# Мовенко Константин, ИС/б-21-2-о

*Machine Learning (ML) models are becoming deeply integrated into our daily lives, with their use expected to expand even further in the coming years. However, as these models grow in importance, potential vulnerabilities — such as biased decision-making and privacy breaches — could result in serious unintended consequences.*

Модели машинного обучения (ML) всё глубже внедряются в нашу повседневную жизнь, и в ближайшие годы ожидается всё большее расширение области их использования. Однако с ростом значимости этих моделей возникают потенциальные уязвимости, такие как необъективное принятие решений и нарушение конфиденциальности, что может привести к серьезным непредвиденным последствиям.

*The 1st International Workshop on Secure, Accountable, and Verifiable Machine Learning (SAFE-ML 2025) aims to bring together experts from industry and academia, with software testing and ML backgrounds, to discuss and address these challenges. The focus will be on innovative methods and tools to ensure correctness, robustness, security, fairness of ML models.*

1-й Международный семинар по безопасному, подотчетному и верифицируемому машинному обучению (SAFE-ML 2025) призван объединить экспертов из индустрии и научных кругов, занимающихся тестированием ПО и ML, для обсуждения и решения этих проблем. Основное внимание будет уделено инновационным методам и инструментам для обеспечения корректности, надёжности, безопасности и справедливости моделей ML.

*Topics of the workshop will cover, but are not limited to:*

*-Privacy preservation of ML models;*

*-Adversarial robustness in ML models;*

*-Security of ML models against poisoning attacks;*

*-Ensuring fairness and mitigating bias in ML models;*

*-Unlearning algorithms in ML;*

*-Explainability and interpretability of ML algorithms;*

*-ML accountability.*

Среди тем семинара будут представлены:

* Сохранение конфиденциальности ML-моделей;
* Устойчивость ML-моделей к недобросовестному использованию;
* Защита ML-моделей от вирусных атак;
* Обеспечение справедливости и снижение предвзятости в ML-моделях;
* Алгоритмы разобучения в ML;
* Объяснимость и интерпретируемость ML-алгоритмов;
* Подотчётность машинного обучения.

*Submission Format:*

*The submissions must conform to the IEEE conference proceedings template, specified in the IEEE Conference Proceedings Formatting Guidelines.*

Формат заявки:

Работа должна соответствовать шаблону материалов конференций IEEE (Институт инженеров электротехники и электроники), указанному в рекомендациях к оформлению материалов конференций IEEE.

*Submissions may fall into the following categories:*

1. *Full Papers (up to 8 pages): Comprehensive presentations of mature research findings or industrial applications;*
2. *Short Papers (up to 4 pages): Explorations of emerging ideas or preliminary research results;*
3. *Position Papers (up to 2 pages): Statements outlining positions or open challenges that stimulate discussion and debate.*

Работы могут относиться к следующим категориям:

1. Полноценные доклады (до 8 страниц): всеобъемлющие презентации результатов состоятельных исследований или найденной пользы для индустрии;
2. Краткие доклады (до 4 страниц): исследование новых идей или предварительных результатов исследований;
3. Позиционные доклады (до 2 страниц): заявления с изложением позиций или открытых проблем, стимулирующие дискуссии и дебаты.

*Submission site: https://easychair.org/my/conference?conf=icst2025. Please be sure to select The 1st International Workshop on Secure, Accountable, and Verifiable Machine Learning as track for you submission.*

Сайт для подачи заявок: <https://easychair.org/my/conference?conf=icst2025>. Пожалуйста, не забудьте выбрать в качестве направления заявки «The 1st International Workshop on Secure, Accountable, and Verifiable Machine Learning».

*Workshop Format:*

*This workshop is held as part of ICST 2025 and will be an in-person event held in Naples, Italy. For details see the main ICST website.*

Формат семинара:

Семинар проводится в рамках ICST 2025 и будет проходить очно в Неаполе, Италия. Подробности см. на главном сайте ICST.

*Accepted paper presentations will have the following duration, depending on pthe aper type:*

*-Full Papers: 22 minutes (including Q&A);*

*-Short Papers: 15 minutes (including Q&A);*

*-Position Papers: 7 minutes (including Q&A).*

Принятые презентации будут иметь следующую продолжительность в зависимости от типа доклада:

* Полноценные доклады: 22 минуты (включая вопросы и ответы);
* Краткие доклады: 15 минут (включая вопросы и ответы);
* Позиционные доклады: 7 минут (включая вопросы и ответы).

*Review Process:*

*The review process will follow a single-blind format, meaning authors are not required to anonymize their submissions.*

Процесс рецензирования:

Процесс рецензирования будет проходить в формате однослепого исследования, то есть авторы не обязаны отправлять работы анонимно.

*Important Dates:*

*Paper Submission: 3rd January, 2025*

*Decision Notification: 6th February, 2025*

*Camera-ready: 8th of March, 2025*

Важные даты:

Крайний срок подачи заявок: 3 января, 2025 г.

Оповещение о рассмотрении: 6 февраля 2025 г.

Итоговый документ: 8 марта, 2025

*Contacts:*

*Any doubts or queries can be addressed to the General Co-Chairs using the following e-mails:*

*-Carlo Mazzocca (cmazzocca@unisa.it)*

*-Alessio Mora (alessio.mora@unibo.it)*

Контакты:

С любыми обращениями и вопросами можно обратиться к генеральным сопредседателям по следующим адресам электронной почты:

* Карло Мацокка (cmazzocca@unisa.it)
* Алессио Мора (alessio.mora@unibo.it)

# Questions

## Why is this conference relevant to you?

This conference is relevant to me because I plan to work in IT-industry and have interest in its perspective directions of research. It could possibly help me understand how to make machine learning systems safe, fair, and reliable. Or maybe just investigate world of scientific AI a bit deeper.

## What is the name of the conference?

SAFE-ML 2025 : International Workshop on Secure, Accountable, and Verifiable Machine Learning.

## What is the main purpose of the conference?

The main purpose of it is to bring together experts from industry and academia to address challenges related to the correctness, robustness, security, fairness, and accountability of current ML-models.

## How many thematic sections are represented at the conference?

Although there is no explicit mention of "sections," there were listed 7 themes, including privacy preservation, adversarial robustness, security, fairness, unlearning algorithms, explainability and accountability of ML.

## Who will be the speakers at the plenary session?

Not mentioned except two co-chairs: Carlo Mazzocca and Alessio Mora. We can find more info on official website of conference or by contacting mentioned people by email.

## What is the deadline for registration at the conference?

Jan 3, 2025

## What does the registration fee include?

Not mentioned. Details could be possibly found on official website.