Міністерство освіти і науки України

NURE

Харківський національний університет радіоелектроніки

ЗБІРНИК

студентських наукових статей

«Автоматизація та приладобудування»

«Automation and Development of Electronic Devices»

ADED-2025

(Випуск 2)

[електронне видання]

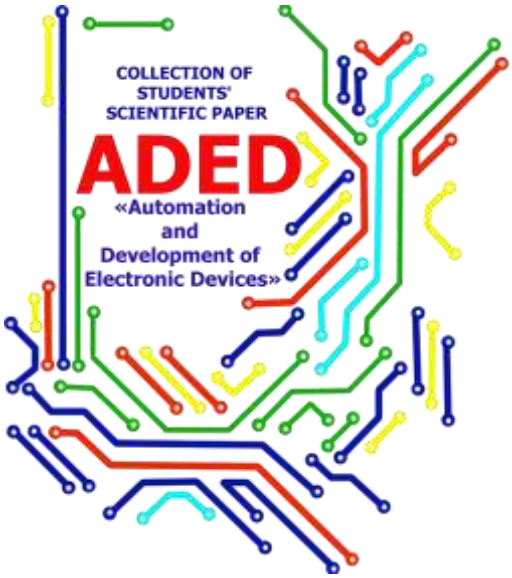
http://nure.ua/department/kafedra-komp-yuterno-integrovanih-tehnologiy-avtomatizatsiyi-ta-mehatroniki-kitam

http://itez.zntu.edu.ua/

http://kafea.kdu.edu.ua

Харків 2025

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки
кафедра комп'ютерно-інтегрованих технологій, автоматизації та робототехніки
(КІТАР)



ЗБІРНИК

студентських наукових статей

«Автоматизація та приладобудування»

«Automation and Development of Electronic Devices»

ADED-2025

(Випуск 2)

[електронне видання]

Харків 2025

ЗМІСТ

УДК 004.056

ЗАХИСТ ДАНИХ У СИСТЕМАХ АВТОМАТИЧНОГО ВІДСТЕЖЕННЯ РОБОЧОГО ЧАСУ

Чередніченко Т.О.
Харківський національний університет радіоелектроніки
Україна, 61000, Харків, пр. Науки 14
E-mail: tymofii.cherednichenko@nure.ua

Аннотація. У даній статті розглянуто та проаналізовано особливості функціонування сучасних систем автоматичного відстеження робочого часу, їх види та принципи побудови. У результаті аналізу виявлено переваги та недоліки існуючих підходів до обробки даних, а також визначено ключові напрями підвищення рівня захисту інформації в подібних рішеннях. Отримані результати можуть бути використані при розробленні нових або вдосконаленні наявних систем обліку робочого часу з урахуванням вимог безпеки персональних даних.

***Ключові слова*:** захист даних, автоматичне відстеження часу, конфіденційність, інформаційна безпека, DPIA.

DATA PROTECTION IN AUTOMATIC WORKING TIME TRACKING SYSTEMS

Cherednichenko T.O.
Kharkiv National University of Radio Electronics
Ukraine, 61000, Kharkiv, 14 Nauky Ave
E-mail: tymofii.cherednichenko@nure.ua

Abstract. This article examines and analyzes the features of modern automated work time tracking systems, their types, and design principles. The analysis reveals advantages and disadvantages of existing data processing approaches and outlines key directions for improving data security levels in such systems. The results can be applied in the development and enhancement of time-tracking systems with regard to data protection requirements.

Keywords: data protection, automated time tracking, privacy, information security, DPIA.

У сучасних умовах цифрової трансформації підприємств автоматизовані системи відстеження робочого часу стають невід'ємною частиною управлінських процесів [1-10]. Вони дозволяють оптимізувати облік робочого дня, підвищити продуктивність персоналу та забезпечити прозорість взаємодії між працівником і роботодавцем. Водночас активне використання таких технологій породжує нові виклики у сфері безпеки та конфіденційності даних.

Інформація, що збирається під час моніторингу – час входу й виходу з системи, місцезнаходження, IP-адреси, активність користувача – є персональними даними, які потребують належного рівня захисту [11-18]. Недотримання принципів оброблення таких даних може призвести до порушення законодавства та зниження довіри з боку працівників.

Актуальність питання захисту даних у системах відстеження часу обумовлена швидким поширенням віддаленої роботи та впровадженням цифрових рішень для контролю діяльності персоналу. Компанії активно застосовують різноманітні інструменти:

– QR-коди для реєстрації присутності [19];
– програмне забезпечення, що фіксує робочий час у фоновому режимі;
– хмарні сервіси для зберігання звітів.

Такі рішення підвищують ефективність управління, однак створюють ризики для приватності працівників. Відповідно до Загального регламенту ЄС про захист даних (GDPR)

та Закону України «Про захист персональних даних», будь-яке збирання інформації має бути законним, пропорційним і здійснюватися з чітко визначеною метою.

Тому дослідження принципів безпечної роботи подібних систем є важливим для забезпечення балансу між контролем та дотриманням прав людини на недоторканність приватного життя.

Забезпечення такого балансу вимагає системного підходу до організації роботи з персональними даними. Ефективний захист інформації у системах відстеження часу ґрунтується на комплексі організаційних і технічних заходів, що охоплюють весь життєвий цикл даних – від моменту їх збирання до знищення. Розглянемо детальніше ключові принципи та механізми, які дозволяють мінімізувати ризики та забезпечити відповідність сучасним вимогам законодавства.

I. Принципи захисту даних у системах відстеження часу.

1. Прозорість та інформування. Захист персональних даних починається з прозорості. Працівники мають бути поінформовані:

– які саме дані збираються та з якою метою вони використовуються;

– хто має до них доступ; та як довго вони зберігаються;

– у який спосіб здійснюється їх передавання.

Інформація про це повинна бути відображена у політиці конфіденційності або внутрішніх регламентах компанії. Також необхідно забезпечити можливість отримання згоди працівника на обробку його персональних даних у зрозумілій формі.

2. Мінімізація даних. Системи відстеження часу мають збирати лише ті дані, що безпосередньо потрібні для виконання визначених функцій:

– для нарахування заробітної плати достатньо фіксувати час початку та завершення роботи;

– для контролю виконання завдань (лише дані про проєкти та їх тривалість);

– моніторинг активності на клавіатурі чи зйомка екрана без службової необхідності є надмірним.

Принцип мінімізації сприяє підвищенню рівня довіри працівників і зменшує ризик порушення законодавства про захист персональних даних.

3. Обмеження терміну зберігання. Персональні дані повинні зберігатися протягом періоду, достатнього для досягнення мети їх обробки. Рекомендується:

– установлювати чітко визначені строки зберігання (наприклад, 6 або 12 місяців);

– автоматизувати процес видалення або анонімізації застарілих записів;

– періодично проводити аудит баз даних для виявлення надлишкової інформації.

Такі заходи забезпечують ефективне управління життєвим циклом даних і відповідають принципам GDPR.

II. Технічні заходи безпеки:

1. Шифрування є одним із головних інструментів захисту інформації. Його застосування доцільне як під час передавання даних мережею, так і при їх зберіганні. Найбільш поширеними є такі методи:

– використання TLS/SSL для захищених з’єднань;

– застосування алгоритмів шифрування AES-256;

– хешування паролів за допомогою bcrypt або Argon2.

Ці технології унеможливлюють несанкціонований доступ у разі кібератак або витоку інформації.

2. Контроль доступу. Ефективна система контролю доступу передбачає:

– визначення ролей користувачів і прав на обробку даних та застосування двофакторної автентифікації;

– ведення журналів дій користувачів;

– регулярну перевірку актуальності прав доступу.

Доступ до інформації повинен надаватися лише уповноваженим особам, зокрема працівникам HR-відділу або системним адміністраторам.

3. Безпека зберігання. Для забезпечення належного рівня безпеки необхідно:

– розміщувати дані на серверах, що відповідають міжнародним стандартам (ISO/IEC 27001, SOC 2) і перевіряти юрисдикцію зберігання даних відповідно до вимог General Data Protection Regulation – GDPR (рис. 1);

– укладати договори про обробку персональних даних із провайдерами хмарних сервісів;

– контролювати процеси резервного копіювання та знищення інформації.

Дотримання цих умов дозволяє мінімізувати юридичні ризики та підвищити рівень довіри користувачів.

Рисунок 1 – Принципи роботи GDPR

4. Оцінка впливу на захист даних (Data Protection Impact Assessment (DPIA)). Оцінка впливу на захист даних є інструментом, що дозволяє виявити потенційні ризики ще на етапі планування системи. Проведення DPIA (рис. 2) сприяє підвищенню прозорості діяльності компанії та дозволяє довести відповідність вимогам законодавства.

Рисунок 2 – Принципи роботи DPIA

Проведення DPIA включає:

– визначити потребу у DPIA – початковий аналіз необхідності проведення оцінки;
– описати обробку – детальний опис процесів обробки персональних даних;
– розглянути консультації – залучення зацікавлених сторін до обговорення;
– оцінити необхідність та пропорційність – аналіз виправданості заходів контролю;
– визначити та оцінити ризики – ідентифікація загроз для прав працівників;
– визначити заходи для зменшення ризиків – розробка превентивних механізмів;
– підписати та зареєструвати результати – формалізація висновків оцінки;
– інтегрувати результати у план – впровадження рекомендацій у діяльність;
– тримати на контролі – постійний моніторинг та перегляд ефективності.

Системи автоматичного відстеження робочого часу є важливим інструментом підвищення ефективності управління персоналом. Проте їх використання потребує відповідального ставлення до обробки персональних даних. Дотримання таких принципів, як прозорість, мінімізація, обмеження терміну зберігання, а також упровадження технічних заходів захисту – шифрування, контроль доступу, безпечне зберігання – дозволяють забезпечити належний рівень інформаційної безпеки. Проведення оцінки впливу (DPIA) є додатковим інструментом управління ризиками, який допомагає компаніям працювати у правовому полі та формувати культуру захисту даних.

На основі проведеного аналізу систем відстеження робочого часу виявлено ключові переваги та недоліки існуючих підходів до обробки персональних даних. Серед переваг слід відзначити оптимізацію управлінських процесів через автоматизацію обліку робочого дня, що спрощує нарахування заробітної плати та підвищує продуктивність персоналу. Застосування цифрових інструментів забезпечує прозорість відносин між працівником і роботодавцем. Використання сучасних методів шифрування та багаторівневого контролю доступу унеможливлює несанкціонований доступ при кібератаках. Розміщення даних на серверах, сертифікованих за міжнародними стандартами, гарантує високий рівень безпеки зберігання інформації. Застосування методології DPIA дозволяє виявляти потенційні ризики на етапі планування системи.

Водночас виявлено суттєві недоліки. Збирання широкого спектру персональних даних створює загрози для конфіденційності працівників при недотриманні принципів мінімізації. Застосування надмірного моніторингу порушує баланс між контролем та правами людини на недоторканність приватного життя. Недотримання вимог законодавства щодо законності та пропорційності обробки даних може призвести до правових санкцій. Відсутність прозорості у політиці конфіденційності знижує рівень довіри персоналу до роботодавця. Складність управління життєвим циклом даних через відсутність чітких строків зберігання та автоматизованих процесів видалення призводить до накопичення надлишкової інформації. Впровадження комплексних технічних та організаційних заходів вимагає значних ресурсів для контролю юрисдикції зберігання, ведення журналів дій та регулярної перевірки прав доступу.

Таким чином, існуючі підходи мають суттєвий потенціал для підвищення ефективності управління персоналом, однак потребують збалансованого впровадження з обов'язковим дотриманням принципів захисту персональних даних для мінімізації ризиків порушення конфіденційності працівників.

У статті проаналізовано проблематику захисту персональних даних у системах автоматизованого відстеження робочого часу в контексті цифрової трансформації підприємств. Встановлено, що впровадження таких систем створює подвійний ефект: з одного боку, оптимізує управлінські процеси та підвищує прозорість взаємодії між працівником і роботодавцем, з іншого – породжує ризики порушення конфіденційності та недотримання законодавчих вимог щодо обробки персональних даних. Систематизовано ключові організаційно-правові принципи захисту даних, які мають застосовуватися при експлуатації

систем відстеження часу: прозорість та інформування працівників, мінімізація обсягу даних що збираються, обмеження термінів їх зберігання. Обґрунтовано, що дотримання цих принципів забезпечує відповідність вимогам GDPR та національного законодавства про захист персональних даних. Визначено комплекс технічних заходів безпеки, необхідних для захисту інформації на всіх етапах її життєвого циклу: шифрування даних при передаванні та зберіганні (TLS/SSL, AES-256), багаторівневий контроль доступу з двофакторною автентифікацією, розміщення даних на серверах, що відповідають міжнародним стандартам (ISO/IEC 27001, SOC 2). Розкрито методологію проведення оцінки впливу на захист даних (DPIA) як превентивного інструменту виявлення ризиків ще на етапі планування системи. Показано, що DPIA включає дев'ять послідовних етапів і дозволяє компаніям документально підтвердити законність обробки персональних даних. Практична цінність дослідження полягає у формуванні цілісного підходу до безпечної експлуатації систем відстеження робочого часу, що дозволяє організаціям збалансувати потреби контролю з дотриманням прав працівників на недоторканність приватного життя.

ЛІТЕРАТУРА:

15. Cherednichenko, T., et al. Features of automatic working time control systems Manufacturing & Mechatronic Systems 2025: Proceedings of IX st International Conference, Kharkiv, October 25-26, 2025: Thesises of Reports. – 2025. – pp. 54-57

16. Danylenko, M. M., et al. Comparative analysis of modern SCADA packages for production automation // International Journal of Academic Engineering Research (IJAER). – 2025. – Vol. 9. – 2. – pp. 26-34

17. Sotnik, S. V. Development of automated control system and registration of metal in continuous casting // Radio Electronics, Computer Science, Control. – 3. – 2024. – pp. 197-211

18. Konieva, A., et al. Main trends in the development of automated image processing systems // «Computer-integrated technologies, automation and robotics» CITAR-2025. – 2025. – pp. 68-72

19. Vasylchenko, Y., et al. Development of Security and Fire Alarm Integrated Automation System at Enterprise // WSEAS Transactions on Systems. – 2025. – 24. – pp. 642-664

20. Sotnik, S. Development of automated control system for continuous casting // Radio Electronics, Computer Science, Control. – 2. – 2024. – pp. 181-189

21. Marunich, R.V., et al. Modern IoT technologies for creating automated access systems // Sustainable smart cities and communities: business and innovation solutions 2025: Proceedings of I st I International Conference, Kharkiv, April 21, 2025: Thesises of Reports. – 2025. – pp. 38-39

22. Sotnik, S. Integration of IoT into security systems: opportunities and risks // International Journal of Academic Engineering Research (IJAER), 2024. – Vol. 8, Issue 11. – pp. 56-61

23. Khalimonov, Y.I., et al. Circular economy in automated systems // Sustainable smart cities and communities: business and innovation solutions 2025: Proceedings of I st I International Conference, Kharkiv, April 21, 2025: Thesises of Reports. – 2025. – pp. 53-54

24. Sotnik, S. Development of a range measurement module on an ultrasonic sensor with a GSM module // Radio Electronics, Computer Science, Control. – 2. – 2025. – pp. 32-44

25. Tverdokhlib, A., et al. Intelligent tools for optimizing information and search engines // Manufacturing & Mechatronic Systems 2024: Proceedings of VIII st International Conference, Kharkiv, October 25-26, 2024, pp. 28-31

26. Sotnik S. V. Analysis of Personal Information Security Issues in Peacetime and Wartime // International Journal of Academic Engineering Research (IJAER), 2024, Vol. 8 Issue 10, pp. 108-113

27. Hubar, A.Y., Sotnik, S.V. Impact of automation and CALS technologies on human factor in production // The 5th International scientific and practical conference “Perspectives of contemporary science: theory and practice” (June 24-26, 2024) SPC “Sci?conf.com.ua”, Lviv, Ukraine, 2024. – c. 243-249

28.Sotnik, S. V. Features of using REST architecture for development of ARS for information systems // Міжнародна науково-практична конференція «Інформаційні системи в управлінні проєктами та програмами», Коблево, 9–13 вересня 2024 р. Збірник праць. – Харків: ХНУРЕ, 2024. – с. 42-45

29. Marunich, R., et al. Approaches to ensuring the effective implementation of IoT technologies in various industries // International Conference «DIGITAL INNOVATION & SUSTAINABLE DEVELOPMENT 2024», 2024 – pp. 22-23

30. Sotnik, S. Evaluating relational database scaling strategies in web engineering // International Conference on Advanced Trends In Radioelectronics and Infocommunications (ATRIC-2025) (May 21–22, 2025), Lviv Polytechnic Publishing House, Lviv, Ukraine, 2025. – pp. 224-228

31.Borysenko, I. A., et al. Chat gpt features in data search // MDPC Publishing, 2023. – pp. 143-149

32. Rudenko, M., et al. Overview of approaches to scaling relational databases in development and adaptation of web applications // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: Тези доповідей XII Міжнародної науково-практичної конференції (10-12 грудня 2024 р., м. Запоріжжя). [Електронний ресурс] /Електрон. дані. – Запоріжжя: НУ «Запорізька політехніка», 2024. – С. 398-402

33. Deineko, Z., et al. Dynamic and Static QR Coding // IJAER, 2022. – pp. 1-6