EUROPEAN CONFERENCE

Conference Proceedings

The IV International Science Conference «ACTUAL PROBLEMS OF PRACTICE AND SCIENCE AND METHODS OF THEIR SOLUTION»

January 31 – February 02, 2022

Milan, Italy

ACTUAL PROBLEMS OF PRACTICE AND SCIENCE AND METHODS OF THEIR SOLUTION

Abstracts of IV International Scientific and Practical Conference

Milan, Italy

(January 31 – February 02, 2022)

UDC 01.1

ISBN – 978-9-40364-508-7

The IV International Scientific and Practical Conference «Actual problems of practice and science and methods of their solution», January 31 – February 02, Milan, Italy. 699 p.

Text Copyright © 2022 by the European Conference (https://eu-conf.com/).
Illustrations © 2022 by the European Conference.
Cover design: European Conference (https://eu-conf.com/).
© Cover art: European Conference (https://eu-conf.com/).
© All rights reserved.

No part of this publication may be reproduced, distributed, or transmitted, in any form or by any means, or stored in a data base or retrieval system, without the prior written permission of the publisher. The content and reliability of the articles are the responsibility of the authors. When using and borrowing materials reference to the publication is required. Collection of scientific articles published is the scientific and practical publication, which contains scientific articles of students, graduate students, Candidates and Doctors of Sciences, research workers and practitioners from Europe, Ukraine, Russia and from neighboring countries and beyond. The articles contain the study, reflecting the processes and changes in the structure of modern science. The collection of scientific articles is for students, postgraduate students, doctoral candidates, teachers, researchers, practitioners and people interested in the trends of modern science development.

The recommended citation for this publication is: Ashtayeva M. Environmental trends in modern landscape design // Actual problems of practice and science and methods of their solution. Abstracts of IV International Scientific and Practical Conference. Milan, Italy 2022. Pp. 22-24.

URL: https://eu-conf.com.

ПРОГНОЗ У СФЕРІ КОНФЕДІЦІЙНОСТІ

Мордвинцев Микола Володимирович
канд. тех. наук, доц.
провідний співробітник науково-дослідної лабораторії
проблем розвитку інформаційних технологій
Харківського національного університету внутрішніх справ

Демидов Захар Георгійович
старший науковий співробітник науково-дослідної лабораторії
проблем розвитку інформаційних технологій
Харківського національного університету внутрішніх справ

Колмик Олег Олександрович
науковий співробітник науково-дослідної лабораторії
проблем розвитку інформаційних технологій
Харківського національного університету внутрішніх справ

Інтернетом люди користуються не тільки для перегляду розважального контенту та листування з друзями, глобальна мережа забезпечує такі базові потреби суспільства, як логістика, робота державних служб і банківських сервісів. Споживачі спілкуються з компаніями в месенджерах та замовляють доставку їжі замість того, щоб ходити по магазинах, наукові конференції відбуваються на віртуальних платформах, а кількість галузей, де віддалена робота стала нормою, продовжує зростати.

Усі ці процеси позначаються у сфері конфіденційності. Компанії хочуть отримати більше інформації про дії своїх клієнтів в інтернеті, щоб підвищувати якість обслуговування, і одночасно з цим ускладнюють процедури авторизації, щоб протистояти шахраям. Влада багатьох країн прагне спростити ідентифікацію користувачів з метою боротьби з кіберзлочинцями та «традиційними» угрупованнями, які координують свою діяльність онлайн. Громадян, у свою чергу, все більше турбують нестачу приватності та залежність від онлайн-сервісів.

Технології збереження конфіденційності стали однією з обговорюваних тем у сфері технічного прогресу, хоча деякі з них — наприклад, NeuralHash або федеративне когортне навчання — викликають неоднозначну реакцію. Проте варто визнати: такі нововведення, як локальна обробка звуку для Siri або приватне обчислювальне ядро Android, це великий крок у бік підвищення конфіденційності користувачів. Крім того, у цій сфері з'явилося багато нових сервісів, створених молодими компаніями, які лише починають монетизувати

свої послуги. Також спостерігається посилення тенденції захисту конфіденційності (яке відображається і в маркетингу, і в технологіях) серед розробників додатків для iOS і Android. Facebook (зараз Meta) теж намагається забезпечити більший рівень приватності своїх користувачів: компанія ввела наскрізне шифрування резервних копій у WhatsApp і позбавилася технології розпізнавання осіб у Facebook.

Якими будуть наслідки цих процесів? Нижче розповідається про основні чинні сили, які, можливо, формуватимуть ландшафт конфіденційності у 2022 році.

1. Технологічні гіганти нададуть людям більше інструментів контролю конфіденційності — у межах. Оскільки компанії по всьому світу змушені дотримуватися безлічі строгих нормативів захисту даних, вони будуть надавати клієнтам своїх сервісів все більше інструментів для контролю конфіденційності. Можливо, за допомогою нових кнопок та перемикачів досвідчені користувачі й справді зможуть встановити рівень приватності, що відповідає їх потребам. Однак тим, хто знається на комп'ютерах трохи гірше, не варто думати, що їх конфіденційність буде захищена за замовчуванням. Навіть якщо за законом компанії зобов'язані зробити це, вони все одно продовжать шукати лазівки, щоб змусити людей вибирати налаштування з меншим рівнем приватності, оскільки їхній прибуток безпосередньо залежить від збору даних.

2. Влада стурбована зростаючим впливом технологічних гігантів та обсягами даних, які вони збирають. Це призведе до конфліктів і компромісів. Влада створює власну цифрову інфраструктуру, щоб спростити доступ до державних служб і, хотілося б вірити, зробити їхню роботу прозорішою. Крім того, таким чином вони розраховують отримувати більше інформації про громадян, щоб краще їх контролювати. Не дивно, що їх дедалі більше цікавлять дані користувачів, що циркулюють у великих комерційних екосистемах. Це призведе до появи нових нормативів — законів про захист, локалізація даних, а також вимог, що визначають, яка інформація та у яких випадках має бути доступна правоохоронним органам. Ситуація з використанням Apple системи CSAM відмінно показала, як складно визначити баланс між шифруванням даних і конфіденційністю користувачів з одного боку - і виявлення злочинних дій з іншого.

3. Машинне навчання - це, звичайно, добре, але скоро стане більше розмов про машинне "розучування". Сучасне машинне навчання зазвичай має на увазі тренування великих нейромереж з використанням колосального списку властивостей, які іноді обчислюються мільярдами (деякі вважають їх аналогами мозкових нейронів, хоча це не зовсім правильно). Нейросети можна навчити як підтримувати прості взаємодії з користувачами, а й запам'ятовувати цілі фрагменти даних, що у свою чергу може призвести до витоків конфіденційної інформації та матеріалів, захищених авторським

правом, або закріплення соціальних забобонів. Крім того, виникає цікаве правове питання: якщо модель машинного навчання тренували з використанням моїх даних, чи можу я, посилаючись, наприклад, на регламент GDPR, зажадати повністю видалити результати цих тренувань із системи? І якщо так, чим це обернеться для компаній, що працюють на основі даних? Все просто: їм доведеться перенавчити моделі з нуля, що може коштувати дорого. У зв'язку з цим можуть з'явитися нові цікаві технології, які не лише перешкоджатимуть запам'ятовуванню (як, наприклад, навчання з використанням методів диференціальної приватності), а й дозволять дослідникам видаляти дані із вже навчених систем.

4. Користувачі та регулюючі органи вимагатимуть зробити алгоритми прозорішими. Складні алгоритми, такі як машинне навчання, все частіше використовуються для прийняття рішень у різних ситуаціях - від оцінки кредитоспроможності позичальників до розпізнавання осіб при показі рекламних оголошень. І поки одні люди насолоджуються принадами персоналізації, для інших вона може стати джерелом неприємних ситуацій чи навіть дискримінації. Уявіть інтернет-магазин, який ділить користувачів на більш-менш цінних за допомогою якогось алгоритму, що визначає показник LTV (довічної цінності клієнта). Перспективні покупці можуть спілкуватися зі співробітниками служби підтримки в живому чаті, а менш щасливих чекає далекий від досконалості чатбот. Алгоритми використовуються в багатьох сферах, тому в майбутньому на нас чекає ще більше дискусій та нових правил навколо пояснення, спростування та коригування рішень, прийнятих автоматизованими системами. З'являться нові дослідження, покликані зробити методи машинного навчання зрозумілішими.

5. Завдяки роботі з дому люди більше уваги приділятимуть захисту конфіденційності — не без допомоги своїх роботодавців. Працюючи з дому в період пандемії, ви, напевно, розширили своє знання IT-сленгу: такі вирази, як «інфраструктура віртуальних робочих столів», «одноразовий пароль», «двофакторні ключі безпеки» тощо, стали відомі навіть продавцям та банківським службовцям . Пандемія закінчиться, але культура роботи з дому може надовго залишитися з нами. Коли співробітники використовують ті самі пристрої для робочих і особистих потреб, периметр корпоративної мережі розширюється. Щоб захистити його, службам безпеки доведеться подбати про підвищення поінформованості персоналу. Це означає, що все більше людей будуть брати участь у тренінгах з кібербезпеки та захисту конфіденційності та застосовувати робочі навички, такі як використання двофакторної авторизації, у звичайному житті.

Підсумовуючи: конфіденційність перетворилася на один із головних предметів дискусії про права особистості та людини, безпеки та ділової етики — між суспільством, бізнесом та владою. Передбачається, що результатом цієї дискусії стане більш прозоре, чесне та розумне використання персональних даних, а відповіді на найгостріші юридичні, соціальні та технологічні питання, пов'язані із захистом конфіденційності, будуть знайдені.