRM platforms, emphasizing its role in ensuring data protection and centralized access management. A comparative overview of the OAuth Scopes approach is also presented, highlighting their conceptual differences, advantages, and appropriate areas of application. Although OAuth Scopes provide flexible and temporary permissions for API interactions, the hierarchical role model remains a fundamental basis for stable, scalable, and structured internal access management in CRM systems.

Ієрархічна модель ролей у CRM – це система, у якій ролі користувачів мають «вертикальні» взаємовідносини: користувач із вищою роллю може переглядати дані підлеглих, але не навпаки [1]. Основні складові цієї моделі включають: користувача, роль, профіль, а також дозволи та рівні видимості (дивись рисунок 1).

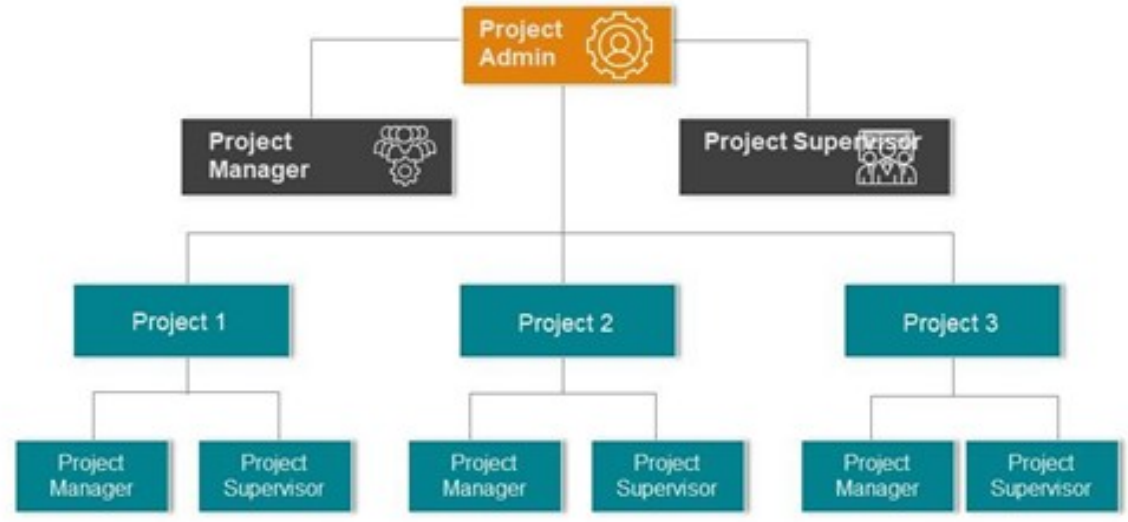

Рисунок 1 – Схема роботи ієрархічної моделі ролей

Ролі визначають, які записи (наприклад, угоди або контакти) користувач може переглядати. Наприклад, регіональний менеджер має доступ до даних своїх підлеглих у межах регіону, але не до інформації інших відділів. Профіль визначає, які дії користувач може виконувати з цими записами – створення, перегляд, редагування, видалення, імпорт чи експорт у різних модулях CRM (ліди, контакти, угоди тощо). Дозволи та видимість встановлюють базовий рівень доступу в межах організації.

Наприклад, певний модуль може бути **“**Public**”** (публічний) – доступний усім, або **“**Private” (приватний) – лише власнику та його керівникам у структурі*)*.

У сучасних інформаційних системах існує кілька підходів до управління доступом користувачів. Найпоширенішими є OAuth Scopes [2, 3] та RBAC (Role-Based Access Control) [3–5] – вони різняться за принципами дії та сферою застосування:

- OAuth Scopes – це рядки дозволів, прив’язані до токенів доступу, які визначають, що саме додаток може робити з даними користувача. Вони тимчасові, більш гнучкі та використовуються переважно для зовнішніх інтеграцій з API, де потрібні короткострокові дозволи.

- RBAC – надає права доступу на основі ролей користувача, групуючи дії відповідно до службових обов’язків. Це статичний підхід, орієнтований на довготривалий внутрішній доступ у корпоративних системах.

Наведемо в таблиці 1 порівняння характеристик обох підходів до управління доступом користувачів.

Таблиця 1 – Порівняння підходів до управління доступом

Характеристика	**OAuth Scopes**	**RBAC**
Тривалість дії	Тимчасова (залежить від токена)	Постійна (на основі ролі)
Рівень деталізації	Високий (для конкретних ресурсів)	Загальний (для всієї ролі)
Гнучкість	Висока, налаштовується динамічно	Нижча, потребує ручного оновлення
Типове застосування	Зовнішні API-інтеграції	Внутрішній доступ користувачів

Попри появу нових методів авторизації, ієрархічна модель ролей (RBAC) залишається важливою, адже вона забезпечує чітку структуру доступу, відображає організаційну ієрархію (наприклад, *“адмін → менеджер → користувач”*), та дозволяє централізовано керувати правами великої кількості працівників.

У системах, де рівень доступу визначається службовими обов’язками, RBAC спрощує адміністрування, підвищує прозорість і забезпечує стабільне довготривале управління доступами.

Хоча OAuth Scopes надають високу точність і безпеку контролю доступу, їхня роль обмежується керуванням конкретними дозволами в межах ресурсів чи API. Вони ефективні для короткострокових технічних сценаріїв, але не замінюють стабільну ієрархічну структуру, яку забезпечує RBAC.

Ієрархічна модель гарантує послідовність, централізований контроль і логічну підпорядкованість прав – це особливо важливо для великих організацій і внутрішніх систем.

Таким чином, ієрархічна модель ролей залишається ключовим елементом сучасних систем безпеки, оскільки забезпечує чітку структуру доступу, що відображає реальну організаційну ієрархію. Вона спрощує управління правами користувачів, знижує ризик помилок у доступах і підвищує контроль над інформацією. Завдяки зрозумілості та масштабованості, ця модель і надалі залишається ефективною основою для побудови безпечних корпоративних систем.

Список джерел

1. Marketing P. C. A complete guide to Roles Hierarchy and Access Controls for sales organisations. *CRM Blog | Pepper Cloud*. URL: https://blog.peppercloud.com/roles-hierarchy-and-access-controls-for-sales-organisations/ (дата звернення: 20.10.2025).

2. Using OAuth 2.0 scopes vs. permissions for app authorization. *Using OAuth 2.0 scopes vs. permissions for app authorization*. URL: https://www.aserto.com/blog/scopes-vs-permissions-authorization (дата звернення: 20.10.2025).

3. Bennett T. OAuth Scopes vs RBAC: Key Differences. *Blog*. URL: https://blog.dreamfactory.com/oauth-scopes-vs-rbac-key-differences (дата звернення: 20.10.2025).

4. What is Role-Based Access Control (RBAC)? Examples, Benefits, and More. *Enterprise IP and DLP Software | Digital Guardian*. URL: https://www.digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more (дата звернення: 20.10.2025).

5. RBAC vs. ABAC Access Control: What's the Difference? - DNSstuff. *Software Reviews, Opinions, and Tips - DNSstuff*. URL: https://www.dnsstuff.com/rbac-vs-abac-access-control (дата звернення: 20.10.2025).

INFORMATION PRACTICE THROUGH DIGITAL ETHICS: WORLDVIEW ASSESSMENT OF AI RELIABILITY

Bagrationi I. O.
Batumi Shota Rustaveli State University
Batumi 6010 / + 995 599 947 668
irma.bagrationi@bsu.edu.ge
Bagratishvili A. N.
Batumi Shota Rustaveli State University
Batumi 6010 / + 995 597 741 855
anri.bagratishvili@gmail.com

Annotation

The paper is devoted to the research and evaluation of ethical regularities of Artificial Intelligence as a certain digital existence in the context of worldview parameters. A critical review of the main provisions and principles surrounding the issue is given, finding and developing the progressive criteria in them and establishing a unique theoretical-worldview concept corresponding to modern requirements. The relationships fixed between the thinking of the fields of humanitarian and exact knowledge around the issue are shown in an original way; a kind of attempt is presented to understand and evaluate the system-conceptual model developed on the basis of moral criteria in the digital world of organized management in a new way.

The discursive resource of the axiological approach and the potential of constructing reflexive conclusions with the dialectical method are utilized and used. It is indicated what probable moral consequences can result from the solution of the intellectual dilemma established in modern digital practice, more specifically, the alternative task of the protocol and software of the creative-argumentative algorithm associated with it, In particular, the latter can only be considered in the format of an admissible possibility or present it in the form of an implemented cybernetic reality. The expected difficulties of interaction between natural and artificial intelligences and appropriate control mechanism paradigms are described and analyzed, namely, the concepts of the ethical value of the artifact are demonstrated - within the framework of essential and principled reliability/unreliability.

Introduction: Challenges in the process of developing moral criteria over time give rise to the need and necessity to review the traditional principles accompanying worldview knowledge. Based on the research question, it is interesting for us to find out what to expect in the field of worldview understanding and evaluation of Artificial Intelligence - from the aspect of ethical dimension. It is significant that two main aspects are still not clearly defined in the field of scientific discourse:

- What is the main function of applied ethics in the practical implementation of constructed knowledge about Artificial Intelligence?
- How well will the system of ethical values work following the software operation of the algorithmic mechanism of the simulated intelligence?

As is generally known, Ethics is a field of humanitarian knowledge, thus it conveys interdisciplinary knowledge and skills on one-world topics and uses open concepts, but when it comes to the concept of Artificial Intelligence, which acts as human intelligence in a certain field, and then Ethics moves from the category of humanitarian thinking to the line of exact sciences. And this is because the computer, as an Artificial Intelligence, must clearly define how to behave, and this is done on the basis of moral considerations, but the same spiritual and moral competences in turn, must already be