К 75-ЛЕТНЕМУ ЮБИЛЕЮ МОЛДОВЯНА АЛЕКСАНДРА АНДРЕЕВИЧА

Доктор технических наук, профессор Молдовян Александр Андреевич родился в селе Чок Майдан, Комратского района Молдавской ССР. В 1974 г. окончил Ленинградский электротехнический институт им. В.И. Ульянова (Ленина) по специальности «Автоматизированные системы управления». В период с 1974 г. по 1994 г. разрабатывал автоматизированные системы управления, из них 14 лет в ПКБ АСУ МИНПРИБОРА СССР. С 1995 г. главный конструктор НТЦ "СПЕКТР" НПК "Красная Заря". С 1996 г. перешел на работу в Специализированный центр программных систем «СПЕКТР», созданный по рекомендации ГОСКОМОБОРОНПРОМа для выполнения НИОКР в области защиты информации. С 2005 г. являлся директором Научного филиала ФГУП «НИИ» ВЕКТОР» – СЦПС «СПЕКТР». С марта 2009 г. работал заместителем директора СПИИРАН по информационной безопасности и научным руководителем научно-исследовательского отдела проблем информационной безопасности. С декабря 2016 г. руководил научно-исследовательским отделом проблем информационной безопасности СПИИРАН. Затем переведен на должность главного научного сотрудника лаборатории проблем компьютерной безопасности СПИИРАН – СПБ ФИЦ РАН.

Молдовян А.А. руководил и участвовал в разработке более 40 НИОКР в области защиты информации, а также создании ряда практически значимых систем защиты информации от несанкционированного доступа, получивших широкое внедрение

на межотраслевом уровне: «Кобра», «Спектр-Z» «Спектр-М», «СГУ-2», «Спектр-2000», «Ключ-П», «Ключ-Ш», «Вектор-01», «ЩИТ-РЖД», «Аура» сертифицированных Гостехкомиссией России, ФСТЭК России, МО РФ и ФСБ России.

Молдовян А.А. активный участник конференций международного и российского уровня. Сопредседатель секции «Информационная безопасность» V и XI Санкт-Петербургских международных конференций «Региональная информатика». Член оргкомитета регулярной Межрегиональной конференции «Информационная безопасность регионов России».

Молдовян А.А. известен как авторитетный ученый, участвовал в работе диссертационных советов при НИИ «Рубин», МГТУ им. Н.Э. Баумана, НИУ ИТМО, СПИИРАН, с 2021 г. член диссертационного совета при СПб ФИЦ РАН. Является экспертом Минобрнауки в научно-технической сфере, представитель СПб ФИЦ РАН в ТК №26 «Криптографическая защита информации». Разработал и читал авторские курсы лекций по проблемам информационной безопасности в НИУ ИТМО, ГУВК и СПГЭТУ-ЛЭТИ. Автор 6 монографий и 15 учебных пособий в области защиты информации.

Существенным вкладом Молдовяна А.А. в развитие науки является его деятельность по подготовке высококвалифицированных кадров. Им подготовлено 14 кандидатов и 2 доктора технических наук. Педагогический стаж составляет 27 лет.

Профессор Молдовян А.А. является руководителем ведущей научной школы Санкт-Петербурга «Криптография: методы, алгоритмы и протоколы для защиты информации в компьютерных системах», с 2022 г. председатель ГЭК НИУ ИТМО по направлению «Информационная безопасность». По результатам исследований в области защиты информации опубликовал более 250 научных работ, в том числе в ведущих журналах мира: «Автоматика и телемеханика» (Россия), «Кибернетика и системный анализ» (Украина), «Journal of Cryptology» (США), «Lecture Notes in Computer Science» (Германия). На созданные изобретения получил более 60 патентов России, США, Германии, Франции, Великобритании, Китая, Кореи и др. стран. Изобретения Молдовяна А.А. в области информационных технологий удостоены Гран-при, 10 золотых и 3 серебряных медалей, а также ряда дипломов на международных выставках в России, Японии, Бельгии, Болгарии, Венгрии и Польше. Правительством Санкт-Петербурга в 1997 г. награжден Дипломом за лучшую разработку военных ученых, внедренных в городское хозяйство города.

Указом Президента РФ награжден медалью «В память 300-летия Санкт-Петербурга» (2003 г.). Удостоен ведомственных наград за вклад в развитие методов, средств и систем защиты информации: значок «Почетный радист» (2002 г.), Почетная грамота МИНПРОМЭНЭНЕРГО (2004 г.), Благодарность ОАО «РЖД» (2004 г.), Памятный знак «90 лет ГРУ ГШ ВС РФ» (2008 г.). Памятная медаль Научного совета по информатизации Санкт-Петербурга «За вклад в развитие информационного общества» (2012 г.). Приказом Гостехкомиссии России награжден медалью «За укрепление государственной системы защиты информации» I степени (2004 г.). Приказом ФСТЭК России награжден знаком «За заслуги в защите информации» (2010 г.). Решением Российской академии наук награжден Почетной грамотой (2021 г.).

Сотрудники СПб ФИЦ РАН, коллеги из многих организаций, его ученики и последователи, а также редакционная коллегия журнала «Информатика и автоматизация» (Труды СПИИРАН) поздравляют Молдовяна Александра Андреевича с юбилеем и желают ему крепкого здоровья и дальнейших творческих успехов!

Список избранных публикаций

1. Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В. Криптография: скоростные шифры. СПб: БХВ-Петербург, 2002. 496 с.
2. Молдовян А.А., Молдовян Н.А., Еремеев М.А. Криптография: от примитивов к синтезу алгоритмов. СПб: БХВ-Петербург, 2004. 458 с.
3. Moldovyan A., Moldovyan N. Data-driven Block Ciphers for Fast Telecommunication Systems. New York: Auerbach Publications, 2008. 185 p.
4. Молдовян А.А., Молдовян Н.А. Новый принцип построения криптографических модулей в системах защиты ЭВМ. Кибернетика и системный анализ. 1993. №5. С. 42–49.
5. Молдовян А.А., Молдовян Н.А. Программно-ориентированная криптосистема с неопределенным алгоритмом шифрования. Управляющие системы и машины. 1995. №6. С. 38–43.
6. Молдовян А.А. Подход к созданию средств защиты информации массового применения. Управление защитой информации. 1998. Т. 2. №1. С. 26–27.
7. Moldovyan A., Moldovyan N. Software Encryption Algorithms for Transparent Protection Technology. Cryptologia. 1998. vol. 22. no. 1. pp. 56–68.
8. Moldovyan A. Fast Block Cipher Based on controlled permutations. Computer Science Journal of Moldova. 2000. vol. 8. no. 3. pp. 270–283.
9. Молдовян А.А. Построение скоростного программмного алгоритма поточного типа на базе псевдовероятностной выборки подключей. Вопросы защиты информации. 2000. №4. С. 53–56.
10. Moldovyan A., Moldovyan N. A Cipher Based on Data-Dependent Permutations. Journal of Cryptology. 2002. vol. 15. pp. 61–72.
11. Молдовян А.А. Новый способ синтеза переключаемых управляемых операционных блоков. Вопросы защиты информации. 2003. №3. С. 38–45.
12. Молдовян А.А., Молдовян Н.А., Еремеев М.И. Защитные преобразования информации в АСУ на основе нового примитива. Автоматика и телемеханика. 2002. №12. С. 147–165.
13. Изотов Б.В., Молдовян А.А. Перспективы создания шифраторов на основе управляемых криптографических примитивов. Известия высших учебных заведений. Приборостроение. 2003. №7. С. 73–79.
14. Moldovyan A., Moldovyan N., Sklavos N., Koufopavlou O. CHESS-64, a Block Cipher Based on Data-Dependent Operations: Design Variants and Hardware Implementation Efficiency. Asian Journal of Information Technology. 2005. vol. 4. no. 4. pp. 320–328.
15. Moldovyan A., Moldovyan N. Blind Collective Signature Protocol Based on Discrete Logarithm Problem. International Journal of Network Security. 2010. vol. 11. no. 2. pp. 106–113.
16. Молдовян А.А. Постквантовая схема ЭЦП, основанная на вычислительной сложности восстановления параметров векторного конечного поля. Вопросы защиты информации. 2023. №4. С. 20–26.
17. Молдовян А.А., Молдовян Н.А., Молдовян Д.Н. Постквантовые двухключевые криптосхемы на конечных алгебрах. Информатика и автоматизация. 2024. Т. 23. №4. С. 1246–1276.

18. Duong T.M., Moldovyan A., Moldovyan N., Nguyen H.M., Do T.B. Structure of 6-dimensional finite non-commutative algebras with many single-sided units. Bulletin of Electrical Engineering and Informatics. 2025. vol. 14. pp. 2017–2030.
19. Moldovyan A., Moldovyan N. A method for enhancing randomization in algebraic signature algorithms on non-commutative algebras. Quasigroups and related systems. 2025. vol. 33. pp. 71–83.
20. Молдовян А.А., Молдовян Д.Н., Костина А.А. Рандомизация в постквантовых алгоритмах ЭЦП с секретной группой. Информатика и автоматизация. 2025. Т. 24. №6. С. 1810–1835.
21. Молдовян А.А. Постквантовый алгебраический алгоритм ЭЦП с тремя скрытыми группами. Вопросы кибербезопасности. 2025. №5(69). С. 78–87.