https://doi.org/10.31891/2219-9365-2025-82-31
УДК 004.05:004.02

ГАЛАГАН Наталія
Державний університет інформаційно-комунікаційних технологій
https://orcid.org/0000-0001-8582-3126
e-mail: n.halahan@duikt.edu.ua
БОРИСЕНКО Ірина
Київський національний університет імені Тараса Шевченка
https://orcid.org/0009-0001-8582-3126
e-mail: borysenko.iryna@knu.ua
ХАБ'ЮК Наталія
Державний університет інформаційно-комунікаційних технологій
https://orcid.org/0009-0005-7917-5528
e-mail: n.khabiuk@duikt.edu.ua
СТАРОДУБЦЕВ Ярослав
Державний університет інформаційно-комунікаційних технологій
https://orcid.org/0009-0007-5787-3661
e-mail: y.starodubtsev@stud.duikt.edu.ua
КОВАЛЬЧУК Нікіта
Київський національний університет імені Тараса Шевченка
https://orcid.org/0009-0001-0499-2452
e-mail: bonita1953112233@gmail.com

КОНЦЕПТУАЛЬНА МОДЕЛЬ ОРГАНІЗАЦІЙНО-ТЕХНІЧНОЇ СИСТЕМИ КІБЕРЗАХИСТУ IoT-ПЛАТФОРМ

У статті розглядається підвищення ефективності безпеки в інтелектуальних мережах із застосуванням технологій Інтернету речей (IoT) шляхом впровадження методу диференційованої конфіденційності. Запропоновано використання методу диференціальної конфіденційності для забезпечення захисту від несанкціонованого доступу до складових частин, програмного забезпечення, баз даних та архівів. обґрунтовано доцільність використання номінально-структурного методу як основи для побудови моделі безпеки, яка дозволяє здійснювати метризацію зв'язків та забезпечує узгодженість між внутрішньою і зовнішньою структурами системи. У статті проаналізовано основні організаційні та технічні заходи безпеки для IoT-середовища, включаючи управління життєвим циклом пристроїв, архітектурою безпеки, навчанням персоналу, шифруванням, моніторингом і конфігураційним управлінням. Розглянуто застосування номінально-структурного методу та введення додаткової функції диференційованої конфіденційності. Представлено математичні моделі та способи досягнення диференційованої конфіденційності. Зазначається, що застосування диференційованої конфіденційності створює анонімні дані шляхом додавання шуму, що сприяє захисту конфіденційності та підвищенню рівня безпеки та надійності роботи системи.

Ключові слова: диференційована конфіденційність, інтелектуальні мережі, IoT

HALAHAN Nataliia
State University of Information and Communication Technologies
BORYSENKO Iryna
Taras Shevchenko National University of Kyiv
KHABIUK Nataliia, STARODUBTSEV Yaroslav
State University of Information and Communication Technologies
KOVALCHUK Nikita
Taras Shevchenko National University of Kyiv

CONCEPTUAL MODEL OF ORGANIZATIONAL AND TECHNICAL SYSTEM FOR CYBER SECURITY OF IoT PLATFORM

The article presents a comprehensive exploration of how the development of Internet of Speech technologies, a subset of the Internet of Things (IoT), contributes to improved security measures through the application of differential confidentiality methods. The central argument of the study is that enhancing security in intelligent systems requires innovative approaches to data protection, especially in environments characterized by constant data exchange and user interaction. The authors propose the integration of differential confidentiality to mitigate risks related to unauthorized access to critical digital resources such as storage units, software platforms, databases, and archival systems. This technique ensures that sensitive information remains protected even when shared or processed, by introducing controlled statistical noise that obscures personal identifiers. A key contribution of the article is the justification of a nominal-structural method as a foundational element of an individualized security model. This method is designed to manage and monitor the interplay between internal and external components of an intelligent system, thereby maintaining system coherence and strengthening resistance to cyber threats. The study outlines how this structural framework facilitates efficient connection management and adaptability to various system states and operational conditions. Furthermore, the paper provides a thorough analysis of both organizational and technical security measures within the IoT ecosystem. These include life cycle management of IoT devices, the development of robust security architectures, the importance of continuous personnel training, implementation of encryption standards, real-time system monitoring, and configuration management.

Additionally, the article explores the mathematical underpinnings of differential confidentiality, offering formal models that support its practical implementation. The authors emphasize the dual impact of this method: while it intentionally adds noise to data for anonymization purposes, it paradoxically strengthens overall system security by preventing precise data extraction, thereby enhancing the integrity and resilience of robotic and intelligent systems.
Key words: differentiated privacy, intelligent measures, IoT

Стаття надійшла до редакції / Received 16.04.2025
Прийнята до друку / Accepted 11.05.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Розв'язання локальних задач проблеми оптимального управління безпекою інтелектуальних мережам із застосуванням IoT, веде до впровадження різних методологічних основ. У результаті методологічної незалежності практичне використання локальних теорій зводиться до загальних оцінок, тому що локальні теорії об'єднані в загальну технологію управління на загальній основі логіко-експертного та номінально-структурного методів [1, 3]**.**

Ефективність процесів управління безпекою великою, а іноді й визначальною мірою залежить від сучасних технологій, які застосовуються в системі функції. Принциповим положенням управління безпекою є вибір математичної моделі, тому застосування номінально-структурного методу та введення додаткової функції диференційованої конфіденційності є доцільним. Диференційована конфіденційність криптографічна характеристика конфіденційності даних, яка може бути застосована для реалізації функцій в системах з інтелектуальними мережами із застосуванням IoT.

Мета статті. Метою дослідження є підвищення ефективності безпеки в інтелектуальних мережам із застосуванням IoT за рахунок використання методу диференціальної конфіденційності.

МАТЕРІАЛИ ТА РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Організаційні та технічні заходи забезпечення безпеки IoT. Слід передбачити захист від будь-якого несанкціонованого доступу до складових частин, програмного забезпечення, баз даних та архівів, важливих для безпеки, для запобігання можливому умисному або ненавмисному внесенню перешкод у роботі, зміні та псуванню програм даних, що можуть створити загрозу для безпеки. Об'єктами захисту від несанкціонованого доступу мають бути:

- мережеві з'єднання між контролерами та приводами;
- датчики, приводи та джерела живлення;
- системи адміністрування IoT;
- протоколи інтелектуальних мереж із застосуванням IoT
- програмне забезпечення.

Для захисту від несанкціонованого доступу в інтелектуальних мережх із застосуванням IoT мають бути передбачені групи заходів безпеки IoT, включаючи політику безпеки, організаційну та технічну практики.

Політика безпеки в основному відноситься до правил і процедур, які повинні бути прописані при побудові технічних систем, щоб допомогти забезпечити хороший рівень кібербезпеки. Крім того, питання конфіденційності виробників, які повинні гарантувати, що їхні рішення не порушують правила конфіденційності та оператори, яким мають забезпечувати конфіденційність пов'язану з ризиками та інформувати про те, як використовувати пристрої IoT без розкриття особистої інформації користувачів [2, 4].

Організаційні принципи та управління є неодмінними факторами та критичними з точки зору безпеки компанії. Такі заходи безпеки пояснюють, як повинні працювати промислові компанії, які організаційні правила та обов'язки вони повинні встановити та який підхід вони мають застосувати до своїх працівників і сторонніх підрядників для ефективної обробки інцидентів кібербезпеки, керувати вразливими місцями та забезпечувати безпеку рішень IoT їх життєвий цикл.

Організаційні практики включають шість наступних категорії рис. 1:

– Життєвий цикл кінцевих точок включає заходи безпеки, пов'язані з безпекою на різних етапах продукту (включаючи кінцеві пристрої та інфраструктуру) життєвий цикл, включаючи процес закупівлі, ланцюжок поставок, передачу, експлуатація та кінець життєвого циклу;

– Архітектура безпеки включає заходи безпеки щодо архітектурного підходу і створення архітектури безпеки.

– Усунення інцидентів включає заходи безпеки щодо виявлення та реагування на інциденти, які можуть виникнути в системі IoT середовища;

– Управління вразливими місцями включає заходи безпеки на процес управління вразливістю, пов'язані з цим дії та вразливість розкриття;

– Навчання та обізнаність включає заходи безпеки щодо рекомендованого підходу, пов’язаного з навчанням та підвищенням рівня безпеки обізнаності співробітників, які працюють з пристроями та системами IoT;

– Управління третьою стороною включає заходи безпеки, пов’язані з управління третьою стороною та контролю доступу сторонньої сторони [5].

Рис. 1. Організаційні заходи безпеки IoT

Окрім впровадження політики та організаційних практик, безпеку також необхідно будувати за допомогою відповідних технічних можливостей рішень IoT і середовища, де вони розгорнуті. Технічні практики включають десять наступних категорій Рис.2:

– Керування довірою та доброчесністю включає забезпечують цілісність і надійність даних і пристроїв;

– Хмарна безпека включає заходи безпеки щодо різних аспектів безпеки;

– Безперервність роботи та відновлення включає заходи безпеки щодо розробки, тестування та перегляду плану компанії по забезпеченню стійкості та безперервності операцій у разі безпеки інцидентів;

– Безпека між машинами включає заходи безпеки щодо зберігання ключів, шифрування, перевірки введених даних і захисту в між машинному зв'язку;

– Захист даних включає заходи безпеки щодо захисту конфіденційних даних на різних рівнях організації та управління доступом до даних;

– Оновлення програмного забезпечення/прошивки включають заходи безпеки щодо перевірки, тестування та виконання патчів;

– Контроль доступу включає заходи безпеки щодо контролю віддаленого доступу, автентифікації, привілеїв, облікових записів і фізичного доступу;

– Мережеві, протоколи та шифрування включають заходи безпеки які можуть допомогти забезпечити безпеку зв’язку за допомогою належної реалізації протоколів, шифрування та сегментації мережі;

– Моніторинг і аудит включає заходи безпеки щодо моніторингу мережевого трафіку та доступності, збір журналів і відгуки;

– Керування конфігурацією включає заходи безпеки щодо конфігурації безпеки, управління змінами в конфігурації, зміцнення пристроїв і перевірка резервного копіювання.

Формалізація структурного підходу до управління безпекою. Якщо розглядати організаційні принципи та технічних можливостей рішень IoT, систему можна представити у вигляді номінальної структури.

Налагоджена системи вкладення зв’язків і відповідностей дозволяє зберегти цілісність системи і показати в системі метризації, що внутрішня структура не залишається байдужою до процесів взаємодії у зовнішній структурі [6].

Нехай задано довільна кінечна множина M або n таких множин в загальному випадку деяких $M_1, M_2, ..., M_n$. Будь-яка множина впорядкованих кортежів з n елементів $Q=\{x_1,x_2,... x_n\}$. таких, що $x_i \in M_i$ прийнято називати n-арною відповідністю. У тому випадку, коли всі елементи x_i належать одній і тій самій множині M і, відповідно, $Q \subseteq M^n$, говорять, що Q – це n-арне відношення. Множина M разом із заданою на ньому множиною зв’язків і відповідностей прийнято називати системою зі зв’язками, або моделлю. Як вже

зазначалося, ми будемо розглядати системи з відносинами або моделі спеціального типу, що представляють впорядковані по вкладенню сукупності зв'язків або відповідностей. Як буде видно далі, такі моделі дозволяють проводити метризацію відповідностей (відносин) величинами зв'язків, які мають властивість узгодженості зв'язків зі структурою [7].

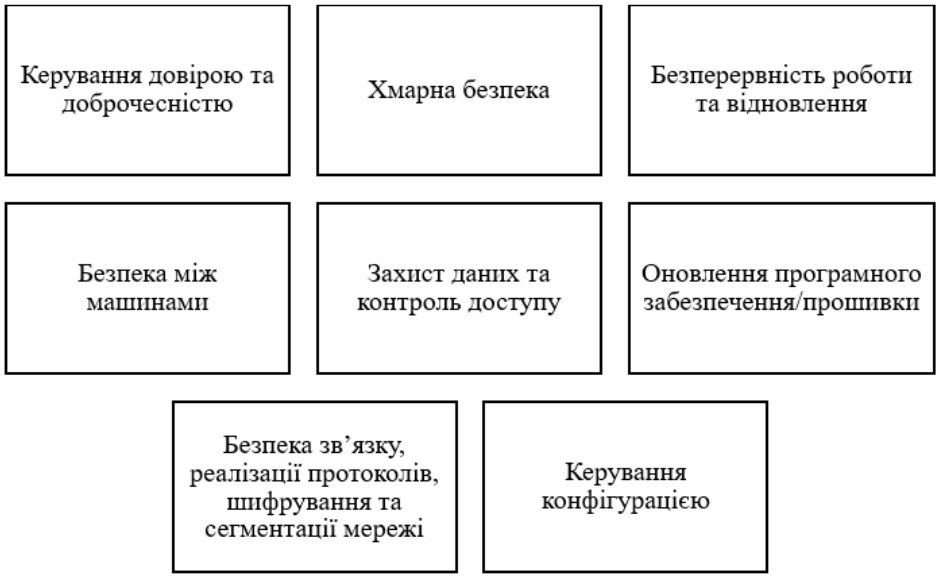

Рис. 2. Технічних можливостей рішень IoT

Нехай $M = M_1 * M_2 * \dots M_n$ – носій системи відповідностей (відносин) або моделі системи з сімейства *n*-арних відповідностей (відносин), таких, що $R_1 \subset R_2 \subset \cdots \subset R_m$ будемо називати *n*-арною структурою: $ST = \langle M, (R_i)_{i \in l_m} \rangle$. Позначимо через Z множину дійсних чисел.

Функція $\varphi: M_1 \times \dots \times M_n \to Z$ неперервна знизу (зверху) на структурі $ST = \langle M, (R_i)_{i \in l_m} \rangle$, якщо для $\forall\, i \in J_m$ існує $\exists\, h_i$, таке, що

1. $(x_1, x_2, \dots, x_n) \in R_i \Leftrightarrow \varphi(x_1, x_2, \dots, x_n) \leq h_i (\geq)$,
2. $R_i \subset R_j \Leftrightarrow h_i < h_j (>)$.

Очевидно, що функція φ може бути неперервна на структурі або як відстань (знизу), або як близькість (зверху), але з точки зору формальних побудов ці випадки не розрізняються, тобто в якості опції φ можна використовувати як коефіцієнти кореляції, так і евклідові відстані без зміни алгоритмів структурного аналізу.

Нехай *C* – множина *n*-арних функцій на заданому носії *M*. Нескладно довести справедливість наступних тверджень:

для будь-якої функції $\varphi \in C$ існує та єдина структура *ST*, на якій φ неперервна;

для будь-якої структури *ST* існує функція φ, яка на ній неперервна.

Якщо функції φ і ψ безперервні на одній і тій же структурі, то їх будемо називати узгодженими. Множини n-арних структур і класів узгоджених функцій є ізоморфними для даного носія. Можна визначити ізоморфізм структур, що дозволяє порівнювати структури, і, очевидно, тобто легко побудувати ізоморфізм фактор-структури *ST* і структури *ST*, безперервні функції яких будуть узгоджені.

Структура $ST = \langle M, (R_i)_{i \in l_m} \rangle$ називається номінальною, якщо для будь-якого $i \in J_m$ відповідність R_i має властивість $R_i \cdot R_i^{(p)} \cdot R_i = R_i$, де операція є композицією відносин.

У випадку, коли носій *M* є декартовим добутком $M_1 \times M_1$, а R_i– бінарні відносини. У цьому випадку структура $ST = \langle M, (R_i)_{i \in l_m} \rangle$, є номінальною, якщо для будь-якого *i* відношення R_i є відношенням еквівалентності. Функція φ, безперервна на номінальної структурі, володіє властивістю, а саме

$$\varphi(x, y) \leq max[\varphi(x, z), \varphi(z, y)] \text{ для } \forall x, y, z \in M. \quad (1)$$

Застосування методу диференційованої конфіденційності. З огляду на потребу точного відображення внутрішньої логіки взаємодії елементів IoT-системи, номінально-структурний підхід до моделювання безпеки можна розширити шляхом включення додаткового параметра — функції диференційованої конфіденційності. Її впровадження дозволяє деталізувати опис відповідностей у структурі, підвищити рівень абстракції моделі та забезпечити формалізований захист конфіденційних даних [8].

Розглянемо математичний механізм реалізації цього підходу.

Простий спосіб вивести функцію таким чином, щоб досягти диференційованої конфіденційності, полягає використання так званого «експоненціального механізму». Цей підхід передбачає побудову відповідної скінченної множини функцій $G = \{g_i, \dots, g_m\} \in R^T$, в якій кожна функція f_D має розумне наближення при деякій функції відстані d. Потім, коли на вхід подається D, вибирається функція шляхом вибірки з множини G з ймовірностями, заданими формулою.

$$P_D(g_i) \propto exp\left\{\frac{-\alpha}{2S} d(g_i, f_D)\right\}, S \stackrel{\text{def}}{=} sup_{D \sim D`} d(f_D, f_{D`}) \quad (2)$$

Така методика забезпечує α-диференційовану конфіденційність в великих технічних системах. Цей метод концептуально привабливий своєю простотою, і в одно час залишається складним для застосування, оскільки набір функцій G може бути дуже великим, щоб забезпечити корисність виділеної функції (у сенсі очікуваної похибки). Оскільки алгоритм, який виводить результати з P_D, повинен отримати константу нормалізації до наведеного вище розподілу, він, очевидно, повинен обчислити ймовірності для кожного g_i , що може бути надзвичайно трудомістким [9].

Для формування загальної алгоритмічної схеми реалізації номінально-структурного підходу задається масив даних, тобто на елементах носія M задаються ознаки, що характеризують ці елементи. Як правило, цей масив даних являє собою деяку статистику значень як якісних, так і кількісних ознак, що описують заданий склад емпіричних елементів.

У загальному випадку за масивом даних, що характеризують елементи структури M, будується функція φ, що визначає топологію подібності між елементами. На рис. 1 наведено схему алгоритму побудови номінальних структур, що визначає класи алгоритмів довільного порядку.

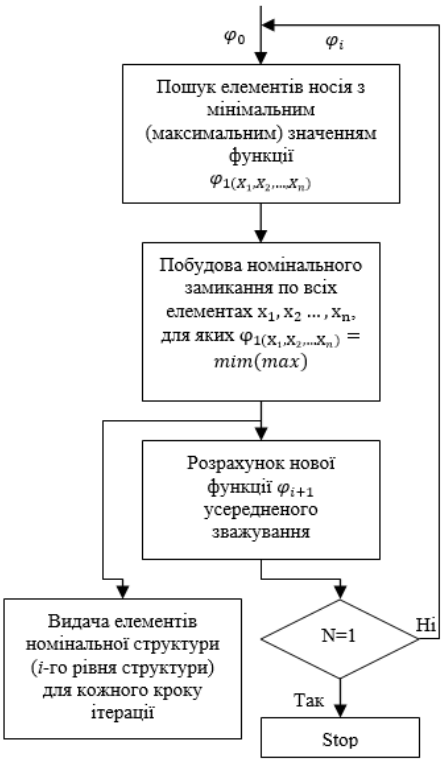

Рис.3 Схема алгоритму побудови номінальних структур системи кіберзахисту IoT платформ

Обсяг структури може бути кількісно оцінений функціоналом *V(φ),* який розраховується за функцією зв'язків *φ.* Для системи зв'язку обсяг структури збігається з величиною найкоротшої зв'язуючої мережі. В даному випадку обсяг структури $V(\varphi)$ можна вирахувати за допомогу формули

$$V(\varphi) = 2\sum_{i-1}^{m}\left(\left|M/\tau_{h_{i-1}}\right| - \left|M/\tau_{h_i}\right|\right)h_i \quad (3)$$

Описаний підхід до дослідження структур складних систем шляхом побудови номінальних структур цієї системи дозволяє успішно вирішувати ряд завдань системного аналізу в управлінні.

Застосування експоненціального механізму по суті відповідав дискретизації простору функцій R^T. Альтернативою є дискретизація вхідного простору T та апроксимація функції , де частини відповідають дискретизації T. Таким чином, апроксимацію можна розглядати як вектор з дійсними значеннями, з одним входом для значення кожного відрізка функції.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Такі методи, можна інтерпретувати як виведення дискретної випадкової величини та виконання визначення конфіденційності по відношенню до σ-поля, що складається з степеневої множини G.

Застосування диференційованої конфіденційності створює анонімні дані шляхом додавання шуму в інтелектуальні мережі з застосуванням IoT. Доданий шум допомагає захистити конфіденційність та підвищити рівень безпеки та надійності роботи системи.

Література

1. Руденко Н. В., Шрам М. М. Забезпечення безпеки логістики у світі великих даних, хмарних обчислень та Інтернету речей // *Наукові записки телекомунікацій*. – 2024. – № 1. – С. 59–69.DOI: https://doi.org/10.31673/2786-8362.2024.010808
2. Руденко Н. В., Луцюк І. В., Сутик А. П. Дослідження безпеки та приватності систем Інтернету речей у мережах мобільного зв'язку // *Зв'язок*. – 2023. – № 6. – С. 19–22.
3. Berlinet, A., & Thomas-Agnan, C. (2004). *Reproducing Kernel Hilbert Spaces in Probability and Statistics*. Kluwer Academic Publishers.
4. Billingsley, P. (1995). *Probability and Measure* (3rd ed.). Wiley-Interscience. Bousquet, O., & Elisseeff, A. (2002). Stability and generalization. *Journal of Machine Learning Research*, 2, 499–526.
5. Charest, A. (2012). *Creation and Analysis of Differentially-Private Synthetic Datasets* (PhD thesis). Carnegie Mellon University. Chaudhuri, K., & Hsu, D. (2012). Convergence rates for differentially private statistical estimation. In *Proceedings of the 29th International Conference on Machine Learning (ICML'12)*.
6. Chaudhuri, K., & Monteleoni, C. (2008). Privacy-preserving logistic regression. In *Advances in Neural Information Processing Systems (NeurIPS 2008)*.
7. Chaudhuri, K., & Monteleoni, C. (2011). Differentially private empirical risk minimization. *Journal of Machine Learning Research*, 12, 1069–1109.
8. Chawla, S., Dwork, C., McSherry, F., & Talwar, K. (2005). On the utility of privacy-preserving histograms. In *Proceedings of the 21st Conference on Uncertainty in Artificial Intelligence (UAI)*. Dwork, C. (2006). Differential privacy. In *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP)*, 1–12.
9. Dwork, C., & Lei, J. (2009). Differential privacy and robust statistics. In *Proceedings of the 41st ACM Symposium on Theory of Computing (STOC)*, 371–380.

References

1. Rudenko N. V., Shram M. M. Zabezpechennia bezpeky lohistyky u sviti velykykh danykh, khmarnykh obchyslen ta Internetu rechei [Ensuring logistics security in the world of big data, cloud computing, and the Internet of Things] // *Naukovi zapysky telekomunikatsii*. – 2024. – No. 1. – P. 59–69. DOI: https://doi.org/10.31673/2786-8362.2024.010808
2. Rudenko N. V., Lutsiuk I. V., Sutyk A. P. Doslidzhennia bezpeky ta pryvatnosti system Internetu rechei u merezhakh mobilnoho zviazku [Study of security and privacy of Internet of Things systems in mobile networks] // *Zviazok*. – 2023. – No. 6. – P. 19–22.
3. Berlinet, A., & Thomas-Agnan, C. (2004). *Reproducing Kernel Hilbert Spaces in Probability and Statistics*. Kluwer Academic Publishers.
4. Billingsley, P. (1995). *Probability and Measure* (3rd ed.). Wiley-Interscience. Bousquet, O., & Elisseeff, A. (2002). Stability and generalization. *Journal of Machine Learning Research*, 2, 499–526.
5. Charest, A. (2012). *Creation and Analysis of Differentially-Private Synthetic Datasets* (PhD thesis). Carnegie Mellon University. Chaudhuri, K., & Hsu, D. (2012). Convergence rates for differentially private statistical estimation. In *Proceedings of the 29th International Conference on Machine Learning (ICML'12)*.
6. Chaudhuri, K., & Monteleoni, C. (2008). Privacy-preserving logistic regression. In *Advances in Neural Information Processing Systems (NeurIPS 2008)*.
7. Chaudhuri, K., & Monteleoni, C. (2011). Differentially private empirical risk minimization. *Journal of Machine Learning Research*, 12, 1069–1109.
8. Chawla, S., Dwork, C., McSherry, F., & Talwar, K. (2005). On the utility of privacy-preserving histograms. In *Proceedings of the 21st Conference on Uncertainty in Artificial Intelligence (UAI)*. Dwork, C. (2006). Differential privacy. In *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP)*, 1–12.
9. Dwork, C., & Lei, J. (2009). Differential privacy and robust statistics. In *Proceedings of the 41st ACM Symposium on Theory of Computing (STOC)*, 371–380.