

Людмила ЗАВАДСЬКА¹, канд. фіз.-мат. наук, ст. наук, співроб.
ORCID ID: 0000-0002-6291-6036
e-mail: ludazavadska@gmail.com

Володимир МОРЕНЕЦЬ², канд. фіз.-мат. наук, асист.
ORCID ID: 0009-0006-0899-4400
e-mail: vmorenets@knu.ua

Ірина РОЗОРА², д-р фіз.-мат. наук, доц.
ORCID ID: 0000-0002-8733-7559
e-mail: irozora@knu.ua

Дмитро САВЧУК³, д-р філософії, доц.
ORCID ID: 0000-0002-3698-6110
e-mail: savchuk@usf.edu

Андрій ФЕСЕНКО¹, канд. фіз.-мат. наук, ст. викл.
ORCID ID: 0000-0002-4489-3256
e-mail: andrey.fesenko@gmail.com

Сергій ЯКОВЛЄВ¹, канд. тех. наук, доц.
ORCID ID: 0000-0002-5647-5043
e-mail: yasv@rl.kiev.ua

¹Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна

²Київський національний університет імені Тараса Шевченка, Київ, Україна

³Університет Південної Флориди, Флорида, США

МИХАЙЛО САВЧУК (19.05.1947–28.08.2024): ЖИТТЯ, ПРИСВЯЧЕНЕ КРИПТОГРАФІЇ

Присвячено пам'яті видатного українського вченого, члена-кореспондента НАН України, лауреата Державної премії в галузі науки і техніки, професора Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського" Михайла Миколайовича Савчука. Проаналізовано науковий доробок вченого, його вагомий внесок у розвиток вітчизняної науки, зокрема в галузі криптографії. Також подано перелік найважливіших наукових праць й отриманих нагород.

Ключові слова: Михайло Миколайович Савчук, кафедра математичних методів захисту інформації, фізико-технічний інститут, кафедра прикладної статистики, факультет комп'ютерних наук та кібернетики, київська наукова школа, криптографія, захист інформації, квантові обчислення.

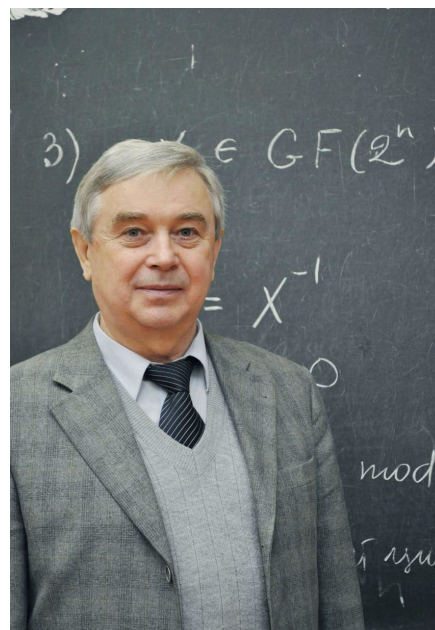
Класифікація відповідно до AMS 2020: 01A70, 94A60.

28 серпня 2024 р. відійшов у засвіти Михайло Миколайович Савчук – видатний криптолог і математик, член-кореспондент НАН України, лауреат Державної премії в галузі науки і техніки, учитель, педагог і неординарна особистість.

Михайло Миколайович народився в Магадані, де працювали його батьки, але дитинство провів у Ніжині, навчався у школі № 3. Ще зі шкільних років він зацікавився математикою, і вже тоді досяг неабияких успіхів: друге місце на Київській олімпіаді з математики, перше місце на Першій Республіканській математичній олімпіаді та постійна участь в обласних і республіканських олімпіадах. Це зумовило подальший шлях юного математика – у 1965 р. він вступив на механіко-математичний факультет Київського державного університету (зараз – КНУ ім. Тараса Шевченка). Тут Михайло Миколайович навчався у спеціалізованій групі за посиленою математичною програмою. Майбутній видатний математик закінчив університет у 1970 р. за спеціальністю "Теорія ймовірностей".

Після закінчення університету Михайло Миколайович проходив військову службу на архіпелазі Нова Земля та працював деякий час на заводі "Арсенал", де займався питаннями оцінювання та підвищення надійності технічних систем. Однак поклик до наукової діяльності взяв своє, і в 1974 р. він переходить працювати в Інститут кібернетики АН УРСР, у нещодавно створений відділ теорії надійності складних систем, який очолював Ігор Миколайович Коваленко. Хоча відділ займався задачами та методами теорії масового обслуговування та теорії надійності, проте тут була створена спеціалізована лабораторія для досліджень у галузі криптографії та криптоаналізу. Саме тут і почав працювати Михайло Миколайович.

Необхідно зауважити, що в радянські часи криптологія була закритою наукою, яку було заборонено навіть обговорювати у відкритих джерелах. Однак один лише набір необхідних знань і вимог для роботи в лабораторії – алгебра, комбінаторика, теорія ймовірностей, математична статистика, теорія інформації, теорія алгоритмів – причарував молодого математика від самого початку. Робота в Інституті кібернетики разом із колегами та співпраця з



М. М. Савчук на лекції з криптографії

іншими закритими лабораторіями Радянського союзу згодом сформувала Київську школу теоретичної криптології на чолі з І. М. Коваленком, яскравим представником якої став і Михайло Миколайович. Там само і були закладені основні напрямки його наукових досліджень: дослідження комбінаторних об'єктів, дослідження властивостей булевих функцій і генераторів псевдовипадкових чисел, алгебраїчні та ймовірнісні методи криптоаналізу. Працюючи в Інституті кібернетики, у 1983 р. Михайло Миколайович захистив кандидатську дисертацію.

Після розпаду Радянського союзу лабораторія криптології опинилась у своєрідному вакуумі: контакти з іншими лабораторіями було обірвано, усю спеціалізовану (секретну!) літературу – вивезено або знищено, а головне – під загрозою опинилась підготовка фахівців у галузі криптології, оскільки через закритість теми не в усіх було навіть просте розуміння важливості криптографічного захисту для інформаційної безпеки держави та наявності експертів у цій галузі. Михайло Миколайович разом з І. М. Коваленком та Л. О. Завадською декілька років намагались організувати хоча б невеликі курси лекцій із криптографії та криптоаналізу в різних київських університетах – і, зрештою, їм це вдалось: у 1996 р. їх запросили читати семестровий курс криптографії в Інституті прикладного та системного аналізу Київського політехнічного інституту, а з 1999 р. – на факультет кібернетики Київського національного університету імені Тараса Шевченка. Усі подальші роки Михайла Миколайовича були тісно пов'язані з факультетом кібернетики (з 2016 його перейменували у факультет комп'ютерних наук і кібернетики), де він працював за сумісництвом на посаді професора кафедри прикладної статистики. Тут він з ентузіазмом передавав студентам свої глибокі знання, викладаючи такі дисципліни, як: проблеми криптографії, оптимізації та аналізу ризиків, основи криптографії, асиметрична криптографія та теорія випадкових процесів.

Після отримання ступеня доктора фізико-математичних наук у 1999 р., Михайло Миколайович 2000 р. очолив щойно створену кафедру математичних методів захисту інформації (ММЗІ) фізико-технічного інституту Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського". Із цього моменту Михайло Миколайович активно, не менш ніж науковою, займався освітньою діяльністю. На очолюваній ним кафедрі було створено унікальні програми підготовки фахівців у галузі криптології, що продовжували традиції Київської школи криптології, зокрема ґрунтовну математичну базу і математичну строгість у викладанні профільного матеріалу. Відповідно до цих програм було розроблено та впроваджено спеціалізовані дисципліни. Сам Михайло Миколайович, окрім двосеместрового курсу криптографії й окремого курсу з методів криптоаналізу, створив нетривіальний курс комбінаторного аналізу, що задавав основу для подальшого розвитку не тільки в галузі криптології, але й у багатьох суміжних галузях. Робота над оновленням змісту навчальних дисциплін не зупинялась ніколи: тільки за останні роки Михайло Миколайович додатково розробив такі дисципліни, як "Математичні основи кодів автентифікації" та "Моделі цінності інформації та ефективність інформаційного захисту", присвячені сучасним фундаментальним проблемам криптології та захисту інформації.

Освітня діяльність кафедри ММЗІ тісно поєднувалась із науковою діяльністю. Колектив кафедри на чолі з Михайлом Миколайовичем упродовж 2000–2024 рр. виконав понад тридцять науково-дослідних проєктів за держбюджетною тематикою та на замовлення таких організацій, як Служба зовнішньої розвідки, Служба безпеки України, Міністерство фінансів, Samsung R&D Україна тощо. Під керівництвом Михайла Миколайовича було захищено три кандидатські дисертації (О. Пометун, С. Яковлев, А. Фесенко) та декілька десятків бакалаврських і магістерських робіт. Багато років Михайло Миколайович був головою секції математики конкурсу наукових робіт школярів "Інтел Техно" (тепер – "Еко-Техно Україна"). У 2018 р. його було обрано член-кореспондентом Національної академії наук України по відділенню інформатики.



М. М. Савчук, Л. О. Завадська та студенти Фізико-технічного інституту



М. М. Савчук разом зі своїми учнями – П. Селюх, А. Фесенком та С. Яковлєвим – на захисті дисертації А. Фесенка



М. М. Савчук, І. М. Коваленко та О. В. Коба



М. М. Савчук і М. М. Леоненко

За свою кар'єру Михайло Миколайович опублікував понад 90 наукових праць, серед яких 3 монографії та 3 авторських свідоцтва на винахід. У 2001 р. за цикл робіт "Ймовірно-статистичні методи в проблемах надійності та безпеки інформаційних технологій" йому було присуджено Державну премію у галузі науки і техніки. Його праці лягли в основу практичних розробок для урядового зв'язку та послугували фундаментом для національної системи криптографічного захисту інформації. Вибрані наукові публікації М. М. Савчука:

- Савчук М. Н. Некоторые предельные теоремы в схеме размещения частиц комплектами // Теория вероятностей и математическая статистика. 1983. Вып. 28. С. 122–130.
- Коваленко И. Н., Левитская А. А., Савчук М. Н. Избранные задачи вероятностной комбинаторики, Київ : Наукова думка, 1986. 224 с.
- Савчук М. Н. Сходимость многомерных случайных процессов, связанных с разделимыми статистиками в схемах размещения, к гауссовским диффузионным процессам // Анализ стохастических систем методами исследования операций и теорем надёжности. Киев : Институт кибернетики АН УССР, 1987. С. 43–47.
- Савчук М. Н. О предельных распределениях максимальной и минимальной частот в схеме размещения случайного числа частиц по ячейкам // Математические методы моделирования и системного анализа в условиях неполной информации. Киев : Институт кибернетики АН УССР, 1991. С. 9–12.
- Савчук М. Н. Предельное поведение случайного времени ожидания до заполнения заданного подмножества ячеек в схеме равномерного размещения частиц комплектами // Модели и методы исследования операций, теории риска и надёжности. Киев : Институт кибернетики НАНУ, 1992. С. 3–10.
- Savchuk M. Some limiting theorems in ball batch allocation scheme with random levels defined by an another allocation scheme // Probabilistic Methods in Discrete Mathematics. Москва : Теория вероятностей и её применения, 1993. С. 428–436.
- Савчук М. Н. Использование метода Монте Карло для идентификации булевых функций большого числа переменных // Кибернетика и вычислительная техника. 1998. Вып. 117. С. 3–7.
- Савчук М. Н. Анализ одного метода улучшения характеристик случайной двоичной последовательности // Кибернетика и вычислительная техника. 1998. Вып. 118. С. 57–61.
- Kovalenko I. N., Savchuk M. N. Some methods of decoding corrupted linear codes // Регистрация, хранение и обработка данных. 1999. Т. 1, № 2. С. 62–68.
- Kovalenko I. N., Savchuk M. N. On a statistical algorithm to decode heavily corrupted linear codes // Applied Probability and Stochastic Processes. Berkeley : Kluwer Academic Publishers, 1999. P. 73–82
- Савчук М. Н. Асимптотический анализ вариационного ряда вероятностей серий различных исходов в полиномиальной схеме // Доповіді НАН України. 1999. № 3. С. 101–105.
- Савчук М. Н., Синявский В. Ф. Об алгоритме определения моментов изменения параметров бернуллиевской последовательности // Проблемы управления и информатики. 1999. № 1. С. 84–89
- Савчук М. М., Фесенко А. В. Симетричні комутативні та локально-комутативні шифри для побудови класичних та постквантових протоколів // Інформаційні технології та комп'ютерна інженерія. 2008. № 2(12). С. 43–51
- Савчук М. Н., Шарапов В. Г. Анализ одного метода тестирования случайных последовательностей, основанного на контекстном моделировании // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2008. Вип. 1(16). С. 82–89.
- Савчук М. Н., Шарапов В. Г. Многомерный статистический тест для двоичных последовательностей // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2008. Вип. 1(18). С. 65–72.
- Савчук М. Н. О работах киевской школы теоретической криптографии // Кибернетика и системный анализ. 2010. № 3. С. 52–68.
- Савчук М. М., Фесенко А. В. Квантові обчислення: огляд та аналіз // Кібернетика та системний аналіз. 2019. № 1. С. 14–29.
- Савчук М. М., Бурлака М. К. Кодування і класифікація перестановок за спеціальним перетворенням з оцінками потужності класів // Вісник Київського національного університету імені Тараса Шевченка. Серія: Фізико-математичні науки. 2019. № 2. С. 35–42.
- Савчук М. М. Захист інформаційних технологій та кібербезпека // Вісник НАН України. 2019. № 11. С. 23–28.
- Лещенко Владислав, Пекарчук Ніна, Савчук Михайло. Порівняльний аналіз складності методів лінеаризації та перебору розв'язання систем нелінійних булевих рівнянь // Захист інформації. 2020. Т. 22, № 1. С. 33–42.

І студенти, і викладачі, і колеги Михайла Миколайовича пам'ятають його як дуже інтелігентну, усміхнену, доброзичливу і тактовну людину – однак водночас принципову в питаннях наукової етики та якості викладання. Навколо нього завжди панувала атмосфера піднесеності та натхненності. Його повага до людей завжди приваблювала до нього та надавала велику вагу його словам та порадам.

Світла пам'ять видатній Людині.

Отримано редакцією журналу / Received: 01.11.24
Прорецензовано / Revised: 12.11.24
Схвалено до друку / Accepted: 26.11.24

Ludmyla ZAVADSKA¹, PhD (Phys. & Math.), Senior Researcher
ORCID ID: 0000-0002-6291-6036
e-mail: ludazavadska@gmail.com

Volodymyr MORENETS², PhD (Phys. & Math.), Assist. Prof.
ORCID ID: 0009-0006-0899-4400
e-mail: vmorenets@knu.ua

Iryna ROZORA², DSc (Phys. & Math.), Assoc. Prof.
ORCID ID: 0000-0002-8733-7559
e-mail: irozora@knu.ua

Dmytro SAVCHUK³, PhD, Assoc. Prof.
ORCID ID: 0000-0002-3698-6110
e-mail: savchuk@usf.edu

Andrii FESENKO¹, PhD (Phys. & Math.), Senior Lecturer
ORCID ID: 0000-0002-4489-3256
e-mail: andrey.fesenko@gmail.com

Serhii YAKOVLEV¹, PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0002-5647-5043
e-mail: yasv@ri.kiev.ua

¹National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine

²Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

³University of South Florida, Florida, USA

MYKHAYLO SAVCHUK (19.05.1947–28.08.2024): A LIFE DEDICATED TO CRYPTOGRAPHY

Dedicated to the memory of the outstanding Ukrainian scientist, corresponding member of the NAS of Ukraine, laureate of the State Prize in Science and Technology, professor of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" Mykhailo Mykolayovych Savchuk. The article analyzes the scientific achievements of the scientist, and his significant contribution to the development of national science, in particular in the field of cryptography. A list of key scientific works and awards received is also provided.

Key words: Mykhailo Mykolayovych Savchuk, Department of Mathematical Methods of Information Protection, Institute of Physics and Technology, Department of Applied Statistics, Faculty of Computer Science and Cybernetics, Kyiv Scientific School, cryptography, information security, quantum computing.

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.